ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

**Е. С. Поликарпов**

# ОСНОВЫ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Учебное пособие

Москва
2020

**ББК 32.972**
**П50**

Рецензенты:
профессор кафедры информационной безопасности
Краснодарского университета МВД России
доктор технических наук, профессор **А. В. Еськов**;
доцент кафедры информационной безопасности
Воронежского института МВД России
кандидат физико-математических наук, доцент **С. П. Алексеенко**

**Поликарпов, Е. С.**

**П50** **Основы компьютерной разведки** : учебное пособие / Е. С. Поликарпов. – М. : Московский университет МВД России имени В.Я. Кикотя, 2020. – 321 с.

ISBN 978-5-9694-0872-2

Учебное пособие необходимо для понимания основ компьютерной разведки, а также выработки стратегии защиты. В пособии описываются передовые способы наблюдения за пользователями, технологии сбора личной и корпоративной информации, социальная инженерия, сниффинг, спуфинг и др.

Предназначено для обучения по специальностям 10.05.05 – Безопасность информационных технологий в правоохранительной сфере, 10.05.01 – Компьютерная безопасность, а также для адъюнктов, докторантов и сотрудников органов внутренних дел, повышающих уровень своих знаний в области информационной безопасности.

ББК 32.972

**ISBN 978-5-9694-0872-2**

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

Разведывательные операции с использованием «плащей и кинжалов» во все времена были частью политики и бизнеса. По мере того, как люди переводили свою деятельность в информационную сферу, разведывательные методы эволюционировали. Сегодня вся информация хранится на электронных устройствах. Информационные технологии имеют ряд преимуществ, но они далеко не совершенны с точки зрения безопасности.

Последние годы мировые державы, не скрывая, привлекают хакеров на государственную службу для укрепления государственного устройства, ведения информационного противоборства, анализа защищенности информационных технологий, а также противодействия киберпреступности. Новостные ленты так и пестрят заголовками об утечке информации или взломе серверов различных компаний. Хакинг быстро превратился в излюбленный метод государственных и частных структур. Кибершпионаж и кибератаки, влияние на выборные институты иностранных государств, остановка производственного процесса и т. д. – компьютерные взломщики могут сделать многое на службе своих государств. В настоящий момент несколько десятков стран официально используют специализированные подразделения по кибербезопасности для военных или разведывательных целей, число которых насчитывается уже более сотни.

В процессе расследования преступлений в сфере компьютерной информации довольно часто возникает необходимость решения вопросов, требующих особых профессиональных знаний. Это особенно важно, учитывая непрекращающийся подъем в развитии высоких технологий. Кроме того, исследуя и моделируя различные компьютерные атаки, можно выявить слабые места в настройках безопасности.

В учебном пособии рассмотрены основные способы, методы и технологии, которые могут применятся при получении доступа к информации компьютерных систем и сетей. Описаны подходы по обеспечению анонимности в киберпространстве. Приведены примеры программного обеспечения для моделирования различных компьютерных атак. Кратко охарактеризованы общие принципы межсетевого взаимодействия компьютерных систем и основные уязвимости сетевых протоколов. Проведен обзор способов обхода базовых механизмов защиты компьютерной системы.

Учебное пособие предназначено для обучения по специальностям в области информационной безопасности, а также специалистов, занимающихся вопросами кибербезопасности и администрированию программно-технических средств защиты информации.

# ГЛАВА I. ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОЙ РАЗВЕДКИ

## § 1. Понятие и классификация компьютерной разведки

В XXI в. большинство людей знают, что правоохранительные и разведывательные органы разных стан, частные компании, вооруженные силы, а также хакеры могут их подслушивать или перехватывать их данные.

Среди множества современных технологий человека интернет разрушил и без того хрупкую стену между безопасностью и свободой. Интернет расширяет нашу свободу общения и в то же время делает нас менее защищенными. Предоставляет новые средства для вторжения в частную жизнь и причинения ущерба национальной безопасности и экономике, а также все более изощренные инструменты отслеживания для компетентных органов.

Разведка в сети и сбор данных являются современной частью национальной безопасности каждого государства. Компьютерная разведка включает в себя мероприятия по проникновению в компьютерные системы или сети, используемые преступником (противником) для получения информации, находящейся в этих системах или сетях или проходящей через них.

Поскольку в настоящее время через интернет передаются огромные объемы данных, которые люди не могут понять в необработанной форме, наблюдение часто приводит к обработке и использованию с помощью алгоритмов или других методов поиска, которые могут запрашивать большие объемы собранной информации для достижения более конкретных целей разведки.

Электронное наблюдение для целей разведки большинство из нас признало бы оправданным, если бы целями являлись национальная безопасность, прогнозирование планов террористов, получение доказательств преступной деятельности и т. д.

В классическом понимании разведкой принято считать деятельность уполномоченных органов, применяющих специальные средства и методы, с целью получения информации о замыслах, планах и мероприятиях противника (иностранных государств, организационных преступных групп, террористических организаций, конкурентов), потенциально или реально угрожающих безопасности объектов защиты (государства, организации, в том числе различных форм собственности).

Традиционная разведывательная деятельность может проводится с использованием агентурного аппарата и технических средств. Эти два направления разведки тесно связаны ввиду того, что агентура (люди) в большинстве случаев использует технические средства при сборе информации. Отличие в преобладании человеческого или технического аспекта.

Многообразие видов носителей информации породило множество видов технической разведки. Ее классифицируют по различным признакам (основаниям классификации). Наиболее широко применяются две классификации: по физической природе носителей информации и видам носителей технических средств добывания (рис. 1.1).

*Оптическая разведка* – получение информации путем приема и анализа электромагнитных излучений ультрафиолетового, видимого и инфракрасного (ИК) диапазонов, которые создаются или переотражаются объектами разведки.

*Радиоэлектронная разведка* – получение информации путем приема и анализа электромагнитного излучения радиодиапазона, создаваемого различными радиоэлектронными средствами.

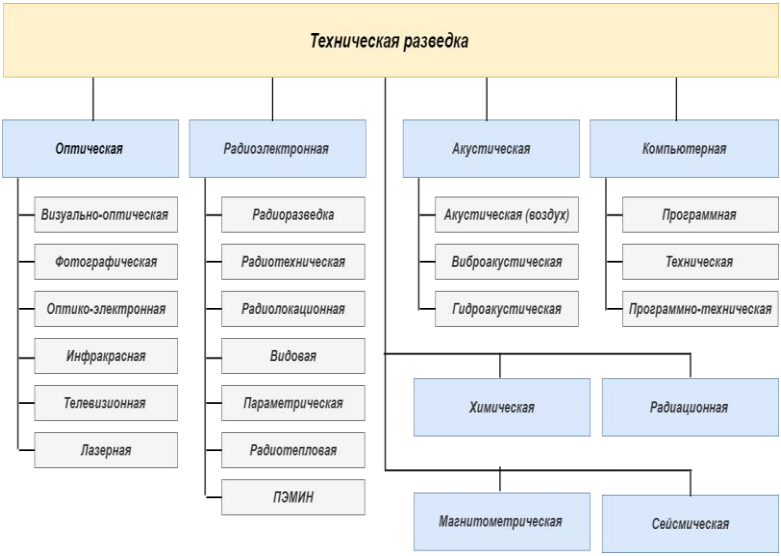


Рис. 1.1. Классификация технической разведки
по носителям информации

*Акустическая разведка* – получение информации путем приема и анализа акустических сигналов, распространяющихся в воздушной среде от различных объектов.

*Магнитометрическая разведка* – получение информации путем обнаружения и анализа изменений магнитного поля Земли под воздействием объектов с большой магнитной массой.

*Химическая разведка* – получение информации путем взятия проб и анализа макрочастиц вещества.

*Радиационная разведка* – получение информации путем измерения уровня и проведения анализа ионизации веществ.

Развитие и распространение вычислительной техники предполагает ведение разведки в информационном пространстве. Классификационный признак для этого относительно нового вида технической разведки – компьютерной разведки отличается от указанных видов рассматриваемой классификационной схемы,

а именно способами добывания информации. Основным таким способом в данном случае является перехват или получение информации в компьютерах и их сетях. Учитывая, что компьютеры становятся основным средством обработки и хранения информации, ее возможности и актуальность непрерывно растут.

*Компьютерная разведка* – это добывание информации из компьютерных систем и сетей, добывание характеристик их программно-аппаратных средств и пользователей.

Основываясь на особенностях обработки, передачи и хранения информации и архитектуре современных компьютерных систем, можно выделить следующие источники информации в компьютерной разведке:

– данные, сведения и информация обрабатываемая, передаваемая и хранимая в компьютерных системах и сетях (электронные документы, базы данных, данные, проходящие через коммутационное оборудование);

– характеристики программных, аппаратных и программно-аппаратных комплексов (в том числе средств защиты информации);

– характеристики пользователей компьютерных систем и сетей (личная информация пользователя, электронная почта, пароли, IP-адрес и т. д.).

К объектам компьютерной разведки можно отнести следующее: компьютерные сети и системы, средства хранения информации, телекоммуникационное оборудование, системное и прикладное программное обеспечение, средства защиты информации в компьютерных системах и сетях и пользователей компьютерных систем.

Субъект компьютерной разведки, сотрудник разведывательного органа, обладающий наивысшей степенью компетенции,

всеми известными (и, возможно, неизвестными) доступными ресурсами, а также мотивацией скрытного добывания защищаемой информации.

В современной литературе представлены достаточно разнообразные классификации компьютерной разведки, отличающиеся полнотой учета признаков. Рассмотрим наиболее распространенные классификации.

По масштабу (рис. 1.2) компьютерную разведку можно разделить на интернет-разведку, сетевую разведку и целевую разведку [36, 37, 38].

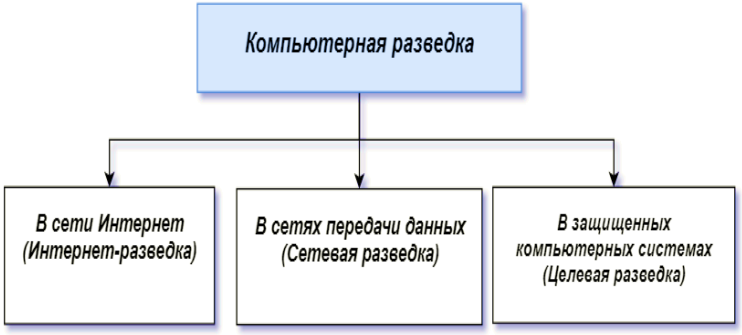


Рис. 1.2. Классификация компьютерной разведки по масштабу

*Интернет-разведка.* Эта компьютерная разведка в открытых информационных ресурсах, осуществляемая методами интеллектуального поиска данных в открытых источниках. Интернет – огромное хранилище полезной информации, и сегодня все без исключения могут найти информацию, удовлетворяющую своим интересам, главное, выбрать мощные поисковые системы и правильно сформировать запрос. Отдельно можно сказать об автоматизации интернет-разведки. К наиболее перспективным и бурно развивающимся можно отнести технологии OSINT.

OSINT (*Open Source Intelligence*) подразумевает сбор и анализ разведданных на основе информации из общедоступных источников. Сюда входят газеты, интернет, книги, телефонные справочники, научные журналы, радиовещание, телевидение, правительственные отчеты, техдокументация, руководства-инструкции и т. д.

Разведданные из открытых источников порой не только не отличаются от секретов, но зачастую могут превосходить их своей ценностью. Общая ценность разведданных определяется рядом аспектов, среди которых оперативность поступления, объем, качество, ясность, легкость дальнейшего использования и стоимость получения.

*Сетевая разведка.* Компьютерная разведка в сетях передачи данных, осуществляемая, как правило, методами перехвата и анализа трафика, а также путем идентификации доступных сетевых узлов, сервисов и программного обеспечения. Сетевая разведка – самый первый шаг при подготовке к проникновению или атаке.

Несовершенство сетевого программного обеспечения и большое количество уязвимостей протоколов межсетевого взаимодействия создает огромное разнообразие сетевых атак. Типы атак и способы реализации могут быть оценены при понимании уязвимостей и ограничений протокола TPC/IP. Интернет в начале своего создания нес совершенно нейтральный характер и предназначался для связи между государственными учреждениями и университетами как помощь учебному процессу и научным исследованиям. Создатели на тот момент не осознавали масштаба распространения. В результате в ранних версия интернет-протокола (IP) отсутствовали механизмы безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Среди основных способов реализации сетевой разведки можно

отметить анализ и перехват трафика (сниффинг), подмена доверенного узла сети (спуфинг), атаки человек по середине (MITM) и т. д.

*Целевая разведка.* Компьютерная разведка в защищаемых информационных системах, осуществляемая путем дестабилизирующего воздействия (компьютерных атак), преодоления защитных механизмов и т. д.

При ведении интернет-разведки компьютерные атаки могут быть направлены на незаконное копирование (например, без регистрации или под чужим именем) информационных ресурсов. При ведении сетевой разведки компьютерные атаки могут быть направлены на создание информационных потоков с требуемым содержанием или в требуемом направлении. Целевые компьютерные атаки имеют несколько этапов, преследующих различные цели.

Компьютерную разведку, обеспечивающую добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей, можно классифицировать по способу ведения разведки на:

– *семантическую,* обеспечивающую добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;

– *алгоритмическую*, использующую программно-аппаратные закладки и недекларированные возможности для добывания данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;

– *вирусную*, обеспечивающую добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;

– *разграничительную*, обеспечивающую добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе несанкционированного доступа (НСД) к информации, а также реализация несанкционированного доступа при физическом доступе к похищенным компьютерам или машинным носителям информации (МНИ);

– *сетевую*, обеспечивающую добывание данных из компьютерных сетей путем реализации зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации через использование выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификацию, перехват управления либо маскирование своих действий;

– *потоковую*, обеспечивающую добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров;

– *аппаратную*, обеспечивающую добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами, ТКУ;

– *форматную*, обеспечивающую добывание информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов представления, передачи и хранения добытых данных в сведения, а затем в информацию для последующего ее представления;

– *пользовательскую*, обеспечивающую добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (рис. 1.3).

Добывание информации с использованием компьютерной разведки осуществляется из различных источников. С учетом этого можно классифицировать компьютерную разведку по объекту разведки (рис. 1.4) [8, 9, 10].


Рис. 1.3. Классификация компьютерной разведки по способу реализации

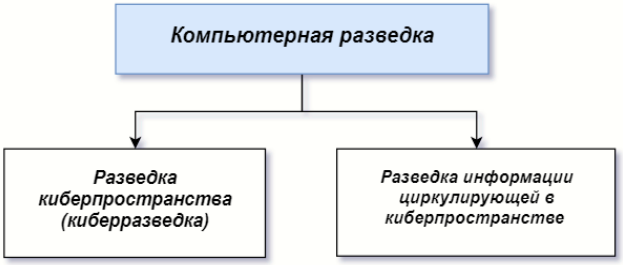


Рис. 1.4. Классификация компьютерной разведки по объекту

Компьютерную разведку также можно классифицировать по методу проведения на легитимные и нелегитимные (компьютерные атаки) (рис. 1.5). К легитимным методам можно отнести следующее: информационный поиск в открытых источниках и сетевой анализ. К нелегитимным методам относится: перехват трафика; проникновение и эксфильтрация данных.

Компьютерную разведку также можно классифицировать по уровню взаимодействия компьютерных систем относительно модели OSI, по используемым методам: технические и не технические (социальная инженерия). Компьютерная разведка может быть обеспечивающая и атакующая (ОС, СУБД, СПО). Все перечисленные классификации связаны, рассмотрим их более подробно.

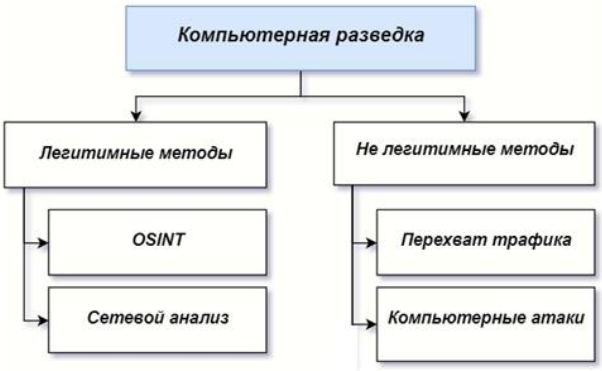


Рис. 1.5. Классификация компьютерной разведки по легитимности

Отдельно можно остановится на нетехнических способах получения информации из компьютерных систем. Социальная инженерия – термин, используемый взломщиками и хакерами для обозначения несанкционированного доступа к информации иначе, чем взлом программного обеспечения, имеющий цель обхитрить людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы. Классическое мошенничество включает звонки по телефону в организацию для выявления тех, кто имеет необходимую информацию, и затем звонок администратору, эмулируя служащего с неотложной проблемой доступа к системе [22]. Более подробно о социальной инженерии рассказано в следующих главах учебного пособия.

Подводя итог, можно сказать, что компьютерная разведка нацелена на информацию, носителями которой являются объекты информационно-коммуникационного пространства (данные, программные и технические средства, используемые в информационных процессах).

## § 2. Отдельные виды технических средств разведки

Техническая разведка предполагает сбор информации с использованием технических разведывательных средств. Возможности технических средств являются одними из основных факторов, определяющих перспективы получения информации. Поэтому органы, обеспечивающие ведение технический разведки, внимательно отслеживают тенденции в развитии технических характеристик средств добывания информации. Наибольшее

влияние на эффективность добывания информации оказывают диапазон частот воспринимаемых средствами частот сигналов, чувствительность, разрешающая способность технического средства, его массагабаритные характеристики и многое другое. Рассмотрим некоторые виды технических средств разведки в соответствии с описанной выше классификацией.

К средствам *оптической разведки* можно отнести оптическую разведывательную систему Cordon-3 (рис. 1.6). Это многоспектральное оптоэлектронное устройство, предназначенное для работы в системах наблюдения и разведки.

Рис. 1.6. Оптическая разведывательная система Cordon-3

Система Cordon-3 может использоваться как самостоятельное устройство с портативной панелью управления RMC-03, так и в составе автоматизированной системы наблюдения. Оптический модуль устройства состоит из тепловизионной камеры, дневной камеры и лазерного дальномера.

Модуль электроники осуществляет Cordon-3: основную и дополнительную обработку цифровых изображений, автоматическое распознаванием целей, их отслеживание, запись необработанных данных, пересылку данных на центральный наблюдательный пункт в цифровом виде.

Еще одним из средств оптической разведки является цифровой бинокль Fortis digital 33X Zoom (рис. 1.7), который предназначен для наблюдения и регистрации подвижных и неподвижных объектов в дневное время суток, ночью, а также в условиях дождя, снегопада и тумана.

Рис. 1.7. Цифровой бинокль Fortis digital 33X Zoom

В цифровом бинокле используется ТВ-камера с высоким разрешением (570 ТВ-линий) и ночной чувствительностью, сопоставимой с приборами ночного видения поколения 2+. Переменное увеличение, автоматический контроль чувствительности, возможность видеозаписи и встроенная память (8 Гб) позволяют обнаруживать и регистрировать человека на расстоянии до 2 000 м и идентифицировать на расстоянии до 300 м. Управление увеличением (zoom) и фокусировка объектива является электронной.

*Радиоразведка* – самый старый вид радиоэлектронной разведки. Она нацелена против различных видов радиосвязи. Основное содержание радиоразведки – это обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций, пеленгование их сигналов, анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения. Одним из

самых функциональных приемников можно отметить IC-R9500 (рис. 1.8). Устройство представляет из себя первоклассный профессиональный связной приемник для широкополосного контроля и обнаружения сигналов, анализа спектра, записи принимаемых станций и многого другого.


Рис. 1.8. Широкополосный сканирующий приемник ICOM IC-R9500

Приемник IC-R9500 способен принимать сигналы SSB, AM, FM (WFM), CW, FSK и P25* в диапазоне частот 0.005–3 335 МГц. Он предусматривает самые различные режимы контроля за появлением сигналов и ведением приема.

Многолетний опыт разработки высокочастотной радиоаппаратуры в сочетании с применением последних достижений в области цифровой техники позволил специалистам корпорации ICOM достичь в новом сканирующем приемнике IC-R9500 уровня +40 dBm точки пересечения по интермодуляционным составляющим третьего порядка (точка IP3), что обеспечило широкий динамический диапазон приемника (109 dB на 14,1 МГц).

Приемник IC-R9500 Sicom2007 предназначается для использования в службах управления связью, осуществляющих слежение за работой радиостанций либо занимающихся мониторингом радиосигналов с анализом спектральных характеристик, а также может вызвать интерес у подготовленных радиолюбителей.

Среди хакеров очень распространены программно определяемые радиосистемы SDR (Software Defined Radio). SDR-приемники – устройства для приема цифровых и аналоговых радиостанций. Для работы используется специализированное программное обеспечение, есть бесплатные версии. Приемники такого типа имеют небольшие размеры, благодаря чему их удобно использовать с планшетами, телефонами, компьютерами, а также встраивать в корпус других приборов.

Внутри такого устройства расположен миниатюрный процессор, который обеспечивает оцифровку радиоволн, в дальнейшем все будет выводиться на компьютер. В отличие от стандартного приемника, где для настройки крутится ручка, что обеспечивает поиск нужной радиостанции, в SDR информация выводится на экран. Все станции, которые на этот момент есть в эфире, здесь отображены. Это удобно, так как больше не нужно наугад искать станцию – необходимая выбирается со списка.


Рис. 1.9. Программно определяемая радиосистема HackRF

HackRF One (рис. 1.9) является одним из самых популярных SDR начального уровня. Он имеет диапазон передачи и приема от 1 МГц до 6 ГГц. Работает в полудуплексном режиме[1], поэтому он может отправлять и получать только попеременно. Он управляется, например, средой разработки SDR GNU Radio.

[1] Полудуплексный режим – способ связи с использованием приемопередающих устройств (модемов, раций, телефонов и т. д.), при котором передача ведется по одному каналу связи в обоих направлениях, но в каждый момент времени передача ведется только в одном направлении.

К средствам акустической технической разведки можно отнести направленный микрофон внутри сигаретной коробки или мобильного телефона (рис. 1.10).

Рис. 1.10. Направленный микрофон внутри сигаретной коробки

Этот исключительно компактный направленный микрофон фиксирует акустические сигналы на расстоянии до 100 м, которые усиливаются в десять раз благодаря встроенному малошумящему мощному усилителю. Благодаря встроенным фильтрам верхних и нижних частот вы можете прослушивать разговоры на расстоянии до 50 м, поскольку они позволяют пропускать особенно голосовые частоты и устраняют нежелательные шумы. Основные характеристики: частота: 20 Гц – 16 КГц (–3 дБ); фильтр верхних/нижних частот: fg = 150 Гц / 5 кГц; питание: стандартная батарея 9 В; потребляемая мощность: макс. 20 мА.

Иногда в комнату можно попасть только через крошечные отверстия или трещины, где только игольчатый микрофон (рис. 1.11) позволит захватывать разговоры внутри помещения. Сигналы усиливаются встроенным усилителем, так что прямое прослушивание через наушники возможно. PKI-2470 оснащен входным разъемом для нашего цифрового рекордера PKI-1865. Звуки регулируются электронным способом. Это означает, что низкие звуки усиливаются больше, чем более громкие, так что громкость поддерживается на постоянном уровне.

Рис. 1.11. Игольчатый микрофон PKI

Электронный стетоскоп PKI-2850 – это недорогая экономичная единица, которая идеально подходит для длительного наблюдения, не входя в помещение, а для прослушивания снаружи – через прочные конструкции (рис. 1.12). Там, где человеческое ухо неадекватно, PKI-2850 делает слышимым то, что раньше казалось невозможным. Карманный блок идеально подходит для ношения на теле, а при необходимости он всегда будет под рукой для быстрой и простой установки. С помощью профессионального усилителя и в сочетании с высокочувствительным контактным микрофоном разговоры и/или шумы можно услышать через стены, окна или любые другие прочные материалы.

Рис. 1.12. Электронный стетоскоп PKI-2850

Отдельное внимание уделим средствам компьютерной разведки. Для ведения компьютерной разведки сегодня можно выделить программно-аппаратные средства и аппаратные средства.

В качестве примера можно привести разработанные компанией PKI различные системы компьютерного мониторинга (рис. 1.13). С помощью этих компьютерных систем мониторинга получение информации становится простым и не может быть обнаружено с помощью системных программ или антивирусных сканеров. PKI-2710 просто подключается между клавиатурой и компьютером. Никакого дополнительного программного обеспечения или драйвера не требуется. PKI-2710 совместим с системами Windows и Linux. 2 Гб памяти записывают внушительный объем данных, которые могут быть считаны в любое время через собственный компьютер. PKI-2710 может поставляться как соединительный штекер PS2, USB и Apple Mac USB. PKI-2715 делает мониторинг компьютера еще более интересным, и это через беспроводное соединение Wi-Fi.

Рис. 1.13. Системы компьютерного мониторинга PKI

AirDrive Forensic Keylogger Pro – это расширенная версия AirDrive Forensic Keylogger с дополнительными возможностями подключения. Он работает и в качестве точки доступа Wi-Fi, и устройства Wi-Fi, обеспечивая такие функции, как отчеты по электронной почте и отметки времени. Сверхмалый, всего 10 мм в длину, и легкий доступ с любого устройства Wi-Fi, такого как компьютер, ноутбук, планшет или смартфон (рис. 1.14).

В отличие от традиционных клавиатурных шпионов, которые работают как флэш-накопители USB, вам не нужно иметь физический доступ к AirDrive Keylogger для извлечения зарегистрированных данных. Просто подключитесь к нему через Wi-Fi, загрузите файл журнала, и все готово. Затем вы можете скрыть кейлоггер, удалив журнал, отключив дальнейшее ведение журнала или даже скрыв сеть WLAN.


Рис. 1.14. Варианты исполнения AirDrive Forensic Keylogger

Основные характеристики AirDrive Forensic Keylogger Pro:

– записывает нажатия клавиш с любой клавиатуры USB;

– самый маленький кейлоггер на рынке, всего 10 мм в длину;

– хранит 8 000 страниц текста;

– 16 Мб встроенной флэш-памяти;

– поддерживает более 40 национальных раскладок клавиатуры;

– работает как точка доступа Wi-Fi или как устройство Wi-Fi;

– отправляет отчеты по электронной почте с записанными данными нажатия клавиш;

– поддерживает метки времени;

– поддерживает потоковую передачу данных по сети;

– возможно подключение с любого компьютера, смартфона или планшета;

– доступ к данным нажатия клавиш из веб-браузера, не требуется никакого программного обеспечения или приложения;

– возможность получать данные удаленно, не касаясь устройства;

– поддерживает сетевую безопасность WEP, WPA и WPA2;

– память защищена аппаратным шифрованием.

Forensic Keylogger Keyboard – это клавиатура для записи нажатий клавиш со встроенным аппаратным кейлоггером (рис. 1.15). Встроенный аппаратный кейлоггер происходит от семейства KeyGrabber Forensic, переключаясь в режим флэш-накопителя для просмотра записанных данных. Он оснащен сложной микросхемой FPGA с 32-кратным алгоритмом дискретизации, обеспечивающим нулевую частоту выпадения символов и полную совместимость со всеми типами USB-топологий. При заказе клавиатуры Forensic Keylogger вы можете выбрать различные модели клавиатуры.

Рис. 1.15. Forensic Keylogger Keyboard

Клавиатура Forensic Keylogger имеет установленный на заводе кейлоггер, основанный на высокопроизводительном KeyGrabber Forensic Keylogger. Модель USB-клавиатуры может быть выбрана для различных производителей, моделей и раскладок клавиатуры (в зависимости от наличия на складе). Это гарантирует полную скрытность, поскольку модуль кейлоггинга не виден невооруженным глазом ни операционной системе (ОС), ни программному обеспечению безопасности.

Еще один представитель клавиатурных шпионов Serial Logger AirDrive Pro (рис. 1.16). Модуль Serial Logger AirDrive Pro – это расширенная версия модуля Serial Logger AirDrive с дополнительными возможностями подключения. Он работает как в качестве точки доступа Wi-Fi, так и в качестве устройства Wi-Fi, обеспечивая такие функции, как отчеты по электронной почте и отметки времени. Положительным моментом является модульная плата форм-фактора и легкий доступ с любого устройства Wi-Fi, такого как компьютер, ноутбук, планшет или смартфон.

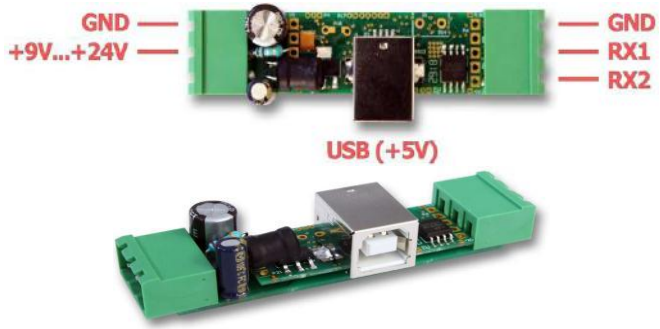


Рис. 1.16. Serial Logger AirDrive Pro

Модуль содержит асинхронный последовательный регистратор, способный записывать потоки данных RS-232 с таких устройств, как принтеры, терминалы, клавиатуры, мыши, сканеры штрих-кода и т. д. Версия Max обладает всеми возможностями

версии Pro, дополненной 16 Гб встроенной памяти, доступной в качестве высокоскоростной USB-флешки (480 Мбит/с). Для последовательного устройства это означает неограниченное хранение данных, доступное как удаленно, так и локально через USB.

Основные характеристики Serial Logger AirDrive Pro:

– журналы асинхронной последовательной передачи (совместимые с RS-232);

– регистрирует два потока одновременно (RX и TX);

– модульный форм-фактор с разъемами клеммной колодки[1];

– 16 Гб встроенной памяти;

– флэш-память промышленного класса;

– работает как точка доступа Wi-Fi или как устройство Wi-Fi;

– отправляет отчеты по электронной почте с записанными данными;

– поддерживает метки времени;

– поддерживает потоковую передачу данных по сети;

– подключение с любого компьютера, смартфона или планшета;

– доступ к данным из веб-браузера, никакого программного обеспечения или приложения не требуется;

– поддерживает сетевую безопасность WEP, WPA и WPA2;

– двойное питание: + 5 В (USB) или + 9 В ... + 24 В постоянного тока (клеммный разъем);

– интегрированный понижающий импульсный источник питания.

[1] Клеммная колодка – электроустановочное изделие, предназначенное для соединения проводов, представляет собой пару (или больше) металлических контактов с узлами крепления к ним проводов.

Модуль кейлоггера AirDrive Forensic Keylogger Module Pro – это расширенная версия модуля судебного кейлоггера AirDrive с дополнительными возможностями подключения (рис. 1.17). Он работает как в качестве точки доступа Wi-Fi, так и в качестве устройства Wi-Fi, обеспечивая такие функции, как отчеты по электронной почте и отметки времени. Сверхкомпактный, всего 12 мм в длину и ширину, и легкий доступ с любого устройства Wi-Fi, такого как компьютер, ноутбук, планшет или смартфон.


Рис. 1.17. Модуль кейлоггера AirDrive Forensic Keylogger Module Pro

Основные характеристики AirDrive Forensic Keylogger Module Pro:

– записывает нажатия клавиш с любой клавиатуры USB;
– быстрая и простая установка внутри клавиатуры;
– самый маленький на рынке кейлоггерный модуль (длина всего 12 мм);
– хранит 8 000 страниц текста;
– 16 Мб встроенной флэш-памяти;
– поддерживает более 40 национальных раскладок клавиатуры;
– совместим со считывателями штрих-кода;
– работает как точка доступа Wi-Fi или как устройство Wi-Fi;
– отправляет отчеты по электронной почте с записанными данными нажатия клавиш;
– поддерживает метки времени;

– поддерживает потоковую передачу данных по сети;

– подключение с любого компьютера, смартфона или планшета;

– доступ к данным нажатия клавиш из веб-браузера, не требуется никакого программного обеспечения или приложения;

– память защищена аппаратным шифрованием.

С 2010 г. USB Rubber Ducky является фаворитом среди хакеров, пентестеров и профессионалов в сфере IT (рис. 1.18). С его дебютом были изобретены атаки с помощью нажатия клавиш и с тех пор, как он захватил воображение своим простым языком сценариев, огромным оборудованием и скрытым дизайном.

Представьте, что вы могли бы подойти к компьютеру, подключить USB-накопитель, и заставить его установить бэкдор, эксфильтровать документы, украсть пароли или любое количество задач на пентест.

Все эти вещи могут быть выполнены с помощью многих хорошо продуманных нажатий клавиш. Если бы вы могли просто сидеть перед этим компьютером с фотографической памятью и безупречной точностью печати, вы могли бы сделать все это за несколько минут.


Рис. 1.18. USB Rubber Ducky

USB Rubber Ducky делает это за считанные секунды. Он нарушает врожденное доверие к компьютерам, выдавая себя за клавиатуру и вводя нажатия клавиш со сверхчеловеческой скоростью.

Shark jack – это портативное средство сетевой атаки, оптимизированное для социальных сетей и оппортунистического аудита проводных сетей (рис. 1.19). По умолчанию он оснащен сверхбыстрой полезной нагрузкой nmap, обеспечивающей быструю и простую разведку сети. Простой язык сценариев и переключатель атаки/постановки на охрану упрощают загрузку, а индикатор RGB обеспечивает мгновенную обратную связь на этапах атаки.

Комплект Combo Kit включает в себя Shark jack плюс кабель USB-C и набор адаптеров, USB-адаптер Ethernet и комплект аксессуаров, а также обертку Essential Gear Hak5.

Рис. 1.19. Портативное средство сетевой атаки Shark jack

USB-«убийца», Meet the USB Kill v3, является CE и FCC. Это утвержденный инструмент тестирования, предназначенный для проверки схемы защиты от перенапряжений электроники до предела и за его пределами (рис. 1.20).

При подключении к устройству USB Killer быстро заряжает свои конденсаторы от линий питания USB. Когда устройство заряжено, 200 В постоянного тока разряжается по линиям данных хост-устройства. Этот цикл зарядки/разрядки повторяется много раз в секунду, пока USB Killer не будет удален.


Рис. 1.20. USB Meet the USB Kill v3

Так, используемый на незащищенном оборудовании USB Killer мгновенно и навсегда отключает целевое оборудование. Не требует батарей, может использоваться неограниченное количество раз. Его компактный размер и корпус в виде флэш-накопителя делают его важным устройством в каждом наборе инструментов для тестировщиков.

USB Kill V3.0 также поставляется в анонимной версии: без логотипа и фирменного стиля, в стандартном футляре USB Flash Drive. Стандартная версия USB Killer имеет логотип USB Kill, высококачественный белый ABS-чехол и съемную пластиковую крышку. Идеально подходит для отраслевых тестеров, так как нет никакой возможности перепутать или подключить устройство по ошибке.

Анонимное издание, созданное для удовлетворения потребностей тестировщиков на проникновение, а также правительства и полиции, является совершенно незаметным. Внутри «универсального» чехла нет логотипа или указания на то, что устройство является USB Kill.

Screen Crab от Hak5 – это скрытый видео-имплантат «Человек посередине» (рис. 1.21). Устройство располагается между устройствами HDMI, например компьютером и монитором, или консолью и телевизором – для скрытого захвата снимков экрана.

Рис. 1.21. Screen Crab от Hak5

Screen Crab настроен для сохранения скриншотов на карту MicroSD. Он также автоматически сгенерирует файл config.txt с настройками по умолчанию. Режим захвата может быть установлен на изображение или видео, интервал захвата может быть установлен в секундах, а параметры хранения могут быть либо остановлены, когда карта MicroSD заполнена, либо может быть непрерывный захват с перезаписью.

Packet Squirrel от Hak5 – это скрытный карманный «человек посередине» (рис. 1.22), разработанный для обеспечения скрытого удаленного доступа, безболезненного захвата пакетов и защищенных VPN-подключений с помощью переключателя. Невероятно маленький и легкий (50x40x15 мм, 24 грамм). Универсальное подключение с двумя гнездами RJ45 Ethernet, хост-портом USB и портом питания micro USB. Платформа Linux с рут-доступом и общими утилитами. Скриптовая кнопка и многоцветный индикатор состояния.

Рис. 1.22. Packet Squirrel от Hak5

Signal Owl от Hak5 – это платформа для разведки сигналов с простой системой полезной нагрузки (рис. 1.23). Он содержит пользовательские утилиты и популярные беспроводные инструменты, такие как Aircrack-ng, MDK4, Kismet и др. Внутренний Wi-Fi оптимизирован для операций ближнего доступа, в то время как поддерживается ряд распространенных приемопередатчиков, таких как GPS, SDR и Bluetooth.

Рис. 1.23. Signal Owl от Hak5

Комбинированный комплект включает в себя Signal Owl плюс мини-USB Bluetooth-адаптер и Hak5 Essential Gear Wrap. В сочетании с пользовательскими утилитами и популярными беспроводными инструментами, такими как Aircrack-ng Suite, MDK4 и Kismet, написание полезных данных не может быть проще. С простой и гибкой структурой и экосистемой полезных данных из репозитория Hak5, начать работу легко.

Alfa AWUS036NH, признанный лучшим хакерским адаптером Wi-Fi для Kali Linux, идеально подходит для мониторинга, прослушивания, ввода пакетов и беспроводного аудита.

AWUS036NH – это беспроводной USB-адаптер IEEE 802.11b/g/n (рис. 1.24). Он также совместим с беспроводными устройствами IEEE 802.11b/g со скоростью 54 Мбит/с. Вы можете настроить AWUS036NH в режиме ad-hoc для подключения к другим беспроводным компьютерам 2,4 ГГц или в режиме инфраструктуры для подключения к беспроводной точке доступа или маршрутизатору для доступа к интернету.


Рис. 1.24. Беспроводной USB-адаптер AWUS036NH

USBNinja – это очень скрытый фреймворк USB, позволяющий удаленно запускать пользовательские полезные данные (рис. 1.25). Во время бездействия USBNinja функционирует как обычный USB-кабель: передача данных, перезарядка и т. д.

Рис. 1.25. Скрытый фреймворк USB USBNinja

Эмулируя действия клавиатуры и мыши, полезные нагрузки полностью настраиваемы и могут быть целенаправленными. USBNinja не может быть обнаружен брандмауэрами, программным обеспечением AV или визуальным осмотром. Это идеальный инструмент для тестеров на проникновение, полиции и правительства.

Inputstick Rat – это беспроводное управление компьютерами с помощью компактной, незаметной USB-флешки (рис. 1.26).

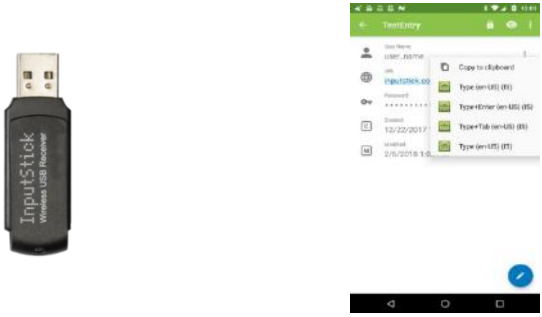


Рис. 1.26. Инструмент удаленного доступа Inputstick Rat

InputStick Remote Admin – компактный, невероятно мощный USB-инструмент удаленного доступа с возможностями беспроводной связи Bluetooth, упакованный в обычный USB-накопитель. Доступ к нему можно получить с любого смартфона BLE:

– радиус действия: до 10 м;

– HID интерфейсы: клавиатура, мышь, геймпад, управление потребителем;

– радиоинтерфейс: Bluetooth (2,4 ГГц, BT4.0);

– шифрование AES-128 (режим CBC) на уровне протокола.

Устройство было впервые представлено в 2019 г. на выставке Milipol Paris, посвященной внутренней безопасности государств, где команда NSO Group представила такое устройство взлома, а новостной сайт Business Insider моментально прокомментировал.

Pegasus – это модульный «badware» (рис. 1.27). Просканировав устройство жертвы, он загружает недостающие модули, чтобы читать SMS и электронную почту жертвы, прослушивать звонки, делать скриншоты, записывать нажатия клавиш, рыться в контактах и истории браузера и др. В общем, он может следить буквально за всем, что делает жертва на взломанном устройстве или рядом с ним.

Рис. 1.27. Модульный комплекс вредоносного ПО «Pegasus»

Pegasus может прослушивать зашифрованные звонки и читать зашифрованные сообщения: фиксируя нажатия виртуальных клавиш, он считывает сообщения до шифрования, а захват экрана позволяет украсть входящие сообщения после расшифровки. То же с записью голоса и звука.

Pegasus хорошо может «прятаться». Так, «зловред» самоуничтожается, если не сможет связаться с командным сервером более 60 дней или же если обнаруживает, что попал не на то устройство, например с другой SIM-картой. Последнее очень даже объяснимо: Pegasus создан для целевого шпионажа, и клиентам, купившим «зловреда» у NSO, неинтересно следить за случайными людьми.

Список средств для ведения компьютерной разведки и специалистов по безопасности, для тестирования на проникновение и взлома был бы неполным без рассмотрения самого популярного программного обеспечения.

Самым универсальным средством можно отметить операционную систему Kali Linux. Она широко известна, как один из лучших инструментов с открытым исходным кодом, является дистрибутивом Linux на основе Debian, который можно назвать швейцарским ножом для сообщества по тестированию на проникновение. Эта операционная система для тестирования пера

включает в себя около 600 различных инструментов с тоннами исчерпывающих функций безопасности.

Когда дело доходит до проблем, связанных с SQL-инъекциями, первый вариант, который приходит в голову – это sqlmap. Этот инструмент аудита VAPT с открытым исходным кодом эффективно обнаруживает недостатки SQL-инъекций и почти все, что не так с вашими серверами баз данных. Его мощный механизм обнаружения способен выявлять и использовать даже самые надуманные недостатки в системах управления базами данных.

Обычно известный как Network Mapper, Nmap является наиболее предпочтительным инструментом для сканирования портов. Nmap – один из наиболее эффективных и настраиваемых инструментов оценки тестирования на проникновение. Может эффективно сканировать угрозы как в крупных, так и в небольших сетях. Nmap обычно используется на предварительных этапах тщательного аудита VAPT, чтобы определить, какие сетевые порты подвержены серьезным угрозам.

Metasploit широко считается одной из ведущих систем тестирования на проникновение по всему миру. Metasploit, поддерживаемый Rapid7, может также использоваться на серверах, в сетях и приложениях. Этот инструмент имеет базовый интерфейс командной строки и бесперебойно работает в Windows, Apple Mac OS и Linux.

Aircrack-NG анализирует уязвимости в сетях Wi-Fi, внедряя обширную коллекцию инструментов оценки тестирования на проникновение. Этот комплект тестирования Wi-Fi собирает пакеты данных вашей сети Wi-Fi и экспортирует их в виде текстовых файлов для дальнейшего анализа. Он также выполняет другие функции, такие как идентификация поддельных точек доступа, оценка возможностей водителя и Wi-Fi-карт и т. д.

Wireshark – это инструмент для тестирования на проникновение, который по своей природе используется в качестве сетевого протокола и анализатора пакетов. Он поддерживает множество полезных протоколов и в основном используется для детальной проверки сетевого и беспроводного трафика. Он также анализирует беспроводное воздушное движение для углубленной оценки безопасности. Это также инструмент с открытым исходным кодом, который можно использовать в Windows, Linux, Mac OS X, Solaris и т. д.

Рассмотренный список описывает только наиболее известные и широко используемые инструменты. В последующих главах мы рассмотрим более обстоятельно перечисленные и другие средства ведения компьютерной разведки.

## § 3. Основные понятия и термины компьютерной разведки

Постоянное развитие информационных технологий и компьютерной техники, а также засилье иностранного языка оказывают значительное влияние на формирование понятий и терминов в области кибербезопасности и компьютерной разведки. Исследователи и представители различных государственных и коммерческих структур используют специализированный язык, который позволяет быстро и эффективно общаться с представителями своей профессии.

Использование такого языка приводит к тому, что для описания одного объекта используется несколько терминов. Различия в терминологии и отсутствие единой стандартизации могут привести к искажению, ошибкам и неправильному пониманию, а также к потере информации и знаний.

Таким образом, для четкого понимания материала учебного пособия и формирования единой терминологической основы рассмотрим основные понятия и термины. В качестве базы для изучения терминологии в области компьютерной разведки приведем следующие нормативные правовые акты:

– Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

– ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (изд. с поправкой)»;

– ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»;

– ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления»;

– ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»;

– ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения»;

– ГОСТ Р 58143-2018 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения».

Выделим ряд терминов из указанных нормативных правовых актов, наиболее употребляемых в области компьютерной безопасности (кибербезопасности).

*Авторизация* – предоставление конкретному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий.

*Анализ трафика* – извлечение информации из видимых характеристик потока (-ов) данных, даже если данные зашифрованы или непосредственно недоступны, причем указанные характеристики включают в себя степени идентичности и месторасположения источника (-ов) и адресата (-ов), наличие и объем потоков, а также частоту и длительность их передачи.

*Атака* – посягательство на систему, которое является следствием продуманного планирования, т. е. умышленного действия, представляющее собой попытку (особенно в плане метода или стратегии) обойти сервисы безопасности и нарушить политику безопасности системы.

*Атака «отказ в обслуживании» (DOS-атака)* – атака на систему, направленная на ограничение ее доступности.

*Аутентификация* – мера безопасности, запроектированная на установление правомерности передачи самого сообщения или

его источника, а также средство проверки авторизационных данных индивидуального пользователя для получения определенных категорий информации.

*Ботнет* – совокупность программных роботов или ботов, которые функционируют автономно. Создатель ботнета может дистанционно управлять работой группы объектов, зачастую в неблаговидных целях.

*Вредоносный код* – программы или код, написанные с целью получения информации о системах или пользователях, уничтожения системных данных, создания благоприятных условий для дальнейшего несанкционированного проникновения в систему, фальсификации системных данных и отчетов, а также внесения путаницы в системные процессы и доставления длительных хлопот обслуживающему персоналу.

*Вредоносная программа* – программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

*Демилитаризованная зона (DMZ)* – хост безопасности или небольшая сеть (называемая также защищенной подсетью), располагаемые между сетями в качестве «нейтральной зоны».

*Доменное имя* – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет.

*Кибербезопасность (киберзащита)* – действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов.

*Коммутатор* – устройство, объединяющее различные сетевые устройства в единый сегмент сети и передающее информацию конкретному устройству.

*Компьютерный вирус* – программа, обладающая способностью к самораспространению по локальным ресурсам средства вычислительной техники, не использующая сетевых сервисов.

*Компьютерная атака* – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

*Компьютерная информация* – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [28].

*Маршрутизатор* – шлюз между двумя сетями, функционирующими на третьем уровне взаимодействия открытых систем (OSI), который перенаправляет и посылает пакеты данных во внутреннюю сеть. Наиболее известные типы маршрутизаторов пересылают пакеты интернет-протокола (IP).

*Метаданные файла* – атрибуты файла, определяемые прикладным программным обеспечением.

*Недекларированные возможности (программного обеспечения)* – функциональные возможности программного обеспечения, не описанные в документации.

*Программная закладка* – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

*Прокси-сервер (proxy-server)* – компьютерный процесс, который перенаправляет протокол между клиентской и серверной

компьютерными системами, представляясь клиенту от имени сервера, а серверу – от имени клиента.

*Сетевая атака* – компьютерная атака с использованием протоколов межсетевого взаимодействия.

*Сигнатура файла* – уникальная цепочка байт или формализованное описание признаков, указывающие на тип файла.

*Сниффинг (несанкционированный анализ трафика)* – перехват и раскрытие содержания сообщений или применение анализа трафика, основанного на выявлении адресата, источника сообщения, частоты или длительности передачи данных и других параметров связи, как средство нарушения конфиденциальности коммуникационной системы.

*Социальная инженерия* – практика заполучения конфиденциальной информации путем психологического воздействия на легальных пользователей.

*Тестирование на проникновение* – вид работ по выявлению (подтверждению) уязвимостей программы, основанный на моделировании (имитации) действий потенциального нарушителя.

*Троянский конь* – компьютерная программа, которая на первый взгляд имеет полезную функцию, но при этом скрытую и потенциально вредоносную функцию, которая позволяет обойти механизмы безопасности путем использования подлинных авторизационных данных субъекта системы, вызывающего программу.

*Утечка информации* – несанкционированное использование, рассекречивание, преобразование или замена в каждом из случаев, данных, программ или конфигурации системы, т. е. в результате и после несанкционированного проникновения.

*Уязвимость программы* – недостаток программы, который может быть использован для реализации угроз безопасности информации.

*Уязвимость* – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (-ая) может быть использован (-а) для реализации угроз безопасности информации.

*Фаззинг* – тестирование, использующее как корректные, так и случайные (включая некорректные) входные данные для проверки, устанавливающее, обрабатываются ли должным образом интерфейсом случайные входные данные или возникает ли ошибочная ситуация (ошибочное условие), указывающая (-ее) на наличие недостатков при разработке (ошибки исходного кода) или при эксплуатации.

*Фаззинг-тестирование программы* – вид работ по исследованию программы, направленный на оценку ее свойств и основанный на передаче программе случайных или специально сформированных входных данных, отличных от данных, предусмотренных алгоритмом работы программы.

*Фишинг* – разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который, на первый взгляд, связан с законным источником.

*Хеш-код* – битовая строка фиксированной длины, являющаяся результатом преобразования входящих данных хеш-функцией.

*Хеш-функция* – функция, выполняющая по определенному алгоритму преобразование входящих данных большого размера в битовую строку фиксированной длины.

*Червь* – компьютерная программа, которая может действовать независимо, распространять свою полную рабочую версию на другие хосты сети и потреблять ресурсы компьютера с их разрушением.

*IP-адрес* – адрес компьютера или устройства, предназначенный для их идентификации и связи с ними с использованием межсетевого протокола Internet и других протоколов.

*MAC-адрес* – аппаратный адрес, который позволяет дифференцировать одно устройство сети от другого.

Настоящие термины будут использоваться нами и в дальнейшем.

## § 4. Нормативно-правовые аспекты компьютерной разведки

Одним из проявлений разведывательной деятельности можно без сомнения считать оперативно-разыскную деятельность (ОРД). Однако разведывательная деятельность, в отличии от ОРД, осуществляется в большинстве случаев за пределами территории Российской Федерации в отношении иностранных государств или их представителей, угрожающих интересам государственной безопасности.

Разведывательная деятельность осуществляется органами внешней разведки Российской Федерации посредством: добывания и обработки информации о затрагивающих жизненно важные интересы Российской Федерации реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц (далее – разведывательная информация); оказания содействия в реализации мер, осуществляемых государством в интересах обеспечения безопасности Российской Федерации [25].

Оперативно-розыскная деятельность – вид деятельности, осуществляемой гласно и негласно оперативными подразделе-

ниями государственных органов, уполномоченных на то настоящим Федеральным законом (далее – органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств [26].

Согласно ст. 13 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ № 144) на территории Российской Федерации право осуществлять оперативно-разыскную деятельность предоставляется оперативным подразделениям органам внутренних дел. Полномочия распределены приказом МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России».

Отдельно можно отметить, что в ФЗ № 144 определены задачи оперативно-разыскной деятельности: выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших; осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших; добывание информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации; установление имущества, подлежащего конфискации.

В реализации основных задач оперативно-разыскной деятельности неизменными остаются способы оперативного получения информации и своевременное ее использование при раскрытии и расследовании преступлений.

Технический прогресс и развитие информационных технологий привлекают внимание преступников. В современной литературе сформировалось понятие киберпреступности. Киберпреступность характеризуется местом совершения преступления, как правило, в сети Интернет, а также средствами совершения преступления, зачастую это компьютерные системы и (или) компьютерные сети. Большой проблемой противодействия киберпреступности на сегодня остается трансграничность и анонимность. Трансграничность киберпреступности дает возможность для совершения преступлений с территории других государств. Кроме того, большинство совершаемых киберпреступлений совершаются с использование технологий анонимности. Установление места нахождения преступника и факта совершения преступных действий, сбор доказательств становятся затруднительными для правоохранительных органов при осуществлении процессуальных действий.

Таким образом, в условиях высокой информатизации компьютерная разведка является единственным решением задач оперативно-разыскной деятельности при противодействии преступлениям в сфере информационных технологий и киберпространстве.

Как уже было отмечено выше, оперативно-разыскная деятельность осуществляется путем проведения оперативно-разыскных мероприятий (ОРМ). Оперативно-разыскные мероприятия представляют собой один из основных источников оперативно-разыскной информации. Перечень ОРМ содержится в ст. 6 ФЗ № 144. Под оперативно-разыскными мероприятиями принято понимать предусмотренные законом действия преимущественно конспиративного характера, осуществляемые должностными лицами оперативных аппаратов в целях получения и проверки оперативной информации об обстоятельствах, имеющих значе-

ние для предупреждения и раскрытия преступлений, осуществления розыскной работы, а также решения иных задач оперативно-розыскной деятельности [26].

По своей архитектуре компьютерные системы могут быть как локальными (все их компоненты находятся на одном компьютере), так и распределенными (компоненты распределены по нескольким компьютерам). Кроме того, компьютерные системы могут быть как открытыми, так и закрытыми для граждан, т. е. доступ к ним ограничен их собственником, владельцем или держателем путем размещения серверного оборудования и рабочих станций компьютерных систем в публично недоступных местах, жилище или ином владении лица, и установкой средств защиты информации. Отдельно стоит отметить портативные средства хранения информации: флэш-накопители, внешние диски и т. д.

Глава 28 УК РФ посвящена общественной опасности, представляющую собой киберпреступления. В сфере компьютерной информации УК РФ выделяет следующие преступления:

– статья 272 УК РФ «Неправомерный доступ к компьютерной информации» предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, его системы или сети;

– статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» предусматривает уголовную ответственность за создание программ для компьютера или внесение изменений в существующие программы, заведомо предназначенных для несанкционированного уничтожения, блокированию, модификации либо копированию информации, нарушения компьютерной информации, а равно

использование либо распространение таких программ или машинных носителей с такими программами;

– статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» предусматривает уголовную ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей, повлекшее уничтожение, блокирование, копирование или модификацию компьютерной информации;

– статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» предусматривает уголовную ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации;

– статья 159.6 «Мошенничество в сфере компьютерной информации» предусматривает уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [28].

Сам термин «компьютерная информация» описан в примечании к ст. 272 УК РФ: сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств

их хранения, обработки и передачи. Понятие «информация» наиболее полно раскрыто в стандарте ИСО 2382/1-93: любой факт, понятие или значение, полученные из данных, а также контекст, выбранный из знаний, или контекст, ассоциированный со знаниями. Исходя из данных положений, компьютерную информацию необходимо сначала закодировать, т. е. представить ее в компьютерную форму, а затем декодировать ее, т. е. представить в форму, доступную для восприятия человеком.

Преступления в сфере компьютерной информации большинством специалистов разделяют на две основные группы:

1) преступления, в которых компьютер используется как средство совершения преступлений;

2) преступления, в которых компьютер является предметом преступных посягательств.

Большинство объектов компьютерной разведки характерны для отдельных видов ОРМ: опрос; сбор образцов для сравнительного исследования; исследование предметов и документов; наблюдение; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи; оперативный эксперимент; получение компьютерной информации.

Примером наблюдения в сетевом информационном пространстве является оперативно-разыскной мониторинг (интернет-мониторинг), который представляет собой комплексную систему ОРМ, обеспечивающих наблюдение за состоянием криминальных процессов в сетевой социальной среде, основанную на использовании средств и методов компьютерной разведки и направленную на сбор, обработку и анализ информации.

Осуществление мониторинга может базироваться на применении в сетевом пространстве различных ОРМ (наведение справок, опрос, наблюдение и др.).

Объектами сетевого оперативно-разыскного мониторинга могут быть все виды информационных ресурсов в интернете. Основными направлениями мониторинга, способными обеспечить высокую интенсивность поступления оперативно-разыскной информации, являются:

– автоматизированный поиск сетевых ресурсов, содержащих запрещенную к распространению информацию;

– изучение сетевых ресурсов, связанных с деятельностью преступных сообществ;

– наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности.

Использование специальных технических средств при проведении ОРМ существенно повышает их эффективность. Более того, на применении специальной техники полностью основаны такие ОРМ, как прослушивание телефонных переговоров, снятие информации с технических каналов связи, контроль почтовых отправлений, наблюдение, получение компьютерной информации и некоторые другие. Мероприятия, основанные на применении специальных технических средств, называются оперативно-техническими [5].

*Снятие информации с технических каналов связи* – это оперативно-техническое мероприятие, заключающееся в контроле и перехвате с помощью специальных средств текстовой, графической и иной информации, передаваемой проверяемыми лицами по техническим каналам связи.

Объектом данного мероприятия является содержание информации, передаваемой проверяемыми лицами по техническим каналам связи, а также сведения о проводимых сеансах связи.

Снятие информации с технических каналов связи осуществляется в отношении передаваемых данных: их сбор производится в реальном масштабе времени путем перехвата за счет использования программного обеспечения и специальной аппаратуры, подключенной к каналу связи (СОРМ). Однако многие из узлов сетевого коммуникационного оборудования содержат собственные устройства памяти, в которых могут какое-то время сохраняться передаваемые данные, также проводится изъятие таких данных. Вместе с тем служебная информация, которая хранится в базе данных оператора связи, не относится к передаваемой по каналу связи, а потому доступ к ней осуществляется путем наведения справок [5].

Исследование предметов и документов – это не процессуальное криминалистическое, научно-техническое или иное исследование объектов, полученных в результате других оперативно-разыскных мероприятий, проводимое в целях выявления признаков преступной деятельности и причастности к ней конкретных проверяемых лиц.

Объектами мероприятия могут выступать предметы, полученные в результате оперативно-разыскных мероприятий несущие на себе следы преступлений (наркотики, оружие, орудия преступлений, компьютерные программы и т. д.).

При необходимости проведения оперативно-технических мероприятий на строго конспиративной основе привлекаются сотрудники подразделений специальных технических мероприятий.

Назначение подразделений специальных технических мероприятий ОВД состоит в организации и проведении оперативно-технических мероприятий по заданиям оперативных-разыскных подразделений, техническом обеспечении оперативно-разыскных мероприятий в целях негласного получения информации

и документирования преступной деятельности, а также координации своей деятельности с оперативно-техническими подразделениями ФСБ России.

Оперативно-разыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов внутренних дел в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-разыскную деятельность.

Необходимо отметить, что осуществление оперативно-разыскных мероприятий и получение компьютерной информации невозможно без участия специалиста. Об этом, в частности, свидетельствует и указание в ч. 4 ст. 6 ФЗ № 144 на то, что оперативно-разыскные мероприятия, связанные с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности и органов внутренних дел.

Формулировка данного оперативно-разыскного мероприятия распространяется на весь перечень обозначенных выше объектов, исследуемых при раскрытии и расследовании преступлений в сфере компьютерной информации.

Должностные лица органов, осуществляющих оперативно-разыскную деятельность, решают ее задачи посредством личного участия в организации и проведении оперативно-разыск-

ных мероприятий, используя помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Запрещается проведение оперативно-разыскных мероприятий и использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, не уполномоченными на то настоящим федеральным законом физическими и юридическими лицами [26].

Сфера борьбы с современной преступностью объективно обусловливает взаимосвязь оперативно-разыскной деятельности и информационных технологий. Средства и методы оперативно-разыскной деятельности в совокупности с информационными технологиями получения информации или данных характеризуют правовую основу одного из направлений компьютерной разведки.

# ГЛАВА II. РАЗВЕДКА В ОТКРЫТЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

## § 1. Разведка в открытых источниках (OSINT)

Военные США впервые придумали термин OSINT в конце 1980-х гг., утверждая, что это вынужденная мера в связи с реформой разведывательной службы и появлению новых информационных требований. В 1996 г. Комиссия Американского разведывательного сообщества (известная как комиссия Aspin–Brown) заявила, что «необходимо приложить больше усилий по использованию общей мировой информации, доступной сейчас из открытых источников». Параллельные усилия НАТО по созданию основы для использования OSINT привели к публикации нескольких справочников, руководств и практических рекомендаций. Согласно справочнику по разведке из открытых источников НАТО от ноября 2001 г. различают четыре различных категории источников информации для OSINT.

*Open Source Data (OSD).* К этой категории источников можно отнести необработанные данные для печати, устный опрос или другую форму информации из первичного источника. Это может быть фотография, запись на магнитофон, изображение коммерческого спутника или личные письма от людей. Примером являются репортеры, которые входили в войска Афганистана или Ирака. Они фотографируют, разговаривают с солдатами, записывают заметки ручкой или карандашом, что можно отнести к необработанным данным.

*Open Source Information (OSI).* OSI состоит из данных, которые объединены, обработаны и отредактированы – это информация чаще широкого распространения. Газеты, книги, трансляции

и общие ежедневные доклады, отчеты. Примером может служить репортер, работающий на стороне противника, который собирает необработанные данные, преобразует их в статью, которая после редактирования печатается в газетах, журналах или транслируется по радио.

*Open Source Intelligence (OSINT).* OSINT – это информация, которая распространяется для узкой аудитории, как правило, руководству, персоналу, для решения конкретных вопросов разведки. OSINT применяет традиционные методы разведки к открытым источникам информации. Например, статья в журнале, созданная из необработанных данных, может обладать значимостью, если на фотографиии к статье изображены здания, где может находиться противник. Так, OSINT может применяться при проведении военной операции.

*Validated OSINT (OSINT-V).* Эта категория представляет собой информацию с очень высокой степенью доверия. Она предоставляется специалистом по разведке по результатам анализа всех возможных источников информации, которая может быть получена из гарантированного открытого источника. Например, репортер принимает фотографии и отчеты на мосту, разведчики знают, что мост очень важен для противника. При этом в ходе операции, из видео, снятого в реальном времени, мост идентифицировали как уничтоженный, чтобы держать повстанцев вдалеке от перемещения предметов снабжения. Таким образом, OSINT-V подтвердит данные и предоставит факты о наличии моста [18, 19].

Безусловно, отслеживать строительство новых зданий, мостов, дорог или аэродромов сложно, но именно это и делает информацию, добытую из открытых источников, чрезвычайно ценной. OSINT-V охватывает области, недоступные для традиционных видов разведки, а ее достоверность можно оспаривать лишь в том

случае, когда предоставлены доказательства для опровержения полученных данных.

В современной практике OSINT злоумышленник или пентестер, собирая информацию из общедоступных источников о конкретной цели, может профилировать потенциальную жертву, чтобы лучше понять ее характеристики и сузить область поиска возможных уязвимостей. Без активного воздействия на цель злоумышленник может использовать полученные данные для построения модели угрозы и разработки плана атаки. Целевые кибератаки, как и военные атаки, начинаются с разведки, а первая стадия компьютерной разведки – это пассивное получение данных без предупреждения цели.

Сбор информации о себе или своей организации также является отличным способом понимания, какая информация вами дана потенциальным злоумышленникам. Как только вы узнаете, какую информацию о вас можно собрать из общедоступных источников, вы сможете использовать ее, чтобы помочь себе или вашей команде безопасности разработать более эффективные стратегии защиты.

Как отмечалось ранее, в качестве открытых источников используются общедоступные информационные ресурсы (в первую очередь интернет). Поиск осуществляется с использованием информационно-поисковых систем. Следует подчеркнуть, что свои собственные национальные поисковые системы имеют только США, Россия и Китай [42].

Каждая информационно-поисковая система имеет в своем составе одну или несколько поисковых машин. Поисковые машины представляют собой набор программ-роботов (поисковых программ), которые осуществляют сбор информации в общедоступных сетях в соответствии с установленными правилами.

Основные термины и определения понятий в области поиска и распространения информации с помощью автоматизированных информационных систем содержатся в ГОСТ 7.73-96 СИБИД «Поиск и распространение информации. Термины и определения». На основании государственного стандарта можно составить классификацию информационно-поисковой системы (рис. 2.1).

*Информационно-поисковая система (ИПС)* – совокупность справочно-информационного фонда и технических средств информационного поиска в нем [30].

*Автоматизированная информационно-поисковая система* – это информационно-поисковая система, реализованная на базе электронно-вычислительной техники [30].

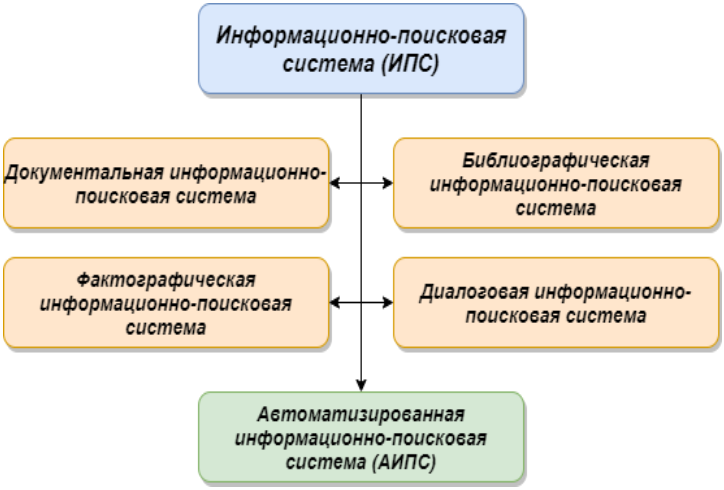


Рис. 2.1. Классификация информационно-поисковых систем

Сегодня применяются и разрабатываются автоматизированные системы поиска и обработки информации, которые позволяют выявлять из множества открытых источников, размещенных в интернете, взаимосвязанные данные, анализ которых

открывает различные сведения о тех или иных информационных сетях, а главное, о циркулирующей в них информации.

Основным компонентом автоматизированной информационно-поисковой системы является поисковая машина (searching engine). Поисковая машина представляет набор программ с веб-интерфейсом, выполняющий сбор и обработку данных в интернете, а также поиск по имеющимся данным и вывод результатов поиска в соответствии с запросом пользователя. Поиск в таких системах проводится по индексам копий сайтов, которые хранятся в базе данных. За автоматический поиск и сбор информации отвечают поисковые-программы роботы (краулеры).

*Краулер «веб-паук»* – программа, являющаяся составной частью поисковой системы и предназначенная для изучения страниц интернета с целью занесения информации о них в базу данных поисковика. Она анализирует содержимое страницы, сохраняет его в специальном виде на сервере поисковой машины, который ей принадлежит, и отправляется по ссылкам на следующие страницы. Владельцы поисковых машин нередко ограничивают глубину проникновения «паука» внутрь сайта и максимальный размер сканируемого текста, поэтому чересчур большие сайты могут оказаться не полностью проиндексированными поисковой машиной.

По принципу действия краулер напоминает обычный браузер. Он заходит на веб-страницу, обрабатывает ее содержимое, сохраняет его в индекс поисковой системы и отправляется по ссылкам на следующие страницы сайта.

В дальнейшем краулер посещает находящиеся в индексе, веб-страницы сайта с целью проверки необходимости обновления индексов, а также поиска новых веб-страниц сайта. Данный про-

цесс будет производиться постоянно, но с определенной периодичностью, что позволит избежать повышенной нагрузки как на сайт, так и на поисковую систему.

Однако не все веб-страницы посещаются поисковым роботом. Сайты, которые трудно найти поисковику, остаются без внимания. Они называются DeepWeb (также называемым скрытым или глубинным интернетом). Согласно некоторым исследованиям глубокая сеть в 100 раз больше, чем индексированная сеть, хотя ее очень трудно измерить. Большинство сайтов, которые относятся к глубинному интернету, делятся на следующие категории:

– частные сайты – на них может не быть прямых ссылок или требоваться авторизация. Они обычно блокируют доступ к роботам-поисковикам;

– сайты с заполнением определенной формы (бланка) – их посещение возможно только после ввода некоторых данных в начальную форму. Например, сайты, продающие авиабилеты, обычно запрашивают информацию о поездке на главной странице, так вы сможете получить доступ только после заполнения определенной формы. Несмотря на то, что вы сможете использовать поисковую систему для поиска расписания рейсов, большинство роботов не смогут преодолеть главную страницу, чтобы получить информацию о расписании;

– страницы с элементами интерактивности – используются JavaScript (далее – JS), Flash или другой подобный язык. Если сайт не находится в исходном HTML-коде веб-страницы, а создается кодом JS, запущенным в браузере, роботу необходимо будет выполнить JS на странице, чтобы найти ссылку, что возможно технически, но выполнение JS значительно замедляет краулера и усложняет работу всей системы;

– OSINT Framework – сервис для знакомства с разведкой в открытых источниках, созданный Джастином Нордином (https://osintframework.com/). Представляет собой ссылки на большую коллекцию ресурсов для самых разных задач, от сбора адресов электронной почты до поиска в социальных сетях или темной сети (рис. 2.2).

При анализе общедоступных ресурсов для проведения классификации удобно использовать объекты поиска (Ф. И. О., никнейм, номер телефона и т. д.). Классификацию современных источников OSINT можно представить в виде блок-схемы (рис. 2.3).

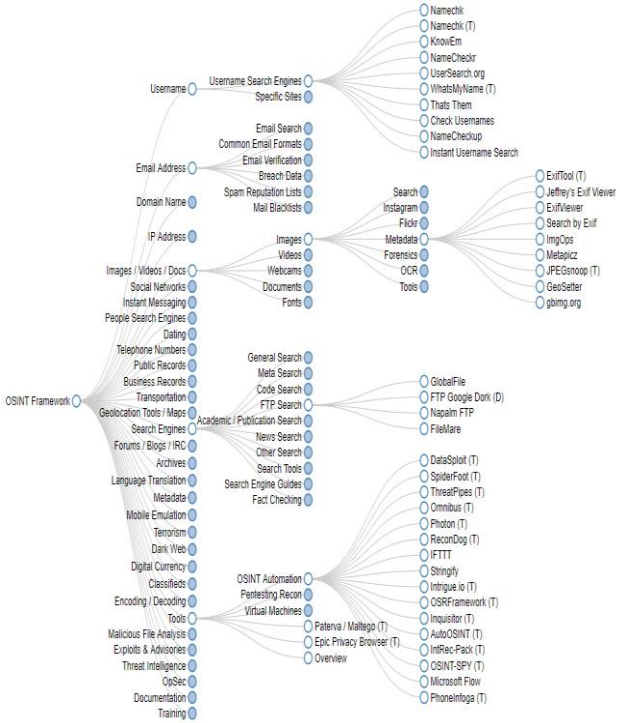


Рис. 2.2. OSINT Framework

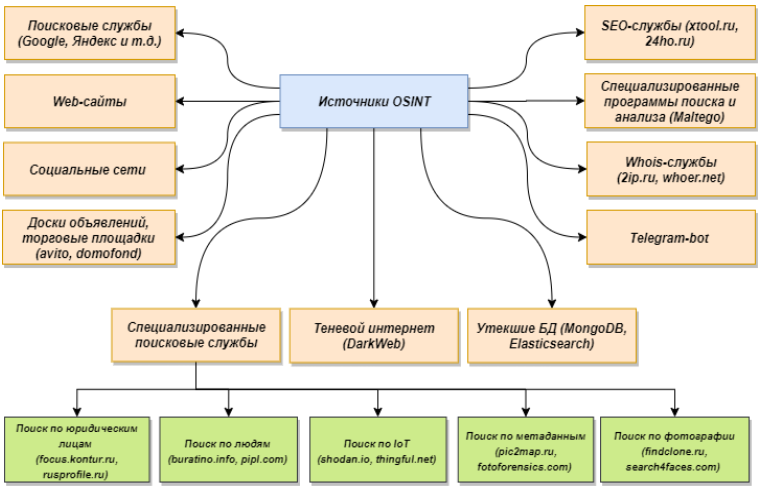


Рис. 2.3. Классификация источников OSINT

Поскольку невозможно установить четкие рамки понятия OSINT, соответствующим инструментом можно считать даже Google, однако узкоспециализированные OSINT-сервисы существуют. Ниже приведена группировка таких сервисов по объекту поиска:

– сервисы для сбора информации по Ф. И. О.: Nomer.org (nomer.center и зеркала), Yandex.people, Mmnt.ru, Kad.arbitr.ru, Spra.vkaru.net, Fio.stop-list.info, Zitely.rosfirm.info, https://buratino.info/, боты в ТГ (@egrul_bot);

– сервисы для сбора информации по номеру телефона: веб-сайты Nomer.org (nomer.center и зеркала), боты в мессенджерах (@AVInfoBot, @SmartSearch_Bot, @mailsearchbot, @get_kontakt_bot);

– сервисы для сбора информации о электронной почте и никнеймах: веб-сайты (Haveibeenpwned.com, Leakedsource.ru,

Dehashed.com, Email.rep, Intelx.io, instantusername.com, Namechk.com, Yasni.com), боты в мессенджерах (@SmartSearch_Bot, @mailsearchbot);

– сервисы для сбора информации по фотографии: Findclone.ru, Vk.watch, Search4faces.com, @AVInfobot, @Falcone_FaceID_bot;

– сервисы для сбора информации по адресу: Nomer.org (nomer.center и зеркала), Rosreestr.ru, Address.stop-list.info, Photomap.ru, Wigle.net (по BSSID точек Wi-Fi), боты ТГ (@FriendsFindBot);

– сервисы для сбора информации о домене: Archive.org (сохраненные архивные версии страниц сайтов), Cashedview.com (сохраненные архивные версии страниц сайтов), Ru.smart-ip.net (гео-IP, трассировка писем), Whois.domaintools.com, Virustotal.com, Xinit.ru, Urlscan.io, Censys.io, Shodan.io, Atsameip.intercode.ca;

– сервисы для анализа СМИ: веб-сайты (Медиалогия, Brand Analytics, Nownews.com); боты (@tgstat, @buzzim_alerts_bot, @MotherSearch_Bot).

Рассматривая инструменты разведки открытых информационных ресурсов в интернете, нельзя не обратить внимание на специализированную операционную систему Buscador Linux. Она подходит как для опытных пользователей, так и для новичков в области сбора данных из сети. Сборка включает в себя следующие основные компоненты, ориентированные на сбор и анализ информации из открытых источников в интернете: браузеры Firefox и Chrome с набором специальных приложений, Tor, Recon-NG, Maltego, Creepy, Metagoofil, MediaInfo, ExifTool TheHarvester, Wayback Exporter, HTTrack Cloner, Web Snapper,

Knock Pages, SubBrute, Twitter Exporter, Tinfoleak, BleachBit, VeraCrypt, KeePass.

Ну, и в завершении обзора инструментов OSINT коснемся набирающего огромную популярность в последнее время дистрибутива Kali Linux, разработанный для хакеров и пентестеров. Дистрибутив содержит множество инструментов, связанных с безопасностью и сетями, которые ориентированы на экспертов в компьютерной безопасности.

Список инструментов Kali Linux довольно обширен и разбит на несколько категорий, позднее мы будем касаться возможностей сетевого сканирования, перехвата трафика и т. д. Утилиты выделены в категорию сбора информации, среди которых:

– Maltego, Recon-ng, MassMine – приложение для добычи и архивирования данных из социальных медиа;

– OSRFramework – это набор библиотек для выполнения задач по разведке на основе открытых источников;

– SpiderFoot – это инструмент с открытым исходным кодом для автоматизированной разведки;

– theHarvester – это инструмент для сбора e-mail адресов, имен доменов, виртуальных хостов, открытых портов/баннеров и имен работников из различных открытых источников и т. д.

## § 2. Сетевая разведка

Сетевое сканирование реализуется с использованием сетевых сканеров, с помощью которых осуществляется сканирование хостов в составе атакуемых информационных сетей, с запуском соответствующих утилит в составе этих сканеров или аналогичных им, встроенных в сканеры программ, а также с применением отдельно функционирующих аналогичных утилит,

специально написанных скриптов и программ. При проведении сканирования можно выявить следующую информацию:

– топологию сети, в которой функционирует атакуемая система. При этом может исследоваться область вокруг атакуемой сети (например, нарушителя могут интересовать адреса доверенных, но менее защищенных хостов). Сбор информации может быть также основан на запросах: к DNS-серверу о списке зарегистрированных (и, вероятно, активных) хостов; к маршрутизатору на основе протокола RIP об известных маршрутах (информация о топологии сети); к некорректно сконфигурированным устройствам, поддерживающим протокол SNMP, позволяющий получать информацию о топологии сети. Если атакуемая сеть находится за межсетевым экраном (МЭ), возможен сбор информации о конфигурации МЭ и о топологии сети за МЭ, в том числе путем посылки пакетов на все порты всех предполагаемых хостов внутренней (защищаемой) сети [16];

– тип операционной системы на атакуемых хостах. Например, широко применяется способ определения типа ОС хоста, основанный на том, что различные типы ОС по-разному реализуют требования стандартов RFC к стеку TCP/IP и реагируют на некоторые запросы. Это позволяет нарушителю удаленно идентифицировать тип ОС, установленной на хосте ИС, путем посылки специальным образом сформированных запросов и анализа полученных ответов (рис. 2.4).

Также можно отметить такой способ определения типа ОС, как простейший запрос на установление соединения по протоколу удаленного доступа telnet (telnet-соединения), в результате которого по «внешнему виду» ответа можно определить тип ОС хоста.

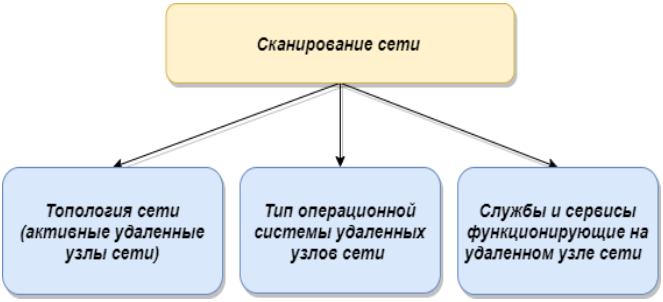


Рис. 2.4. Информация, выявляемая при сканировании сети

Наличие определенных сервисов также может служить дополнительным признаком для определения типа ОС хоста [16].

1. *Функционирующие на хостах сервисы.* Определение сервисов, исполняемых на хосте, основано на способе выявления «открытых портов», направленном на сбор информации о доступности хоста.

Первое, что можно сделать при построении топологии сети, – это идентифицировать работающие узлы. На первый взгляд может показаться, что идентификация работающих в сети компьютеров слишком простая задача, не требующая отдельного внимания, ведь достаточно запустить сетевой сканер, и работающие в данный момент сетевые узлы будут обнаружены. На самом деле сейчас в локальных сетях очень часто используют фильтрацию сетевого трафика и межсетевое экранирование, в результате далеко не каждый сетевой сканер обнаружит все работающие в данный момент хосты. Без тонкой настройки средств сканирования эти узлы так и останутся «невидимыми» [2].

Для идентификации активных узлов в локальной сети можно использовать различные протоколы сетевого и транспортного уровня, такие как ICMP, UDP и TCP.

2. *Исследование сети с помощью прокола ICMP.* ICMP относится к служебным протоколам и используется для выявления

ошибок на сетевом уровне. Как правило, в локальных сетях его не блокируют, так как он часто используется самими системными администраторами для поиска неполадок в сети. Благодаря этому с помощью ICMP можно производить исследование работающих в сети компьютеров.

Рассмотрим основные принципы работы данного протокола. Сообщения ICMP передаются в виде IP-дейтаграммы, т. е. к ним прибавляется заголовок IP. Существуют несколько типов сообщений ICMP. Каждый имеет свой формат, при этом все они содержат следующие три поля: 8-битного целого числа, обозначающего тип сообщения (TYPE); 8-битного поля кода (CODE), который конкретизирует назначение сообщения; 16-битного поля контрольной суммы (CHECKSUM).

Все типы сообщений ICMP можно условно, поделить на две группы:

1) сообщения об ошибках, например Destination unreachable;
2) запросы и ответы, например Echo Request и Echo Reply.

Начнем с рассмотрения сообщений об ошибках. Они содержат заголовок и первые 64 бита данных пакета IP, при передаче которого возникла ошибка. Это делается для того, чтобы отправитель смог более точно проанализировать причину ошибки, так как все протоколы прикладного уровня стека TCP/IP содержат наиболее важную информацию для анализа именно в первых 64 битах своих сообщений. Для большинства сообщений об ошибках задействовано поле кода. В основном для исследования сети используются Echo Reply, Echo Request и Timestamp. Полный список полей можно найти в стандарте Request for Comments (RFC), содержащем технические спецификации и стандарты сетевых протоколов [2].

Идентификация (т. е. обнаружение) сетевых устройств с помощью протокола ICMP может быть выполнена двумя способами: посылка запроса, получение ответа; вызов ситуации ошибки, получение сообщения об ошибке.

В основу идентификации заложен следующий принцип. Узел, отправляющий ICMP-запрос, устанавливает значения полей Identifier, эти значения позволяют определить ответы, пришедшие от разных узлов. Для того, чтобы отличить несколько ответов, пришедших от одного узла, используется поле Sequence Number. В поле Code записывается ноль, поле данных произвольно (например, алфавит). Отвечающая сторона должна заменить значение поля Type на 0 и отправить дейтаграмму обратно.

Наилучшим способом определения доступности узла является посылка сообщения ICMP Echo (Type 8). Если система работает и отсутствует фильтрация трафика данного типа, то в ответ придет сообщение ICMP Echo Reply (Type 0).

Для выполнения обнаружения узла обычно используется утилита ping, входящая в состав большинства ОС. В синтаксисе консольной утилиты ping указывается IP-адрес или имя сетевого узла (ping mail.ru), в результате получаем ответ удаленной системы. Однако у нее есть существенный недостаток: все узлы опрашиваются последовательно, что существенно увеличивает продолжительность опроса.

Обращение сразу к нескольким узлам (диапазона) с использованием ICMP-запросов (Echo) называется ICMP Sweep или Ping Sweep. Для исследования большой сети потребуется утилита, способная посылать ICMP-запросы параллельно. Однако, говоря о Ping Sweep, стоит отметить, что из-за параллельной отправки множества ICMP-запросов системы обнаружения атак легко определят такое сканирование.

3. *User Datagram Protocol (UDP) исследование сети*. Метод определения доступности узла с использованием протокола UDP называется UDP Discovery. Если в ответ на пакет было получено сообщение ICMP Destination Unreachable (Port Unreachable), это означает, что узел недоступен и порт, указанный в UDP-пакете, закрыт. В случае неполучения ответа от узла возможны следующие варианты:

- узел выключен или недоступен;
- включена фильтрация трафика;
- указанный в UDP-пакете порт открыт.

Использование протокола UDP для обнаружения устройств неэффективно в силу следующих причин. Во-первых, это высокая степень фильтрации UDP-трафика. Так как из-за архитектурных особенностей (отсутствие механизма подтверждения доставки) UDP используют мало служб (самыми известными являются DNS, SNMP, Syslog), то этот протокол часто фильтруется в сети. Вторым недостатком использования UDP является непредсказуемое поведение системы при получении UDP-пакета на открытый порт. Дело в том, что многие сканеры отправляют при сканировании пустые пакеты. Допустим, такой пакет отправили на 53-й порт сервера DNS. Получив его на открытый порт, система попытается прочитать содержимое. При этом на уровне приложений будут ожидаться данные определенного формата (команды, параметры и т. д.). Но так как там никаких данных нет, сервис вполне может повести себя не совсем корректно или, что еще хуже для исследующего, отразить данный инцидент в своих журналах событий.

Некоторые разработчики смогли обойти второй недостаток UDP-сканирования. В сканере Retina этот метод реализован с учетом указанных недостатков. На данные порты отправляется не пустой UDP-пакет, а осмысленный запрос, на который должен

прийти ответ. Таким образом, реакция будет в любом случае (открыт порт или закрыт), что повышает достоверность этого метода при идентификации сетевых объектов.

4. *Исследование с помощью TCP.* Метод определения доступности узла с использованием протокола TCP называется TCP Ping. Протокол TCP используется гораздо большим числом различных служб и приложений. В нашем случае это основной инструмент исследования сети, так как средства межсетевого экранирования и системы обнаружения вторжений, как правило, разрешают отправку пакетов на наиболее распространенные сетевые порты. Например, вряд ли где-то будут запрещать электронную почту или веб.

При проведении сканирования важным является выбор значений следующих полей: Source Port, Destination Port, Сочетание флагов (поле Flags) [2].

Выбор порта источника зависит от фильтрации трафика различного типа, а правильный выбор порта получателя необходим из соображений возможной фильтрации (обычно это наиболее распространенные порты – 21, 22, 23, 25, 80).

Но основным при исследовании сети с помощью TCP является выбор правильного сочетания флагов. В качестве примера рассмотрим синтаксис утилиты hping с различным сочетанием флагов. Эта утилита позволяет генерировать специальные ICMP/UDP/TCP пакеты и просматривать ответы удаленного хоста в стиле обычной утилиты ping:

hping <узел> [опции].

Флаги TCP: F – fin флаг FIN; S – syn флаг SYN; R – rst флаг RST; P – push флаг PUSH; A – ack флаг ACK; U – urg флаг URG; X – xmas флаг X неиспользуемый (0x40); Y – ymas флаг Y неиспользуемый (0x80).

Посылка TCP-пакета с установленным флагом SYN может быть использована для определения доступности узла следующим образом: если в ответ на такой запрос пришел пакет с установленными в заголовке флагами SYN, ACK или RST, то узел доступен. Если же ответ не приходит, то узел либо недоступен, либо данный тип трафика фильтруется.

Один из этапов сетевой разведки – это определение типа и версии операционной системы, установленной на определенном сетевом узле, основанной на методах Fingerprinting, которые представляют собой анализ наборов открытых портов, анализ баннеров сервисов прикладного уровня, анализ результатов идентификации сервисов и приложений. Самым простым методом определения операционной системы является отклик открытых портов сетевого узла. Использование команд служб прикладного уровня, например команды SYST протокола FTP можно отнести к еще одному способу. Ну, и наконец, вывод о типе ОС может быть сделан по результатам идентификации сервисов и приложений.

Метод, основанный на наблюдении, называется «TCP/IP Stack Fingerptinting». Рассмотрим некоторые методы опроса стека TCP/IP удаленного хоста:

1. *FIN-исследование.* Перед началом непосредственного исследования хост сканирует порты сервера и определяет, какие порты являются открытыми. Затем на любой открытый порт сервера хост посылает FIN-пакет (TCP-пакет на завершение соединения) или любой другой пакет без флагов SYN и ACK. В соответствии с RFC 793 сервер должен ответить на такой пакет RST-пакетом, однако некоторые ОС типа Windows, BSDI, CISCO, HP/UX, MVS и IRIX не посылают ничего в ответ.

2. *Исследование поля Window TCP-пакета.* Анализируя принятые от сервера TCP-пакеты, целесообразно обратить внимание на поле Window в их заголовках, поскольку значение этого поля является своеобразной константой, характеризующей ОС. В некоторых случаях для однозначного определения типа ОС достаточно извлечь значение поля Window в TCP-заголовке принятого от сервера пакета. Например, ОС AIX – единственная операционная система, имеющая значение Window=0x3F25. «Полностью переписанный» стек TCP/IP в ОС Windows NT5, равно как и OpenBSD и FreeBSD, имеют Window=0x402E.

3. *Исследование скорости генерирования ICMP-сообщений.* Согласно RFC 792 протокол ICMP использует протокол IP в качестве средства доставки. Очевидно, что ICMP-сообщения занимают определенную часть полосы пропускания канала связи, что снижает общую скорость передачи данных. По этой причине некоторые продвинутые ОС, следуя рекомендации RFC 1812, ограничивают количество отправляемых в канал связи ICMP-сообщений об ошибках. Так, Linux ограничивает количество ICMP-сообщений об ошибке типа «получатель недоступен» (Destination Unreachable) до 80 сообщений в 4 с, с простоем 0,25 с, если это ограничение было превышено.

Единственный способ проверить скорость генерирования ICMP-сообщений сервером – это послать на некоторый закрытый UDP-порт с большим номером набор пакетов и подсчитать количество принятых ICMP-сообщений. Этот тест является очень медленным, и, кроме того, вызывает относительно большую нагрузку на сеть.

Идентификация служб и сервисов, запущенных на компьютерах сети, тоже является одной из важных задач для подготовки и проведения атаки на компьютерные системы. Рассмотрим основные способы идентификации сетевых сервисов:

1. *Сканирование портов UDP* – програмное средство, разработанное для поиска хостов сети, в которых открыты нужные порты. Дело в том, что за многими распространенными приложениями закреплены определенные номера портов и протоколы транспортного уровня. Так, HTTP использует порт 80, FTP – 20 и 21, а SSH – 22 и т. д. И, хотя значения портов по умолчанию можно легко изменить, но все же открытый порт с определенным номером является верным признаком того, что на узле работает именно данное приложение. Остается только определить, какие порты открыты на узле.

Метод сканирования портов UDP используется для определения, какие UDP-порты на сканируемом узле являются открытыми. На требуемый порт сканируемой машины отправляется UDP-пакет (обычно пустой). Если в ответ было получено ICMP-сообщение «Destination Unreachable», это означает, что порт закрыт. В противном случае (нет ответа) считается, что сканируемый порт открыт [2].

С UDP-сканированием связаны следующие проблемы:

– возможная потеря UDP-пакетов, в таком случае ответ также не будет получен, и порту может быть ошибочно присвоен статус «открыт»;

– высокая степень вероятности фильтрации UDP или (и) ICMP-трафика. Результат тот же, что и в предыдущем случае: порт может быть ошибочно посчитан открытым.

Все это приводит к тому, что в случае неполучения ответа от узла нельзя быть уверенным в том, что порт открыт. Первая проблема решается введением двух параметров, которыми можно регулировать достоверность UDP-сканирования: количество посылаемых UDP-пакетов, время ожидания ответа. Вторая проблема гораздо сложнее. Для ее решения разработчики сканеров

используют различные усовершенствования. Рассмотрим один из таких способов.

Перед сканированием заданных пользователем портов UDP-сканер проводит сканирование портов из начала диапазона 1–65 535 (230–240), из середины диапазона (2050–2060) и из конца диапазона (45 270–45 280). Как видно, выбранные порты с большой долей вероятности окажутся закрыты.

2. *Анализ баннеров.* Это наиболее распространенный метод сбора информации о запущенных на сканируемом узле службах. Данный метод заключается в анализе приветствий, выводимых службами при подключении на заданный порт. Часто «баннеры» содержат информацию об используемой службе вплоть до номера версии. Тут стоит отметить, что далеко не все сетевые службы являются абсолютно переносимыми, это вдобавок дает возможность делать предположения об используемой операционной системе. Например, если в баннере присутствует IIS, то сервер работает под Windows, а если SSH, то, скорее всего, перед нами Unix.

Обращение к почтовому серверу приведет к следующему отклику:

```
telnet smtp.ru 25
220 smtp.ru ESMTP Sendmail 11 8. 11 2/8 11 2. Thu, 10Jan 2011 18 34: 19
+0400
```

В данном баннере видно использование почтового сервера Sendmail, распространяемого бесплатно вместе с исходными кодами [17]. Вот как выглядит отклик файлового сервера Synology USB Station 2. telnet 192.168.1.2 5000:

```
<1 DOCTYPE HTML PUBLIC "-//IETF//DTP HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved
<a href=http://(null)/webman/index.cgi>here</a>.</p>
<hr>
<address>Apache/2.2.16 (Unix) Server at Port 5000</adresse>
</body></html>
```

Судя по строке Apache/2.2.16 (Unix) Server, на этом устройстве используются веб-сервер Apache и специально собранная версия Unix, и вот как выглядит отклик на аналогичный запрос одного бюджетного маршрутизатора:

```
HTTP/1. O 400 Bad Request
Server: WL520 gc/httpd
Date: Thu, 05 Apr 2012 21:10:25 GMT
Content-Type: text/html
Connection: close
<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY BGCOLOR=»#cc9999»><H4>400
Bad Request</H4>
Can t parse request.
</BODY></HTML>
```

В отклике нет ни имени, ни версии веб-сервера или операционной системы. Однако стоит обратить внимание на WL520GC, который обладает большой функциональностью.

3. *Mail-bouncing* – это автоматическое сообщение от системы электронной почты, информирующее отправителя предыдущего сообщения о том, что сообщение не было доставлено или возникла другая проблема с доставкой. В основном сервер возвращает ответное письмо с сообщением об ошибке отправки, если e-mail адрес получателя не существует (hard bounce) или

временно недоступен (soft bounce). Функция анализа баунсов предназначена для того, чтобы поддерживать актуальность текущих списков рассылки, удаляя несуществующие адреса, и чтобы избежать блокировки спам-фильтрами. В данных уведомлениях содержится некоторая информация о почтовых серверах, участвующих в процессе доставки письма, например, на основе нескольких баунсов можно узнать некоторое число узлов внутренней сети (не имея к ней непосредственного доступа) и топологию почтовых пересылок. Кроме того, почтовый протокол позволяет отправлять письма с явным указанием нескольких промежуточных пунктов пересылки. В анализаторе существуют настройки почтовых серверов, которые можно редактировать, удалять или дополнять собственными, что предоставляет возможность отправить письмо, которое, проделав заданный маршрут внутри исследуемой сети, вернется к отправителю. Пересылка писем, заданная таким образом, позволяет использовать mail bouncing как метод сетевой разведки.

Специализированные программные продукты для проведения описанных действий называют сетевыми сканерами, которые условно можно поделить на две группы:

1) сканеры портов (Nmap, Network Utility, SuperScan, Zmap);

2) сканеры уязвимостей (XSpider, Nessus, Retina Network Security Scanner, OpenVAS, Max Patrol и т. д.).

Собирая и анализируя информацию в открытых компьютерных сетях, появляется возможность сформировать полноценный профиль атакуемой системы и определить существующие и потенциальные уязвимости. Первый этап компьютерной разведки начинается с предварительного сбора информации, который может быть организован пассивным способом с помощью OSINT и сканирования сети без предупреждения цели. Таким образом можно использовать полученную информацию для построения модели угрозы, разработки плана атаки или защиты.

# ГЛАВА III. АНОНИМНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ

## § 1. Технологии обеспечения анонимности в интернете

Исследуя удаленные сетевые узлы (хосты) и проводя сканирование сети (не только расположенные в анонимных сетях, но и самые обычные сайты), в первую очередь следует задуматься об обеспечении анонимности своего компьютера.

При запросе страницы веб-сайта компьютеру приходится обмениваться с сервером определенной информацией, и этот процесс не ограничивается передачей вам для просмотра HTML-кода запрошенной веб-страницы. В процессе обмена сервер может получить с компьютера клиента и другую информацию, в том числе идентифицирующую тип компьютера, предыдущий посещенный веб-сайт, идентифицирующие адреса электронной почты и т. п.

Чтобы более четко уяснить возможности по вашей идентификации, имеющиеся у серверов интернета, можно обратиться к веб-сайту по адресу (https://2ip.ru/) который предоставляет услуги по анализу информации, которую может извлечь веб-сервер из клиентского компьютера. Этот сервер достаточно точно определит операционную систему клиентского компьютера, используемый браузер, время запроса и IP-адрес сервера провайдера интернета и многое другое (рис. 3.1).

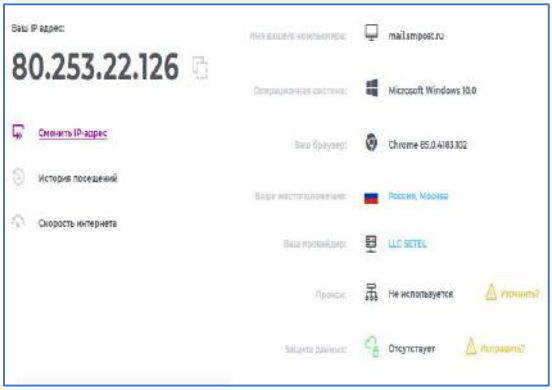


Рис. 3.1. Пример идентификация клиентского компьютера

Обладание такой информацией выдает ваше местоположение для этого нужно только просмотреть на сервере удаленного доступа провайдера все регистрационные журналы и найти запись, фиксирующую информацию о подключении клиентского компьютера с данным IP-адресом в указанное время. Так что многие веб-сайты на загруженной веб-странице отображают предупреждение о том, что серверу известен IP-адрес клиентского компьютера и в случае проведения мероприятий по компьютерной разведке скрытность не гарантируется.

На сегодняшний день обеспечение анонимности в интернете строится на следующих двух технологиях: *шифрование* и *построение сложной цепочки прокси-серверов*, а также их комбинирование.


Рис. 3.2. Принцип работы прокси-сервера

Прокси-сервера в наше время являются очень полезным и удобным средством защиты личной информации, которыми с каждым днем пользуется все большее количество людей. Глобально, когда говорят прокси-сервер, то имеют в виду что-то, выступающее посредником между клиентом и адресатом (рис. 3.2). Существуют различные виды прокси-серверов, каждый из которых обладает своими преимуществами и недостатками. Несмотря на то, что видов прокси-серверов достаточно много, часто используемыми являются лишь несколько из них, которые рассмотрим далее.

*HTTP-proxy* – самый распространенный. Он предназначен для организации работы браузеров и других программ, использующих протокол HTTP. Браузер передает прокси-серверу URL ресурса, прокси-сервер получает его с запрашиваемого веб-сервера (или с другого прокси-сервера) и отдает браузеру.

*HTTPS-proxy* – буква «S» в названии означает «secure» – безопасность. HTTPS выделяют в отдельную группу. Обычно этот протокол применяют, когда требуется передача информации с использованием шифрования.

По мнению ряда специалистов в области информационной безопасности Socks является самым прогрессивным прокси-сервером способным надежно защитить вашу личную информацию. На данный момент существует два основных вида протокола Socks4 и Socks5, обладающие определенными отличиями. Протокол представляет собой транслятор (что-то вроде прокси-сервера), но в отличие от обычных прокси Socks-клиент расположен между прикладным и транспортным уровнем в модели OSI, а Socks-сервер находится на прикладном уровне. Это означает, что такой сервер не привязан больше к протоколам высокого уровня. Сам протокол разработан для того, чтобы приложения, работающие на

основе TCP и UDP, могли использовать ресурсы сети, доступ к которым ограничен архитектурой или настройками.

Вследствие того, что Socks не имеет никакого отношения к HTTP, то данный вид прокси игнорирует все вопросы, связанные с модернизацией заголовков HTTP-запросов. Socks-сервер будет передавать все данные в чистом виде от первого лица, т. е. от себя, другими словами, анонимны. Технология Socks легко поддерживает построения в цепь.

В любом случае прокси-сервер не обеспечит необходимый уровень анонимности и не защитит вас от специальных служб так как весь трафик в открытом виде проходит через прокси-сервер третьих лиц. Для обеспечения достаточного уровня анонимности сегодня применяется шифрование (туннелирование).

*Туннелирование в компьютерных сетях* – процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. В интернете последнее время для обеспечения анонимности используют VPN-сервисы (серверы).

*Виртуальная частная сеть* – территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, сети Интернет, сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных.

Туннелирование не представляет собой ничего нового. IPSec (VPN) – это, возможно, самый широко известный способ туннелирования, наиболее близким продолжением которого является SSH-туннелирование, несмотря на некоторые различия, основной принцип работы у них одинаков (рис. 3.3).


Рис. 3.3. Общий принцип работы туннелирования

Широко используются следующие протоколы VPN: PPTP, L2TP, OpenVPN, SSTP, SSL и TLS. Практически все VPN-сервисы предлагают выбор из двух протоколов: OpenVPN и PPTP. Реже предлагается протокол L2TP+IPSec. И совсем единицы предлагают протокол SSTP.

Отдельно стоит отметить сервисы, предоставляющие DoubleVPN, когда перед тем, как выйти в интернет, траффик проходит два разных VPN-сервера в разных странах, или даже QuadVPN, когда используется четыре сервера, которые пользователь может выбрать сам и расположить в произвольном порядке.

Один из самых популярных способов обеспечения анонимности – *луковая маршрутизация* – это распределенная оверлейная сеть, созданная для анонимизации приложений, таких как веб-браузеры, SSH, клиенты мгновенных сообщений. Клиенты выбирают маршрут в сети и создают цепочку, в которой каждый узел (или луковый маршрутизатор) знает только предыдущий и следующий узлы цепочки и не имеет понятия об остальных. Трафик проходит по цепочке в виде ячеек фиксированного размера, которые раскрываются (расшифровываются) с использованием симметричного ключа на каждом узле (подобно слоям луковицы) и передаются дальше (рис. 3.4).

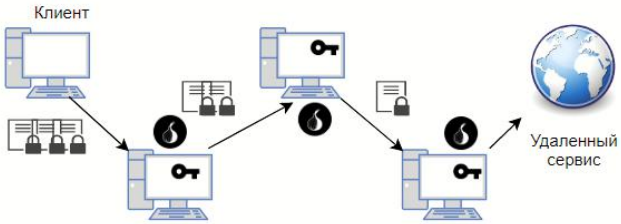


Рис. 3.4. Упрощенная схема работы луковой маршрутизации

Несмотря на то, что системы, использующие луковую маршрутизацию, развернуты во многих уголках планеты, единственная установка, которая действительно работала долго, была экспериментальной и работала она на одном единственном компьютере. Но даже эта простая установка системы обслуживала соединения более чем с 60 тыс. различных IP-адресов со всего света, обрабатывая около 50 тыс. ежедневно. Однако, множество просчетов в проектировании и развертывании так и не были исправлены, а проект не обновлялся годами.

Луковая маршрутизация изначально требовала отдельного уровня для каждого протокола каждого приложения. Большинство прокси так и не были написаны, т. е. множество приложений никогда не поддерживались. Tor использует стандартный и близкий к SOCKS прокси-интерфейс, позволяя поддерживать множество программ, работающих по TCP без изменений.

*Tor (The Onion Router)* представляет из себя, цепочку узлов через которую пользователь подключается к интернету. Как правило, цепочка состоит из трех узлов, каждому из них неизвестны адреса клиента и ресурса одновременно (рис. 3.5). Кроме того, Tor шифрует сообщения отдельно для каждого узла, а открытый трафик виден только выходному роутеру. По некоторым оценкам Tor – это десять управляющих узлов, около 4 200 НОД, в том числе около 900 выходных узлов.

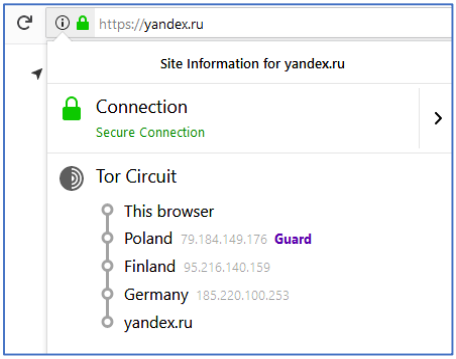


Рис. 3.5. Пример построения цепочки Tor

Каждый пользователь запускает на своем компьютере программу, называемую луковым прокси, для получения информации из серверов каталогов, установления цепочек в сети и обработки соединений от пользовательских приложений. Эти луковые прокси принимают TCP-потоки и мультиплексируют их по цепочкам. Луковый маршрутизатор на другом конце цепочки соединяет пользователя с адресом назначения и передает данные дальше.

Каждый луковый маршрутизатор поддерживает долгосрочный идентификационный ключ и краткосрочный луковый ключ. Идентификационный ключ используется для подписи TLS-сертификатов, дескриптора лукового маршрутизатора (объединение его ключей, адресов, скорость передачи, политики точки выхода и т. п.), каталогов (используется серверами каталогов). Луковый ключ используется для расшифровки запросов от пользователей на установление цепочки и для согласования временных ключей. TLS-протокол также устанавливает краткосрочный ключ соединения при общении между луковыми маршрутизаторами. Краткосрочные ключи меняются периодически и независимо друг от друга, для того чтобы уменьшить ущерб от компрометации ключа.

*Чесночная маршрутизация* – это более совершенная реализация луковой маршрутизации, используемой в проекте TOR. Основы и принципы чесночной маршрутизации и чесночного шифрования разработал Майкл Фридман[1]. Позже эта идея была доработана и внедрена разработчиками проекта I2P (проект невидимого интернета).

Сеть I2P (invisible internet project) является оверлейной (работает поверх другой сети, например интернета), устойчивой (отключение узла не повлияет на функционирование сети), анонимной (невозможно или трудно определить IP-адрес узла). При передаче данных между узлами сети применяется шифрование. В ней есть свои сайты, форумы и другие сервисы.

Основу I2P составляет защищенная децентрализованная анонимная компьютерная сеть с малым временем отклика и свойствами автономности, отказоустойчивости и масштабируемости. Конечной задачей I2P является ее способность функционировать в жестких условиях, даже под давлением организаций, обладающих значительными финансовыми или политическими ресурсами. Все компоненты сети доступны в виде исходного кода и бесплатны.

I2P строго разделяет программное обеспечение, участвующее в сети: маршрутизаторы и анонимные концы (цели), связанные с отдельными приложениями. Конечные пользователи, как правило, имеют несколько локальных адресов на маршрутизаторе, например, один прокси для IRC-серверов, другой для поддержки пользовательского анонимного веб-сервера и еще один

[1] Майкл Хартли Фридман (род. 21 апреля 1951 г.) – математик из исследовательской группы в Калифорнийском университете в Санта-Барбаре, в 1986 г. был удостоен Филдовской премии. Вместе с Р. Кирби показали, что гипотеза Пуанкаре справедлива для n = 4.

для торрентов и т. д. При этом, когда используется I2P, информация о действиях пользователя, а также о том, что пользователь подключен к определенному маршрутизатору, скрывается.

В I2P есть два главных понятия – туннель и сетевая база NetDB, которая в той или иной мере распределена по всем клиентам I2P [44].

*Туннель* – это ориентированный путь через явно выбранный список маршрутизаторов. Поскольку в сети I2P используется многоуровневое шифрование, каждый из маршрутизаторов может расшифровать только один слой. Расшифрованная информация слоя содержит IP-адрес следующего маршрутизатора, а также зашифрованную информацию, которая перенаправляется далее. Каждый туннель имеет начальную точку (первый маршрутизатор, также известный как шлюз) и конечную точку. Однако сообщения по туннелю могут быть отправлены только в одну сторону, а для получения обратного сообщения требуется создать еще один туннель.

Соответственно, для работы сети создаются туннели двух типов: исходящий, который отправляет сообщение от создателя туннеля; входящий, который передает сообщение обратно создателю туннеля.

Процесс передачи данных в сети I2P проиллюстрирован на рис. 3.6, где отправитель создает исходящий туннель, а принимающая сторона устанавливает входящий туннель. Входящий шлюз принимающей стороны позволяет получать сообщения от других пользователей и пересылать их до конечной точки. При передаче сообщения исходящая конечная точка должна отправить сообщение на входящий шлюз принимающей стороны. Для этого отправитель добавляет в зашифрованное сообщение соответствующие инструкции. Как только исходящая конечная точка

расшифрует сообщение, она получит инструкцию по пересылке сообщения на правильный входящий шлюз [44].

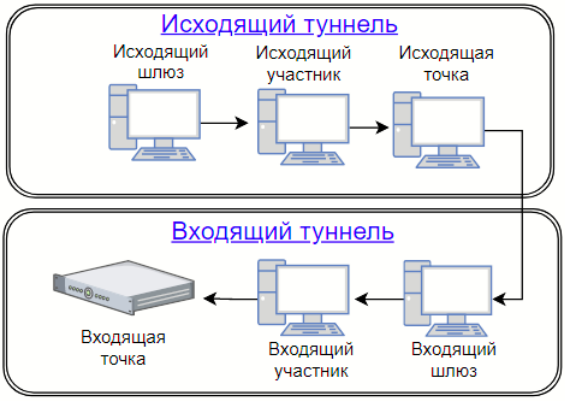


Рис. 3.6. Передача данных в сети I2P

*Сетевая база данных NetDB.* Существует два типа метаданных, хранящихся в NetDB: routerInfo и leaseSet. Метаданные routerInfo содержат информацию о маршрутизаторах, необходимых для обмена данными (их открытые ключи, адреса и т. д.), а leaseSet предоставляет маршрутизаторам информацию, необходимую для связи конкретных точек и создания из шлюзов туннеля, который позволяет достичь получателя. Маршрутизаторы пересылают свои данные routerInfo в NetDB напрямую, а данные leaseSet направляются через исходящий туннель для обеспечения анонимности, чтобы избежать корреляции маршрутизатора с его leaseSet [44].

Для создания собственных входящих и исходящих туннелей пользователь производит поиск для сбора данных в NetDB, routerInfo и составляет списки пиров, которые может использовать в качестве транзитных участков в своих туннелях. Затем отправляет сообщение в первый транзитный участок с запросом на

создание туннеля и перенаправление запроса далее. Процедура выполняется до тех пор, пока туннель не будет построен.

Рассмотрим следующий пример: Катерина хочет послать сообщение Михаилу, она сначала выполняет поиск в NetDB, чтобы найти значение leaseSet Михаила и получить информацию о текущих входящих туннелях Михаила. Затем она выбирает один из своих исходящих туннелей и отправляет сообщение по нему с инструкциями для исходящей конечной точки, чтобы переслать сообщение на один из входящих шлюзов туннеля Михаила. Когда в исходящем туннеле конечная точка получает эти инструкции, она передает сообщение с запросом, и когда входящий шлюз туннеля Михаила получает запрос, он направляется вниз по туннелю к маршрутизатору Михаила (рис. 3.7).

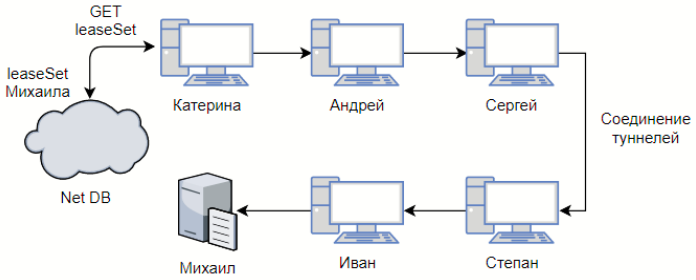


Рис. 3.7. Процесс построения туннеля в сети I2P

Если Катерина хочет, чтобы Михаил ответил на сообщение, она должна передать инструкцию как часть самого сообщения. Это может быть сделано путем создания более высокого слоя, осуществляемого в потоковой библиотеке. Опционально, Катерина может также сократить время отклика, вкладывая свое последнее значение leaseSet в сообщение, так что Михаилу, когда он решит ответить, не придется делать поиск в NetDB для обращения к Катерине [44].

Несмотря на то, что сами туннели при помощи многослойного шифрования защищены от несанкционированного доступа к участникам внутри сети («транспортный слой» зашифрован сам по себе), необходимо добавить дополнительный слой шифрования, чтобы скрыть сообщение отправителя на пути от исходящей до конечной точки туннеля и входящего шлюза. Это обеспечивается так называемым чесночным шифрованием, которое позволяет маршрутизатору Катерины обернуть несколько сообщений в одно «чесночное», зашифрованное открытым ключом, что не даст промежуточному участнику определить количество сообщений и их содержимое. Так, для установки связи между Катериной и Михаилом сообщение будет зашифровано открытым ключом, опубликованным в leaseSet Михаила, что позволит ему прочитать зашифрованное сообщение на маршрутизаторе Михаила.

Чесночная маршрутизация – это технология анонимного зашифрованного обмена информацией через компьютерную сеть, используемая в анонимной сети I2P и являющаяся расширением луковой маршрутизации, на которой основан проект Tor.

Суть этой технологии в том, что при использовании многослойного шифрования единственное сообщение (так называемый чеснок) может содержать в себе множество «зубчиков» – полностью сформированных сообщений вместе с инструкциями по их доставке. В один «чеснок» в момент его формирования перед отправкой закладываются множество «зубчиков», являющихся зашифрованными сообщениями как нашего узла, так и чужими, т. е. транзитными. Является ли тот или иной «зубчик» в «чесноке» нашим сообщением или это чужое транзитное сообщение, которое просто проходит через нас, знает только создатель «чеснока», никто иной узнать эту информацию не может. Чесночная технология применяется тогда, когда нужно отправить,

зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации.

Например, если некоторый маршрутизатор просит другой маршрутизатор поучаствовать в общем туннеле, он помещает этот запрос в «чеснок», шифрует его открытым алгоритмом и передает через туннель. Если же клиент хочет отправить сообщение в точку назначения, маршрутизатор отправителя обернет данные этого сообщения (вместе с другими сообщениями) в «чеснок», зашифрует этот «чеснок» открытым алгоритмом, опубликованным в leaseSet получателя, и передаст его через соответствующие туннели.

Инструкции, присоединенные к каждому «зубчику» внутри зашифрованного слоя, включают возможность запроса, чтобы «зубчик» был отправлен локально к удаленному маршрутизатору или к удаленному туннелю на удаленном маршрутизаторе. В этих инструкциях есть поля, позволяющие промежуточному узлу запрашивать задержку отправки в определенный промежуток времени или условия встречи.

Отдельным интересным примером анонимных сетей являются сети, построенные на основе Wi-Fi. Тогда как при традиционном подходе транспортные функции любой анонимной сети выполняет интернет, использование беспроводных решений позволяет достичь независимости от провайдеров.

## § 2. Анонимные операционные системы

Анонимность может быть обеспечена комплексом специализированных программных продуктов, объеденных в одной операционной системе. Существует множество ОС, нацеленных на обеспечение анонимности в сети (Tails, Whonix, Kodachi, Subgraph, Qubes и т. д.).

*Tails (The Amnesic Incognito Live System)* – это дистрибутив Linux на основе Debian, предназначенный для обеспечения конфиденциальности и анонимности. Все исходящие соединения маршрутизируются через сеть Tor, а все не анонимные соединения блокируются. Система предназначена для загрузки с Live CD или Live USB и не оставляет следов на машине, на которой она использовалась. Проект Tor является главным спонсором Tails. Эта операционная система рекомендована Фондом свободы прессы, а также использовалась Эдвардом Сноуденом для разоблачения PRISM.

Операционная система запускается очень быстро. После создания флешки для выхода в интернет потребуется от одной до двух минут, если у вас хорошее оборудование. Tails позволяет быстро подключаться к сети Tor, использовать мессенджеры и подключаться через защищенный канал, генерировать и сохранять пароли и очищать файлы метаданных.

В основе Tails лежит задача обеспечения анонимности и безопасности пользователя в сети, при этом сохраняя удобство и простоту использования. И делает это неплохо. Вся система работает в режиме Live, загруженном в оперативную память. Tails не устанавливается на SSD или HDD. По окончании сеанса невозможно определить, что пользователь делал на компьютере, даже если кто-то получит полный доступ к устройству.

Эту ОС не рекомендуется использовать в качестве постоянной. После выключения или перезапуска системы все загруженные файлы (например, история браузера) удаляются.

Вы можете создать постоянный зашифрованный раздел и хранить на нем пароли и файлы различных типов, но эти файлы не должны быть конфиденциальными.

Для запуска Tails вам понадобится устройство с объемом оперативной памяти не менее 1 Гб и устаревшим процессором.

Оптимальные характеристики устройства для Tails: 8 Гб ОЗУ и двухъядерный процессор.

К минусам данной операционной системы следует отнести проблему установки сторонних программ. Установка приложений на Tails – сложная задача. Часто возникают непредвиденные ошибки, даже если все сделано правильно. Может случиться так, что после нескольких перезагрузок установленное программное обеспечение может просто исчезнуть. Если вам необходимо систематически работать со сторонним программным обеспечением, то лучше создать собственный дистрибутив, который будет соответствовать вашим потребностям.

Цель Tails не оставлять следов, проблемой может быть что угодно, кроме доступа к сети Tor и хранения файлов. Лучше всего использовать Tails для получения быстрого доступа к сети, подключения к удаленному веб-ресурсу, работы с документами, связи по зашифрованному каналу, отправки и получения криптовалют.

*Whonix* – это дистрибутив Linux на основе Debian, ранее известный как TorBOX. Создан для обеспечения анонимности с помощью VirtualBox и Tor. Все программное обеспечение, поставляемое с этой ОС, предварительно настроено для работы с максимальными настройками безопасности.

ОС Whonix состоит из двух виртуальных машин: *Whonix Gateway* и *Whonix Workstation*, подключенных через изолированную сеть. Шлюз работает исключительно через Tor и действует как шлюз в сеть, рабочая станция работает в полностью изолированной сети.

Все сетевые подключения возможны только через Tor. Единственный доступ к сети для рабочей станции – это шлюз. Весь трафик, все приложения и процессы проходят через Tor.

Приложения не могут получить доступ к интернету в обход Tor. Приложения могут видеть только локальный IP-адрес. Часовой пояс невозможно отследить, часы установлены на UTC, а HTTP-заголовки Timestamp отправляются на случайно выбранные веб-серверы.

Возможность реализации различных последовательностей Tor + VPN является большим преимуществом этой оперативной системы. Вы можете настроить систему так, чтобы сначала весь трафик проходил через VPN, затем через Tor, а затем снова через VPN.

Рассматриваемая система имеет широкие возможности настройки, которые иногда невозможно сделать в Tails. Существует множество программ и настроек, которые позволяют построить собственную систему анонимности и безопасности, удалить следы использования файлов, использовать мессенджеры, работать с разными типами файлов и т. д.

Whonix, безусловно, хорошая система для анонимного доступа в интернет, но использовать ее на постоянной основе будет довольно проблематично, поскольку Whonix построен на виртуализации. Например, вы можете столкнуться с трудностями при работе с внешними носителями. Если вам нужно подключить USB-устройство, она сначала пройдет через основную ОС, например, Windows, затем через VirtualBox и, наконец, достигнет системы Whonix, и это не самый безопасный способ.

*Kodachi* тоже основана на Debian. Цель Kodachi предоставление максимально анонимного и безопасного доступа к сети и защитить саму систему. Весь трафик проходит через VPN, затем через сеть Tor с шифрованием DNS. Бесплатная VPN уже предварительно настроена.

Это хорошо сбалансированная система, мощный инструмент для построения систем анонимности и безопасности во всех

смыслах. Лучше всего эту ОС использовать вместе с зашифрованными носителями, на которых может храниться конфиденциальная информация.

Kodachi позиционируется как антикриминалистическая ОС, которая действительно затрудняет криминалистический анализ дисков и оперативной памяти. XFCE используется в качестве среды рабочего стола для Kodachi, дизайн системы очень похож на MacOS. Параметры системы и сети отображаются в режиме реального времени на рабочем столе, что позволяет контролировать систему, а также отслеживать работу сетей Tor и VPN.

Kodachi поддерживает DNScrypt, протокол и служебную программу, которая шифрует запросы к серверам OpenDNS с использованием эллиптической криптографии. Он устраняет ряд типичных проблем, таких как утечки DNS и оставление следов сетевой активности на серверах провайдера.

Если вам нужно скрыть IP-адрес в P2P-сетях, вы можете использовать PeerGuardian. Если вам нужно работать с подозрительными процессами, их можно легко изолировать с помощью встроенной песочницы Firejail. Прекрасным вариантом является возможность быстро изменить узлы выхода Tor с возможностью выбора конкретной страны с помощью Multi Tor.

В Kodachi есть большое количество предустановленного программного обеспечения для решения любых задач, например, для шифрования информации (VeraCrypt, TrueCrypt), для отправки конфиденциальных сообщений (GnuPG, Seahorse, Enigmail, GNU Privacy Guard Assistant) для сокрытия следов (MAT, Nautilus Wipe, Nepomuk Cleaner, BleachBit). Кроме того, у Kodachi есть собственный браузер на основе Tor Browser, из которого его разработчики вырезали некоторые проблемные модули Tor.

*Qubes OS* использует интересный принцип для запуска приложений. Каждое приложение работает на отдельной виртуальной машине. Приложения делятся на классы в зависимости от уровня важности. Так, браузер работает на одной виртуальной машине, мессенджер на другой. Для пользователя обе программы кажутся запущенными в одном рабочем пространстве. Изоляция приложений означает, что в случае проникновения вредоносного ПО личные файлы не будут скомпрометированы. Qubes OS работает только после установки на внутренний диск, live-режима у нее нет.

*Subgraph OS* – это запуск пользовательских приложений в изолированных песочницах. Для этого используется подсистема Oz. Oz состоит из демона (системной службы), который получает запросы на создание песочниц, Xpra X-сервера и набора специальных утилит. Сегодня Subgraph OS находится на стадии разработки и доступна только альфа-версия, но программа уже позиционируется как коммуникационная платформа для защиты от сетевых эксплойтов и вредоносных атак.

Subgraph и Qubes неплохи, но недостаточно хороши, чтобы поставить их в лидеры: Subgraph OS недоработанна, а Qubes слишком сложна в настройках [71].

## § 3. Анонимные сервисы мгновенного обмена сообщениями

В ноябре 2012 г. Дэвид Петрэус ушел в отставку с поста директора ЦРУ, проработав немногим больше года. До этого он служил в армии США, в том числе в качестве командующего американскими войсками в Ираке и Афганистане. По официаль-

ной версии Дэвид Петрэус передавал по электронной почте секретные документы своей любовнице строго засекреченные материалы его командования в Афганистане. Агенты ФБР при содействии компании Google сумели вычислить IP-адреса обоих преступников и связать их с другими неанонимными почтовыми аккаунтами. Петрэус был вынужден подать в отставку.

В 2013 г. Эдвард Сноуден раскрыл тысячи секретных документов Американского агентства национальной безопасности (АНБ). Летом того же года американская газета The Guardian опубликовала серию документов, в которых говорилось о том, что АНБ получает доступ к пользовательским данным из Google, Apple и Facebook. Действия Сноудена вызвали глобальные дискуссии о национальной безопасности и конфиденциальностью в интернете.

В марте 2015 г. появились новости о том, что Хиллари Клинтон использовала личные адреса электронной почты, подключенные к частному серверу в течение четырех лет своего пребывания на посту государственного секретаря. В результате чего, по некоторым оценкам, в руки разведки попало как минимум 1 200 писем с государственными секретами.

Обмен сообщениями в электронном виде стал настолько обыденным и удобным, а в отдельных случаях даже необходимым. Универсальность современных систем обмена сообщениями гарантирует, что электронная почта будет с нами в течение многих лет. Поэтому необходимо уделить особое внимание обеспечению приватности обмена электронной корреспонденцией.

Анонимность при переписке достигается, например, использованием *ремейлера*. Это компьютер, получающий сообщение и переправляющий его по адресу, указанному отправителем. В процессе переадресовки все заголовки (headers), содержащие информацию об отправителе, уничтожаются, поэтому конечный

получатель лишен всякой возможности выяснить, кто автор сообщения. Ремейлеров в сети много, некоторые из них позволяют указывать фиктивный адрес отправителя, большинство же прямо указывают в заголовке, что сообщение анонимно.

Все ремейлеры можно разделить на анонимные и псевдоанонимные. Когда вы используете псевдоанонимный ремейлер, оператор знает адрес вашей электронной почты. Это необходимо, если вы хотите получить ответ на свое письмо. Ваша секретность полностью зависит от честности оператора. На практике это означает, что кто-то может добраться до вас, например суд, если вынудит оператора раскрыть информацию. Преимущество псевдоанонимных ремейлеров состоит в том, что они являются «дружественными» вам. Цена, которую вы платите за «простоту и дружбу», – меньший уровень безопасности. Действительно, анонимные ремейлеры обеспечивают большую секретность. Однако они намного сложнее в использовании.

Если вам нужна максимальная секретность, ответ на все это один: шифровать или использовать компьютерную стеганографию (тайнопись). Шифрование сообщений – это единственный способ, при котором можно гарантировать, что переданная информация будет сохранена в тайне.

Сегодня пользователи интернета все чаще выбирают для общения мессенджеры с высоким уровнем безопасности, осознавая возможности специальных служб. Лидером в области сохранения прав и свобод человека в информационном пространстве, безусловно, является фонд электронных рубежей (Electronic Frontier Foundation (EFF), далее – фонд).

В результате исследований фонда оказалось, что среди приложений, которые обладают высоким уровнем конфидециальности, можно выделить следующие: Silent Text, Silent Phone, TextSecure, ChatSecure+Orbot, CryptoCat, Signal/RedPhone. Среди

решений для настольного компьютера с открытым исходным кодом можно отметить Bitmessage.

*Bitmessage* – это децентрализованный, зашифрованный, одноранговый мессенджер без доверия, написанный на Python с графическим интерфейсом Qt (рис. 3.8). Мессенджер использует библиотеку криптографии на основе эллиптических кривых PyElliptic для шифрования всех сообщений. Метаданные как тема сообщения также зашифрованы. Кроме того, мессенджер использует одноранговую сеть без доверия (P2P), и сообщения перенаправляются всеми остальными пользователями. Каждый клиент в сети пытается расшифровать и прочитать все сообщения, которые проходят через его соединение, но только легитимный клиент с соответствующим закрытым ключом может прочитать сообщение.

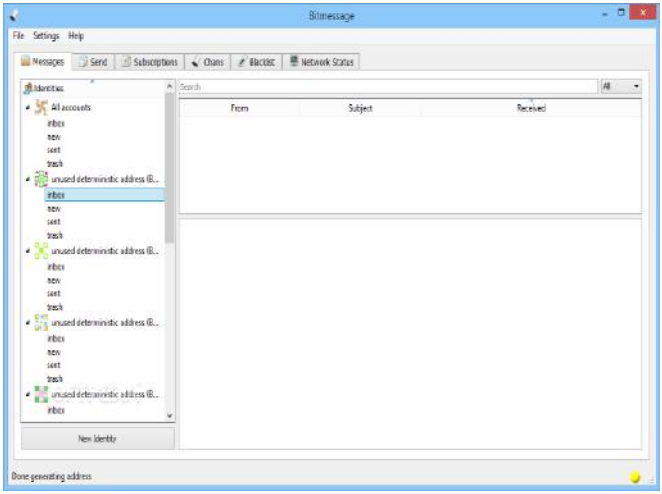


Рис. 3.8. Оконный интерфейс Bitmessage

Адрес получателя на самом деле является RIPEMD-160 открытого ключа, используемого для шифрования. Например, BM-

2cSwb3miRwL6ZPeKoChP5z1Sqwe5GW2aHL является действительным адресом. Обратите внимание, что префикс «BM» используется для распознавания протокола Bitmessage.

Bitmessage использует socks и может быть настроен на использование с Tor для маршрутизации трафика. Однако Bitmessage не использует шифрование между узлами и поэтому открыт для возможной атаки Sybil со стороны выходных узлов Tor. В основном репозитории мессенджера не реализована поддержка протокола I2P, но реализация, работающего только через I2P, существует на Github.

*Jabber* – старое название XMPP-протокола для мгновенного обмена сообщениями, которое до сих пор популярно у пользователей. Устройство XMPP-сети очень простое. Она распространяется по всему миру, например jabber.ru. Вы выбираете себе сервер, регистрируетесь на нем аналогично тому, как регистрируетесь на любом сайте (если, конечно, владелец сервера предоставил возможность регистрации). В момент регистрации на сервере вам создается аккаунт, дается логин и пароль. Большинство XMPP-серверов для регистрации требуют только логин и пароль, при этом не используя никакой привязки к мобильному устройству, почте или иным персональным данным. Новый аккаунт можно зарегистрировать за считанные секунды, а на одном устройстве одновременно использовать хоть сто аккаунтов [72].

Для общения по XMPP-протоколу используются специальные программы-клиенты. Их немало, и они есть на всех популярных мобильных и десктопных платформах. Самые известные из них это Pidgin, Adium, Xabber и Psi+.

Отличие Jabber-сети от других мессенджеров в децентрализации, т. е. отсутствии единого центра. Вы сами можете настроить и обслуживать свой сервер, хранить или не хранить логи,

определить политику сбора данных и сотрудничества с правоохранительными органами. По этой же причине Jabber сложно подвергнуть государственной цензуре.

Между тем XMPP является лучшим решением в тех случаях, когда необходим максимальный уровень защиты коммуникации при мгновенном обмене сообщениями. Просто в протоколе XMPP по умолчанию нет надежного шифрования, но его можно добавить. Для того, чтобы общение через XMPP стало максимально анонимным и безопасным, необходимо подключаться к Jabber-серверу только через Tor, всегда использовать OTR/PGP-шифрование и случайный логин. Это три фундаментальных правила безопасного общения через XMPP.

Как уже было отмечено ранее, самое надежное решение при обеспечении конфиденциальности своей переписки – это шифрование. Наиболее распространенные среди пользователей – OTR и GPG решения. Все перечисленные способы шифрования используются в анонимных системах мгновенного обмена сообщениями.

Считается, что PGP надежнее, но зато у OTR есть одно важное преимущество: даже если ваш приватный ключ OTR попадет в чужие руки, то предыдущая переписка не будет скомпрометирована, поскольку публичный и приватный ключи используются только для первичной аутентификации пользователей, а все дальнейшие сообщения шифруются уже с помощью одноразовых AES-ключей.

*Off-the-Record (OTR)* означает «не для записи». Это способ отправки зашифрованных мгновенных сообщений в сети. OTR построено на сквозном шифровании, благодаря которому интернет-провайдер, правительство не могут видеть содержимое ваших сообщений. Протокол использует комбинацию AES (Advanced Encryption Standard) симметричного шифрования, с обменом ключами по алгоритму Диффи – Хеллмана, и хеширование SHA-2.

Новый ключ генерируется для каждого нового сеанса чата. Протокол поддерживает взаимную аутентификацию пользователей с использованием общего секрета через протокол «социалистического миллионера». Кроме того, эти сообщения не содержат цифровых подписей, которые могли бы связать их с источником. Таким образом реализуются функции сквозного шифрования, совершенной секретности, взаимной аутентификации и отклоняемая аутентификации (анонимности).

*Pretty Good Privacy (PGP)* – это система шифрования, используемая как для отправки зашифрованных писем, так и для шифрования файлов. С момента своего изобретения в 1991 г. PGP стал фактическим стандартом защиты электронной почты. PGP использует комбинацию шифрования с симметричным ключом и шифрование с открытым ключом. Открытым ключом шифруются данные и проводится аутентификация (проверка цифровой подписи). Закрытый ключ используется для расшифрования и создания цифровой подписи. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal. Аутентификация основана на хешировании, могут использоваться алгоритмы MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384, SHA-512. Обобщенная схема работы шифрования PGP изображена на рис. 3.9.

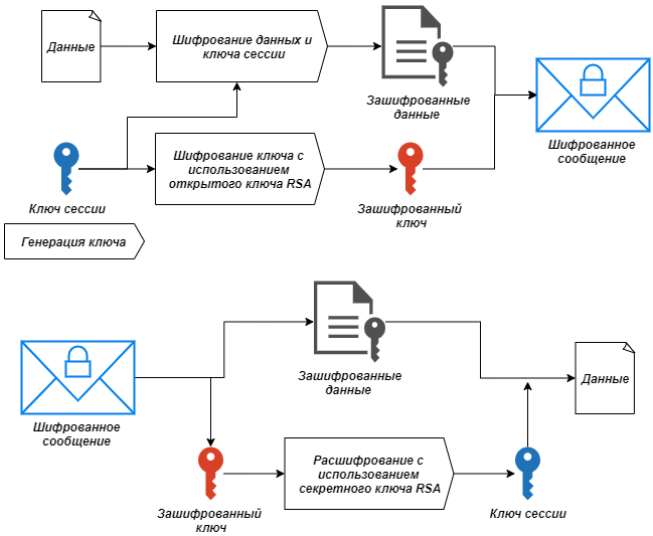


Рис. 3.9. Схема шифрования и расшифрования PGP

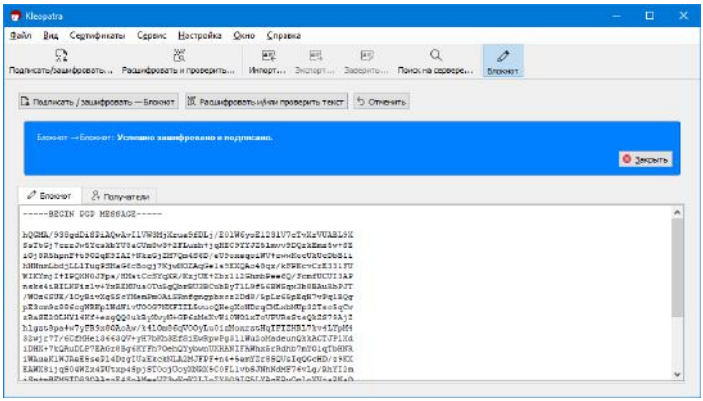


Рис. 3.10. Оконный интерфейс Gpg4win

*GnuPG* – это полная и бесплатная реализация стандарта OpenPGP, как определено в RFC 4880 (также известном как PGP). GnuPG позволяет вам шифровать и подписывать ваши данные и сообщения. Программное обеспечение оснащено универсальной системой управления ключами, а также модулями доступа

для всех видов каталогов открытых ключей. GnuPG, также известный как GPG, инструмент командной строки с функциями для легкой интеграции с другими приложениями. Доступно множество интерфейсных приложений и библиотек. GnuPG поддерживает Secure/Multipurpose Internet Mail Extensions (S/MIME) и Secure Shell (SSH).

В качестве примера можно привести GNU Privacy Guard для Windows (Gpg4win) – бесплатное программное обеспечение, которое позволяет пользователям безопасно защищать электронные письма, папки и файлы с помощью шифрования и цифровых подписей (рис. 3.10). Gpg4win содержит несколько компонентов свободного программного обеспечения: инструмент шифрования GnuPG, менеджер сертификатов (OpenPGP), плагины для Microsoft Outlook и Microsoft Explorer (GpgOL, GpgEX) и альтернативный менеджер сертификатов (GPA).

Безопасность вашей личной информации и безопасность вашего компьютера являются индивидуальной задачей. Как показывает практика, наиболее надежный метод – это шифрование. Основная часть современных систем анонимности основана на криптографических алгоритмах.

## § 4. Технологии компьютерной стеганографии

Стеганографию используют те, кто желает передать секретное сообщение. Технологии стеганографии используюися достаточно давно и включают практически любой метод сокрытия секретного сообщения в контейнере. Например, использование невидимых чернил для сокрытия секретных сообщений в безобидных сообщениях; сокрытие документов, записанных на микроточки, которые могут быть размером от одного мм в диаметре, или внутри кажущейся законной корреспонденции; и даже за

счет использования многопользовательских игровых сред для обмена информацией (рис. 3.11).

Такие технологии реализованы и в цифровом мире, где такой файл, как изображение, может быть незаметно закодирован с помощью информации. Например, значения пикселей, яркость и настройки фильтра для изображения обычно изменяются, чтобы повлиять на эстетический вид изображения.

Рис. 3.11. Примеры использования стеганографии

В современной компьютерной стеганографии для повышения безопасности данные сначала шифруются, а затем вставляются с использованием специального алгоритма в контейнер, который может представлять из себя файл определенного формата, такого как изображение, аудио- и видеофайл и т. д. Секретное сообщение может быть встроено в обычные файлы данных множеством различных способов. Наиболее распространенные методы компьютерной стеганографии приведены в табл. 3.1 [4].

*Таблица 3.1*

**Методы компьютерной стеганографии**

| Методы компьютерной стеганографии | Краткая характеристика методов | Недостатки | Преимущества |
|---|---|---|---|
| 1. Методы использования специальных свойств компьютерных форматов данных | | | |
| 1.1. Методы использования зарезервированных для расширения полей компьютерных форматов данных | Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой | Низкая степень скрытности, передача небольших объемов информации | Простота использования |
| 1.2. Методы специального форматирования текстовых файлов | | | |
| 1.2.1. Методы использования известного смещения слов, предложений, абзацев | Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами | 1. Слабая производительность метода, передача небольших объемов информации.<br>2. Низкая степень скрытности | Простота использования. Имеется опубликованное программное обеспечение реализации данного метода |
| 1.2.2. Методы выбора определенных позиций букв (нулевой шифр) | Акростих – частный случай данного метода (например, начальные буквы каждой строки образуют сообщение) | | |
| 1.2.3. Методы использования специальных свойств полей форматов, не отображаемых на экране | Методы основаны на использовании специальных скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне) | | |

*Окончание табл. 3.1*

| | | | |
|---|---|---|---|
| 1.3. Методы скрытия в неиспользуемых местах гибких дисков | Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке) | 1. Слабая производительность метода, передача небольших объемов информации. 2. Низкая степень скрытности | Простота использования. Имеется опубликованное программное обеспечение реализации данного метода |
| 1.4. Методы использования имитирующих функций (mimic-function) | Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение | 1. Слабая производительность метода, передача небольших объемов информации. 2. Низкая степень скрытности | Результирующий текст не является подозрительным для систем мониторинга сети |
| 1.5. Методы удаления идентифицирующего файл заголовка | Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок, оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок | Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю | Простота реализации. Многие средства (White Noise Storm, S-Tools), обеспечивают реализацию этого метода с PGP шифроалгоритмом |
| 2. Методы использования избыточности аудио- и визуальной информации | | | |
| 2.1. Методы использования избыточности цифровых фотографий, цифрового звука и цифрового видео | Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации | За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик | Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т. п. |

Добавление водяного знака, товарного знака или других идентифицирующих данных, скрытых в мультимедийных или других файлах содержимого, является одним из распространенных способов использования стеганографии. Цифровые водяные знаки (ЦВЗ) – это метод, который часто используется онлайн-издателями для определения источника мультимедийных файлов, которые, как выяснилось, распространяются без разрешения.

Стеганография отличается от криптографии, но их совместное использование повышает безопасность передаваемой информации и предотвращает обнаружение секретной связи. Использование стеганографии в сочетании с шифрованием дает преимущества по сравнению с обменом данными только с шифрованием.

Основное преимущество использования стеганографии для сокрытия данных по сравнению с шифрованием заключается в том, что она помогает скрыть тот факт, что в файле скрыты конфиденциальные данные или другое содержимое, несущее скрытый текст. В то время как зашифрованный файл, сообщение или полезная нагрузка сетевого пакета четко маркируются и идентифицируются как таковые, использование стеганографических методов помогает скрыть присутствие защищенного канала.

Раздел стеганографии о выявлении факта передачи скрытой информации в анализируемом сообщении называют стеганоанализ. В некоторых случаях под стеганоанализом понимают также извлечение скрытой информации из содержащего ее сообщения и (если это необходимо) дальнейшую ее дешифровку.

Соответственно, попытку определить наличие сообщения и его смысл называют атакой на стеганографическую систему. Задача стеганоаналитика состоит в раскрытии стеганографической системы и определении тайно переданного сообщения. В отли-

чие от криптографии, под раскрытием (взломом) стеганографической системы принято понимать нахождение такой ее конструктивной либо иной уязвимости, которая позволяет определить факт сокрытия информации в контейнере, и возможность доказать данное утверждение третьей стороне с высокой степенью достоверности. Учитывая это, аналогично криптографическим атакам, атаки на стеганографические системы можно разделить на следующие классы:

– *атаки со знанием только модифицированного контейнера* – аналог криптографической атаки со знанием шифртекста. Стеганоаналитик в этом случае обладает только модифицированным контейнером, по которому он пытается определить наличие сокрытого сообщения. Данный вид стеганографических атак является базовым, по которому оцениваются стеганосистемы;

– *атаки со знанием немодифицированного контейнера* возможны в случае, когда стеганоаналитик также обладает способностью узнавать, какой именно немодифицированный контейнер был использован для сокрытия сообщения. Данная атака определяет возможность определения факта сокрытия сообщений в дальнейшем в зависимости от наличия однажды перехваченного контейнера и раскрытого сообщения;

– *атаки с выбором сообщения* подразумевают, что стеганоаналитик имеет возможность указывать, какие именно сообщения будут сокрыты, но при этом не имеет возможности указать контейнер, который будет для этого использоваться. Стойкость к данной атаке характеризует надежность системы к перехвату и отслеживанию сообщений, посланных с использованием одного и того же контейнера. Данный вид атак иногда также позволяет определить тип примененной стеганографической системы;

– *атаки с выбором контейнера*, аналогично предыдущим, позволяют определить стойкость стеганосистемы к раскрытию в случае повторного использования одного и того же сообщения с различными контейнерами;

– *атаки по подмене и имитации* не призваны определить факт наличия сообщения или извлечь его, их применяют для модификации скрытой информации либо имитации такой передачи;

– *атаки по противодействию передаче информации* используют для уничтожения сокрытой информации и снижения пропускной способности каналов скрытой передачи данных.

Программное обеспечение для стеганографии используется для выполнения множества функций для сокрытия данных, включая шифрование данных для подготовки их к скрытию внутри другого файла, отслеживание того, какие биты текстового файла обложки содержат скрытые данные, и извлечения скрытых данных предполагаемым получателем.

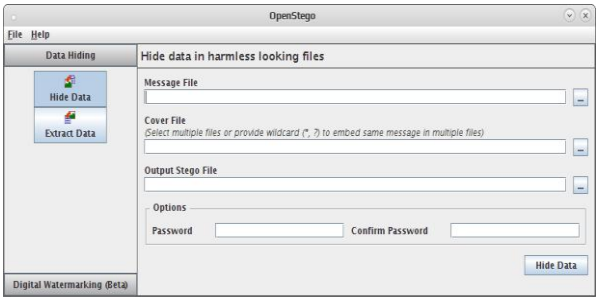


Рис. 3.12. Оконный интерфейс программы OpenStego

Существуют программы с открытым исходным кодом и другие бесплатные программы для стеганографии. OpenStego – это стеганографическая программа с открытым исходным кодом для сокрытия информации в изображениях методом стеганографии и/или добавления на изображения «водяных знаков» (рис. 3.12).

Есть онлайн-сервисы для сокрытия секретных файлов в изображениях BMP или аудио WAV, например, http://stylesuxx.github.io/-steganography (рис. 3.13).

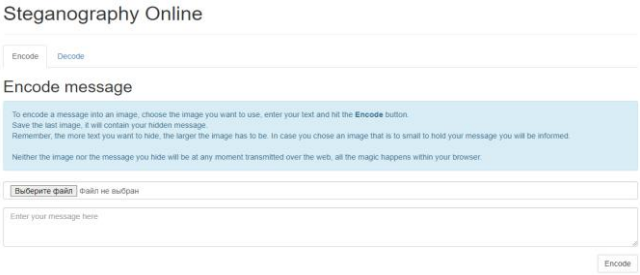


Рис. 3.13. Steganography Online

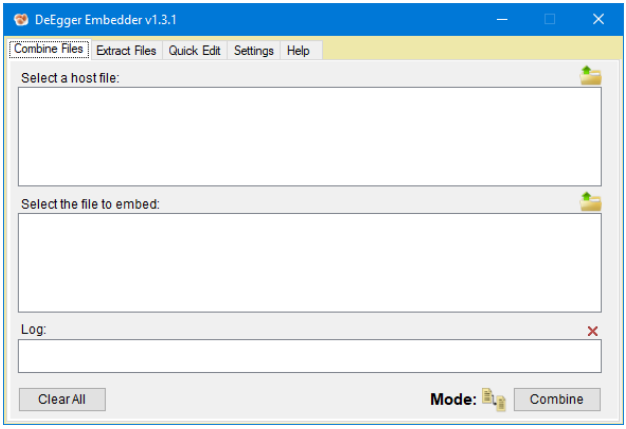


Рис. 3.14. Оконный интерфейс программы DeEgger Embedder

Еще одна бесплатная программа для стеганографии – это DeEgger Embedder (рис. 3.14). Программа поддерживает в качестве контейнеров PNG, JPG, видеофайлы AVI и музыкальные MP3. О ходе операций ведется подробный лог, который отображается прямо в главном окне. Кроме того, скрытые файлы могут быть дополнительно защищены шифрованием.

# ГЛАВА IV. ТРАССИРОВКА И ИДЕНТИФИКАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

## § 1. Общий подход к идентификации в интернете

Идентификация, отслеживание пользователя в интернете или веб-трекинг (трассировка), подразумевает расчет и установку уникального идентификатора для каждого пользователя, посещающего определенный сайт. Изначально это не задумывалось, как способ контроля пользователей, а было призвано приносить пользу. Например, отличить обычных пользователей от ботов или же предоставить возможность хранить предпочтения пользователей и применять их при последующем визите. Но в то же самое время данная возможность приглянулась рекламной индустрии: с середины 90-х гг. XX в. здесь стали активно использовать небольшие фрагменты данных, отправленные веб-сервером и хранимые на компьютере пользователя, также известные как cookie.

Уникальные идентификаторы пользователя в интернете можно условно разделить на технические (IP-адрес, MAC-адрес) и семантические (адрес электронной почты, никнейм).

Каждый компьютер, подключенный к интернету, имеет свой уникальный адрес даже при временном подключении, который однозначно задает местонахождение компьютера в сети. Эта специальная система адресов носит название IP-адрес.

IP-адрес всегда имеет длину 32 бита и состоит из четырех частей, которые называются октетами (octet). Четыре части объединяются в запись, в которой каждый октет отделяется точкой, например 198.68.191.10.

Структура каждого 32-битного IP-адреса делится на две части – префикс и суффикс, которые образовывают двухуровневую иерархию. Префикс означает физическую сеть, к которой подключен компьютер, а суффикс – отдельный компьютер в этой сети. Первая часть адреса принадлежит к префиксу, а вторая – к суффиксу, определяются значениями первых четырех бит, и соответственно этому IP-адреса делятся на три основные класса A, B и C. Для обеспечения максимальной гибкости IP-адреса выделяют организациям в зависимости от количества сетей и компьютеров в ней соответственно этим классам.

Для удобства в сети Интернет используется доменный способ адресации Domain Name System (далее – DNS). Все пространство адресов абонентов делится на области, которые называются доменами. Такой адрес читается налево, на крайний правой позиции есть домен первого уровня, который предоставляет наиболее общую информацию. Он может быть двух видов: указывать на тип организации (собственника компьютера) или на локализацию, т. е. страну, в которой компьютер находится.

Домен, который указывает на страну, состоит из двух литер, которые, как правило, повторяют международный код государства: ua – Украина, ru – Россия, us – США, uk – Великобритания, fr – Франция.

Для удобства сетевого администрирования запросов в доменной системе имен (DNS) с целью получения доменного имени, IP-адреса или другой информации из записей DNS используют консольную команду nslookup.

Программа командной строки nslookup имеет два режима: интерактивный и неинтерактивный.

Если необходимо выполнить поиск только одного фрагмента данных, рекомендуется использовать неинтерактивный режим.

В качестве первого параметра введите имя или IP-адрес компьютера, который требуется найти. Во втором параметре введите имя или IP-адрес сервера DNS-имен. Если опустить второй аргумент, nslookup использует сервер DNS-имен по умолчанию.

Если необходимо найти более одного фрагмента данных, можно использовать интерактивный режим. Введите дефис (-) для первого параметра, а также имя или IP-адрес сервера DNS-имен для второго параметра. Если оба параметра не указаны, средство использует сервер DNS-имен по умолчанию. При использовании интерактивного режима можно:

– прерывать интерактивные команды в любое время, нажав клавиши CTRL + B (для выхода введите Exit);

– рассматривать встроенную команду как имя компьютера, поставив перед escape символ ( ); нераспознанная команда интерпретируется как имя компьютера;

– использовать синтаксис команды nslookup: nslookup [опции] [имя/адрес] [сервер имен].

Для построения маршрута отправляемых пакетов данных, а также отображения некоторых подробностей о пути используют стандартные утилиты операционных систем. Иногда эту процедуру называют командой трассировки маршрута.

Такая команда для ОС Linix Traceroute, а для Windows Tracert эти команды отображают путь, по которым проходит пакет информации от источника до места назначения, что позволяет определить место потери данных в сети и может означать отказ узла.

Поскольку каждый переход в записи отражает новый сервер или маршрутизатор между исходным ПК и намеченной целью, просмотр результатов сканирования команд определяет «медленные» узлы, которые могут отрицательно повлиять на ваш сетевой трафик.

Синтаксис команд выглядит следующим образом:

– tracert [ -d ] [ -h MaxHops ] [ -w TimeOut ] [ -4 ] [ -6 ] цель [ /? ];

– traceroute [-dFInrvx] [-f first_ttl] [-g шлюз] [-i iface] [-m max_ttl] [-p порт] [-q nqueries] [-s src_addr] [-t tos] [-w waittime] [-z pausemsecs] хост [пакет].

Команда tracert доступна из командной строки во всех операционных системах Windows, включая Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP и более старые версии.

Существуют графические утилиты или удаленные сервисы, выполняющие функции трассировки маршрута, как и консольные утилиты Traceroute и Tracert. Например, Open Visual Traceroute предназначен для визуального отображения маршрута следования пакетов в сетях TCP/IP. Точки отображаются на глобусе. Он написан на Java.

Internet Assigned Numbers Authority (далее – IANA) организация по стандартизации и контролю за распределением глобальных IP-адресов. IANA делегирует распределение блоков IP-адресов региональным интернет-регистратурам (далее – RIR). Каждый RIR выделяет адреса для разных регионов мира. Региональные интернет-реестры являются компонентами системы реестра интернет-номеров, которая описана в IETF RFC 7020. Сегодня выделяют пять региональных интернет-реестров:

1. African Network Information Center (AfriNIC) – выполняет распределение интернет-ресурсов в Африке.

2. Американский реестр для Internet Numbers (ARIN) – выступает интернет-провайдером в Антарктиде, Канаде, части Карибского бассейна, а также в США.

3. Asia-Pacific Network Information Center (APNIC) – распределяет веб-ресурсы в Восточной Азии, Океании, Южной Азии и Юго-Восточной Азии.

4. Сетевой Информационный Центр (LACNIC) – выступает провайдером в странах Латинской Америки и некоторых странах Карибского бассейна.

5. Réseaux IP Européens (англ. Network Coordination Centre RIPE, NCC) – региональный интернет-регистратор, выполняет распределение веб-ресурсов в Европе, Центральной Азии, России и Западной Азии.

Просмотреть информацию о любом доменном имени просто: нужно обратиться к сервисам Whois.

*Whois* – это сервис, позволяющий ознакомиться с информацией о владельце домена или IP-адреса, содержит информацию о наименовании предприятия, местонахождении, e-mail, номере телефона. В некоторых случаях контактная информация Whois может быть скрыта в связи с политикой приватности распорядителя сервиса. Серверы Whois, управляемые RIR, могут запрашиваться напрямую, чтобы определить интернет-провайдер, ответственный за конкретный ресурс.

В настоящее время популярные веб-запросы Whois могут выполняться из ARIN, RIPE и APNIC.

## § 2. Идентификация браузеров (Browser Fingerprint)

Браузеры собирают информацию для лучшего взаимодействия с пользователем, разрешая Cookie, JS и другие расширения. Рекламодатели используют такую информацию для отслеживания пользователей с удаленных устройств в интернете с целью получения индивидуальной уникальной идентификации – отпечатка браузера.

Принцип распознавания отпечатков браузера основан на различных технологиях просмотра, используемым типом оборудования, операционной системой, типом и конфигурацией браузера для создания уникального отпечатка (Browser Fingerprint).

Как только пользователь начинает просматривать веб-страницы, данные его браузера используются для создания этого отпечатка. Наиболее значительными факторами, влияющими на уникальность отпечатка, являются шрифты, плагины и пользовательские агенты. Среди уникальных элементов пользователя, участвующих в просмотре веб-страниц и отображаемых в отпечатке браузера, можно отметить:

– параметры конфигурации (разрешение экрана, часовой пояс, язык и т. д.);

– параметры программного обеспечения (ОС, тип и версия браузера, шрифты, установленные плагины и т. д.);

– параметры аппаратного обеспечения (тип процессора, настройки сети, наличие микрофона веб-камеры и т. д.);

– динамические атрибуты (элемент HTML5, JS и т. д.).

Для доступа к контенту веб-сервера используют веб-браузеры, например Mozilla Firefox, Safari или Google Chrome. Эти приложения используют протокол HTTP для запроса данных из веб-сайтов для отображения в удобном для пользователя виде. Контент передается через IP-пакеты, которые, помимо пользовательских данных, также содержат информацию о клиенте и могут использоваться на стороне сервера для определения отпечатка браузера.

Специалисты выделяют два основных способа снятия отпечатков браузера: пассивный и активный.

*Пассивное снятие* отпечатков браузера основано на сборе информации браузера, полученной без использования специальных

приложений (технологий). По сути, это информация, которая содержится в данных заголовка IP-пакетов по умолчанию и поэтому в любом случае достигает веб-сервера. Она включает IP-адрес, используемый порт и тип браузера. Но также включены базовые конфигурации, такие как желаемые типы файлов (HTML, XHTML, XML), наборы символов (например, UTF-8) или языки (обычно язык браузера или операционной системы). Заголовок HTTP также предоставляет в некоторых случаях информацию об используемой операционной системе и исходной странице.

Заголовок протокола HTTP используется для передачи веб-контента, не имеет фиксированного размера, в отличие от данных заголовка TCP и IP. Помимо этого, есть возможность содержать определяемые пользователем записи, для этого требуются различные стандартизированные поля, некоторые из которых имеют фундаментальное значение для создания отпечатка браузера. В частности, это касается следующих данных заголовка:

– HTTP referer (исходная страница): если пользователь достигает страницы B по ссылке со страницы A, URL-адреса страницы A передается на сервер страницы B в качестве реферера. В определенных обстоятельствах определенные пользователи всегда переходят с определенной начальной страницы на целевую страницу, что также полезно для создания отпечатка пальца, как и параметры GET, содержащиеся в URL-адресе;

– User-Agent (описание клиента): с каждым HTTP-запросом соответствующий клиент обычно предоставляет свое описание в поле User-Agent. Помимо обозначения и номера версии, заголовок HTTP также предлагает место для комментария, в котором многие браузеры перечисляют базовую платформу или операционную систему;

– принять (разрешенные форматы вывода): браузер использует поле «принять», чтобы сообщить серверу, какие типы

содержимого он может обрабатывать и, следовательно, желает использовать их в качестве возможных форматов вывода. Помимо HTML, особенно востребованы XHTML (Extensible Hypertext Markup Language) и XML (Extensible Markup Language). Если поле отсутствует, клиент поддерживает все типы контента;

– Accept-Charset (разрешенные наборы символов): в дополнение к выходному формату клиент может также определить желаемый набор символов, который сервер должен использовать в своем ответе. В основном это UTF-8 и стандарт ISO/IEC 8859-1;

– Accept-Encoding (принятые форматы сжатия): для оптимизации времени загрузки веб-проекта обычно сжимают веб-контент перед его отправкой. Поэтому браузер должен распаковать сжатые данные, прежде чем он сможет их отобразить. В поле Accept-Encoding он сообщает серверу, с которым осуществляется связь, какие форматы сжатия он поддерживает. Список возможных процедур, поддерживаемый IANA, включает gzip, deflate, exi и br;

– Accept-Language (принятые языки): клиенты используют запись HTTP Accept-Language, чтобы указать, какую языковую версию они предпочитают. Если это доступно для посещаемого веб-сайта, веб-сервер доставляет его. Принудительный язык является результатом того языка, который используется браузером или операционной системой. Некоторые браузеры также предлагают возможность указания дополнительных языковых требований в настройках.

*Активное снятие* – метод, при использовании которого специально запрашивается информация, не предоставляемая автоматически при вызове веб-ресурса. Этот запрос выполняется, например, с приложениями или подключаемыми модулями JS, которые расширяют функциональные возможности браузера, в

основном Adobe Flash и Microsoft Silverlight. Таким образом, помимо прочего, можно получить расширенную информацию о браузере, а также подробные данные об операционной системе и экране пользователя (ширина, высота, разрешение). Дополнительная информация, может быть, например, об установленных шрифтах или часовом поясе, в котором находится пользователь.

Для активного снятия отпечатков браузера оператор вебсайта должен активно запрашивать информацию о клиенте. Таким образом, запрошенные свойства и данные являются характеристиками, которые неочевидны из данных заголовка клиентских пакетов. Поскольку для этой цели приложения должны выполняться на стороне браузера, пользователь теоретически может подтвердить снятие отпечатков пальцев в любое время, проанализировав исходящие пакеты данных или исходный код HTML или JS. Однако в большинстве случаев процесс будет оставаться скрытым от посетителей, как и в случае с сопоставимыми процессами отслеживания.

Свойства, которые можно запрашивать через браузер пользователя, в основном те же, что и при пассивном снятии отпечатков.

Отслеживание возможно с помощью объекта Navigator, который является возможным свойством для оконных объектов, т. е. окон, которые открываются в браузере. Даже если для объекта Navigator не определен общий стандарт, он по-прежнему поддерживается всеми распространенными браузерами. Кроме того, он пересылает на веб-сервер следующую информацию:

– navigator.appName – пересылает имя браузера, например, «Opera» или «Netscape»;

– navigator.appVersion – сообщает серверу о версии браузера и, в некоторых случаях, также об операционной системе и даже о типе процессора. Возможная запись, например, «5.0 (Windows)»;

– navigator.cookieEnabled – свойство cookieEnabled можно использовать для проверки, поддерживает ли браузер файлы cookie – «true» или деактивировал ли их пользователь – «false»;

– navigator.language – необходим для определения языка браузера. Он поддерживается всеми распространенными браузерами (Internet Explorer с версии 11.0, Firefox с версии 1.0) и примерно соответствует записи HTTP Accept Language. Примеры допустимых языковых кодов: «en», «en-US» или «de»;

– navigator.platform – указывает платформу, используемую пользователем. Возможные значения: Win32, MacIntel, Linux i686, iPhone, Android и SunOS;

– navigator.userAgent (подробный идентификатор браузера также можно просмотреть с помощью активного отпечатка браузера) – не отличается от информации заголовка HTTP с тем же именем и предоставляет такие значения, как имя, версия и платформа браузера в сводке. В следующем примере показана возможная строка: «Mozilla / 5.0 (Windows NT 6.1; WOW64; rv: 53.0) Gecko / 20100101 Firefox / 53.0».

Информацию об экране посетителя веб-сайта также можно получить через окно браузера JS. В этом случае объект экрана используется как подобъект, который, как и объект Navigator, не указан в стандарте, но поддерживается всеми распространенными браузерами. На сервер передается до пяти свойств отображения с помощью соответствующего сценария:

– screen.width – предоставляет информацию об общей ширине экрана (в пикселях) пользователя;

– screen.height – сообщает серверу общую высоту (в пикселях) пользовательского дисплея;

– screen.availWidth – указывает фактически доступную ширину отображения (в пикселях), доступную пользователю. Для

этого ширина функций интерфейса, таких как панель задач Windows, вычитается из общего значения;

– screen.availHeight – указывает фактически доступную высоту отображения (в пикселях), доступную пользователю. Как и в случае с доступной шириной, размеры элементов интерфейса вычитаются из общего значения;

– screen.colorDepth – сообщает веб-серверу о глубине цвета (бит на пиксель), доступной пользователю для отображения изображений. colorDepth можно приравнять к свойству pixelDepth, которое также возвращает значение глубины цвета, но поддерживается не всеми браузерами.

Часовой пояс, в котором находится пользователь, можно определить с помощью метода JS getTimezoneOffset ( ). Строго говоря, это разница во времени между UTC (Uniform Coordinated Time) и по местному времени в минутах. Настройки операционной системы используются в качестве справочных значений.

Настройки операционной системы также должны использоваться для отслеживания системных цветов. Для этого функция JS getComputedStyle ( ) должна захватывать оптику, выбранную пользователем для оконных рам, кнопок и т. д. Это зависит от поддержки CSS (каскадных таблиц стилей). Язык таблиц стилей позволяет создавать элементы веб-сайта, которые автоматически принимают системные настройки цвета посетителя.

Интернет-браузеры изначально были разработаны для отображения простых HTML-документов, включая отдельные изображения. Однако со временем требования к клиентским программам значительно возросли из-за все более сложных веб-проектов: в дополнение к мультимедийным форматам, таким как аудио- и видеофайлы, также быстро стали применяться интерактивные элементы. Чтобы браузер мог отображать этот разный контент, разработчикам пришлось расширить набор функций

приложений. Это было сделано с помощью подключаемых модулей, которые до сих пор используются для этой цели. С помощью JS установленные плагины можно проверить и, таким образом, использовать для определения отпечатка пальца браузера.

Самым широко используемым подключаемым модулем в мире является Adobe Shockwave Flash, который требуется для воспроизведения Flash-анимации. Кроме того, Flash был преобладающим форматом для видео во всемирной паутине в течение многих лет, поэтому расширение, включающее Flash Player, стало обязательным. Даже если благодаря HTML5 теперь есть более серьезная и безопасная альтернатива для предоставления и воспроизведения видеоконтента, плагин по-прежнему устанавливается в различных браузерах. Исключение составляют большинство стандартных браузеров на мобильных устройствах, не имеющих соответствующего расширения.

Расширение Silverlight от Microsoft добавляет в браузер функциональные возможности, аналогичные Shockwave Flash. Плагин для поддержки интерактивных элементов, как правило, гораздо реже, чем, например, Adobe Flash, и также больше не поддерживается многими популярными версиями браузеров. Однако для снятия отпечатков браузера именно это может оказаться полезным, поскольку браузер, в котором установлен этот плагин, явно отличается от множества других.

Таким образом, на стороне посещаемых сайтов могут использоваться различные методы для идентификации и отслеживания пользователей. Чаще всего это файлы cookie для отслеживания, но также может включать отпечатки браузера, что является более хитрым способом отслеживания пользователей. Существуют удаленные сервисы для проверки своего браузера на открытость к такой идентификации, например:

– Whoer (https://whoer.net/ru) – анализирует и показывает информацию, которую мы невольно оставляет при серфинге в интернете;

– Panopticlick (https://panopticlick.eff.org/) – один из сайтов, который проверяет отпечатки вашего браузера;

– BrowserLeaks (https://browserleaks.com/) – представляет собой набор инструментов для тестирования безопасности и показывает, какие именно личные данные могут оказаться в виртуальном мире без вашего разрешения;

– AmlUnique (https://amiunique.org/) – очень информативный и простой в использовании сервис проверки уникальности браузера.

## § 3. Идентификация пользователя локальной сети

Публичные IP-адреса и разрешенные частные IP-адреса в интернете назначаются и управляются региональным интернет-регистратором. В компьютерных сетях используются два основных метода распределения IP-адресов, это NAT и DHCP.

*Трансляция сетевых адресов (NAT)*. Позволяет переводить частные, не маршрутизируемые IPv4-адреса на один или несколько глобально маршрутизируемых IPv4-адресов, тем самым сохраняя маршрутизируемые IP-адреса организации (рис. 4.1).

NAT позволяет вам не раскрывать реальные IP-адреса хостов, которым необходим доступ к общедоступным адресам, и управлять трафиком путем выполнения переадресации портов. Используется для решения проблем проектирования сети, позволяя сетям, идентичным подсети IP, общаться друг с другом.

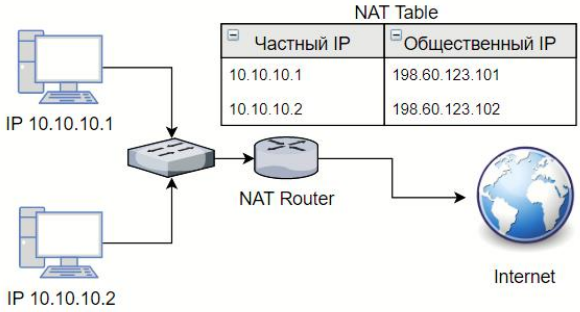


Рис. 4.1. Трансляция сетевых адресов

Если вы используете частные IP-адреса в своих внутренних сетях, то необходимо использовать NAT для перевода частных адресов на общедоступные адреса, которые могут быть перенаправлены во внешние сети.

NAT позволяет одному устройству с одним реальным, зарегистрированным IP-адресом представлять целую сеть систем в интернете. Чтобы сохранить пространство публичных IP-адресов и реализовать значимую сетевую безопасность, системные администраторы обычно используют рассматриваемый метод. NAT отделяет сети организации от интернета, создавая частную сеть «внутри» и интернет «вовне». Незарегистрированные IP-адреса в частной сети должны применять NAT для коммуникации в интернете.

Протокол динамической конфигурации хоста (DHCP) является стандартным протоколом, определенным RFC 1541 (заменен RFC 2131), который позволяет серверу динамически распределять IP-адресацию и информацию о конфигурации клиентам. Обычно сервер DHCP предоставляет клиенту следующую информацию: IP-адрес, маска подсети, шлюз по умолчанию.

Также может быть предоставлена другая информация, такая как адреса DNS. Системный администратор настраивает DHCP-сервер с параметрами, которые обрабатываются клиентом.

Существует три способа, которыми DHCP-сервер назначает или передает IP-адрес клиенту:

1. *Автоматическое распределение*. DHCP-сервер назначает постоянный IP-адрес клиенту из своих IP-пулов.

2. *Динамическое распределение*. DHCP-сервер назначает многократный IP-адрес из IP-пулов адресов клиенту в течение максимального периода времени, известный как аренда. Этот метод распределения адресов полезен, когда клиент имеет ограниченное количество IP-адресов. Они могут быть назначены тем, которым нужен только временный доступ к сети (рис. 4.2).

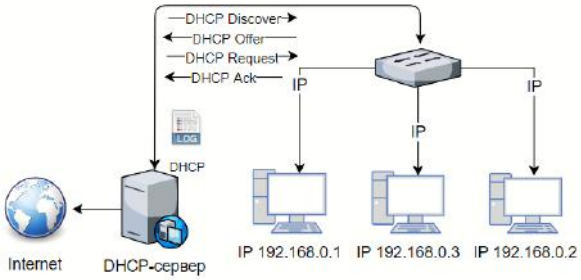


Рис. 4.2. Динамическое распределение IP-адресов

3. *Статическое распределение*. Сетевой администратор выбирает IP-адрес для назначения клиенту, а DHCP-сервер отправляет его клиенту. Статическое распределение DHCP является постоянным, это делается путем настройки DHCP-сервера и выбора зарезервированного адреса для соответствия MAC-адресу клиентского устройства.

В отношении DHCP хорошо то, что распределение IP-адресов обычно записывается в журнал независимо от операционной

системы, которую использует сервер DHCP. Вы сможете определить, какая система (по адресу MAC) имела определенный IP-адрес в определенное время.

Например, вы подозреваете, что некий инсайдер незаконно получил доступ к вашему e-mail, когда вы уезжали на десять дней. По возвращении вы ожидали увидеть сотни e-mail сообщений, однако удивились, когда после соединения со своим почтовым сервером, получили только четыре новых сообщения.

Вы обратились к техническому персоналу и спросили, не было ли с почтовым сервером каких-либо проблем, когда вы были в отпуске. Вас заверили, что проблем не было вообще. Вы немного смущены отсутствием какой-либо почты, пока системный администратор позже не обнаружил запись в журналах почты, которая показывает, что неавторизованный пользователь зарегистрировался на POP-сервере с помощью вашей учетной записи 12/5/00 в 6:43:27 и затем снова в 6:47:45 вечера. Согласно почтовому журналу доступ к вашей учетной записи почты получил IP-адрес 10.0.2.8. Вы понимаете, что подозреваемый должен был сделать запись в почтовом журнале. Теперь необходимо определить, кто имел IP-адрес 10.0.2.8 в это время.

Вы нашли сервер DHCP и получили журналы DHCP. Так как сервер DHCP находится на системе Windows, необходимо просмотреть файл DhcpSrvLog для определения, кто имел IP-адрес 10.0.2.8 во время обращения к вашей учетной записи почты. Далее следует фрагмент из записей сервера DHCP на Windows. Чтобы облегчить работу, можно воспользоваться имеющимся в файле DhcpSrvLog ID-события. Вы ищете в файле ID-события 10 и ID-события 11, которые показывают IP-адрес, выделенный определенному MAC-адресу:

Microsoft DHCP Service Activity Log
Event ID Meaning
00 The log was started.
01 The log was stopped.
02 The log was temporarily paused due to low disk space.
10 A new IP address was leased to a client

В строках 1 и 3 отметим, что система, называемая lappie-XX, обновила IP-адрес 10.0.2.8. Подозрительная система имеет MAC-адрес 00104BDF3720.

Теперь вам необходимо определить, у кого из ваших сотрудников есть система lappie-XX с MAC-адресом 00104BDF3720 [52].

Многие организации учреждают управление конфигурацией, которое требует специальные соглашения об именах систем. Это значительно упрощает трассировку источника незаконного доступа по имени системы.

Соответственно, это также упрощает атакующему использование системного имени кого-то другого. Чтобы проследить MAC-адрес до истинного владельца, необходимо определить владельца системы, а затем осуществить поиск в этой системе исчезнувшей почты:

11 A lease was renewed by a client.
12 A lease was renewed by a client.
13 An IP address was found to be in use on the network.
14 A lease request could not be satisfied because the scope's addres pool was exhausted.
15 A lease was denied.
16 A lease was deleted.
17 A lease was expired.
20 A BOOTP address was leased to a client.
21 A dynamic BOOTP address was eased to a client.
22 A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23 A BOOTP IP address was deleted after checking to see it was not in use.
50 Codes above 50 are used for Rogue Server Detection information.

```
ID Date, Time, Description, IP Adress, Host Name, MAC Adress
1) 11,12/05/00,18:35:38,Renew,10.0.2.8,lappie-XX.,00104BDF3720
2) 11,12/05/00,18:35:40,Renew,10.0.2.78,TEST2.company.com,006097CC6172
3) 11,12/05/00,15:35:40,Renew,10.0.2.8,lappie-XX.,00104BDF3720
4) 11,12/05/00,18:39:33,Renew,10.0.2.78,TEST2.company.com,006097CC6172
5) 11,12/05/00,18:39:43,Assing,10.0.2.94,005056AC0208
6) 17,12/05/00,18:47:55,Expired,10.0.2.21
```

Существуют три диапазона IP-адресов, которые зарезервированы для частного использования: от 10.0.0.0 до 10.255.255.255, от 172.16.0.0 до 172.31.255.255 и от 192.168.0.0 до 192.168.255.255. Подобные адреса никогда не будут распределены публично и являются незарегистрированными номерами; они могут использоваться только внутри организации. Любые пакеты, имеющие IP-адрес источника или места назначения в этих трех диапазонах, никогда не встречаются в интернете. Считайте данные адресные пространства как не маршрутизируемые.

Системы, выполняющие NAT, поддерживают временную таблицу. Она называется таблицей трансляции адресов. Эта таблица отслеживает каждый текущий сеанс между частной сетью и интернетом, чтобы пересылать необходимым образом пакеты. Как только система NAT получает пакет из внутренней системы, она сохраняет внутренний системный зарезервированный не маршрутизируемый IP-адрес и номер порта источника в таблице трансляции адресов. Таблица трансляции адресов содержит такую информацию: компьютер-источник; IP-адрес компьютера-источника; номер порта компьютера-источника; IP-адрес системы NAT; присвоенный номер порта системы NAT.

Система NAT использует таблицу трансляции адресов для маршрутизации трафика между компьютером-источником и удаленным хостом. Проблема для исследования в том, что такая

таблица недоступна в системах UNIX, выполняющих NAT. Однако можно видеть активные трансляции в маршрутизаторе Cisco, выполняя следующую команду: show ip nat translations.

Трассировка владельца IP-адреса, когда он находится позади системы, выполняющей NAT, может быть трудной.

Системы имеют возможность ведения журналов событий, но смогут ли они записать полезную информацию NAT. Это зависит от того, как была сконфигурирована система. Например, Cisco Internetworking Operating System (IOS) поддерживает NAT, всевозможным образом, но не ее журналы. Единственным способом документировать трансляции NAT в маршрутизаторе Cisco является автоматизация запроса.

Система NAT работает путем реконструкции заголовков IP внутренних пакетов, покидающих сеть, делая каждый IP-адрес источника одним и тем же. Пакеты ответа, приходящие не из сети, транслируются и пересылаются соответствующей внутренней системе. Фактически внешние системы в интернете знают только один IP-адрес – адрес системы, выполняющей NAT.

Рассмотрим необходимость и принципы определения MAC-адреса системы. IP работает на третьем, или сетевом, уровне модели OSI. IP работает независимо от уровня канала данных или выбранной физической реализации сети. Независимо от того, используется ли сетевой адаптер Token Ring, Ethernet или FDDI, IP все равно работает. Однако, чтобы сетевые адаптеры общались друг с другом, они должны иметь свои собственные схемы адресации. Адаптер Ethernet не понимает кадры, посланные из адаптера Token Ring, и наоборот. Таким образом, компьютеры применяют для коммуникации уникальный адрес на сетевом адаптере. Он называется адресом протокола управления доступом к среде (MAC) компьютера. Проще всего представлять адрес MAC как физический, аппаратный адрес системы.

Протокол разрешения адреса (ARP) является протоколом на основе TCP/IP (другие пакеты протоколов также могут использовать ARP), который отображает логический IP-адрес в физический MAC-адрес. ARP используется, когда машина знает IP-адрес машины, с которой она хочет общаться. Однако она должна знать ее MAC-адрес, чтобы создать правильные кадры уровня канала данных. Важно понимать, что ARP используется для контакта машин в той же локальной сети (LAN). MAC-адрес никому не виден вне вашего шлюза.

Каждая машина поддерживает таблицу ARP, которая отображает адреса MAC в соответствующие IP-адреса. Эта таблица обновляется примерно каждые 30 с на большинстве систем при условии, что не существует исходящих соединений с удаленной машиной, которые находятся в таблице ARP. Можно представлять таблицу ARP как содержащую MAC-адреса машин, с которыми ваша система общалась за последние 30 с.

Можно использовать команду arp -a для перечисления содержимого таблицы системы ARP (называемой обычно кэш-памятью arp).

Если требуется узнать MAC-адрес системы, можно использовать одну из следующих команд:

- на машинах с Windows 9x используйте winipcfg;
- на системах с Windows NT/2000 применяйте ipconfig /all;
- на системах Unix, таких как Linux и Solaris, используйте ifconfig-a.

Важно понимать, что атакующие могут изменить свой MAC-адрес, чтобы скрыть идентичность. Атакующему необходимо просто определить MAC-адрес машины, которую он хочет имитировать. Зная MAC-адрес, который надо подделать, можно изменить свой MAC-адрес в системе Unix или Windows.

В действительности не существует причин для запрета изменять MAC-адрес своего интерфейса. Чтобы предотвратить такие модификации, необходимо сконфигурировать: DHCP для отображения IP-адресов только в определенные MAC-адреса; коммутаторы для отображения определенных физических портов в определенные MAC-адреса.

Например, MAC-адреса действительно имеют значение при расследовании компьютерного инцидента, но если атака осуществлена вне сети, то идентификатор вряд ли окажется полезным.

Рассмотрим следующую ситуацию. Джон уходит с работы ежедневно в 17:00 и перед уходом выключает свой компьютер. Его коллега Боб, когда Джон ушел с работы раньше, настроил свой компьютер, изменив IP-адрес и интерфейс NetBIOS так, чтобы они совпали с параметрами настроек Джона, затем просмотрел сайты с неприемлемым контентом, а в 17:00 вернул прежние настройки своей системы. Вход Боба в IP-адрес и NetBIOS Джона может привести к увольнению второго.

Журналы сетевого мониторинга показывают, что IP-адрес Джона просматривал сайты с неприемлемым контентом в рабочие часы. Если сетевой мониторинг организации записывает MAC-адреса всех пересылаемых в сети пакетов, то можно будет увидеть, что MAC-адрес, который инициировал незаконный просмотр веб-сайтов, не принадлежит сетевому адаптеру Ethernet в компьютере Джона.

Сегодня существует много способов идентифицировать и трассировать пользователя в сети. Изначально слежка за пользователем была придумана с целью отличить реального пользователя от бота. Затем этим способом воспользовались рекламные компании. Идентифицировать пользователя можно и по структуре локальной сети, настройкам сетевых протоколов. А именно IP-адрес, MAC-адрес, номера портов для исходящих и входящих

TCP/IP-соединений, локальный IP (если пользователь скрыт за прокси). Также широко развит механизм идентификации браузера пользователя.

## § 4. Ложные информационные системы (Honeypot)

В последние несколько лет возрастает интерес к кибербезопасности. Пассивные средства защиты информации вытесняются активными. Вместо того чтобы ждать компьютерной атаки, многие организации предпочитают превентивные меры. Примером может служить ложная информационная система (ЛИС) – одна из наиболее распространенных технологий отслеживания и идентификации в компьютерной сети. В этом параграфе уделим внимание понятию, классификации и области применения ложных информационных систем.

ЛИС можно рассматривать как обычную систему, подключенную к сети, но созданную, чтобы быть приманкой. Она заманивает хакеров и фиксирует все их действия. Такое средство позволяет изучить стратегию злоумышленника и определить, каким образом могут быть нанесены удары по реально существующим объектам безопасности.

Несмотря на то, что за последние несколько лет ЛИС стали значительно популярнее, следует отметить, что они существуют уже довольно давно. В западной литературе ложные информационные системы принято называть honeypot (с англ. «горшочек с медом»). С учетом исследований и развития указанных технологий, а также современных возможностям виртуализации ложные информационные системы позволяют решать следующие задачи:

– захват данных («прослушивание» сетевого трафика и фиксация данных для последующего анализа);

– сбор и объединение данных от различных программных и аппаратных компонентов компьютерной сети, в частности сенсоров, межсетевых экранов, систем обнаружения вторжений, маршрутизаторов и т. д.;

– определение «свой-чужой» и переадресация несанкционированных запросов на ложные компоненты;

– фильтрация событий (для автоматической отбраковки несущественных и фокусировки на значимых событиях);

– обнаружение действий нарушителя;

– трассировка и идентификация нарушителя (определение типа, квалификации и др.);

– обеспечение невозможности использования скомпрометированных компонентов (ресурсов) для атаки или для нанесения вреда другим системам после проникновения нарушителя в ЛИС;

– распознавание плана (стратегии) действий нарушителя; контроль его действий и реагирование на них: оповещение администратора о компрометации, блокирование действий нарушителя и т. д.;

– формирование плана действий компонентов ЛИС по имитации целевой информационной системы;

– заманивание и обман нарушителя (привлечение внимания, сокрытие реальной структуры защищаемой системы и ресурсов, камуфляж, дезинформация) за счет эмуляции сетевых сегментов, серверов, рабочих станций, в том числе передаваемого трафика, и их уязвимостей, автоматическое реагирование на действия нарушителя, например, оповещение администратора;

– удаленное администрирование, документирование, ввод сигнатур, профилей и др. (обеспечивает централизованное управление ЛИС, основанную на правилах безопасности реакцию системы, подготовку отчетов и анализ тенденций), обеспечение интерфейса с администратором безопасности.

Существует различные способы создания ложных информационных систем. Для понимания архитектуры построения рассмотрим их классификацию (рис. 4.3) [16].

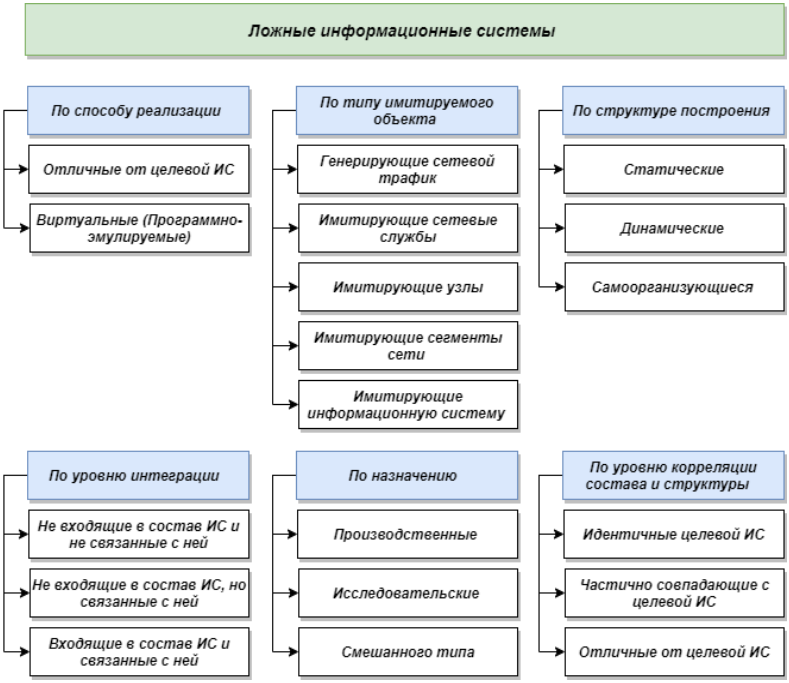


Рис. 4.3. Классификация ЛИС

По способу реализации ЛИС разделяются на реальные и виртуальные. В реальных ЛИС отсутствуют компоненты, имитирующее поведение аппаратного обеспечения, а виртуальные, наоборот, содержат такие компоненты.

Тип имитируемого объекта определяет функциональные возможности ЛИС, а также уровень взаимодействия со средствами НСД. Уровень взаимодействия ЛИС со средствами НСД характеризует возможности, предоставляемые ЛИС средству НСД по реализации компьютерной атаки. Чем больше возможностей предоставляется средствам НСД, тем больше информации можно собрать об их действиях, но тем больше становится объем работ по установке и поддержке функционирования ЛИС и выше риск ее компрометации.

ЛИС, имитирующие работу вычислительной сети, дополнительно включают функции по организации взаимодействия между имитируемыми узлами.

В зависимости от типа структуры выделяют статические, динамические и самоорганизующиеся ЛИС. Статические ЛИС сохраняют свою топологию и состав программного обеспечения в изначально заданном состоянии. В динамических ЛИС изменяется с течением времени их структура, например в процессе функционирования такой ЛИС могут появляться или исчезать какие-либо элементы. Если же структура ЛИС изменяется в зависимости от действий средств НСД, то это самоорганизующаяся ЛИС.

Уровень интеграции в целевую ИС определяет место ЛИС относительно этой системы, а также способ взаимодействия с ней. Также системы могут работать отдельно, параллельно и в составе целевой защищаемой информационной системы. ЛИС, расположенная отдельно от целевой системы, – это территориально удаленная система, использующая проводные и беспроводные каналы для связи и взаимодействия с целевой системой. ЛИС, работающая параллельно целевой системе, размещается на одной территории и подключается к целевой системе с использованием единого пограничного узла. Также компоненты ЛИС могут находиться в составе целевой системы.

По назначению ЛИС могут быть производственными, исследовательскими и смешанными. Производственные ЛИС снижают вероятность успешного осуществления НСД к защищаемой информации за счет увеличения времени ее поиска. Исследовательские ЛИС применяются для изучения средств НСД, используемых ими алгоритмов с целью построения более эффективных механизмов; защиты информации в целевых системах. Смешанные системы сочетают в себе возможности производственных и исследовательских ЛИС.

Также существенной характеристикой ЛИС является ее степень сходства с целевой информационной системой. Чем ЛИС более сходна с целевой системой, тем труднее с помощью средств НСД выявить обман, но в то же время в случае компрометации ЛИС противник может получить достоверные сведения о составе и структуре целевой системы.

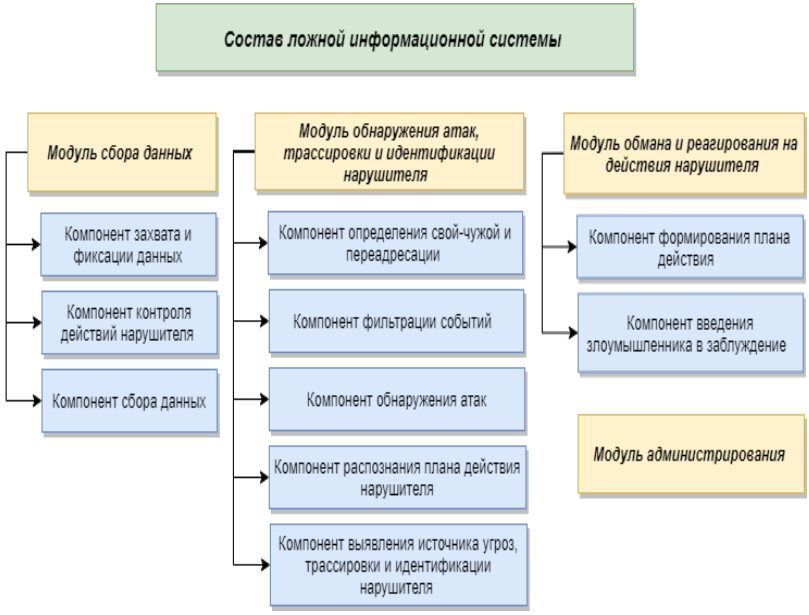


Рис. 4.4. Состав компонентов ЛИС

На сегодняшний день применяются, в основном, статические ЛИС, имитирующие работу сетевых служб. Работа таких средств позволяет оказывать противодействие распространенным в сети Internet сетевым атакам на веб-серверы, серверы баз данных, почтовые серверы (спам) и др. Типовой состав компонентов такой ЛИС приведен на рис. 4.4.

Однако такие ЛИС имеют «узкую специализацию» и не позволяют эффективно противодействовать средствам НСД, функционирующим в локальном сегменте компьютерной сети и использующим для обнаружения методы пассивного прослушивания сетевого трафика, а также методы анализа сетевого окружения, что создает условия для быстрой компрометации ИС.

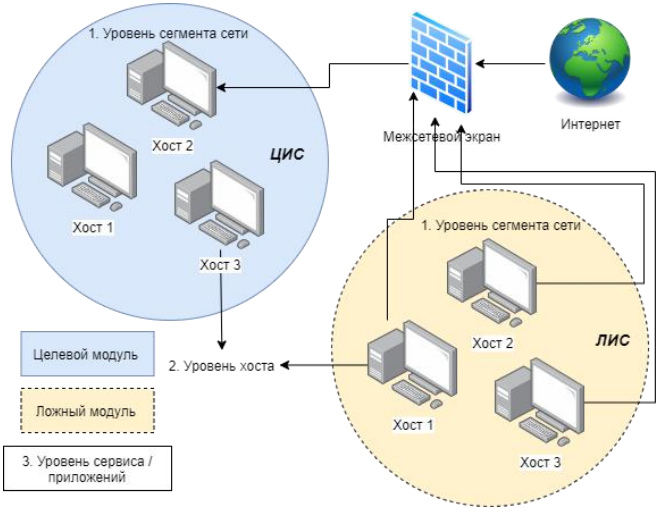


Рис. 4.5. Архитектура ЛИС и уровни введения в заблуждение

Архитектуру ЛИС в общем случае можно представить в виде трех уровней введения в заблуждение (рис. 4.5) [16]:

1) уровень сегмента (основных компонентов целевой системы): на данном уровне имитируется защищаемая целевая система в целом, и при обнаружении атаки злоумышленник перенаправляется с целевой системы на компоненты введения в заблуждение;

2) уровень хоста: на данном уровне предполагается размещение компонентов, имитирующих отдельные хосты, в компьютерной сети целевой системы;

3) уровень сервиса (приложения): в рамках хоста целевой системы каждый сервис (приложение) формируется следующим образом: целевой модуль сервиса (приложения) вместе с модулем обмана «вкладывается в обертку», в режиме санкционированного использования при вызове сервиса/приложения управление передается целевому модулю, при обнаружении несанкционированного обращения управление передается модулю обмана.

Некоторые современные программные средства создания ложных информационных систем, сгруппированные по типу имитируемого объекта представлены в табл. 4.1[1].

*Таблица 4.1*

**Современные средства создания ЛИС по типу имитируемого объекта**

| Класс ЛИС | Наименование программного продукта |
|---|---|
| Генерирующие сетевой трафик | Hping, Nemesis, Karat, Honeycomb |
| Имитирующие сетевые службы | Honeyport Manager, PatriotBox, KFSensor, Jackpot, HoneyWeb, ManTrap, Bubblegum Proxypot, Sendmail SPAM Trap, LaBrea, Arpd, SSH honeypot, Amun, HoneyWRT, Honeymail, Honeytrap, HoneyMysql, MongoDB-HoneyProxy, WebTrap |
| Имитирующие узлы сети | Honeyd, Specter, VMWare (Workstation, ESX), XenServer, VirtualBox, Hyper-V, Pwnypot |
| Имитирующие сети (сегменты сетей) | Honeynets, VMWare (Workstation, ESX), XenServer, VirtualBox, Honeyd, SIREN |

[1] Огромный список ложных информационных систем можно посмотреть по ссылке URL: https://github.com/paralax/awesome-honeypots.

Подводя итог, можно еще раз отметить, что ложные информационные системы используются для сбора данных и поведении об источнике компьютерной атаки. Тип атаки, используемые методы, их успешность или частота отказов, образцы вредоносных программ и т. д. могут быть извлечены из журналов ЛИС. Службы кибербезопасности могут принимать меры на основе полученных и проанализированных разведданных. Администраторы безопасности получают возможность заранее занести в черный список подозрительное поведение до того, как системы будут заражены.

# ГЛАВА V. КОМПЬЮТЕРНЫЕ АТАКИ И УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

## § 1. Понятие и классификация атак на компьютерные системы

Обострение международной обстановки существенно увеличивает интенсивность действий технической разведки иностранных государств. В ближайшие годы следует ожидать дальнейшей эволюции компьютерных угроз на основе искусственного интеллекта и инструментов машинного обучения. В данной главе мы рассмотрим классификацию компьютерных атак и уязвимостей информационных систем.

В предыдущих главах рассмотрены способы сбора информации и особенности обеспечения анонимности. Эффективность на этапе сбора информации является залогом успеха реализации атаки. Первое, что необходимо сделать, это собрать информацию о компьютерной системе (ОС, открытые порты, сетевые сервисы, прикладное программное обеспечение и т. д.). Затем выявляются наиболее уязвимые места целевой системы, воздействие на которые приводит к нужному результату.

Атакой на компьютерную систему принято считать преднамеренные действия, использующие уязвимости в системном, прикладном и сетевом программном обеспечении (в том числе уязвимости протоколов сетевого взаимодействия) приводящие к установлению контроля над операционной средой или осуществления НСД к информации. Атаки на компьютерные системы разнообразны, как и объекты, против которых они направлены. Технологически большинство компьютерных атак использует ряд

уязвимостей, изначально присущих системному, прикладному сетевому программному обеспечению.

Определение атаки сформулировано во многих стандартах. Так, ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» дает следующее определение: «посягательство на систему, которое является следствием продуманного планирования, т. е. умышленного действия, представляющее собой продуманную попытку (особенно в плане метода или стратегии) обойти сервисы безопасности и нарушить политику безопасности системы».

Также определение атаки сформулировано в ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления» и выглядит следующим образом: «попытки уничтожить, подвергнуть опасности, преобразовать или вывести из строя информационную систему и/или содержащуюся в ней информацию, или иным образом затронуть политику безопасности».

Для уточнения области воздействия атаки в отдельных государственных стандартах вводится понятие компьютерной атаки и сетевой атаки. Они сформулированы в ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», более расширенное определение сетевой атаки также сформулировано в ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (см. § 3 главы 1).

Обилие видов атак и разнообразие формулировок позволяет разделить их на классы. В литературе выделяют пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные и т. д. В качестве основы классификации компьютерных атак будем использовать упомянутый выше стандарт ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009, где рассмотрены общепризнанные типы атак (рис. 5.1) [32].

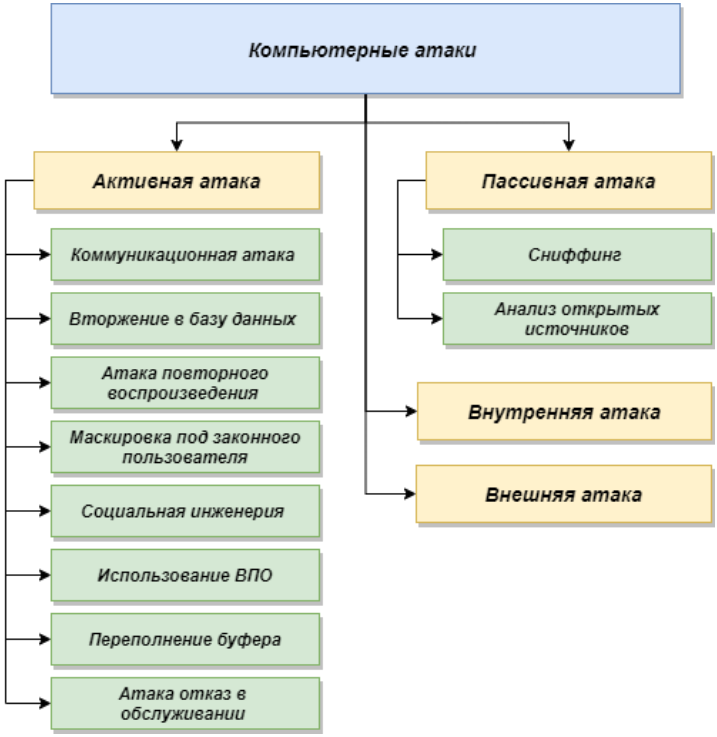


Рис. 5.1. Классификация компьютерных атак

Активная атака – имеет целью преобразовать ресурсы системы или воздействовать на ее работу. К активным атакам можно отнести следующие виды:

1. *Коммуникационная атака* имеет целью нарушить коммуникацию с системой промышленной автоматики и контроля.

Коммуникационные атаки бывают нескольких видов. Данные атаки могут осуществляться на нескольких уровнях внутри системы, начиная с уровня процессора компьютера и далее по восходящей, и инициироваться за пределами предприятия, как в случае атаки вида «отказ в обслуживании» (DoS) для коммуникационных систем.

2. *Вторжение в базу данных* – форма атаки на веб-сайт, управляемый базой данных, в ходе которой злоумышленник реализует неавторизованные команды, пользуясь ненадежным кодом в системе, соединенной с интернетом, и действуя в обход межсетевого экрана. Атаки с вторжением в базу данных применяют для похищения информации из базы данных, которые в нормальном режиме недоступны, и/или получения доступа к хост-компьютерам организации через компьютер, содержащий базу данных. Ярким примером является *SQL-инъекция*, которая включает в себя отправку запроса в веб-приложение с командами SQL, добавленными таким образом, что веб-приложение передает их в обрабатываемую базу данных.

3. *Атака повторного воспроизведения.* Из коммуникационных путей систем управления могут быть скопированы сигналы, которые впоследствии могут быть воспроизведены для обеспечения доступа к защищенным системам или фальсификации данных в системе промышленной автоматики и контроля. Потенциальные злоумышленники могут воспроизводить сигналы управления доступом, биометрические сигналы и другие сигналы системы для получения несанкционированного доступа к защищенным участкам или системам, сокрытия незаконной деятельности или выполнения ложных отвлекающих маневров. Система может реализовывать в себе серию путей для сбора данных, оповещения и контроля, что позволит предотвратить сбор

всей информации (с целью ее дальнейшего воспроизведения) через единичное подключение, для всей подсистемы, узла оборудования, приложения или базы данных.

4. *Фиктивная авторизация и маскировка под законного пользователя (спуфинг).* Спуфинг – маскировка под легального пользователя или сетевой ресурс. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции». В контексте вычислительных сетей понятия «фиктивная авторизация и маскировка под законного пользователя» используются для описания разнообразных способов, которыми можно обмануть аппаратное или программное обеспечение. Злоумышленники могут подделать заголовок электронного письма, чтобы сообщение выглядело как поступившее от какого-либо источника или адресата, отличных от подлинного. IP-спуфинг, например, задействует обманный трюк, благодаря которому сообщение выглядит как поступившее с авторизованного IP-адреса. Еще одно называние таких атак MITM (Man in the middle) человек посередине. Наиболее распространенные виды спуфинга это:

1) *MAC-Spoofing*. MAC-адрес, изменяется таким образом, чтобы компьютер атакующего идентифицировался как участник сетевого обмена целевых систем. Подмена MAC-адресов интересна для атакующего, если их цель находится в той же подсети, что и он. MAC работает на уровне канала передачи данных и поэтому используется только локально. Чтобы обмануть за пределами локальной сети, нужно обманывать более высокий уровень, например сетевой уровень;

2) *IP-Spoofing*. Подмена IP-адреса аналогична подмене MAC-адресов, описанной выше. Диапазоны IP-адресов часто используются для определения доступа к определенным службам,

поэтому может быть получен несанкционированный доступ благодаря подмене IP-адреса. IP-Spoofing часто используется для ввода команд или данных в существующий поток данных между хостом и другими хостами. Чтобы полностью захватить поток данных, атакующий должен изменить таблицы маршрутизации, чтобы пакеты были перенаправлены на поддельный хост. Более подробную информацию об IP-спуфинге мы рассмотрим в главе удаленные сетевые атаки.

3) *DNS-Spoofing* (известен также как отравление DNS-кэша). Представляет собой вид атаки, когда DNS-кэш заполняется поддельными данными, в результате чего пользователь перенаправляется на вредоносный сайт.

5. *Социальная инженерия.* К факторам угрозы относятся также получение или попытки получения конфиденциальных данных путем обмана. Социальная инженерия эффективна потому, что ее жертвы по своей сущности хотят доверять другим людям и готовы прийти на помощь. Жертвы социальной инженерии раскрывают информацию, не ведая о том, что она будет использована для атак на компьютерную сеть.

Частный случай атак класса социальной инженерии это – *фишинг*. Разновидность посягательств на безопасность, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который, на первый взгляд, связан с законным источником. Фишинг основан на социальной инженерии, человек склонен верить в надежность брендов, связывая их с авторитетностью.

6. *Использование вредоносного программного обеспечения (кода).* Назначением вредоносного кода может быть сбор информации о системах или пользователях, уничтожение системных

данных, создание закладки для дальнейшего несанкционированного проникновения в систему, фальсификация системных данных и отчетов или внесение путаницы в системные процессы и создание сложностей обслуживающему персоналу. Вредоносные коды, используемые в ходе атак, могут принимать форму вирусов, червей, автоматических эксплоитов или троянских коней.

*Вирус* – это программа или часть кода внутри другой программы, которая загружается в компьютер без ведома пользователя и функционирует против его воли. Вирусы могут также самотиражироваться. Все компьютерные вирусы создаются человеком. Простой вирус, способный производить копию самого себя снова и снова, может быть создан относительно легко. Такой уже опасен, поскольку он быстро завладеет всей доступной памятью и будет препятствовать работе системы. Еще более опасная разновидность вируса, способного передаваться по сетям в обход систем безопасности.

Автоматический код-эксплойт вносится в систему для сбора информации или оповещения кого-либо или других систем о конкретных событиях или взаимодействиях. Относительно простой код-эксплойт способен собирать информацию для предстоящих несанкционированных проникновений, получения финансовой выгоды или статистических данных (маркетинг). Автоматический код-эксплойт может использовать другие ресурсы или приложения, которые находятся уже в самой системе, для умножения своих возможностей по сбору информации или уничтожению данных. Полностью автоматический код-эксплойт обычно называют червем. Червь представляет собой автономную программу или алгоритм, который самотиражируется в пределах компьютерной сети и обычно выполняет вредоносные действия, такие как расходование компьютерных ресурсов и, возможно, остановка работы системы.

*Троянский конь* – это вредоносная программа, которая маскируется под полезное приложение. В отличие от вирусов, троянские кони (также известны как «трояны») не самотиражируются, но могут быть такими же вредоносными. Одна из наиболее коварных разновидностей троянских коней – это программа, которая предлагает очистить компьютер от вирусов, но вместо этого вносит в него новые вирусы.

Вредоносный код может быть внесен с созданием ботнета, т. е. совокупности машин с нарушенной безопасностью, которые реализуют программы в рамках общей инфраструктуры контроля и управления. Создатель ботнета может управлять группой компьютеров дистанционно, как правило, в неблаговидных целях.

7. *Переполнение буфера*. Переполнение буфера, наиболее распространенное средство атаки на компьютер или сеть. Эта атака редко запускаются сама по себе и обычно является частью смешанной атаки. Переполнение буфера использует ошибки в алгоритмах, в которых буферы разрешены для переполнения. Если буфер заполнен сверх его возможностей, данные, заполняющие его, могут затем переполняться в соседнюю память, а затем могут либо повреждать данные, либо использоваться для изменения исполнения программы. Существует два основных типа переполнения: переполнение буфера стека (наиболее распространенная форма) и переполнение кучи (динамически распределяемой памяти).

*Переполнение стека.* Стек – это область памяти, которую процесс использует для хранения данных, таких как локальные переменные, параметры метода и обратные адреса. Часто буферы объявляются в начале программы и поэтому хранятся в стеке. Каждый процесс имеет свой собственный стек и свою собственную кучу (как объясняется в следующем разделе).

Переполнение буфера стека является одним из первых типов переполнения буфера, который обычно используется для получения контроля над процессом. Если процесс, управляющий буфером, не делает адекватных проверок, атакующий может попытаться помещать данные, размер которых больше размера буфера. Это означает что, когда буфер заполнен, оставшиеся данные в него переполняют буфер и перезаписывают соседнюю память. Атакующий может поместить вредоносный код в буфер, в котором часть смежной памяти часто содержит указатель на следующую строку кода для выполнения. Таким образом, переполнение буфера может указать на начало буфера и, следовательно, начало вредоносного кода. А переполнение буфера стека может дать управление процессу.

*Переполнение кучи (heap).* Похоже на переполнение стека, но, как правило, сложнее создать. Куча похожа на стек, но хранит динамически распределенные данные. Куча обычно не содержит обратных адресов, таких как стек, поэтому сложнее получить контроль над процессом, чем при использовании стека. Однако куча содержит указатели на данные и функции. Успешное переполнение буфера позволит манипулировать выполнением процесса. Примером может быть переполнение строкового буфера, содержащего имя файла, так что имя файла теперь является важным системным файлом. Затем атакующий может использовать этот процесс для перезаписывания системного файла (если у процесса есть правильные привилегии).

8. *Атака «отказ в обслуживании».* Атаки типа «отказ в обслуживании» (DoS) или ухудшение его качества воздействуют на работоспособность сети, операционной системы или прикладных ресурсов. Распространенной формой атаки с целью сетевого отказа в обслуживании является распределенная атака DDoS, ко-

торая использует множественные устройства с нарушенной безопасностью для причинения значительного ущерба сети, устройству или приложению. Различают следующие виды атак «отказ в обслуживании»:

1) *атаки DoS на основе хоста* – нацелены на атаку компьютеров. Целенаправленная уязвимость в операционной системе, прикладном программном обеспечении или конфигурации хоста;

2) *сетевые атаки DoS* – нацелены на сетевые ресурсы в попытке нарушить законное использование. Сетевые DoS обычно наводняют сеть и целевые пакеты межсетевого взаимодействия. Чтобы реализовать наводнение, должно быть отправлено такое количество пакетов, что целевой компьютер не сможет обрабатывать. Основные методы затопления – это TCP Floods, ICMP Echo Request, UDP Floods;

3) *распределенные атаки DoS (DDoS)* – это относительно недавняя разработка сетевой атаки. Атаки DDoS работают с использованием большого количества узлов для одновременной атаки на цель или цели.

9. *Атака на расширение (повышение) привилегий.* Чтобы спланировать и осуществить эффективную атаку на систему, факторы угрозы должны во многих случаях сначала получить привилегированный доступ. Благодаря расширенным привилегиям злоумышленник может совершать действия, которые в противном случае будут запрещены. Например, атаки брутфорса работают, подбирая все возможные комбинации, которые могут составлять пароль. Вопрос только в том, сколько времени потребуется для подобной атаки. По мере увеличения длины пароля, в среднем для поиска правильного пароля время увеличивается экспоненциально.

10. *Атаки с физическим повреждением* имеют цель разрушение или выведение из строя физических компонентов (т. е. аппаратного обеспечения, устройств хранения программного обеспечения, соединительных элементов, датчиков и контроллеров), которые являются частью системы промышленной автоматики и контроля. Такие атаки могут принимать форму физических атак непосредственно на компоненты или физических атак посредством кибератак, которые инициируют действия системы, ведущие к физическому ущербу, повреждению или выходу из строя компонента.

Пассивная атака имеет целью заполучить или использовать информацию системы без воздействия на ресурсы системы. Сбор пассивной информации может дать потенциальному злоумышленнику много ценных сведений. Факторы угрозы обычно включают в себя пассивную информацию при случайных вербальных коммуникациях с сотрудниками и подрядчиками. Однако лица, находящиеся на территории или за территорией производственных объектов, могут также получать пассивную информацию посредством визуальных наблюдений. Сбор пассивной информации может включать в себя сбор данных о пересменах, функционировании оборудования, материально-техническом снабжении, графиках патрулирования и прочих уязвимостях. Сбор пассивной информации иногда трудно обнаружить, особенно если информацию собирают малыми частями и из нескольких источников. Постоянное наблюдение над необычайно любопытными посетителями, фотографами и персоналом (зачастую за пределами мест исполнения их служебных обязанностей) может помочь организациям выявить сбор пассивной информации, особенно если при этом тщательно проверяются их биографические данные.

Примером пассивной атаки является сниффинг.

*Сниффинг* – это отслеживание данных в потоке информации. Самыми известным способом сниффинга является перехват данных в потоке информации. Сниффинг может быть весьма изощренным. Инструменты сниффинга общедоступны и позволяют перехватывать данные в различных коммуникационных сетях. Такие устройства обычно используются для управления конфигурациями, поиска и устранения неисправностей в сетях и анализа трафика данных, однако их можно также использовать для сбора специальных данных о любом взаимодействии в пределах сети. Например, при сниффинге пакетов данных и паролей злоумышленник тайно подключается к сети через удаленную станцию или компьютер. Инструмент сниффинга затем пассивно отслеживает информацию, пересылаемую внутри сети, и фиксирует ее на дисковом запоминающем устройстве, причем эти данные можно в дальнейшем загрузить и анализировать для получения идентификационной информации и паролей пользователя.

*Внутренняя атака* – это атака, инициированная субъектом в пределах периметра безопасности инсайдером, т. е. субъектом, который наделен правами на получение доступа к ресурсам системы, но использует их в целях, не одобренных теми, кто предоставил эти права.

*Внешняя атака* – это атака, инициированная за пределами периметра безопасности неавторизованным или неуполномоченным пользователем системы (им может быть и инсайдер, атакующий за пределами периметра безопасности). Потенциальными злоумышленниками, осуществляющими внешнюю атаку, могут быть как простые любители пошутить, так и организованные преступные группы, международные террористы и враждебные правительства.

## § 2. Уязвимости информационных систем

Современные информационные системы состоят из множества взаимосвязанных компонентов. Это создает большую область реализации атаки для потенциального проникновения в систему и компрометации информации. Хакеры и взломщики получают несанкционированный доступ, обнаруживая слабые места в ОС, средствах защиты и прикладных программах. В профессиональной терминологии слабые места в информационной системе называют уязвимостями.

Как результат, уязвимость способствует успешной атаке, эксплатирующей опасную ошибку в программе. Например, когда сотрудник компании оформляет увольнение, а администратор защиты забывает отключить его учетную запись с доступом информационным ресурсам, то это создает для компании условия для преднамеренных и непреднамеренных угроз. Однако большинство уязвимостей основаны на технических особенностях информационных систем.

Действующий ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» формулирует уязвимость следующим образом: *уязвимость* – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (-ая) может быть использован (-а) для реализации угроз безопасности информации [33].

Другими словами, это недостаток в компьютерной системе, использование которого, приводит к нарушению целостности, доступности и конфиденциальности.

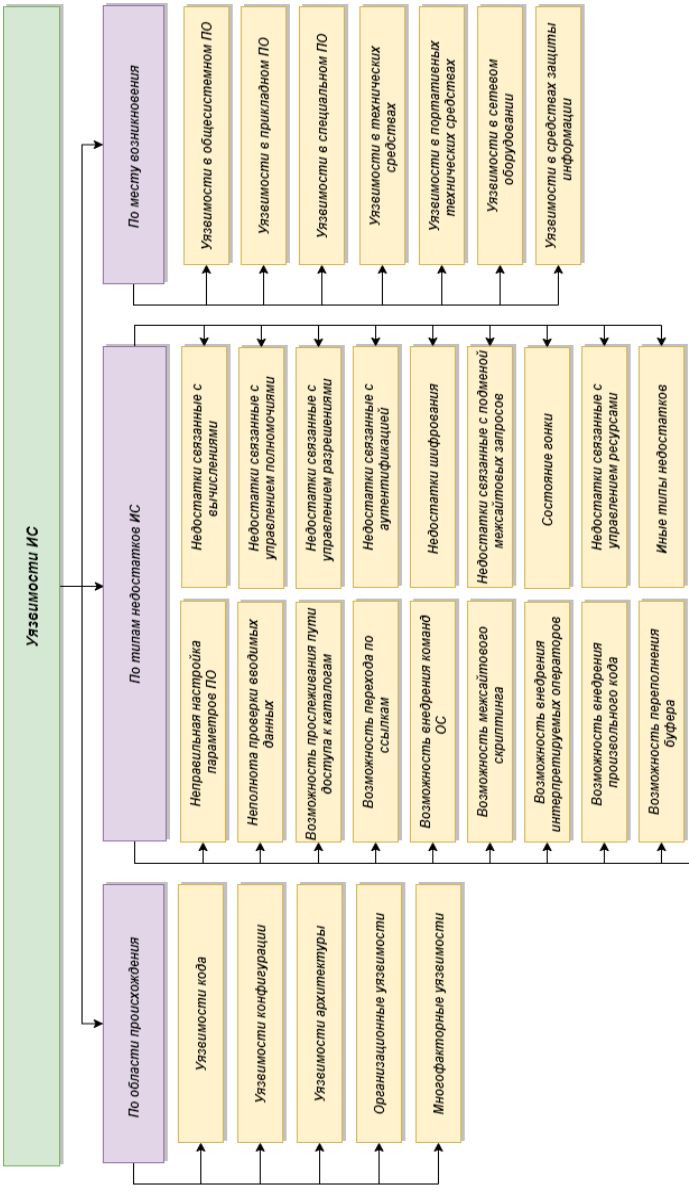


Рис. 5.2. Классификация уязвимостей информационных систем

Существуют различные классификации уязвимостей в информационных системах. Рассмотрим приведенную в ГОСТ Р 56546-2015 (рис. 5.2). Уязвимости ИС по области происхождения подразделяются на следующие классы:

– *уязвимость кода.* Уязвимость, появившаяся в процессе разработки программного обеспечения;

– *уязвимость конфигурации.* Уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы;

– *уязвимость архитектуры.* Уязвимость, появившаяся в процессе проектирования информационной системы;

– *организационная уязвимость.* Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственным за защиту информации;

– *многофакторная уязвимость.* Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.

Уязвимости ИС по типам недостатков подразделяются на следующие:

– *недостатки, связанные с неправильной настройкой параметров ПО*. Неправильная настройка параметров ПО заключается в отсутствии необходимого параметра, присвоении параметру неправильных значений, наличии избыточного числа параметров или неопределенных параметров ПО;

– *недостатки, связанные с неполнотой проверки вводимых (входных) данных*. Недостаточность проверки вводимых (входных) данных заключается в отсутствии проверки значений, избыточном количестве значений, неопределенности значений вводимых (входных) данных;

– *недостатки, связанные с возможностью прослеживания пути доступа к каталогам*. Прослеживание пути доступа к каталогам заключается в отслеживании пути доступа к каталогу (по адресной строке / составному имени) и получении доступа к предыдущему/корневому месту хранения данных;

– *недостатки, связанные с возможностью перехода по ссылкам*. Переход по ссылкам связан с возможностью внедрения нарушителем ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Для файловых систем недостатками являются символьные ссылки и возможности прослеживания по ним нахождения ресурса, доступ к которому ограничен;

– *недостатки, связанные с возможностью внедрения команд ОС*. Внедрение команд ОС заключается в возможности выполнения пользователем команд ОС (например, просмотра структуры каталогов, копирование, удаление файлов и др.);

– *недостатки, связанные с межсайтовым скриптингом (выполнением сценариев)*. Межсайтовый скриптинг обычно распространен в веб-приложениях и позволяет внедрять код в веб-страницы, которые могут просматривать нелегитимные пользователи. Примерами такого кода являются скрипты, выполняющиеся на стороне пользователя;

– *недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки*. Недостатки связаны с внедрением интерпретируемых операторов

языков программирования (например, операции выбора, добавления, удаления и др.) или разметки в исходный код веб-приложения;

– *недостатки, связанные с внедрением произвольного кода*. Недостатки связаны с внедрением произвольного кода и части кода, которые могут приводить к нарушению процесса выполнения операций;

– *недостатки, связанные с переполнением буфера памяти*. Переполнение буфера возникает в случае, когда ПО осуществляет запись данных за пределами выделенного в памяти буфера. Переполнение буфера обычно возникает из-за неправильной работы с данными, полученными извне, и памятью, при отсутствии защиты со стороны среды программирования и ОС. В результате переполнения буфера могут быть испорчены данные, расположенные следом за буфером или перед ним. Переполнение буфера может вызывать аварийное завершение или зависание ПО. Отдельные виды переполнений буфера (например, переполнение в стековом кадре) позволяют нарушителю выполнить произвольный код от имени ПО и с правами учетной записи, от которой она выполняется;

– *недостатки, связанные с неконтролируемой форматной строкой*. Форматная строка в языках C/C++ является специальным аргументом функции с динамически изменяемым числом параметров. Ее значение в момент вызова функции определяет фактическое количество и типы параметров функции. Ошибки форматной строки потенциально позволяют нарушителю динамически изменять путь исполнения программы, в ряде случаев – внедрять произвольный код;

– *недостатки, связанные с вычислениями*. Подразделяются на следующие виды:

а) некорректный диапазон, когда ПО использует неверное максимальное или минимальное значение, которое отличается от верного на единицу в большую или меньшую сторону;

б) ошибка числа со знаком, когда нарушитель может вводить данные, содержащие отрицательное целое число, которые программа преобразует в положительное нецелое число;

в) ошибка усечения числа, когда часть числа отсекается (например, вследствие явного или неявного преобразования, или иных переходов между типами чисел);

г) ошибка индикации порядка байтов в числах, когда в ПО смешивается порядок обработки битов (например, обратный и прямой порядок битов), что приводит к неверному числу в содержимом, имеющем критическое значение для безопасности;

– *недостатки, приводящие к утечке/раскрытию информации ограниченного доступа*. Утечка информации – преднамеренное или неумышленное разглашение информации ограниченного доступа (например, существуют утечки информации при генерировании ПО сообщения об ошибке, которое содержит сведения ограниченного доступа). Недостатки, приводящие к утечке/раскрытию информации ограниченного доступа, могут возникать вследствие наличия иных ошибок (например, ошибок, связанных с использованием скриптов);

– *недостатки, связанные с управлением полномочиями (учетными данными)*. К этому типу относят, например, нарушение политики разграничения доступа, отсутствие необходимых ролей пользователей, ошибки при удалении ненужных учетных данных и др.;

– *недостатки, связанные с управлением разрешениями, привилегиями и доступом.* К ним относят, например, превыше-

ние привилегий и полномочий, необоснованное наличие суперпользователей в системе, нарушение политики разграничения доступа и др.;

– *недостатки, связанные с аутентификацией*. Сюда относят возможность обхода аутентификации, ошибки логики процесса аутентификации, отсутствие запрета множественных неудачных попыток аутентификации, отсутствие требования аутентификации для выполнения критичных функций;

– *недостатки, связанные с криптографическими преобразованиями (недостатки шифрования)*. К этим недостаткам относят ошибки хранения информации в незашифрованном виде, ошибки при управлении ключами, использование несертифицированных средств криптографической защиты информации;

– *недостатки, связанные с подменой межсайтовых запросов*. Подмена межсайтового запроса заключается в том, что используемое ПО не осуществляет или не может осуществить проверку правильности формирования запроса;

– *недостатки, приводящие к «состоянию гонки»*. «Состояние гонки» – ошибка проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода. «Состояние гонки» является специфической ошибкой, проявляющейся в случайные моменты времени;

– *недостатки, связанные с управлением ресурсами*. К этому типу относят недостаточность мер освобождения выделенных участков памяти после использования, что приводит к сокращению свободных областей памяти, и отсутствие очистки ресурса и процессов от сведений ограниченного доступа перед повторным использованием и др.;

– *иные типы недостатков*. По результатам выявления уязвимостей ИС перечень типов недостатков может дополняться.

Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие:

– *уязвимости в общесистемном (общем) ПО*. В этот тип недостатков включают уязвимости ОС (уязвимости файловых систем, уязвимости режимов загрузки, уязвимости, связанные с наличием средств разработки и отладки ПО, уязвимости механизмов управления процессами и др.), уязвимости систем управления базами данных (уязвимости серверной и клиентской частей системы управления базами данных, уязвимости специального инструментария, уязвимости исполняемых объектов баз данных (хранимые процедуры, триггеры) и др.), уязвимости иных типов общесистемного (общего) ПО;

– *уязвимости в прикладном ПО*. К ним относят уязвимости офисных пакетов программ и иных типов прикладного ПО (наличие средств разработки мобильного кода, недостатки механизмов контроля исполнения мобильного кода, ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации, и др.);

– *уязвимости в специальном ПО*. К этим недостаткам относят уязвимости ПО, разработанного для решения специфических задач конкретной ИС (ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации, недостатки механизмов разграничения доступа к объектам специального ПО и др.);

– *уязвимости в технических средствах*. К ним относят уязвимости ПО технических средств (уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах,

уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости), иные уязвимости технических средств;

– *уязвимости в портативных технических средствах*. К данным уязвимостям относят уязвимости ОС мобильных (портативных) устройств, уязвимости приложений для получения с мобильного устройства доступа к интернет-сервисам, уязвимости интерфейсов беспроводного доступа, иные уязвимости портативных технических средств;

– *уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании*. К ним относят уязвимости маршрутизаторов, коммутаторов, концентраторов, мультиплексоров, мостов и телекоммуникационного оборудования иных типов (уязвимости протоколов и сетевых сервисов, уязвимости средств и протоколов управления телекоммуникационным оборудованием, недостатки механизмов управления потоками информации, недостатки механизмов разграничения доступа к функциям управления телекоммуникационным оборудованием и др.);

– *уязвимости в средствах защиты информации*. Сюда включают уязвимости в средствах управления доступом, средствах идентификации и аутентификации, средствах контроля целостности, средствах доверенной загрузки, средствах антивирусной защиты, системах обнаружения вторжений, средствах межсетевого экранирования, средствах управления потоками информации, средствах ограничения программной среды, средствах стирания информации и контроля удаления информации, средствах защиты каналов передачи информации, уязвимости в иных средствах защиты информации (ошибки программирования, недостатки, связанные с возможностью обхода, отключения, преодоления функций безопасности, другие уязвимости).

На территории Российской Федерации одной из основных организаций, отвечающих за обеспечение информационной безопасности в ключевых системах информационной инфраструктуры, включая компьютерные сети органов государственной власти и компьютерные сети критичных объектов инфраструктуры и предприятий, является Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

Для обеспечения деятельности по сертификации средств защиты информации и обнаружения уязвимостей программного обеспечения ФСТЭК России с 2014 г. поддерживает собственный реестр известных угроз информационной безопасности и уязвимостей программного обеспечения – Банк данных угроз безопасности информации (далее – БДУ ФСТЭК России)[1] [73].

Все хранящиеся в БДУ ФСТЭК России записи имеют единообразный формат и включают: текстовое описание уязвимости, дату обнаружения уязвимости, названия, версии и производителей уязвимого ПО, информацию о типе ошибки, классе уязвимости и текущем ее статусе (потенциально возможная либо подтвержденная производителями ПО или независимыми исследователями уязвимость, устранена ли уязвимость в новых версиях ПО). Также записи содержат оценку критичности уязвимости и сопутствующий вектор CVSS, пометку о наличии известных готовых сценариев эксплуатации уязвимости и возможного результата эксплуатации уязвимости, указание уязвимых аппаратных платформ или ОС, список возможных методов противодействия уязвимости и ссылки на источники дополнительной информации по уязвимости (включая идентификаторы данной уязвимости в иных реестрах и базах данных) [73].

[1] URL: http://www.bdu.fstec.ru/.

Общие требования к структуре описания уязвимости описаны в ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

*Описание идентификации* уязвимости должно включать следующие элементы: идентификатор уязвимости, наименование уязвимости, класс уязвимости, наименование программного обеспечения (ПО) и его версия.

*Описание для работ по анализу уязвимостей* должно включать следующие элементы: идентификатор типа недостатка, тип недостатка, место возникновения (проявления) уязвимости, способ (правило) обнаружения уязвимости, возможные меры по устранению уязвимости.

*Детальное описание уязвимости* описание может включать следующие элементы: наименование ОС и тип аппаратной платформы; язык программирования ПО; служба (порт), которую (-ый) используют для функционирования ПО; степень опасности уязвимости; краткое описание уязвимости; идентификаторы других систем описаний уязвимостей; дата выявления уязвимости; автор, опубликовавший информацию о выявленной уязвимости; критерии опасности уязвимости.

Дополнительно описание уязвимости ИС может включать прочую информацию в составе следующих элементов: описание реализуемой технологии обработки (передачи) информации; описание конфигурации ПО, определяемой параметрами установки; описание настроек ПО, при которых выявлена уязвимость; описание полномочий (прав доступа) к ИС, необходимых нарушителю для эксплуатации уязвимости; описание возможных угроз безопасности информации, реализация которых возможна при эксплуатации уязвимости; описание возможных последствий от эксплуатации уязвимости ИС; наименование организации, которая опубликовала информацию о выявленной

уязвимости; дата опубликования уведомления о выявленной уязвимости, а также дата устранения уязвимости разработчиком ПО; другие сведения.

Стандарт *Common Vulnerabilities and Exposures* (далее – CVE)[1], разработанный американской некоммерческой исследовательской корпорацией MITRE Corporation в 1999 г., представляет собой основной документ в области унифицированного именования и регистрации обнаруженных уязвимостей программного обеспечения. Данный стандарт определяет формат идентификаторов, содержимого записей об отдельных обнаруженных уязвимостях, процесс резервирования идентификаторов для новых обнаруженных уязвимостей и пополнения соответствующих баз данных.

В рамках поддержки проекта MITRE CVE основными задачами таких организаций, как CVE Numbering Authorities, CNAs, являются:

– *поиск и сбор информации* об уязвимостях программного обеспечения (в случае производителей и вендоров ПО, их область ответственности ограничена непосредственно их собственными продуктами и сервисами);

– *классификация* найденных уязвимостей;

– *резервирование CVE-идентификаторов* для найденных уязвимостей;

– *актуализация соответствующей информации* в двух официальных каталогах: реестре уязвимостей CVE List[2] MITRE Corporation и базе данных уязвимостей National Vulnerability Database (далее – NVD)[3], поддерживаемой национальным Институтом Технологий и Стандартов США.

---

[1] URL: http://cve.mitre.org.
[2] URL: https://cve.mitre.org/cve/.
[3] URL: https://nvd.nist.gov/.

На текущий день базы уязвимостей MITRE CVE List и NVD содержат более 100 тыс. записей об отдельных уязвимостях, обнаруженных за период с 1999 г. по настоящее время. При этом, хотя сами базы данных различаются на уровне функциональных возможностей, предоставляемых пользователям, сами списки записей об уязвимостях фактически идентичны друг другу. Формально CVE List выступает изначальным источником записей для базы данных NVD, а специалисты, отвечающие за поддержку базы NVD, производят уточненный анализ и сбор доступной информации по уязвимостям, зарегистрированным в CVE List (например, собирают ссылки на сторонние источники информации об уязвимости и мерах по ее устранению или предотвращению эксплуатации).

Идентификаторы CVE имеют формат CVE-YYYY-NNNN, отражая в первых четырех цифрах год регистрации уязвимости и в последующих четырех-шести цифрах – уникальный в рамках этого года номер уязвимости.

Для каждой из обнаруженных уязвимостей запись в базе содержит краткое описание типа и причин уязвимости, уязвимые версии ПО, оценку критичности уязвимости в соответствии со стандартом Common Vulnerability Scoring System (далее – CVSS) и ссылки на внешние источники с информацией об уязвимости – чаще всего, таковыми выступают информационные бюллетени на сайтах производителей программного обеспечения или исследовательских организаций.

В плане пользовательского функционала в CVE List поддерживаются возможности простейшего поиска среди записей (по ключевым словам, и CVE-идентификаторам) и скачивания архивов записей за любой выбранный год в различных форматах (HTML, XML, CVRF, CSV или Plain Text). Также возможно автоматическое получение обновлений в машиночитаемом виде

через специальный data feed CVE Change Log (он позволяет как отслеживать появление новых идентификаторов CVE, так и изменения в записях для уже существующих).

Для базы NVD, в свою очередь, доступны продвинутые функции поиска уязвимостей, по ключевым словам, временным диапазонам создания/модификации записи, компонентам CVSS-метрики и т. п. Кроме того, доступны скачивание всех записей базы данных в XML, а также получение информации об обновлениях базы в виде RSS-подписки и JSON data feed.

Преимуществом базы данных MITRE CVE List и NVD является ежедневное обновление реестров известных уязвимостей. При обнаружении новой уязвимости производителем ПО или исследовательской организацией (или подтверждении наличия уязвимости вендором ПО в ответ на сообщение от частных исследователей или организаций, не входящих в CVE (Numbering Authorities), под нее оперативно регистрируется новый идентификатор CVE и создается запись в базе, после чего происходит периодическое обновление информации. В качестве примера рассмотрим некоторые типы уязвимостей:


*Meltdown (CVE-2017-5754)* – аппаратная уязвимость категории «утечка по стороннему каналу», обнаруженная в ряде микропроцессоров, в частности производства Intel и архитектуры ARM. Уязвимость позволяет локальному атакующему (при запуске специальной программы) получить несанкционированный доступ на чтение к привилегированной памяти (памяти, используемой ядром операционной системы).


*Spectre (CVE-2017-5753)* – группа аппаратных уязвимостей, ошибка в большинстве современных процессоров, позволяющих проводить чтение данных через сторонний канал в виде общей иерархии кэш-памяти. Затрагивает большинство современных микропроцессоров, в частности архитектур x86/x86_64 (Intel и AMD) и некоторые процессорные ядра ARM. Уязвимость потенциально позволяет локальным приложениям (локальному атакующему при запуске специальной программы) получить доступ к содержимому виртуальной памяти текущего приложения или других программ.


*BlueBorne (CVE-2017-1000251)* – общее название восьми опасных уязвимостей электронных устройств, работающих с различными имплементациями Bluetooth в Android, iOS, Windows и Linux. Позволяют выполнить на устройстве произвольный вредоносный код, получить полный контроль над устройством, осуществить атаку «человек посередине».

Специалисты, занятые аудитом защищенности компьютерных систем, благодаря мониторингу баз данных уязвимостей, получают возможность проверить наличие актуальных уязвимостей в тестируемой ими сети или убедиться в их отсутствии, руководствуясь структурированным списком известных уязвимостей и составом ПО в тестируемой сети. Как правило, специалисты такого рода менее заинтересованы в оперативности обновления выбранного реестра уязвимостей, зато для них критичны охват и качество покрытия выбранной базой данных состава ПО тестируемой сети и всего множества потенциальных

уязвимостей. В этой связи обязательный к использованию список для аудита включает официально признанные реестры уязвимостей, такие как БДУ ФСТЭК России и MITRE CVE List. Так, при тестировании на проникновение дополнительную пользу могут принести реестры известных Proof of Concept сценариев эксплуатации уязвимостей и готовых эксплойтов.

# ГЛАВА VI. ОСНОВЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

## § 1. Понятие и классификация атак класса социальной инженерии

Сегодня человеческий фактор в информационной безопасности играет более важную роль, чем 20 лет назад, когда интернет не был коммерческим и его пользователями были лишь специалисты. Многие компании, которые думают, что проблему информационной безопасности можно решить просто с помощью аппаратных и программных средств, сильно заблуждаются. Технологии безопасности, которым мы привыкли доверять, – физическая, техническая и даже криптографическая защита и многие другие – остаются бессильны против методов социальной инженерии.

Понятие социальная инженерия имеет много значений. Рассмотрим несколько определений.

*Социальная инженерия* – термин, использующийся взломщиками и хакерами для обозначения несанкционированного доступа к информации иначе, чем взлом программного обеспечения, с целью обхитрить людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы.

Также *социальную инженерию* можно определить, как манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации.

Понятие социальной инженерии сформулировано в ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1.

Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики» (см. § 3 главы 1).

Таким образом, этот метод несанкционированного доступа основан на использовании слабостей человека и считается очень разрушительным. Атакующий получает информацию, например, путем сбора данных о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего. Атакующий может позвонить работнику компании (под видом технической службы) и узнать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе.

Сегодня социальная инженерия – одна из распространенных угроз для информационных систем. Крупнейшие организации в области кибербезопасности, например, Positive Technologies и InfoWatch, в своих аналитических отчетах отмечают стремительный рост атак класса социальной инженерии. Относительная простота технической составляющей атаки и социально-психологический аспект позволяют злоумышленникам получить информацию конфиденциального характера, необходимую для хищения денежных средств с банковских карт, шантажа и т. д. Основные области применения социальной инженерии изображены на на рис. 6.1.

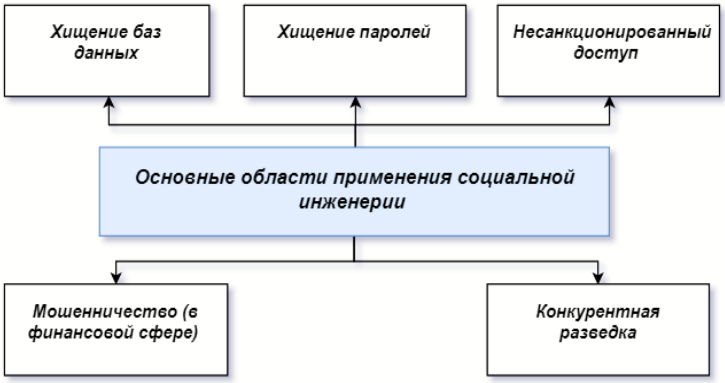


Рис. 6.1. Основные области применения социальной инженерии

*Мошенничество.* Чаще всего заключается в несанкционированных действиях в финансовой сфере. Социальные хакеры используют все возможные способы, для того чтобы завладеть доверием людей, с целью использования их платежных сервисов.

*Хищение паролей.* В области социальной инженерии хищение паролей, как правило используется в целях получения доступа к персональным (банковским) данным частных лиц.

*Хищение базы данных*. Путей хищения базы данных достаточно много. Вот наиболее значимые из них: база данных уходит вместе с уволенным сотрудником. Атакующий может временно устроиться в фирму, у которой надо украсть информацию и через некоторое время уволиться; воспользоваться беспечностью сотрудников, которые оставляют важные документы на столах; подглядеть за действиями сотрудников за компьютером; представившись работником по обслуживанию компьютеров, получить прямой доступ к необходимой информации.

*Несанкционированный доступ.* С помощью методов социальной инженерии злоумышленники получают доступ к сети организации. Тем временем, пока администраторы по безопасности ставят брандмауэры и антивирусы, разрабатывают сложную

систему допусков и паролей, атакующие проникают в сеть с помощью ничего не подозревающих пользователей.

*Конкурентная разведка (информация о маркетинговых планах организации.* Социальная инженерия помогает верно оценить возможности инвесторов, вырвать у соперников выгодный тендер, провести успешную маркетинговую кампанию – сделать это с помощью методов социальной инженерии проще всего.

Пользователи компьютерных систем используют широкий спектр информационных технологий, чтобы облегчить, автоматизировать и улучшить повседневные задачи: совместное использование компьютеров в организациях, внутренние или внешние коммуникации, блоги и т. д. Это позволяет мгновенно обмениваться информацией и устанавливает постоянный канал связи с клиентами и партнерами. Учитывая широкий диапазон современных информационных технологий, атаки социальной инженерии имеют большой потенциал.

Современные средства коммуникации сильно изменили связь между сотрудниками, что позволило обеспечить быстрый обмен информацией. Существуют сложные технологии, которые защищают безопасность передачи данных. Однако большинство этих мер направлены на технические атаки, в то время как нападениям социальной инженерии уделяют меньше внимания. В корпоративных средах личная связь часто заменяется электронными письмами или мгновенными сообщениями, создавая новую платформу атаки для социальных инженеров. Очевидно, что атаки социальной инженерии, поступающие от внутренних учетных записей или электронной почты с поддельными внутренними адресами, скорее всего, ускользнут от бдительности потенциальной жертвы.

Как и в случае внутренней коммуникации, используются внешние сервисы электронной почты, облачного хранения данных, блогов и т. д. Для внешней связи присутствуют те же проблемы, что и во внутренней коммуникации. Однако, поскольку контролируемая зона становится более размытой, не вся информация может быть передана внешнему каналу связи. Самый сильный потенциальный риск внешней коммуникации состоит в большом разнообразии возможных каналов связи. Кроме того, современные технологии увеличивают количество внешних каналов, за счет использования личных средств коммуникации. Мобильные устройства с корпоративной информацией используются в небезопасных средах, таких как кафе или общественный транспорт. Конечно, на большинстве этих устройств установлены системы безопасности, однако эти системы не защищают от социальных атак.

Для классификации атак социальной инженерии выделим четыре основные категории: канал, оператор, метод и сценарий (рис. 6.2). Атаки могут выполняться по следующим каналам:

1. Электронная почта – наиболее распространенный канал для фишинговых и атак обратной социальной инженерии.

2. Приложения для обмена мгновенными сообщениями – популярны среди социальных инженеров как инструменты для фишинга и обратных атак социальной инженерии. Они также могут быть легко использованы для получения личных данных.

3. Телефон, IP-телефония – обычные каналы атаки для социальных инженеров, через которые их жертва предоставляет конфиденциальную информацию.

4. Социальные сети – предлагают множество возможностей для атак социальной инженерии. Учитывая их потенциал для со-

здания поддельных идентификаторов и их сложной модели обмена информацией, они облегчают для атакующих скрывать свою личность и собирать конфиденциальную информацию.

5. Облачные службы – используются для получения информации о характере совместной работы. Атакующие могут поместить файл или программное обеспечение в общий каталог, чтобы передать информацию жертве.

6. Веб-сайты – чаще всего необходимы для совершения waterholing-атак. Кроме того, они могут использоваться в сочетании с электронной почтой для фишинговых атак.

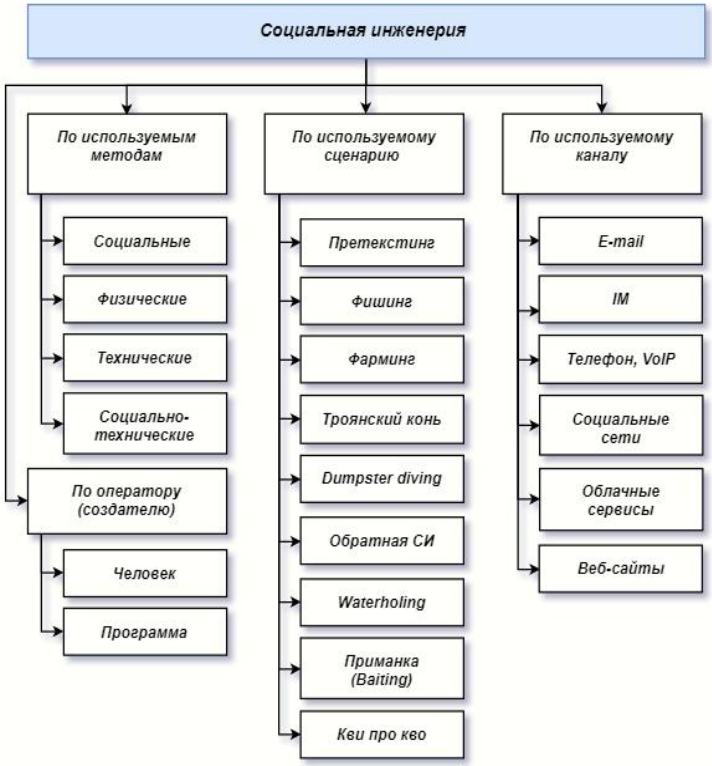


Рис. 6.2. Классификация атак социальной инженерии

Можно также классифицировать атаки по оператору. Так, оператором атаки социальной инженерии может быть:

– человек (количество целей ограничено из-за меньшей емкости по сравнению с атакой, производимой программным обеспечением);

– программное обеспечение. Например, наборы инструментов социальной инженерии (SET), которые можно использовать для создания писем с spear-фишингом. Основным преимуществом автоматических атак является то, что количество возможных целей, за короткий промежуток времени, значительно выше, чем исключительно человеческих атаках.

Кроме того, классифицируем атаки социальной инженерии на четыре метода: физические, технические, социальные и социально-технические методы.

1. *Физические методы* – необходимо выполнить какую-то физическую деятельность, чтобы собрать информацию о будущей жертве. Это может варьироваться от личной информации, например номера социального страхования, даты рождения, до действительных учетных данных для компьютерной системы. Часто используемым методом является dumpster diving, т. е. поиск мусора организации. Корзина может быть ценным источником информации, в которой могут быть личные данные о сотрудниках, руководства, заметки и даже распечатки конфиденциальной информации, такие как учетные данные пользователя. Если получить доступ к рабочему месту целевого объекта, можно узнать пароли, которые иногда записывают на записках. Менее сложные физические атаки включают кражу или вымогательство для получения информации.

2. *Социальные методы.* Самым важным аспектом успешных атак социальной инженерии являются социальные методы.

Таким образом, атакующие полагаются на социально-психологические аспекты, такие как убеждения, чтобы манипулировать их жертвами. Примеры методов убеждения включают использование (предполагаемых) полномочий, чтобы повысить шансы на успех таких нападений, атакующие часто пытаются наладить отношения с их будущими жертвами. Наиболее распространенный тип социальных атак осуществляется по телефону.

3. *Технические методы.* Технические атаки в основном осуществляются через интернет. Интернет особенно интересен для социальных инженеров при получении паролей, поскольку пользователи часто используют одинаковые (простые) пароли для разных учетных записей. Большинство людей также не знают, что они свободно предоставляют тем, кто будет их искать, большое количество личной информации. Атакующие часто используют поисковые системы для сбора личной информации о будущих жертвах. Существуют также инструменты, которые могут собирать информацию из разных веб-ресурсов. Одним из самых популярных инструментов такого типа является Maltego. Сайты социальных сетей – один их самых ценных источников информации.

4. *Социально-технические методы.* Успешные атаки в области социальной инженерии часто объединяют несколько или все различные подходы, рассмотренные выше. Однако социально-технические подходы создали самое мощное оружие социальных инженеров. Одним из примеров является так называемая приманка *(baiting)*: атакующие оставляют зараженные носители в местах, где их могут найти будущие жертвы. Например, USB-накопитель, содержащий троянского коня. Атакующие дополнительно используют любопытство людей, добавляя заманчивые этикетки к этим приманкам (носителям), таким как «секретно» или «списки увольнения персонала».

Еще одна распространенная комбинация технических и социальных подходов – фишинг. Фишинг обычно осуществляется через e-mail или сервисы мгновенного обмена сообщениями, нацелены на большую группу пользователей. Отдельные специалисты утверждают, что классические фишинг-атаки используются для реализации более сложной атаки spear-фишинг – целенаправленные сообщения, выполненные после первоначальной обработки данных. Для примера сначала используются сайты социальных сетей для получения данных, затем отправляются сообщение, похожее на сообщение, присланное одним из друзей. Следовательно, spear-фишинг считается комбинацией технологических подходов и социальной инженерии.

Границы отдельных методов расширяемы и в большинстве случаев комбинируются.

Все техники (сценарии) социальной инженерии основаны на особенностях сознательного поведения людей. Рассмотрим основные виды:

1. *Претекстинг* – это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определенную информацию, или совершить определенное действие. Этот вид атак применяется обычно по телефону. Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: выяснение имени сотрудника, занимаемой им должности и названия проектов, над которыми он работает) с тем, чтобы обеспечить доверие цели.

2. *Фишинг* – это попытка получить конфиденциальную информацию или заставить кого-то действовать желаемым образом, маскируясь как заслуживающий доверия объект на электронном средстве связи. Как правило, предназначены для

больших групп людей. Фишинг-атаки могут выполняться практически на любом канале, от физического до прикладного, социальных сетей или даже облачных сервисов. Обычно атакующий посылает e-mail, подделанный под официальное письмо, например, от банка или платежной системы, требующее «проверки» определенной информации, или совершения определенных действий. Это письмо обычно содержит ссылку на фальшивую вебстраницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести конфиденциальную информацию: от домашнего адреса до PIN-кода банковской карты. Атаки, предназначенные для конкретных лиц или компаний, называются гарпунами. Данный вид атаки требует, чтобы атакующий сначала собрал информацию о предполагаемых жертвах, при этом уровень успеха выше, чем при обычном фишинге. Если фишинг-атака нацелена на большие цели на предприятиях, атака называется «китобойный промысел».

Фишинг является одним из самых распространенных сценариев социальной инженерии. Выделяют следующие виды:

– почтовый фишинг: жертве отправляется электронное письмо, в котором содержится просьба выслать те или иные конфиденциальные данные. К примеру, от имени интернет-провайдера с похожего почтового адреса отправляется письмо, в котором написано, что по провайдеру нужно узнать логин и пароль для доступа в интернет указанного пользователя, так как сам провайдер по тем или иным техническим причинам этого сделать не может;

– онлайновый фишинг: мошенники один в один копируют какой-либо из известных сайтов, причем для него выбирается очень похожее доменное имя, и создается идентичный дизайн. Решив совершить в магазине покупку, пользователь вводит свои логин, пароль и номер пластиковой карты, после чего все эти

данные становятся известными. Вскоре мошенник незамедлительно использует кредитную карту жертвы;

– телефонный фишинг (вишинг, voice phishing) – назван так по аналогии с фишингом – распространенным сетевым мошенничеством. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие вишинга в том, что, так или иначе, задействуется телефон. Схемы обмана те же самые, однако в случае вишинга в сообщении содержится просьба позвонить на определенный городской номер. При этом зачитывается сообщение, в котором потенциальную жертву просят сообщить свои конфиденциальные данные. Например, ввести номер карты, пароли, коды доступа или другую личную информацию в тоновом наборе;

– комбинированный фишинг – объединение предыдущих видов фишинга. Также, как и в онлайновом фишинге, создается поддельный сайт, а потом как в почтовом фишинге пользователям отсылаются письма с просьбой зайти на этот сайт. Популярные фишинговые схемы: мошенничество с использованием брендов известных корпораций, подложные лотереи, ложные антивирусы и программы для обеспечения безопасности.

3. *Фарминг* – это техника скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура (файл hosts, система доменных имен (DNS). Суть фарминга в автоматической отсылке пользователей на поддельные сайты. Фарминг гораздо сложнее, чем фишинг, так как в отличие от последнего этот метод хищения данных не требует отсылки писем потенциальным жертвам и соответственно их ответа на них. Это, естественно, более изощренный, хотя и технически намного более сложный метод мошенничества, чем фишинг. Но зато при фарминге у пользователя практически нет

причин проявлять свою недоверчивость: писем никто не присылал, на сайт никто заходить не просил. Пользователь сам по своему желанию решил зайти на сайт банка. Однако попал не на оригинальный, а на поддельный сайт.

Опасность фарминга многие исследователи связывают еще и с тем, что с целью его развития атакующие будут предпринимать все больше атак на DNS-серверы и эти атаки будут все изощреннее.

Популярные методы реализации фарминг-атак: изменение файла HOSTS, изменение файла HOSTS вместе с изменением его местоположения, модификация настроек DNS-серверов, регистрация ложного DHCP-сервера.

4. *Троянский конь*: атакующий отправляет письмо по электронной почте, содержащее во вложении критическое обновление антивируса, или компромат на сотрудника. Такая техника остается эффективной, пока пользователи будут слепо кликать по любым вложениям.

5. *Dumpster diving* – это практика проверки мусора частных лиц или компаний, чтобы найти выброшенные предметы, содержащие конфиденциальную информацию, которая может быть использована для компрометации системы или конкретной учетной записи пользователя.

6. *Плечевой серфинг (shoulder surng)* относится к использованию методов прямого наблюдения для получения информации, например, для подглядывания через чье-то плечо за экраном или клавиатурой.

7. *Обратная социальная инженерия* – это атака, где обычно устанавливается доверие между атакующим и жертвой. Нападавшие создают ситуацию, в которой жертва нуждается в решении проблемы, а затем представляют себя как того, кто может

решить проблему и тем самым получает доступ к привилегированной информации. Конечно, атакующие пытаются выбрать человека, который, по их мнению, имеет информацию, способную им помочь.

8. *Waterholing* – направленная атака, при которой атакующий компрометирует веб-сайт, представляющий интерес для жертвы. Своего рода приманка для жертвы. Название атаки образовано от ситуации, когда хищники в естественных условиях, поджидают возможности атаковать свою добычу рядом с водоемами.

9. *Приманка (Baiting) или «дорожное яблоко»* – это атака, в ходе которой зараженный вредоносными программами носитель оставляется в месте, где его могут найти целевые жертвы.

Например, атакующий может подбросить диск, снабженный корпоративным логотипом, и ссылкой на официальный сайт компании цели, и снабдить его надписью «заработная плата руководящего состава за год». Диск может быть оставлен на полу лифта или в вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить свое любопытство.

10. *Кви про кво*: атакующий может позвонить по случайному номеру в компанию и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» цель вводит команды, которые позволяют атакующему запустить вредоносное программное обеспечение.

Особенностью способов проведения атак с помощью социальной инженерии является то, что они базируются на получении доступа к информации без применения технических и программных средств получения доступа к защищаемой информации и основываются на слабостях человека, например словоохотливости или жажде известности.

Проведем обзор самых современных атак социальной инженерии. Эти атаки часто нацелены на личную информацию из онлайновых социальных сетей или других облачных сервисов и могут выполняться автоматизированным способом. В целом современные атаки социальной инженерии имеют три направления: социальные сети, облачные сервисы хранения информации, приложения сотовых телефонов. Рассмотрим их особенности и краткую характеристику в соответствии с указанным направлением воздействия:

1. *Online Social Networks (OSN)*. В то время как более традиционные формы социальной инженерии используют информацию, собранную посредством dumpster diving или телефонных звонков, OSN содержат множество личных данных которые могут быть использованы в качестве исходного источника для атак социальной инженерии. Информация, собираемая из OSN, легко обрабатывается. Так, информация о сотрудниках целевой компании может быть собрана в автоматическом режиме и использована для автоматизированной социальной инженерии.

При технике фишинга активно используется инфомация из соцсетей (социальный фишинг). Исследователи заметили, что, когда фишинг-сообщения электронной почты олицетворяли друга цели, показатель успеха увеличился с 16 % до 72 %. Следовательно, социальный аспект не только имеет ценность для оператора социальной сети, но и для атакующего. Это особенно важно, если в нем содержится дополнительная информация, например, действительный адрес электронной почты или недавняя связь между жертвой и другом, которого атакующий может олицетворять.

Общение в социальной сети, выраженное в личных сообщениях, комментариях на стене, может использоваться для определения языка, обычно используемого для обмена сообщениями

между жертвой и его друзьями. Так, контекстно-зависимый спам увеличивает внешний вид подлинности традиционных спам-сообщений. Существует три атаки, связанные со спамом: атаки на основе отношений, атаки с несимметричным атрибутом и атаки с общими атрибутами. Первые используют исключительно информацию о взаимоотношениях, превращая их в спам или эквивалент социальному фишингу. Две другие атаки используют дополнительную информацию из социальных сетей между целью спама и поддельным другом. Примером непривязанной атаки являются поздравительные открытки, которые, как представляется, происходят от друга цели. Общие атрибуты, например фотографии, в которых помечены как спам-цель, так и ее поддельный друг, могут быть использованы для контекстно-зависимого спама. Поддержка безопасности связи может быть использована для автоматического извлечения личной информации из онлайновых социальных сетей [53].

Исследование Sophos, опубликованное в 2007 г., по случайно выбранным пользователям Facebook, показало, что примерно 41 % пользователей социальных сетей приняли запросы дружбы от поддельного профиля. Кроме того, поддельные профили могут быть неправильно использованы для проникновения в социальные сети. Sophos создал профиль для вымышленного американского аналитика кибер-угрозы под названием Robin Sage получил доступ к конфиденциальной информации военных и сообщества информационной безопасности.

В данных исследованиях также были изложены особенности реализации двух сложных атак поддельного профиля, которые могут быть использованы для проникновения в закрытые группы пользователей социальных сетей. Один из них клонирование профиля, когда злоумышленники клонируют существующие профили пользователей и пытаются повторно отправить запрос

на добавление в друзья (друзьям пользователя). Второй вид атак представляет собой создание дублированного профиля в социальной сети, где целевой пользователь еще не имеет профиля, а затем рассылает запросы друзьям [53].

2. *Облачные сервисы*. Облачные сервисы предоставляют новый канал, через который социальные инженеры могут проводить атаки. Пользователи часто сотрудничают с другими лицами, не работающими в одном месте, поэтому обмен информацией о облачном сервисе стал популярным. В этом случае атакующий использует эту ситуацию, используя облако в качестве канала для атаки. Недавние публикации описывали множество возможных атак в облаке, например, атакующий, помещающий вредоносный файл в облако другого пользователя, а затем используя социальную инженерию, заставляет открыть вредоносный файл. Вредоносное программное обеспечение может использоваться для извлечения личной информации из учетной записи жертвы, которая затем используется для выполнения более целенаправленных атак. Уровень доверия между пользователями общей папки или файла не всегда на должном уровне. Поэтому социальные инженеры могут использовать это, применяя фальшивый идентификатор или скомпрометированную учетную запись пользователя, чтобы предложить жертве поделиться определенной информацией с атакующим в облаке.

Одна из самых слабых сторон облачных сервисов заключается в том, что пользователи компании и отдельные пользователи теряют контроль над своими данными, когда они хранят и получают доступ к нему удаленно. На традиционных серверах, принадлежащих самой компании, он может ограничивать доступ и настраивать параметры доступа. В облачных сервисах ответственность за это переносится на третью сторону. Поэтому, если облачная служба используется для обмена конфиденциальной

информацией, определенный уровень доверия должен устанавливаться не только между взаимодействующими пользователями, но и между облачной хостинговой компанией и пользователем.

3. *Мобильные приложения.* Увеличение использования мобильных приложений в деловых и частных областях акутализирует их для атак социальной инженерии. В деловых коммуникациях приложения для мобильных сообщений и электронной почты представляют большой интерес для социальных инженеров. Деятельность компании часто предполагает использование мобильных телефонов и планшетов. Все больше сотрудников используют свои смартфоны для проверки электронной почты своих компаний или для чтения документов, хранящихся в облаке. Однако многие пользователи эксплуатируют очень уязвимые приложения для смартфонов, которые могут быть неправильно использованы для проведения социальных инженерных атак.

Спуфинг идентификатора может быть сделан на популярных мобильных приложениях обмена сообщениями, таких как WhatsApp, Viber. Социальный инженер может использовать это, чтобы отправить сообщение жертве, притворяясь одним из его друзей. Следует отметить, что многие приложения для смартфонов очень уязвимы и способны передавать конфиденциальную информацию, так некоторые приложения запрашивают разрешения на доступ к конфиденциальным данным на устройстве пользователя. Если атакующий скачивает такое приложение, то он может подвергнуться спланированной целенаправленной атаке. В некоторых случаях, хакер просто копирует популярные приложения для смартфонов и использует их для совершения атаки [53].

## § 2. Защита от атак социальной инженерии

Атаки в области социальной инженерии обычно включают в себя некоторые формы психологических манипуляций, обманывая иначе ничего не подозревающих пользователей или сотрудников в передаче конфиденциальных или конфиденциальных данных. Как правило, социальная инженерия использует электронную почту или другие сообщения, которые вызывают у жертвы срочность, страх или иные подобные эмоции, что приводит к тому, что атакуемый быстро раскрывает конфиденциальную информацию, щелкает нужную ссылку или открывает вредоносный файл. Поскольку социальная инженерия связана с человеческим фактором, предотвращение этих атак может быть сложным для реализации.

Социальные инженеры используют убеждения, дружелюбие, доброту и манипулирование людьми, чтобы заполучить ценную информацию. Существует комбинация подходов, включая обучение, информирование о методах социальных инженеров. В результате в комплексную политику безопасности должны быть включены гарантии, предназначенные для уменьшения степени ущерба, который может вызвать социальная инженерия.

*Сегрегация доступа*. Необходимо обеспечить, чтобы пользователи имели доступ только к информации и системам, которые им необходимы для работы, такая организация может ограничить объем ущерба, который может вызвать социальный инженер с доступом к системе.

*Ведение журналов доступа.* Убедившись, что ведется журнал доступа, компания сможет узнать, к чему атакующий смог получить доступ, прежде чем его заблокировать. Это позволит

принимать обоснованные решения о масштабах убытков, с которыми сталкивается компания, и необходимости в немедленном реагировании.

*Регулярное резервное копирование.* Некоторые атакующие могут довольствоваться просто кражей информации жертвы, другие могут быть больше заинтересованы в том, чтобы просто нанести вред, удалив данные компании. Поэтому необходимо регулярно выполнять резервное копирование и обеспечивать, чтобы атакующий не смог уничтожить резервную копию.

*Автоматическая отмена пользовательских привилегий при обнаружении подозрительной активности*. Когда атакующий входит в систему, он будет искать файлы или приложения, представляющие интерес, просматривая каталоги компьютера или выполняя поиск на диске и скачивая как можно больше информации на свой компьютер. Используя системы обнаружения вторжений, компании могут автоматически отслеживать аномальные уровни использования диска и сети и закрывать доступ подозрительной учетной записи в течение нескольких секунд.

Социальной инженерии трудно избежать, однако можно предсказать поведение людей и ориентировать их воздерживаться от предоставления конфиденциальной информации. Можно отметить ряд общепринятых действий по предотвращению атак социальной инженерии.

*Обучение сотрудников*. Важно постоянно обучать сотрудников распознавать тактику социальной инженерии, а также иметь систему отчетности для повышения осведомленности о нападениях и, самое главное, осуществлять политику компании. Сотрудники могут быть хорошо осведомлены о том, как выглядят социальные инженерные ситуации, но это не значит, что они на 100 % безопасны. Если существуют строгие правила, сотрудники с меньшей вероятностью станут жертвами, потому что они

не будут нарушать политику компании и, следовательно, подвергать риску свою работу. Эти правила помогают сместить вину или ответственность от сотрудника.

*Физические данные.* Социальным инженерам вообще не нужно быть убедительными или применять психологические приемы, они просто могут собирать информацию, которая остается открытой. Каталоги учебных заведений или работодателя, визитные карточки, онлайн-базы данных, номера телефонов, квитанции, электронные письма, социальные сети – все это источники, которые могут быть полезны для атакующего и содержат либо всю необходимую информацию, нужную атакующему, либо небольшую часть, полезную для начала работы в крупном масштабе.

*Незаметные сотрудники*. Уверенные сотрудники, обладающие методами управления человеком без технических средств считаются одними из лучших специалистов в области социальной инженерии.

Неизвестное лицо может входить в бизнес, искать вход в ваш дом или звонить, заявляя, что они из коммунальных служб и должны выполнить техническое обслуживание, обновления или устранить проблему, о которой сообщалось ранее. Вход в ваш дом или бизнес должен быть заранее согласованным, а не внезапным.

Всегда проверяйте того, кто запрашивает ваш пароль или учетные данные, задавайте как можно больше вопросов, при этом остерегайтесь подозрительного поведения, особенно будьте бдительны, если у вас спрашивают имена родственников и место рождения и т. п. Часто злоумышленники предлагают восстановить забытый пароль и могут задавать ряд вопросов о средней школе, родном городе, как звали любимого учителя, марку первого авто-

мобиля или имя домашнего животного. Не стоит забывать, что ответы на эти вопросы угрожают вашей безопасности. Старайтесь придумывать сложные пароли, чтобы должным образом защитить конфиденциальную информацию о кредитных картах, банковских выписках, каталогах и квитанциях.

Если вам позвонили незаметные сотрудники и представились работниками службы безопасности банка, то спросите, почему они действительно нуждаются в той или иной информации, уточните причину проверки, задавайте вопросы о подробностях проверки и т. д., или сразу прекращайте разговор.

Хорошей практикой является создание централизованной базы данных, которая регистрирует попытки социальной инженерии. Например, если секретарь получает звонок, от менеджера, который запрашивает пароль, должна быть возможность сообщить об инциденте ответственному лицу или отделу, где он будет зарегистрирован. Это позволяет обнаружить шаблоны и быть более осторожным, ведь вы знаете, что кто-то пытается получить информацию, которая может быть использована для проникновения в вашу сеть.

Помимо тех, что уже упоминались здесь, есть много других приемов, которые могут использовать социальные инженеры или хакеры. Поскольку большинство атак социальной инженерии происходят через компьютеры, ноутбуки, мобильные телефоны, планшеты и т. д., то необходимо защищать свои персональные устройства. Некоторые из превентивных мер, которые вы можете предпринять, включают в себя активацию брандмауэров, установку антивируса, настройку фильтров электронной почты и использование антифишинговых инструментов, которые предупредят вас о рисках.

# ГЛАВА VII. ПОВЫШЕНИЕ ПРИВИЛЕГИЙ В ОПЕРАЦИОННОЙ СИСТЕМЕ

## § 1. Базовые технологии безопасности операционной системы

На практике результат того или иного метода доступа, в значительной степени, зависит от архитектуры и конфигурации конкретной компьютерной системы, являющейся объектом этой атаки. Сегодня основным средством для работы по-прежнему остается персональный компьютер, поэтому рассмотрим методы несанкционированного доступа именно к нему.

В базовой архитектуре пользователь может защитить свои данные на уровне basic input output system (далее – BIOS) и операционной системы. Понимание возможностей механизмов защиты указанных систем, поможет в дальнейшем подобрать необходимые инструменты. Защиту компьютерной системы с помощью BIOS можно считать физическим методом блокировки.

*BIOS* – это система ввода-вывода, выполняющая процедуры низкого уровня, которые тестируют компьютер после включения питания. Именно она запускает операционную систему. Почти все BIOS имеют возможность задать пароль включения. Если пароль задан, то ОС запустится только после его ввода. То есть вы физически вводите пароль, как при открытии сейфа и не зависите от работы какой-либо программы. Блокировка загрузки в BIOS, запрашивает пароль сразу после включения питания компьютера, а это безусловный плюс – отсутствует возможность доступа к настройкам для изменения приоритета загрузки. Ко-

нечно, такая защита легко снимается, хотя для этого нужно получить доступ к материнской плате. Способы обхода защиты BIOS описаны в § 2 седьмой главы.

Системное программное обеспечение (операционная система) является важнейшим компонентом любой компьютерной системы. Реализация политики безопасности в каждой конкретной операционной системе во многом обеспечивает комплексную безопасность всей системы.

Операционная система – это специально организованная совокупность программ, которая управляет ресурсами системы (ЭВМ, вычислительной системы, других компонентов ИВС) с целью наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами. Операционные системы, подобно аппаратуре ЭВМ, на пути своего развития прошли несколько поколений. ОС первого поколения были направлены на ускорение и упрощение перехода с одной задачи пользователя на другую задачу (другого пользователя), что поставило проблему обеспечения безопасности данных, принадлежащих разным задачам.

Под механизмами защиты ОС будем понимать все средства и механизмы защиты данных, функционирующие в составе операционной системы. Операционные системы, в составе которых эти средства есть, часто называют защищенными системами.

Основными способами защиты от несанкционированного доступа к информации являются аутентификация, авторизация (определение прав доступа субъекта к объекту с конфиденциальной информацией) и шифрование информации.

Кратко остановимся на основных механизмах защиты, встроенных в современные универсальные ОС. Сделаем это применительно к возможности реализации принятой нами для рассмотрения концепции защиты конфиденциальной информации.

Основные защитные механизмы ОС семейства Unix в общем случае базируются на следующем: идентификация и аутентификация пользователя при входе в систему; разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа; аудит, т. е. регистрация событий.

В отличие от семейства ОС Unix, где все задачи разграничительной политики доступа к ресурсам решаются средствами управления доступом к объектам файловой системы, доступ ОС Windows разграничивается собственным механизмом для каждого ресурса. Другими словами, при рассмотрении механизмов защиты ОС Windows встает задача определения и задания требований к полноте разграничений (это определяется тем, что считать объектом доступа).

Также, как и для семейства ОС Unix, здесь основными механизмами защиты являются: идентификация и аутентификация пользователя при входе в систему; разграничение прав доступа к ресурсам, в основе которого лежит реализация дискреционной модели доступа (отдельно к объектам файловой системы, к устройствам, к реестру ОС, к принтерам и др.); аудит, т. е. регистрация событий.

*Аутентификация* (англ. authentication – реальный, подлинный) – это процедура проверки подлинности (легальности) пользователя, т. е. мы должны удостовериться, что пользователь, пытающийся получить доступ к системе именно тот, за кого себя выдает.

*Авторизация* (англ. authorization – разрешение, уполномочивание) – это процесс проверки (подтверждения) прав доступа к какому-либо объекту. Процесс авторизации может быть применен только к аутентифицированному пользователю. Перед тем, как проверить право доступа, необходимо выяснить личность объекта, которому мы собираемся предоставить право пользователя.

Для аутентификации в компьютерных системах традиционно используется сочетания имени пользователя и некой секретной фразы (пароля), позволяющей определить, что пользователь именно тот, за кого себя выдает. Существуют также и иные способы аутентификации, например по токену, но в данной главе рассматривается парольная аутентификации. Рассмотрим механизм парольной аутентификации, реализованный в операционных системах семейства Windows [64].

Прежде всего начнем с локальной аутентификации, когда пользователь хочет войти непосредственно на рабочую станцию, не входящую в домен. Сразу после того, как пользователь ввел свой логин и пароль, они передаются подсистеме локальной безопасности Local Security Authority (LSA) (рис. 7.1), которая сразу преобразует пароль в хеш.

*Хеширование* – это одностороннее криптографическое преобразование, делающее восстановление исходной последовательности невозможным. В открытом виде пароль нигде в системе не хранится и не фигурирует (пароль знает только пользователь).

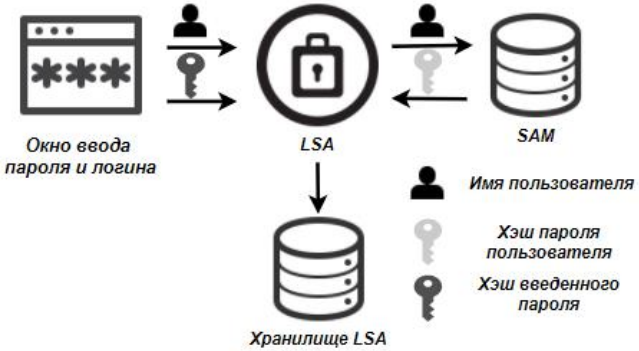


Рис. 7.1. Ввод и передача пароля пользователя в LSA

Затем служба LSA обращается к диспетчеру учетных записей безопасности Security Accounts Manager (далее – SAM) и сообщает

ему имя пользователя. Диспетчер обращается в базу SAM и извлекает оттуда хеш пароля указанного пользователя, сгенерированный при создании учетной записи (или в процессе смены пароля). Служба LSA сравнивает хеш введенного пароля и хеш из базы SAM. В случае их совпадения аутентификация считается успешной, а хеш введенного пароля помещается в хранилище службы LSA и находится там до окончания сеанса пользователя.

В случае входа пользователя в домен. Для аутентификации используются иные механизмы, прежде всего протокол Kerberos, однако, если одна из сторон не может его использовать, по согласованию могут быть использованы протоколы NTLM и даже устаревший LM.

Протокол *LAN Manager (LM)* был основан в 90-х гг. XX в. под разработкой Windows и впервые был представлен в Windows 3.11 для рабочих групп, откуда перекочевал в семейство Windows 9x. Мы не будем рассматривать этот протокол, так как он уже давно не встречается, однако его поддержка, в целях совместимости, присутствует до сих пор. И если современной системе поступит запрос на аутентификацию по протоколу LM, то, при наличии соответствующих разрешений, он будет обработан. Разберемся, каким образом создается хеш пароля для работы с протоколом LM, не вдаваясь в подробности обратим ваше внимание на основные ограничения. Пароль регистронезависимый и приводится к верхнему регистру. Длина пароля составляет 14 символов, а более короткие пароли дополняются при создании хеша нулями. Пароль делится пополам и для каждой части создается свой хеш по алгоритму DES.

Исходя из современных требований к безопасности можно сказать, что LM-хеш практически не защищен и будучи перехвачен очень быстро расшифровывается. Сразу оговоримся, прямое

восстановление хеша невозможно, однако в силу простоты алгоритма шифрования возможен подбор соответствующей паролю комбинации за предельно короткое время.

В целях совместимости LM-хеш создается при вводе пароля и хранится во многих система Windows. Это делает возможной атаку, когда системе целенаправленно присылают LM-запрос и она его обрабатывает. Избежать создания LM-хеша можно изменив политику безопасности или используя пароли длиннее 14 символов. В системах, начиная с Windows Vista и Server 2008, LM-хеш по умолчанию не создается.

*NT LAN Manager (NTLM)*. Новый протокол аутентификации появился в Windows NT и действует на сегодняшний день, а до появления Kerberos в Windows 2000 – был единственным протоколом аутентификации в домене NT.

Сегодня протокол NTLM, точнее его более современная версия NTLMv2, применяется для аутентификации компьютеров рабочих групп. В доменных сетях Active Directory по умолчанию применяется Kerberos, однако если одна из сторон не может применить этот протокол, то по согласованию могут быть использованы NTLMv2, NTLM и даже LM.

Принцип работы NTLM имеет много общего с LM (эти протоколы обратно совместимы), но есть и существенные отличия. NT-хеш формируется на основе пароля длиной до 128 символов по алгоритму MD4, пароль регистрозависимый и может содержать не только ACSII символы, но и Unicode, что существенно повышает его стойкость по сравнению с LM. Работа по протоколу NTLM реализуется по схеме (рис. 7.2) [51].

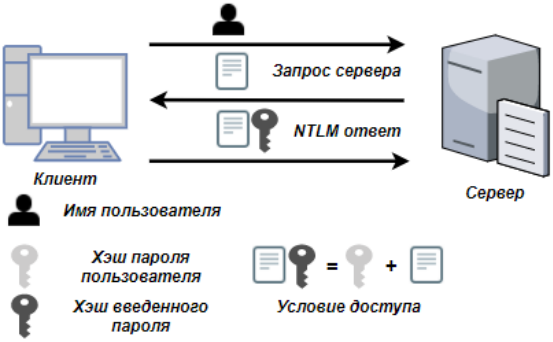


Рис. 7.2. Принцип работы по протоколу NTLM

Допустим, локальный компьютер хочет получить доступ к некоторому файловому ресурсу на другом ПК, который мы будем считать сервером, при этом совсем не обязательно наличие на этом ПК северной ОС или серверных ролей. С точки зрения протокола NTLM клиент – это тот, кто обращается, сервер – к кому обращаются.

Чтобы получить доступ к ресурсу, клиент направляет серверу запрос с именем пользователя. В ответ сервер передает ему случайное число, называемое запросом сервера. Клиент, в свою очередь, шифрует данный запрос по алгоритму DES, используя в качестве ключа NT-хеш пароля, однако несмотря на то, что NT-хеш 128-битный, в силу технических ограничений используется 40- или 56-битный ключ (хеш делится на три части и каждая часть шифрует запрос сервера отдельно).

Зашифрованный хешем пароля запрос сервера называется ответом NTLM и передается обратно серверу (по протоколу SMB), сервер извлекает из хранилища SAM хеш пароля того пользователя, чье имя было ему передано, и выполняет аналогичные действия с запросом сервера, после чего сравнивает по-

лученный результат с ответом NTLM. Если результаты совпадают, значит пользователь клиента действительно тот, за кого себя выдает, и аутентификация считается успешной.

В случае доменной аутентификации процесс протекает несколько иначе. В отличие от локальных пользователей, хеши паролей, которые содержатся в локальных базах SAM, хеши паролей доменных пользователей хранятся на контроллерах доменов. При входе в систему LSA отправляет доступному контроллеру домена запрос с указанием имени пользователя и имени домена, дальнейший процесс происходит, как показано выше.

В случае получения доступа к третьим ресурсам схема немного изменяется (рис. 7.3). Получив запрос от клиента, сервер точно также направит ему запрос сервера, но получив NTLM-ответ, он не сможет вычислить значение для проверки на своей стороне, так как не располагает хешем пароля доменного пользователя, поэтому он перенаправляет NTLM-ответ контроллеру домена и отправляет ему свой запрос сервера. Получив эти данные, контроллер домена извлекает хеш указанного пользователя и вычисляет на основе запроса сервера проверочную комбинацию, которую сравнивает с полученным NTLM-ответом, при совпадении серверу посылается сообщение, что аутентификация прошла успешно [64].

Как видим, хеш пароля ни при каких обстоятельствах по сети не передается. Хеш введенного пароля хранит служба LSA, хеши паролей пользователей хранятся либо в локальных хранилищах SAM, либо в хранилищах контроллера домена.

Но, несмотря на это, протокол NTLM не может считаться защищенным. Слабое шифрование делает возможным достаточно быстро восстановить хеш пароля, а если использовался не только NTLM, но и LM-ответ, то и восстановить пароль.

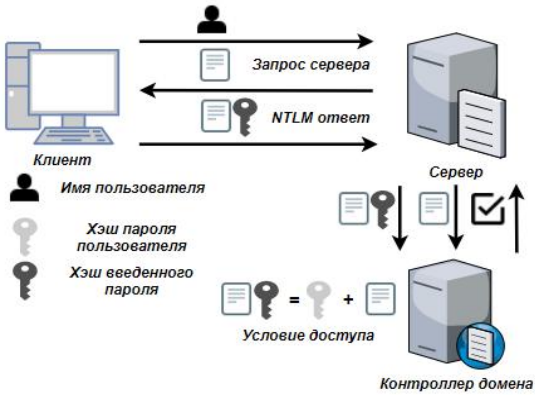


Рис. 7.3. Принцип доменной аутентификации

Однако перехваченного хеша может оказаться вполне достаточно, так как NTLM-ответ генерируется на базе пароля пользователя и подлинность клиента сервером никак не проверяется, то возможно использование перехваченных данных для неавторизованного доступа к ресурсам сети. Отсутствие взаимной проверки подлинности также позволяет использовать атаку, когда атакующий представляется клиенту сервером и наоборот, устанавливая при этом два канала и перехватывая передаваемые данные.

Осознавая, что протокол NTLM не соответствует современным требованиям безопасности, с выходом Windows 2000 Microsoft представила вторую версию протокола NTLMv2, который был серьезно доработан в плане улучшений криптографической стойкости и противодействия распространенным типам атак. Начиная с Windows 7 Server 2008 R2, использование протоколов NTLM и LM по умолчанию выключено.

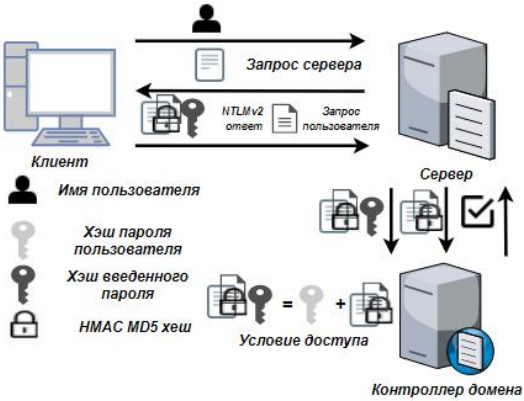


Рис. 7.4. Схема с контроллером домена по протоколу NTLMv2

Рассмотрим схему с контроллером домена (рис. 7.4). В случае его отсутствия схема взаимодействия не меняется, только вычисления, производимые контроллером домена, выполняются непосредственно на сервере [64].

Как и в NTLM, клиент при обращении к серверу сообщает ему имя пользователя и имя домена, в ответ сервер передает ему случайное число – запрос сервера. Клиент, в свою очередь, также генерирует случайное число, куда, кроме прочего, добавляется метка времени, которое называется запрос клиента. Наличие метки времени позволяет избежать ситуации, когда атакующий первоначально накапливает перехваченные данные, а потом с их помощью осуществляет атаку.

Запрос сервера объединяется с запросом клиента и от этой последовательности вычисляется хеш HMAC-MD5. После чего от данного хеша берется еще один хеш HMAC-MD5, ключом в котором выступает NT-хеш пароля пользователя. Получившийся результат называется NTLMv2-ответом и вместе с запросом клиента пересылается серверу.

Криптостойкость данного алгоритма является актуальной и сегодня, известно только два случая взлома, данного хеша.

Один из них произведен компанией Symantec в исследовательских целях. Можно с уверенностью сказать, что в настоящий момент нет массовых инструментов для атак на NTLMv2, в отличие от NTLM, взломать который достаточно легко.

Сервер, получив NTLMv2-ответ и запрос клиента, объединяет последний с запросом сервера и также вычисляет HMAC-MD5, затем передает его вместе с ответом контроллеру домена. Тот извлекает из хранилища сохраненный хеш пароля пользователя и производит вычисления над HMAC-MD5 хешем запросов сервера и клиента, сравнивая получившийся результат с переданным ему NTLMv2-ответом. В случае совпадения серверу получает сообщение об успешной аутентификации.

При этом, как вы могли заметить, NTLMv2, как и его предшественник, не осуществляет взаимную проверку подлинности, хотя в некоторых материалах в сети это указывается.

Подводя итог, выделим два рубежа защиты: BIOS и операционная система. Оба подразумевают парольную аутентификацию. Пароль можно получить у пользователя (социальная инженерия) или при непосредственном доступе к системе. Возможности социальной инженерии будут рассмотрены в отдельной главе. При доступе к компьютерной сети путем анализа сетевого трафика можно перехватить протоколы (SMB), содержащие хеш паролей. В случае физического доступа пароль компьютерной системы можно получить на этапе ввода, но для этого необходимо внедрение клавиатурного шпиона (кейлоггера). Другой вариант – это извлечение хеша пароля из служебного файла. Хешированные пароли можно попытаться восстановить. Сегодня существует способы полного перебора по словарям и радужным таблицам, но обо всем по порядку.

## § 2. Способы обхода механизмов защиты BIOS

Несмотря на то, что BIOS отличное средство защиты, существуют способы обхода пароля, установленного в ней. Пароль BIOS (также, как и иные основные настройки системы) хранится в памяти CMOS[1] (КМОП), которая требует питания от элемента, установленного на материнской плате (рис. 7.5). Отсюда и следует один из простых способов обхода пароля, точнее его сброса вместе со всеми настройками, хранящимися в BIOS.

CMOS требует постоянного питания для сохранения данных, поэтому, убрав элемент питания на некоторое время (примерно на 24 ч), мы добьемся очистки BIOS. После необходимо снова вставить батарейку на нужное место, и задать необходимые параметры при запуске и загрузить операционную систему.


Рис. 7.5. Элемент питания CMOS

Способ эффективный, но долгий, к тому же элемент питания на некоторых моделях материнских плат крайне сложно извлечь без использования дополнительных инструментов, поэтому

[1] CMOS (англ. complementary metal-oxide-semiconductor) – комплементарная структура металл-оксид-полупроводник) – набор полупроводниковых технологий построения интегральных микросхем и соответствующая ей схемотехника микросхем. Подавляющее большинство современных цифровых микросхем – КМОП.

стоит прибегнуть к способу сброса с использованием специальной перемычки или кнопки на материнской плате (рис. 7.6), описанному в инструкции по применению.


Рис. 7.6. Перемычка для сброса CLR CMOS

На многих материнских платах существуют специальные разъемы для очистки памяти CMOS, которые обычно расположены в непосредственной близости от батарейки (узнать местоположение такого разъема можно из схемы материнской платы, приведенной в инструкции к ней или на сайте компании-изготовителя). Для очистки памяти CMOS необходимо замкнуть эти разъемы, после чего включить компьютер и заново выставить настройки BIOS.

Попадаются редкие ситуации, когда нет возможности использовать способы, описанные выше, но есть еще один вариант. Он заключается во вводе вместо неизвестного пароля BIOS инженерного пароля для данной системной платы. Перед тем как вводить аварийный пароль, необходимо выяснить производителя BIOS, поскольку у каждого производителя они, как правило, разные. Определить производителя можно различными способами, самый простой – посмотреть на экран в момент загрузки. Вверху обычно указан производитель и версия. Чтобы

успеть зафиксировать этот момент, нажмите на клавиатуре клавишу Pause. Если вместо необходимой информации вы видите лишь заставку производителя материнской платы, нажмите Tab.

Существует немало программного обеспечения как платного, так и свободно распространяемого для дешифрации забытого пароля, хранящегося в энергонезависимой памяти CMOS. Но, к сожалению, универсальных «взломщиков» паролей не существует. Даже профессиональные версии, как правило, ориентированы на определенный набор поддерживаемого оборудования. Из свободно распространяемого ПО неплохими возможностями обладает CmosPwd. Возможна дешифрация паролей следующих производителей: ACER/IBM BIOS; AMI BIOS; AMI WinBIOS 2.5; Award 4.5x/4.6x/6.0; Compaq (1992); Compaq (New version) IBM (PS/2, Activa, Thinkpad); Packard Bell; Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107; Phoenix 4 release 6 (User); Gateway Solo – Phoenix 4.0 release 6; Toshiba; Zenith AMI.

## § 3. Способы обхода парольной аутентификации

В настоящее время в операционных системах защита паролем является основной базовой системой защиты. Доступ к данным в этом случае возможен только при знании оригинального пароля, обычно это слово или фраза. Так, программа или система при попытке доступа к защищенным данным запрашивает текстовый пароль. Этот пароль проверяется с оригинальным значением и, если эти значения совпадают, система разрешает доступ к защищенным ресурсам, в противном случае отклоняет его. Основной недостаток парольной защиты состоит в том, что программе или системе необходимо где-то хранить оригинальный пароль, чтобы

впоследствии была возможность сравнивать его с вводимыми значениями.

Для хранения паролей всех пользователей и управления ими используется система Security Accounts Manager (SAM). Информация там хранится не в явном виде (хеш), поэтому, для того чтобы узнать пароль, придется затратить много времени и ресурсов, особенно если он достаточно сложный. Есть случаи, когда достаточно сбросить или поменять пароль. Также можно отключить службы, которые ответственны за проведение аутентификации. В качестве способов преодоления парольной аутентификации операционной системы можно выделить следующие: обход приглашения на ввод пароля; сброс пароля; получение дампа хешированных паролей для последующей атаки полным перебором. Для указанных случаев разработано немало утилит, часто объединяющих в себе несколько способов.

1. *Обход приглашения на ввод пароля.* Осуществляется за счет изменения содержимого или остановки ядра ответственного за парольную аутентификацию и позволяет войти в защищенную паролем учетную запись без ввода пароля. Пароль при этом не изменяется и не сбрасывается. В качестве примера можно указать на BootRoot и Kon-Boot.

С помощью технологии BootRoot можно в стандартном загрузочном секторе выполнить код, который во время загрузки остановит ядро Windows. eEye BootRootKit – это NDIS «бэкдор», который работает по типу boot-вируса и демонстрирует использование технологии BootRoot.

Kon-Boot – прототип программы, благодаря которой во время загрузки можно менять содержимое ядра Linux или Windows. Kon-Boot позволяет войти в систему Linux с правами root без ввода пароля или повысить привилегии текущего пользователя. В случае с системами Windows с помощью Kon-Boot

можно войти в любой защищенный паролем профиль без знания самого пароля.

2. *Сброс пароля.* Для сброса пароля используют внешний носитель информации (CD-диск или USB-диск), на который предварительно загружают специальную утилиту. Большинство операционных систем Windows хранят пароли в зашифрованном виде в файле SAM. Этот файл является частью реестра Windows и остается недоступным до тех пор, пока операционная система является активной. Большинство утилит позволяют редактировать или заменять ветку реестра, отвечающую за аутентификацию.

Для сброса пароля учетной записи пользователя в операционной системе Windows можно воспользоваться утилитой Offline NT Password and Registry Editor. Программа протестирована на следующих версиях: NT 3.51, NT 4, Windows 2000, Windows XP, Windows 2003 Server, Vista, Windows 7 и Server 2008.

Reset Windows Password является самым мощным программным инструментом для восстановления или сброса паролей учетных записей Windows: пользователей, администратора, пользователей Active Directory, администратора домена. Программа максимально ориентирована на неподготовленного пользователя и легка в работе.

Password Renew сбросит или установит новый пароль для любого локального пользователя, создаст новую учетную запись с правами администратора или даст root-права существующему.

3. *Получение дампа хешированных паролей.* Доступ к хешированным паролям дает возможность к различным атакам. При получении физического доступа к системе лучше всего извлечь дамп хешированных паролей. Пароли в хешированном виде могут хранится в одном из следующих мест:

– в локальной SAM-базе, где хранятся LM/NTLM-хеши локальных пользователей;

– в кэше LSA, в который попадают LM/NTLM-хеши доменных пользователей, стираемые после перезагрузки;

– в специальном кэше, где сохраняются MSCache-хеши паролей десяти последних пользователей, которые авторизовались на данном хосте (пароли кэшируются, чтобы можно было войти в систему, если связь с доменом временно отсутствует).

Если используется контроллер домена, есть еще Active Directory. Из каждого из указанных мест можно извлечь дамп паролей. Большинство приведенных ниже способов давно известны, и их можно использовать при необходимости.

*Привилегия SeDebugPrivilege.* Начнем с ситуации, когда у нас есть физический доступ к интересующей нас системе. В этом случае NTLM/LM-хеши можно получить с помощью специальных утилит. В большинстве своем эти инструменты требуют высоких привилегий, так как они необходимы для работы с динамически подключаемыми библиотеками (*.dll) с помощью SeDebugPrivilege. Будем считать, что у нас есть аккаунт с правами администратора.

Самыми известными утилитами для создания дампа хешей являются pwdump и fgdump. Работать с ними достаточно просто, да и по функциям они очень похожи.

Pwdump выводит найденные хеши непосредственно в консоль. Вторая же сохраняет результат в файлах 127.0.0.1 PWDUMP (хеши паролей локальных пользователей) и 127.0.0.1 CACHEDUMP (закэшированные хеши паролей доменных пользователей).

Одна из наиболее интересных опций, которую поддерживают обе утилиты, позволяет получать хеши с удаленных машин. Чтобы выполнить этот прием с помощью pwdump, необходимо выполнить команду:

```
> pwdump -o mytarget.log -u MYDOMAIN\someuser -p \
'lamepassword' 10.1.1.1
```

Здесь 10.1.1.1 – адрес удаленной машины, MYDOMAIN\someuser – аккаунт пользователя, lamepassword – пароль пользователя, а mytarget.log – файл для сохранения результатов. В отличие от pwdump, fgdump умеет получать хеши не только с одной машины, а сразу с нескольких:

```
> fgdump.exe -f hostfile.txt -u MYDOMAIN\someuser -T 10
```

В данном случае hostfile.txt – файл, содержащий список хостов, а «-T 10» – количество параллельно работающих потоков. На полученный хеш можно провести атаку брутфорс с помощью специальных утилит. Примечательно, что некоторые из них для большего удобства поддерживают формат вывода fgdump.exe.

*Дамп паролей с помощью теневого копирования томов (Volume Shadow Copy Service).* Как мы уже знаем, хеши паролей локальных пользователей хранятся, в том числе и в файле SAM, правда, в зашифрованном виде. Поэтому, чтобы прочитать их, требуется еще один файл – SYSTEM. Эти два файла представляют собой системные ветви реестра, которые ОС постоянно использует, поэтому доступ к ним невозможен даже администратору. Из-за этого многим приложениям, которые извлекают хеши паролей, приходится идти на ухищрения, чтобы получить доступ к этим ветвям. Мы же, чтобы скопировать эти файлы, воспользуемся легальным механизмом, который предоставляет сама ОС.

Этот механизм, позволяющий делать «мгновенный снимок» тома, называется Volume Shadow Copy Service (теневое копирование тома). Он появился в ОС Windows начиная с версий XP и Server 2003. Эта технология автоматически используется, например, при создании архива System State с помощью утилиты ntbackup или при создании снимка для общей папки (Volume

Shadow Copy for Shared Folders). Суть идеи состоит в том, что при теневом копировании будут созданы копии важных системных файлов (в частности, SAM и SYSTEM), доступ к которым мы сможем легко получить. Чтобы избавиться от лишних команд в консоли, можно воспользоваться небольшой утилитой vssown.vbs, управляющей созданием копий. Для начала запускаем сервис теневого копирования: cscript vssown.vbs/start. Затем создаем новую теневую копию: cscript vssown.vbs/create. Теперь смотрим список всех теневых копий: cscript vssown.vbs/list.

Созданная нами копия будет самой последней. Из всей информации нас интересует Device object со значением «\?\GLOBALROOT\Device\Harddisk VolumeShadowCopy14» (14-й номер теневой копии). Дальнейшие манипуляции предельно просты. Копируем интересующие нас файлы:

```
copy\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy14\
windows\systen32\config\SYSTEM
copy\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy14\
windows\systen32\config\SAM
```

После этого эти файлы можно попытаться восстановить, например, в утилите типа SAMInside для расшифровки полученных хешей.

Используя предыдущий прием, можно легко получить хеши паролей не только локальных, но и вообще всех доменных пользователей. Правда, только если у нас есть доступ к контроллеру домена. Предположим, мы создали теневую копию и скопировали файлы SAM и SYSTEM.

Active Directory хранит данные о пользователях в файле NTDS.DIT, так что нужно скопировать и его:

```
copy\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy14\
windows\ntds\ntds.dit
```

Данные о пользователях хранятся в зашифрованном виде, поэтому их нужно будет расшифровывать с помощью файла SYSTEM. У нас есть файлы SYSTEM и NTDS.DIT, но как нам получить список пользователей и их хешей? Для дальнейших манипуляций подойдет любой другой Linux-дистрибутив, хотя все то же самое можно осуществить из Windows. Загружаемся, скачиваем архив и распаковываем его. Далее собираем библиотеку libesedb:

```
cd libesedb
chmod +x configure
./configure && make
```

Теперь можно приступать к дампу хешей. Прежде всего извлекаем таблицу, содержащую зашифрованные данные:

```
cd esedbtoolls
.\esedbdumphash ../ ../ntds.dit
```

У нас появился файл /libesedb/esedbtools/ntds.dit.export/-datatable. Теперь его надо расшифровать при помощи ключа, который содержится в SYSTEM:

```
cd ../ ../creddump/
python ./dsdump.py ../SYSTEM
../libesedb/esedbtool/ntds.dit.export/datatable
```

На выходе получаем хеши всех пользователей домена. Интересно, что можно извлечь еще и предыдущие пароли пользователей (их хеши). Для этого в инструментарии имеется отдельная утилита, которую легко задействовать:

```
python ./dsdumphistory.py ../system
../libesedb/esedbtools/ntds.dit.export/datatable.
```

Если их удастся взломать, вполне можно проследить закономерность, в соответствии с которой пользователь меняет свои пароли (очень часто она существует).

Если есть физический доступ к компьютеру, то можно не только загрузить с внешнего носителя утилиту, которая автоматически монтирует все разделы, которые может найти, и извлекает логины и хеши паролей из файлов SAM и SYSTEM. Например, BootPass – загрузочный диск, на диске размещены полнофункциональные программы для сброса и редактирования паролей Windows и BIOS. Диск содержит следующие программы:

– Kon-Boot – прикладная программа, которая изменяет содержимое ядра Windows во время загрузки, обходя систему авторизации Windows и позволяя войти в защищенную паролем учетную запись без ввода пароля;

– Active@ Password Changer – программа, которая позволяет сбросить пароль администратора операционной системы Windows;

– Windows Password Killer – профессиональный инструмент для сброса забытого пароля Windows;

– Password Reset – программа позволяющая разблокировать учетную запись Windows;

– CIA Commander – используется для восстановления пароля Windows;

– Paragon Password Cleaner – позволяет обнулять пароли для любых пользователей в системе Windows;

– Windows Key Enterprise – представляет собой простой в использовании инструмент для получения доступа в любую систему Windows. Программа позволяет сбросить пароль любого пользователя без необходимости переустановки операционной системы;

– Volkov NTFSdos – позволяет сбросить пароли пользователей, редактировать реестр, получить доступ к файлам и папкам на жестком диске NTFS/FAT32;

– Reset Windows Password – лучшая профессиональная программа для сброса, изменения или восстановления паролей всех типов учетных записей Windows;

– Elcomsoft System Recovery – мгновенно сбрасывает пароли к учетным записям, в то же время включая ряд атак, с помощью которых в ряде случаев за короткое время могут быть найдены оригинальные пароли;

– Proactive Password Auditor – помогает администраторам проверить безопасность локальных вычислительных сетей, выполняя аудит пользовательских паролей;

– SAMInside – профессиональная программа для восстановления паролей пользователей Windows;

– Password Renew – сбрасывает или устанавливает новый пароль для любого локального пользователя, создает новую учетную запись с правами администратора или дает права рута существующему;

– NTPWEdit – это программа для редактирования паролей в системах семейства Windows;

– UserManager – предполагает редактирование свойств учетных записей, сброс паролей;

– WindowsGate – позволяет обойти проверку пароля учетной записи на гостевой системе.

После получения дампа хешированных паролей необходимо их восстановить. Специальные криптографические алгоритмы свертки паролей, которые работают только в одну сторону, – это функции одностороннего преобразования (хеш-функции). То есть можно получить хеш от пароля, но пароль из хеша не получится. При создании учетной записи, пользователь вводит начальный пароль, который, однако, не хранится в открытом виде, а хешируется с помощью однонаправленной функции. Получаемый

хеш пароля сохраняется в системе. В дальнейшем, при попытке входа, система запрашивает у пользователя пароль, также хеширует его и полученный хеш сравнивает с оригинальным хешем, сохраненным ранее. Если эти значения совпадают, то пароль, естественно, тоже. Более подробно было описано выше. Таким образом, оригинальный текстовый пароль не хранится в системе.

В области информационной безопасности и тестах на проникновения, нередко возникает задача, когда нужно взломать пароль. Это может быть хеш пароля администратора системы Windows, пароль к беспроводной точке доступа или любой другой хеш, который вам удалось добыть. В этих случаях для взлома хеша и получения пароля используется техника *хешкракинга* (англ. hash cracking).

Восстановление паролей к хешам – сложный и трудоемкий процесс, для которого требуются хорошие знания в разных областях – криптографии, комбинаторике и программировании. Один из самых популярных методов, с помощью которого осуществляется восстановление пароля по его хешу, – это брутфорс (bruteforce).

*Брутфорс* – атака на компьютерную систему через подбор паролей путем перебора всех возможных комбинаций символов до нахождения комбинации, подходящей в качестве пароля. Такие атаки являются одним из самых эффективных способов преодоления парольной аутентификации компьютерных систем.

Атака брутфорс подразумевает последовательный подбор разных символов до момента, когда не будет выбрана необходимая комбинация. Скорость подбора зависит от производительности компьютера и сложности пароля. Можно выделить следующие основные типы атак брутфорс:

1. *Предварительная атака* – это быстрая проверка хешей пользователей на простые пароли типа «123», «qwerty», «99999» и др.

2. *Атака полным перебором* – это полный перебор всех возможных паролей в каком-либо диапазоне, например, «аааааа», «zzzzzz» и т. д.

3. *Атака по маске* – эта атака используется, если известна какая-либо информация о пароле.

4. *Простая атака по словарям*, в этой атаке происходит простая проверка хешей на пароли из словарей.

5. *Комбинированная атака по словарям*, в этой атаке пароли формируются из нескольких слов, взятых из разных словарей, что позволяет восстанавливать сложные пароли вида «superadmin», «admin*admin» и др.

6. *Гибридная атака по словарям* – атака позволяет изменять пароли из словарей (к примеру, перевести пароль в верхний регистр, добавить в конце пароля символ и т. д.) и проверять их в качестве паролей пользователей.

7. *Атака по Rainbow-таблицам (радужным таблицам)* – атака использует поиск пароля по предварительно рассчитанным Rainbow-таблицам.

Современные видеокарты, поддерживающие технологию CUDA, AMD OpenCL, позволяют перебирать все возможные комбинации шестизначных паролей меньше, чем за минуту, а семизначные – не больше, чем за шесть минут. Используя технологии типа CrossFire и Stream, можно и вовсе объединять видеокарты в один массив для более эффективного перебора. Скорость перебора значения при этом может быть рассчитана по формуле:

$$t = ((W)/N1 + N2 + N3 + \ldots + Nn)/2,$$

где среднее время (t) перебора (W) на N-м количестве видеокарт.

Перебор по радужным таблицам – это тот же перебор, только с использованием заранее сгенерированных специальным образом таблиц. Его очень эффективно применять против длинных паролей. Скорость перебора ограничивается лишь скоростью процессора и быстродействием памяти. Принцип действия простых радужных таблиц состоит в задании диапазона символов (например, a … z) и максимальной длины пароля. Затем просчитываются все возможные варианты и создаются миллионы цепочек. Каждая цепочка вычисляется по следующей формуле:

P0 -> hash(P0) -> H1 -> R(H1) ->
P1 -> hash(P1) -> H2 -> R(H2) ->
P2 ...,

где P – пароль, hash – функция хеширования, R – функция редукции.

Таким образом, из первоначального пароля с помощью функции хеширования получается хеш, из которого на выходе функции редукции получается следующий пароль и процесс повторяется сначала, что ведет к созданию цепочек. В каждой такой цепочке сохраняется только первоначальное и конечное значение. Хранение только первого и последнего элементов является операцией, ведущей к компромиссу, сохраняя при этом память за счет временных затрат на криптоанализ.

Для восстановления искомого пароля он подвергается хешированию и функции редукции, а затем ищется в таблице. Для этого создается цепочка ключей, начиная с R(Hn) до максимальной длины цепочки. Если Hn окажется полученным с помощью пароля, использованного при создании таблицы, то мы в итоге получим ключ, соответствующий последнему ключу соответствующей цепочки. Этот последний ключ был сохранен в таблице вместе с первым ключом цепочки. Используя первый ключ

цепочки, можно восстановить всю цепочку и значение, стоящее перед R(Hn). Это и есть тот ключ, который использовался для генерации Hn, т. е. наш искомый пароль.

## § 4. Клавиатурные шпионы

Один из наиболее распространенных способов получения (перехвата) пароля – это использование программных или аппаратных закладок. Такие программные закладки также нацелены на определение легальных полномочий пользователей и их прав доступа к компьютерным ресурсам.

Программа или устройство для скрытной записи информации о нажимаемых пользователем клавишах принято называть клавиатурным шпионом. У этого термина есть ряд синонимов: кейлоггер – keylogger, keyboard logger, spyware; реже встречается снупер – snooper, snoop (совать нос в чужие дела).

Как правило, современные клавиатурные шпионы не просто записывают коды вводимых клавиш, но и «привязывают» клавиатурный ввод к текущему окну и элементу ввода (например, интернет-браузеру). Кроме того, многие клавиатурные шпионы отслеживают список запущенных приложений, умеют делать снимки экрана по заданному расписанию или событию, шпионить за содержимым буфера обмена и решать ряд задач, нацеленных на скрытое слежение за пользователем. Записываемая информация сохраняется на диске и большинство современных клавиатурных шпионов могут формировать различные отчеты, передавать их по электронной почте или сети. Кроме того, ряд современных клавиатурных шпионов пользуются RootKit-технологиями для маскировки следов своего присутствия в системе. RootKit – программа или набор программ, который позволяет скрыть присутствие в системе вредоносного ПО.

Клавиатурные шпионы по общим принципам работы можно разделить на три группы:

1. *Имитаторы.* В операционную систему внедряется программа, имитирующая ввод пароля для входа в систему. Программа (далее – имитатор) переходит в режим ожидания ввода пользовательского пароля. Как только пользователь идентифицирует себя и введет свой пароль, имитатор сохраняет эти данные. После чего происходит выход из системы, и в результате пользователь видит настоящее окно для входа в систему. Он вновь вводит пароль, полагая, что допустил ошибку при предыдущем вводе.

2. *Фильтры.* Перехватывают все данные с клавиатуры компьютера. Кейлоггер просто сохраняет нажатие клавиш в файле на жестком диске или передает по сети. Программные шпионы более сложной реализации фильтруют информацию, выделяя пароли и логины.

3. *Заместители.* Подменяют библиотеки ядра операционной системы, отвечающие за парольную аутентификацию. Клавиатурные шпионы такой реализации могут быть созданы практически для любой многопользовательской платформы.

Для понимания принципов работы клавиатурных шпионов рассмотрим их алгоритмы при использовании в операционной системе Windows. Модель аппаратного ввода операционной системы – это основа для создания и внедрения клавиатурного шпиона программной реализации (рис. 7.7).

При возникновении неких событии ввода (нажатии клавиш, перемещении мыши) события обрабатываются соответствующим драйвером и помещается в системную очередь аппаратного ввода.

В системе имеется особый поток необработанного ввода, называемый Raw Input Thread (RIT), который извлекает события из системной очереди и преобразует их в сообщения. Полученные

сообщения помещаются в конец очереди виртуального ввода одного из потоков (виртуальная очередь потока называется Virtualized Input Queue – VIQ). При этом RIT сам выясняет, в очередь какого конкретно потока необходимо поместить событие. Для событий мыши поток определяется поиском окна, над которым расположен курсор мыши. Клавиатурные события отправляются только по активному потоку, т. е. потоку, которому принадлежит окно, где работает пользователь. На самом деле это не совсем так: на рис. 7.7 показан поток A, не имеющий очереди виртуального ввода. В данном случае получается, что потоки A и B совместно используют одну очередь виртуального ввода. Это достигается при помощи вызова API-функции AttachThreadInput, которая позволяет одному потоку подключиться к очереди виртуального ввода другого потока [69].

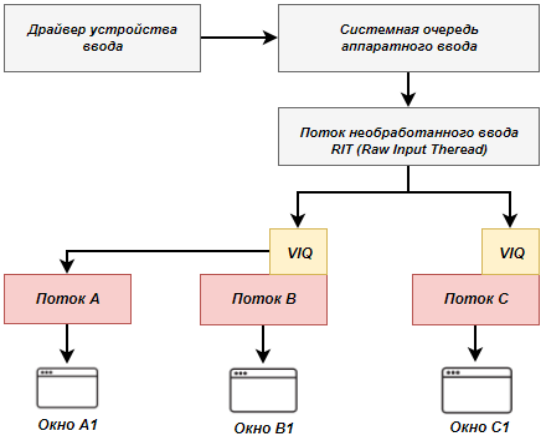


Рис. 7.7. Модель аппаратного ввода системы Windows

Следует отметить, что поток необработанного ввода отвечает за обработку специальных сочетаний клавиш, в частности Alt+Tab и Ctrl+Alt+Del.

Работа большинства клавиатурных шпионов в операционных системах Windows реализуются на следующих алгоритмах: слежение за клавиатурным вводом при помощи ловушек; слежение за клавиатурным вводом при помощи опроса клавиатуры; слежение за клавиатурным вводом при помощи перехвата API-функций; клавиатурный шпион на базе драйвера.

*Слежение за клавиатурным вводом при помощи ловушек*. Данная методика является классической для клавиатурных шпионов. Суть метода состоит в применении механизма ловушек (hook) операционной системы. Ловушки позволяют наблюдать за сообщениями, которые обрабатываются окнами других программ. Установка и удаление ловушек производится при помощи хорошо документированных функций API библиотеки user32.dll (функция SetWindowsHookEx позволяет установить ловушку, а UnhookWindowsHookEx – снять ее). При установке ловушки указывается тип сообщений, для которых должен вызываться обработчик ловушки. В частности, есть два специальных типа ловушки (WH_KEYBOARD и WH_MOUSE) для регистрации событий клавиатуры и мыши соответственно. Ловушка может быть установлена для заданного потока и для всех потоков системы. Ловушка для всех потоков системы очень удобна для построения клавиатурного шпиона [69].

Код обработчика событий ловушки должен быть расположен в DLL. Это требование связано с тем, что DLL с обработчиком ловушки проецируется системой в адресное пространство всех процессов GUI. Интересной особенностью является то, что проецирование DLL происходит не в момент установки ловушки, а при получении процессом GUI первого сообщения, удовлетворяющего параметрам ловушки.

*Слежение за клавиатурным вводом при помощи опроса клавиатуры.* Данный алгоритм основан на периодическом опросе

состояния клавиатуры. Для опроса состояния клавиш в системе предусмотрена специальная функция GetKeyboardState, возвращающая массив из 255 байт, в котором каждый байт содержит состояние определенной клавиши на клавиатуре. Данный метод уже не требует внедрения DLL в GUI-процессы и в результате шпион менее заметен.

Однако изменение статуса клавиш происходит в момент считывания потоком клавиатурных сообщений из его очереди, и в результате подобная методика работает только для слежения за GUI-приложениями. От этого недостатка свободна функция GetAsyncKeyState, возвращающая состояние клавиши на момент вызова функции.

Недостатком клавиатурных шпионов такого типа является необходимость периодического опроса состояния клавиатуры с достаточно высокой скоростью (не менее 10–20 опросов в секунду).

*Слежение за клавиатурным вводом при помощи перехвата API-функций.* Данная методика не получила широкого распространения, но тем не менее она может с успехом применяться для построения клавиатурных шпионов. Методики перехвата функций API реализуется с помощью RootKit. Разница между RootKit и клавиатурным шпионов в данном случае невелика: шпион будет перехватывать функции с целью мониторинга, а не с целью модификации принципов работы и результатов вызова [69].

Простейшим способом может быть перехват функций GetMessage, PeekMessage и TranslateMessage библиотеки User32, что позволит вести мониторинг всех сообщений, получаемых GUI-приложениями.

*Клавиатурный шпион на базе драйвера.* Данный метод еще более эффективен, чем описанные выше методы. Возможны как минимум два варианта реализации этого метода – написание

и установка в систему своего драйвера клавиатуры вместо штатного или установка драйвера-фильтра[1] [69].

Кроме программных клавиатурных шпионов возможны и аппаратные средства: установка устройства слежения в разрыв кабеля клавиатуры (например, устройство может быть выполнено в виде переходника PS/2); встраивание устройства слежения в клавиатуру; считывание данных путем регистрации ПЭМИН (побочных электромагнитных излучений и наводок); визуальное наблюдение за клавиатурой.

Рис. 7.8. Аппаратный кейлоггер
(клавиатурный шпион) для USB клавиатуры

Аппаратные клавиатурные шпионы используются намного реже, чем программные, например, клавиатурный шпион Nano для USB клавиатуры с 8 Мб памяти (рис. 7.8). Данное устройство предназначено для перехвата данных, вводимых с клавиатуры пользователем. Передаются абсолютно все данные – пароли, тексты, вводимые веб-адреса и т. д. Серия кейлоггеров Nano обладает всеми функциями и возможностями аппаратного USB кейлоггера, но, при подключении к системному блоку, его практически невозможно разглядеть. Кейлоггер Nano оснащен встроенной памятью в 8 Мб, которая позволяет вести непрерывную

[1] Применение драйвера-фильтра, на наш взгляд, является наиболее корректной методикой. Хороший вариант реализации описан на сайте www.wasm.ru, другой вариант можно найти в Windows DDK, пример называется kbfiltr.

запись данных на протяжении восьми месяцев и более. Для просмотра собранных данных необходимо ввести пароль, после чего устройство переключается в режим флэш-диска и чтение информации осуществляется как с обычной флэшки. В Wi-Fi версии чтение информации можно осуществлять через e-mail отчеты или с удаленного компьютера по требованию, с помощью специального ПО (входит в комплект).

Кейлоггер Nano представлен в двух вариантах: USB и USB Wi-Fi. Если Вам необходимо осуществлять простой и эффективный мониторинг USB клавиатуры, то версии USB будет вполне достаточно. Если есть беспроводная Wi-Fi сеть, куда может подключиться кейлоггер Nano, то вы можете воспользоваться преимуществом удаленного доступа и сделать выбор в пользу версии USB Wi-Fi.

Еще один вариант кейлоггера с объемом встроенной памяти 2 Гб – устанавливается внутрь клавиатуры (рис. 7.9). Работает по принципу Keylogger Flash.

Рис. 7.9. Встраиваемый аппаратный кейлоггер

На рис. 7.10 и 7.11 представлены программные клавиатурные шпионы, находящиеся в свободном доступе. В ряде случаев свободный доступ ограничивает их функционал. Если вы хотите программу, которая не будет обнаруживаться антивирусами, за нее придется заплатить. В платной версии предоставляются следующие возможности: полная скрытность на системном трее, в

прикладных программах, запись абсолютно всех нажатых клавиш; указание запущенных программ и процессов, окон, сайтов; запись чатов; самозащита от удаления; защита паролем; отсылка логов на электронную почту через прокси-сервер; самоуничтожение по времени или событию.

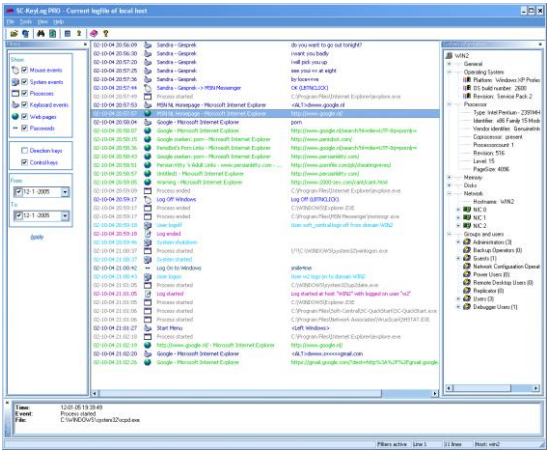

Рис. 7.10. Интерфейс клавиатурного шпиона SC-KeyLog

SC-KeyLog – кейлоггер, способный вести журнал нажатых клавиш, при этом шифруя полученные данные (рис. 7.10). Имеется возможность удаленного просмотра log-файла. SC-KeyLog, как и любая программа такого рода, позволяет фиксировать тексты любых типов электронной почты, сообщений интернет-мессенджеров, изменения в текстовых файлах, информацию, вводимую на веб-страницах, кликов мышей, названий открытых окон, времени запуска/завершения программ, времени входа/выхода пользователя, избранного браузера, набранных паролей пользователей и многое другое.

Клавиатурный шпион Elite Keylogger трудно поддается обнаружению, работая в режиме низкоуровневого драйвера. Программа хороша тем, что ее не надо предварительно запускать: она запускается вместе с системой, даже чуть раньше, что дает

возможность схватить логины и пароли при загрузке Windows. Программу невозможно удалить (нужно знать пароль администратора программы), ее невозможно найти: она не отображается в области уведомлений (tray), не выдает никаких окон и прочего, что могло бы выдать работу (рис. 7.11).

Последние методы внедрения, используемые приложениями, не требуют никакого взаимодействия с пользователем. Известны такие программы, как «скачиваемые налету»: клавиатурный шпион доставляется на компьютер пользователя без его ведома, либо при посещении определенной веб-страницы, либо при открытии заархивированных файлов, либо при нажатии на всплывающее окно, содержащее активный элемент типа ActiveX, Java Applet и т. д. Элементы клавиатурных шпионов также могут содержатся в мультимедийных файлах, а иногда даже в драйверах для нового оборудования.


Рис. 7.11. Интерфейс клавиатурного шпиона Elite Keylogger

# ГЛАВА VIII. ПОЛУЧЕНИЕ ИНФОРМАЦИИ С КОМПЬЮТЕРНОЙ СИСТЕМЫ

## § 1. Основы хранения информации в компьютерных системах

Источниками информации для компьютерной разведки являются данные, сведения и информация, обрабатываемая, передаваемая и хранимая в компьютерных системах и сетях, путем применения логических операций и приемов. В данной главе уделим внимание физическому доступу к электронному носителю информации. Для понимания принципов добывания информации разберемся с теоретическими основами ее хранения в компьютерных системах.

Устройства хранения информации в компьютере разделяются на оперативную память или оперативное запоминающееся устройство (далее – ОЗУ), необходимые для хранения промежуточных результатов вычислений, и долговременную память – нужна для хранения данных, файлов и т. д.).

ОЗУ – хранилище информации, требующее постоянного обновления, чтобы в нем содержалась разная информация, необходимая в данный момент. В оперативной памяти компьютера любая информация хранится только до выключения устройства. Если вам нужно сохранить документ и вернуться к работе над ним завтра, его нужно записать на долговременное устройство хранения, например диск. Рассмотрим самые распространенные типы дисков и устройств хранения.

*Жесткие магнитные диски или НЖМД, винчестер* – это основное хранилище информации больших объемов, основанное на принципе магнитной записи, скрыт внутри корпуса систем-

ного блока и является основным накопителем данных в большинстве компьютеров. Информация в НЖМД записывается на жесткие пластины, покрытые слоем ферромагнитного материала. Носитель информации совмещен с накопителем и обычно установлен внутри системного блока компьютера.

*Флэш-память* – это энергонезависимый тип памяти, представляет собой микросхему, помещенную в миниатюрный плоский корпус. Для считывания или записи информации карта памяти вставляется в специальные накопители, встроенные в мобильные устройства или подключаемые к компьютеру через USB-порт. Карты флэш-памяти не имеют в своем составе движущихся частей, что обеспечивает высокую сохранность данных при их использовании в мобильных устройствах (портативных компьютерах, цифровых камерах и т. д.). Их существует огромное множество: SD, MMC, CompactFlashType I и II, MemoryStick, MemoryStickDuo, TransFlash, miniSD, microSD, RS-MMC, SmartMedia, MiniDisk и др.

В большинстве современных операционных систем диски делятся на несколько независящих друг от друга частей (разделов). В ОС класса DOS/Windows эти разделы называются логическими дисками. Логическим дискам назначаются буквы, также для них можно задать метку (для наглядности), например: C: (Система) или D: (Данные). Информация о разделах диска (основная загрузочная запись) хранится в начале жесткого диска.

Сегодня активно используется и формат основной загрузочной записи Master Boot Record (MBR) и совершенно новый стандарт в виде таблицы разделов GUID (глобальный уникальный идентификатор), который сокращенно обозначается как GUID Partition Table (GPT). Новый формат является более прогрессив-

ным, поскольку поддерживает логические диски с объемом более 2 ТБ и новую систему ввода/вывода Unified Extensible Firmware Interface (UEFI) вместо привычного всем BIOS.

Если в вашей системе используется структура разделов MBR (рис. 8.1), то первый процесс выполнения загрузит BIOS. Базовая структура ввода-вывода включает в себя микропрограмму загрузчика. Микропрограмма загрузчика содержит низкоуровневые функции, такие как ввод с клавиатуры, доступ к видеодисплею, осуществление дисковых операций ввода-вывода и код для загрузки начальной стадии загрузчика. До того, как BIOS может определить загрузочное устройство, он выполняет последовательность функций системной конфигурации, начиная со следующих: самотестирование при включении питания; обнаружение и инициализация видеокарты; отображение стартового экрана BIOS; осуществление быстрой проверки памяти (RAM); конфигурация устройств plug and play; определение загрузочного устройства.


Рис. 8.1. Структура диска с MBR

Как только BIOS определил загрузочное устройство, он считывает первый дисковый сектор этого устройства в память. Первый сектор диска – это и есть главная загрузочная запись (рис. 8.2) размером 512 байт состоящая из трех объектов: первая стадия загрузчика (446 байт); таблица разделов диска (16 байт на

раздел × четыре раздела) – MBR поддерживает только четыре раздела (подробнее об этом ниже); подпись (2 байта).

На следующем этапе MBR сканирует таблицу разделов и загружает в оперативную память загрузочный сектор Volume Boot Record (VBR). VBR обычно содержит начальный загрузчик программ – Initial Program Loader (IPL), этот код инициирует процесс загрузки.

| Address | | Description | | Size in bytes |
|---|---|---|---|---|
| Hex | Dec | | | |
| 0000 | 0 | **Code Area** | | **≤ 446** |
| *01B8* | *440* | *Optional disk signature* | | *4* |
| *01BC* | *444* | *Usually null: 0x0000* | | *2* |
| 01BE | 446 | **Table of primary partitions** (four 16-byte partition structures) | | **64** |
| 01FE | 510 | 55h | **MBR signature**: 0xAA55 | **2** |
| 01FF | 511 | AAh | | |
| **MBR total size: 446 + 64 + 2 =** | | | | **512** |

Рис. 8.2. Структура первого сектора диска

Процесс загрузки GPT имеет ряд отличий. На том же этапе загрузки в структуре разделов GPT (рис. 8.3) происходит следующее. GPT использует UEFI, в котором нет такой, как у MBR, процедуры хранения в загрузочном секторе первой стадии загрузчика с последующим вызовом второй стадии загрузчика.

Unified Extensible Firmware Interface (UEFI) – унифицированный расширяемый интерфейс прошивки является более продвинутым интерфейсом, чем BIOS. Он может анализировать файловую систему и самостоятельно загружать файлы.

После включения компьютера UEFI сначала выполняет функции системной конфигурации, также, как и BIOS. Это управление энергопотреблением, установка дат и других компонентов управления системой.


Рис. 8.3. Структура диска с GPT

Затем UEFI считывает GPT – таблицу разделов GUID. GPT располагается в первых секторах диска, сразу после сектора 0, где по-прежнему хранится главная загрузочная запись для Legacy BIOS. GPT определяет таблицу разделов на диске, на которой загрузчик EFI распознает системный раздел EFI. Системный раздел содержит загрузчики для всех операционных систем, установленных на других разделах жесткого диска. Загрузчик инициализирует менеджер загрузки Windows, который затем загружает операционную систему.

При сравнении двух подходов можно выделить следующие различия:

– GPT допускает неограниченное количество основных разделов, в то время как MBR допускает только четыре основных, а остальные – дополнительные;

– GPT позволяет создавать разделы любого размера, в то время как MBR имеет ограничение в 2 ТБ;

– GPT хранит копию данных раздела, позволяя восстановить их в случае повреждения основного заголовка GPT, а MBR хранит только одну копию данных раздела в первом секторе жесткого диска, что может привести к потере всей информации в случае повреждения информации о разделах;

– GPT хранит значения контрольной суммы для проверки, что данные не повреждены, и может выполнить необходимое восстановление из других областей диска в случае повреждения; MBR не имеет возможности узнать о повреждении данных, вы можете узнать об этом только, если компьютер откажется загружаться или исчезнет раздел.

Каждый раздел или логический диск делится на две части: в первой находится служебная информация о диске (структура папок, файловая система и т. д.), во второй – данные пользователя (файлы). Такое деление, начиная с метаданных, позволяет оптимизировать дисковое пространство, быстрее искать файлы, а также повысить надежность работы. Служебная информация о диске – это информация о размере раздела, типе файловой системы и т. д. Для компьютера необходимо корректно найти нужные данные на разделе [59].

Служебная информация о файлах и папках – это файловые записи, содержащие имена файлов, размер, отметки даты/времени и другую техническую информацию.Сюда включают точные физические расположения (адреса) данных файлов на диске. На том же диске обычно имеется резервная копия этой информации.

На разных файловых системах данная информация хранится по-разному, например, в файловой системе FAT32 она находится в таблице размещения файлов (англ. File Allocation Table, далее – FAT), в то время как в файловой системе New Technology File System (англ. файловая система новой технологии, далее – NTFS) в главной файловой таблице (англ. Master File Table, далее – MFT).

FAT – это линейная табличная структура со сведениями о файлах. В файловой системе FAT логическое дисковое пространство любого логического диска делится на две области: системную область и область данных.

Системная область создается и инициализируется при форматировании и состоит из следующих компонентов, расположенных друг за другом (рис. 8.4): загрузочная запись (boot record – BR); зарезервированные сектора (reserved sector – RS); таблицы размещения файлов (FAT); корневой каталог (root directory – Rdir).

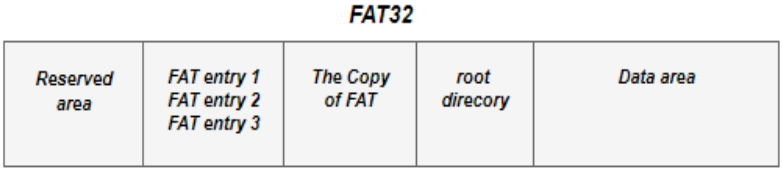


Рис. 8.4. Структура логического диска с файловой системой FAT32

На сегодняшний день самой распространенной файловой системой на компьютерах пользователей является NTFS, которая пришла на смену FAT.

NTFS содержит ряд значительных усовершенствований и изменений, существенно отличающих ее от других файловых систем. В отличие от FAT работа на дисках большого объема происходит намного эффективнее, имеются средства для ограничения доступа к файлам, введены механизмы, повышающие надежность файловой системы, сняты многие ограничения на максимальное количество дисковых секторов и/или кластеров. Одним из основных понятий при работе с NTFS является том (volume).

Все дисковое пространство делится на две неравные части (рис. 8.5). Первая часть тома отводятся под главную файловою таблицу MFT (Master File Table) – это пространство может увеличиваться в размере. Эта область тома всегда держится пустой, чтобы самый главный служебный файл MFT не фрагментировался при росте. Вторая часть тома представляет собой обычное пространство для хранения файлов.

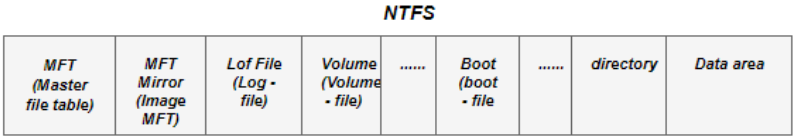


Рис. 8.5. Структура логического диска с файловой системой NTFS

Таблица размещения файлов представляет карту области данных, в которой описывается состояние каждого участка области данных. Область данных разбивают на кластеры.

Кластер – это один или несколько смежных секторов в логическом адресном пространстве области данных (рис. 8.6). В таблице FAT кластеры, принадлежащие одному файлу (или некорневому каталогу), связываются в цепочки. Файл или каталог занимает целое число кластеров. Последний кластер при этом может быть задействован не полностью, что приведет к заметной потере дискового пространства при большом размере кластера. На жестких дисках кластер занимает в зависимости от объема раздела от 2 до 32 секторов. Слишком большой размер кластера ведет к неэффективному использованию дискового пространства, особенно в случае большого количества маленьких файлов.

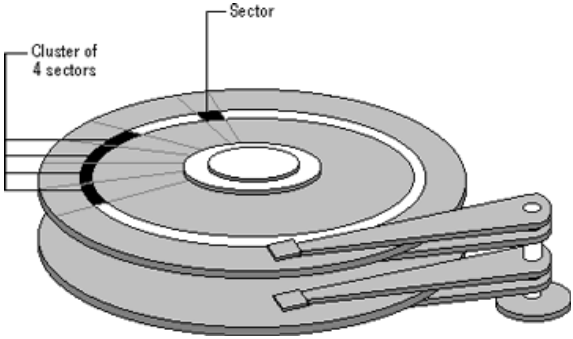


Рис. 8.6. Расположение кластера и сектора

По умолчанию размер кластера для файловой системы NTFS в Windows NT 4.0 и более поздних версий равен 4 Кб. Это обусловлено тем, что сжатие файлов в NTFS невозможно для дисков с большим размером кластера. NTFS поддерживает размеры кластеров от 512 байт до 64 Кб. Стандартом считается кластер размером 2 Кб или 4 Кб. В файловой системе FAT32 размер кластера можно выбрать от 1024 байт до 32 Кб.

Знание особенностей расположения файлов на диске позволяет понять, как их можно наиболее эффективно извлекать или восстановить в случае утраты. Далее мы рассмотрим методы копирования информации с носителей информации, способы восстановления служебных разделов диска и основные способы восстановления информации на логическом диске.

## § 2. Способы восстановления удаленных файлов

Все случаи восстановления данных не могут быть унифицированными. Иногда данные и структуру каталогов можно восстановить полностью, а иногда бывает лишь частичное восстановление. В этих случаях восстанавливается только содержимое файлов, а другие параметры, такие как имена, структура каталогов, – где они находились, временные отметки извлечь невозможно. Также возникают ситуации, когда файлы оказываются поврежденными и не подлежат восстановлению.

Знание особенностей расположения файлов на диске позволяет понять, как их можно восстановить в случае утраты. Рассмотрим принципы хранения файлов на диске.

Жесткий диск очень часто делится на несколько логических диска (тома). Каждый раздел может иметь свою файловую систему, которая не зависит от других разделов. Информация о разделах диска хранится в начале жесткого диска Master Boot Record

& Partition Table (MBR&PT) Ее обычно называют «таблицей разделов». Типовая структура разделов показана на рис. 8.7 [70].

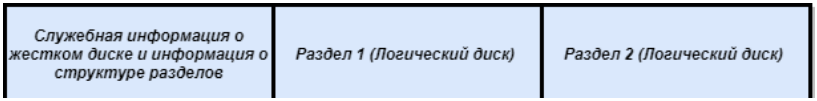


Рис. 8.7. Структура жесткого диска

Служебная информация о жестком диске и информация о структуре разделов являются метаданными. Это информация о данных на диске. Логический диск тоже делится на две части: информация о диске (структура папок, файловая система и т. д.), данные пользователя (файлы, базы данных). Такое деление, начиная с метаданных, позволяет оптимизировать дисковое пространство, быстрее искать файлы, а также повысить надежность работы. На рис. 8.8 показана типичная структура логического диска [70].


Рис. 8.8. Структура логического диска

Служебная информация о диске – это информация о размере раздела, типе файловой системы и т. д. Информация о файлах и папках – это файловые записи, содержащие имена файлов, размер, отметки даты/времени и другую техническую информацию. Также эта информация включает точное физические расположения (адреса) данных файлов на диске. На том же диске обычно имеется резервная копия этой информации.

При необходимости прочесть файл компьютер прежде всего обращается к информации о файлах и папках и ищет запись о данном файле. Далее осуществляется поиск адреса файла и переход к конкретному месту на диске, затем читаются данные файла.

Для файлов, которые находятся на диске в одном месте (расположены рядом), все происходит достаточно просто. Однако файлы на диске могут быть фрагментированы, т. е. занимать несколько несмежных областей. Это происходит достаточно часто, но большинство пользователей об этом не догадываются. Кроме того, если вы посмотрите на файл в проводнике Windows или в Finder (Mac OC), то всегда увидите только один файл, так как все операции по сбору частей файла происходят внутри операционной системы. Адреса всех фрагментов файла, хранимые в информации о файлах и папках, сразу же находятся при попытке его чтения. Данная информация и то как она извлекается крайне важны при восстановлении файлов.

При удалении файла не происходит мгновенного разрушения его данных. Вместо этого вносятся некоторые изменения в информацию о файлах и папках, показывающие, что файл был удален. В некоторых операционных системах файл просто помечается как удаленный, при этом сохраняются все метаданные о файле до тех пор, пока они не будут перезаписаны метаданными о новом файле. Именно так происходит удаление файлов в файловых системах ОС Windows. В других операционных системах (например, Mac OS X) полностью разрушается файловая запись об удаленном файле. Если сведения о файле в информации о файлах и папках в зависимости от операционной системы либо сохраняются, либо сразу удаляются при удалении файла, то сами данные файла во всех операционных системах остаются нетронутыми до тех пор, пока данное место на диске не потребуется для записи другого файла. Если же на диск не записываются другие файлы, то информация о файле и его данные будут на нем сохранены.

Как уже было отмечено ранее, в том месте диска, где хранится информация о данных файла, также содержится резервная

копия информации о файлах и папках. При этом там может находиться и некоторая дополнительная информация о структуре файлов и папок, расположенных в различных местах диска.

Если файлы на электронном носителе перезаписаны, то их не удастся восстановить рассмотренными методами.

Есть два способа восстановления файлов, которые не были перезаписаны. Во всех утилитах восстановления используется либо один из них, либо оба [70].

*Способ 1* – восстановление файлов посредством анализа информации о файлах и папках. Это самый первый метод, используемый в программах восстановления данных, так как при его успешном применении восстанавливаются файлы с оригинальными именами, путями, отметками даты/времени и сами данные. Работа утилиты восстановления файлов начинается с попытки чтения и обработки первой копии информации о файлах и папках. В некоторых случаях (например, при случайном удалении файла) это единственное, что требуется для восстановления файлов.

Если первая копия информации о файлах и папках сильно повреждена, то утилита сканирует диск и ищет вторую копию информации о файлах и папках. При этом также производится детальный поиск дополнительной информации о структуре папок и файлов, которая может находиться в области диска, где хранятся данные. После этого вся найденная информация обрабатывается и воссоздается оригинальная структура папок и файлов.

Если файловая система диска серьезно не повреждена, то вполне вероятно удастся полностью восстановить структуру папок и файлов.

При сильном же повреждении файловой системы данный метод не позволит воссоздать полную структуру папок. В этом

случае восстановленные файлы будут находиться в папках с присвоенными им виртуальными именами. На рис. 8.9 можно увидеть эти папки в программах R-Studio и R-Undelete.

*Способ 2* – восстановление файлов при помощи сканирования файлов известных типов (поиска файлов по сигнатурам). Если при помощи первого метода на удастся добиться желаемого результата, то следует произвести поиск файлов по сигнатурам. Этот метод позволяет восстановить больше данных, однако при этом не удается получить оригинальные имена файлов, отметки даты/времени или полную структуру папок и файлов на диске.

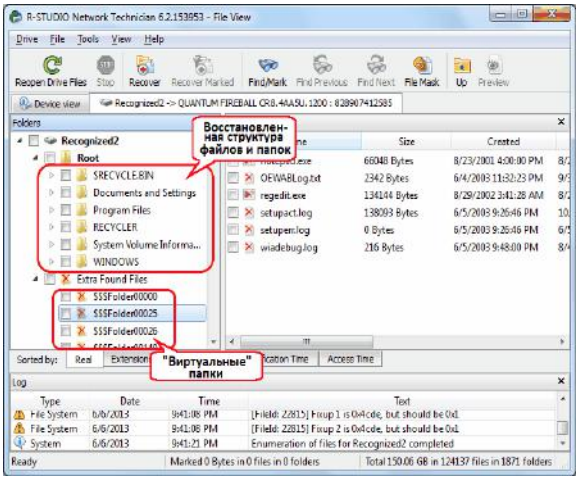


Рис. 8.9. Структура восстановленных файлов и папок

При поиске во время сканирования файлов известных типов (поиск файлов по сигнатурам) анализируется содержимое диска и производится поиск по файловым сигнатурам.

*Файловая сигнатура* – это общий для определенного типа файлов шаблон данных, находящийся в начале или в конце файла. Почти каждый тип файлов имеет, по крайней мере, одну файловую сигнатуру. Например, все файлы типа png (portable

network graphics, переносимая сетевая графика) начинаются с последовательности символов «‰PNG» и многие MP3 файлы начинаются с последовательности символов «ID3». Такие файловые сигнатуры позволяют отнести данные на диске к определенному типу файлов и далее восстановить.

После сканирования файлов известных типов R-Studio и R-Undelete найденные файлы помещают в категорию «дополнительно найденные файлы (Extra Found Files)», где они будут структурированы по расширениям на основе идентифицированной файловой сигнатуры и где им будет присвоено некое шаблонное имя, например, порядковый номер (рис. 8.10, 8.11).

*Ограничения поиска файлов по сигнатурам.* Несмотря на то, что при помощи данного метода можно получить наилучшие результаты при восстановлении данных с сильно поврежденной файловой системой, в нем имеются определенные ограничения. Прежде всего необходимо учитывать, что в одних файлах – файловая сигнатура имеется в начале и в конце файла, в других – только в начале, а в-третьих, вообще отсутствует какая-либо различимая файловая сигнатура.

Если утилита восстановления данных найдет файловую сигнатуру в начале и в конце файла, то он будет распознан и восстановлен. Если файл не имеет сигнатуры в конце, то утилита восстановления может восстановить его, допуская что он заканчивается в начале следующего файла. И, если файлы не имеют сигнатуры (например, зашифрованные диски, хранящиеся в файле-контейнере), то при помощи поиска файлов по сигнатурам не удастся получить какие-либо данные и на их месте будет показано нераспределенное дисковое пространство.

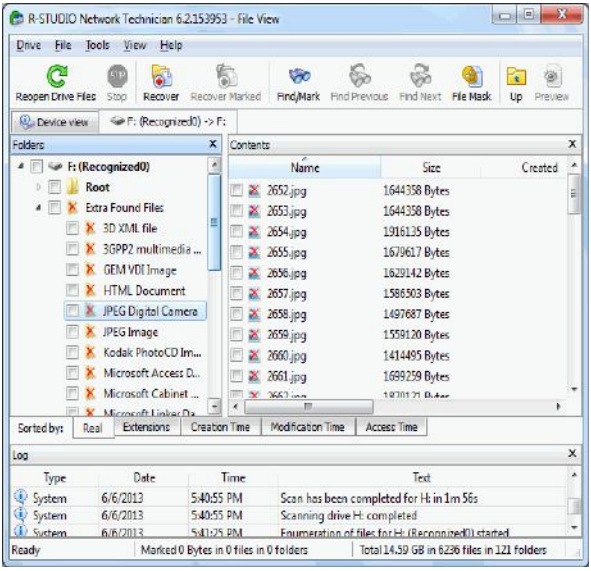


Рис. 8.10. Файлы, найденные на логическом диске путем сканирования файлов известных типов

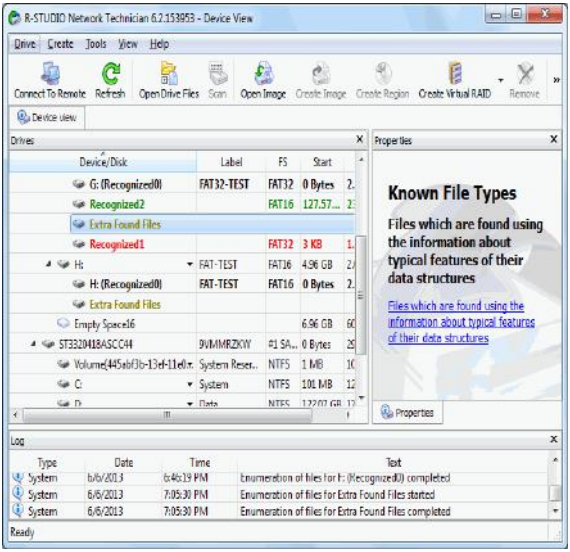


Рис. 8.11. Файлы, найденные вне логического диска путем сканирования файлов известных типов

Также все это может быть осложнено еще и фрагментацией файлов. Более того, файлы, не имеющие сигнатуры в конце, после восстановления могут содержать в конце некую последовательность не относящихся к ним символов (рис. 8.12) [59].

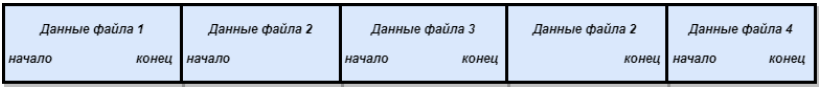


Рис. 8.12. Данные файла на диске

В ситуации, изображенной на рис. 8.12, файлы 1 и файл 3 будут успешно восстановлены, а файлы 2 и 4 – нет. Пояснение этому вы найдете в табл. 8.1 [70].

*Таблица 8.1*

| Файл | Условие | Результат |
|---|---|---|
| Файл 1 | Нет сигнатуры в конце файла, однако файл заканчивается в том месте, где начинается сигнатура в начале файла 2 | Файл успешно восстановлен |
| Файл 2 | Фрагментированный файл. Файл 3 пересекается с файлом 2 | Файл не восстановлен. Утилита посчитает, что файл заканчивается в месте начала файла 3. Вторая часть файла 2 будет утрачена |
| Файл 3 | Смежный файл с сигнатурой в начале и в конце | Файл успешно восстановлен |
| Файл 4 | Нет сигнатуры в конце файла, за файлом следует нераспределенное пространство | Файл не восстановлен. Утилита посчитает что файл заканчивается в месте начала файла N, и нераспределенное пространство будет добавлено в конец файла 4 |

Помимо проблем с фрагментацией при поиске файлов по сигнатурам также можно получить ложные результаты. Например, в любом файле могут находиться символы ID3, которые при этом не будут являться файловой сигнатурой. Например, текст, который вы сейчас читаете, содержит указанные символы ID3, но это не MP3 файл. Поэтому при поиске файлов по сигнатурам

часть данного текста может ошибочно распознаться как начало MP3 файла.

Помимо описанных выше методов, используемых в программах восстановления данных, есть также некоторые дополнительные параметры поиска и способы восстановления данных, которые позволяют получать лучшие результаты. Профессиональные программы восстановления файлов (например, R-Studio) предоставляют пользователям возможность самим задавать файловые сигнатуры любой степени сложности, т. е. создавать пользовательский известный тип файла.

Между тем необходимо отметить следующее. Повреждения файловой системы могут приводить к непредсказуемым результатам. Состояние файлов в этом случае будет зависеть от того, что вызвало их утрату, от общего состояния диска до сбоя в работе системы или утраты данных, а также от действий, которые были предприняты до начала восстановления данных.

Не следует предпринимать попыток восстановления данных с физически неисправных дисков. Если вы подозреваете что ваш диск физически неисправен, то лучше обратитесь к специалистам лаборатории по восстановлению данных с соответствующим оборудованием и опытом. Какие-либо дальнейшие действия с таким диском наверняка вызовут еще большие повреждения ваших данных, что приведет к тщетности дальнейших попыток их восстановления.

*Случай 1* – восстановление файлов с жесткого диска с поврежденной служебной информацией. Если диск не был соответствующим образом смонтирован или извлечен (например, из-за сбоя электропитания или ошибки пользователя), то часть или все метаданные на нем могут оказаться поврежденными или утраченными. При этом оказывается утраченной только исходная

служебная информация о жестком диске и информация о структуре разделов, а оставшаяся часть данных на диске будет сохранена. В этом случае программы восстановления данных анализируют сохранившуюся на диске информацию о файлах и папках и восстанавливают все файлы и папки. Поиск известных типов файлов в таких случаях вряд ли понадобится. Это самый простой случай восстановления данных и, как правило, позволяет получать наилучшие результаты [70].

*Случай 2* – восстановление файлов с заново разбитого на разделы жесткого диска (физического диска). Случай заново разбитого на разделы диска во многом схож с первым случаем, единственное основное отличие состоит в том, что при создании нового раздела на диск записываются новые данные. При этом на диске перезапишется служебная информация о физическом диске. Однако остальная информация сохранится, в том числе и информация о файлах и папках. Таким образом при помощи программ восстановления можно отсканировать диск, найти эту информацию и восстановить файлы и папки, которые не были затронуты данными нового раздела. Поиск известных типов файлов, как и в первом случае, вряд ли понадобится [70].

*Случай 3* – восстановление файлов с переформатированного раздела (логический диск). Как правило, при переформатировании утрачивается больше данных, чем при разбиении диска на разделы. Все зависит от того, какое было выполнено форматирование [70].

При полном форматировании все данные раздела перезапишутся определенными шаблонами (обычно 00 или FF), что приведет к невозможности восстановления каких-либо файлов с раздела.

При быстром форматировании часть или все данные информации о файлах и папках перезаписываются, но при этом данные

о файлах сохраняются. При помощи программ восстановления можно отсканировать диск, найти то, что осталось от предыдущей файловой системы, и далее восстановить файлы и папки. Результаты восстановления при помощи первого метода могут очень сильно различаться в зависимости от того, какая была файловая система до и после переформатирования. Поиск известных типов файлов в этом случае может весьма пригодиться, даже если вам не удастся найти какие-либо файлы при помощи первого метода.

*Случай 4* – восстановление файлов с диска с поврежденной файловой системой. Данный случай во многом зависит от того, насколько сильно повреждена файловая система. Вспомните, что на диске имеются две копии информации о файлах и папках. Если повреждена только одна копия, то программа восстановления данных сможет прочесть данные из резервной копии и восстановить всю информацию и сами данные файлов. Если же повреждены обе копии, то шансы восстановления данных представляются достаточно мрачными. Здесь, как и в третьем случае, может помочь поиск известных типов файлов [70].

*Случай 5* – восстановление файлов, утраченных при их переносе на диск. Если компьютер зависает или происходит какой-либо другой сбой во время дефрагментации диска или операции разбиения диска на разделы, то результаты восстановления данных могут не дать какого-либо положительного результата. Обычно это наихудший сценарий при восстановлении файлов. Информация о файлах и папках может выглядеть неповрежденной, однако метаданные при этом будут указывать на неверные физические адреса файлов, которые находились в процесс переноса во время сбоя в работе. Например, данные могут находиться уже в другом месте, однако в информации о файлах и папках это

отображено еще не будет. Или же в информацию о файлах и папках будет уже записана новая информация, но некоторые или все файлы еще не будут перенесены. В этом случае даже поиск известных типов файлов может не помочь, так как многие файлы возможно будут фрагментированы [70].

## § 3. Поиск и извлечение паролей пользователя

Сегодня самым распространенным способом аутентификации является защита при помощи паролей, но не стоит забывать о многочисленных недостатках традиционной аутентификации (пароли могут подобрать, подсмотреть или просто угадать), а также о том, что пароли хранятся в кэше или служебных файлах прикладного программного обеспечения (главный недочет).

Браузеры, почтовые клиенты и другие программы часто предлагают сохранять пароли, что является удобным.

Если в короткие сроки необходимо найти тот или иной пароль, который использовал пользователь (на удаленных сервисах), отличным вариантом могут быть программы от NirSoft: WebBrowserPassView, Mail PassView, MessenPass и др. У программ очевидные названия. Так, первая получает пароли из веббраузеров, вторая – от почтовых клиентов, а третья получает информацию от клиентов для обмена мгновенными сообщениями. Это абсолютно бесплатные программы, без рекламы, у многих из них есть интерфейс командной строки, они нетребовательны к ресурсам. Но они работают только под Windows и у них закрыт исходный код: в таком случае программа может не только извлекать пароли, но и передавать их третьим лицам.

*WebBrowserPassView* извлекает пароли из Internet Explorer, Microsoft Edge, Chrome, Opera, Safari, Firefox и Yandex Browser, причем поддерживаются самые последние версии (рис. 8.13).

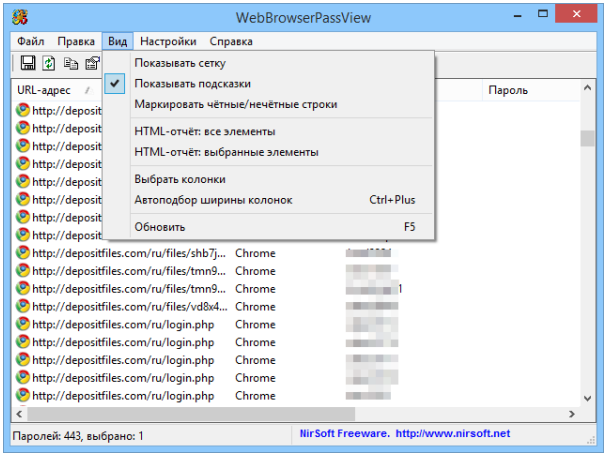


Рис. 8.13. Пример извлечения паролей из браузеров с помощью WebBrowserPassView

*MailPassView* позволяет восстановить пароли из внушительного списка почтовых приложений: Outlook Express; Microsoft Outlook 2000 (только учетные записи POP3 и SMTP); Microsoft Outlook 2002–2016 (учетные записи POP3, IMAP, HTTP и SMTP); Windows Mail; IncrediMail; Eudora; Netscape 6.x/7.x; Mozilla Thunderbird; Group Mail Free; Yahoo Mail, если пароль сохранен в приложении Yahoo Messenger; Hotmail/MSN mail, если пароль сохранен в приложении MSN Messenger; Gmail, если пароль сохранен в приложениях Gmail Notifier, Google Desktop или Google Talk (рис. 8.14).

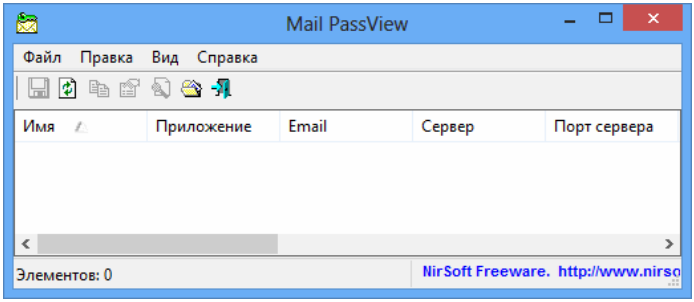


Рис. 8.14. Пример извлечения паролей из браузеров с помощью MailPassView

Mail PassView не может восстановить пароль из почтового клиента, за исключением The Bat. Однако The Bat сам может сообщить тебе сохраненный пароль. Для этого нужно в настройках почтового ящика включить лог, а затем просмотреть файл POP.log после проверки почты (точнее после подключения к POP-серверу).

Популярной в недавнем времени и встречающейся до сих пор файловый менеджер Total Commander тоже хранит пароли. Можно восстановить пароли к FTP, используя утилиту Windows Commander FTP crack.

Необходимо найти на компьютере файл WCX_FTP.INI, в нем хранятся зашифрованные пароли к FTP. Копируем зашифрованный пароль в окно программы и нажимаем кнопку Show (рис. 8.15).

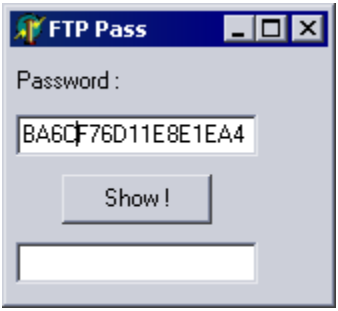


Рис. 8.15. Пример извлечения паролей FTP

На сайте NirSoft можно найти много утилит для восстановления паролей. Подробно мы их все рассматривать не будем, ограничимся выборочным списком:

1. *MessenPass* – восстанавливает пароли из мессенджеров, таких как Miranda, Yahoo Messenger, ICQ Lite, Windows Messenger и др.

2. *IE PassView* – инструмент просмотра паролей для IE, поддерживает версии до восьмой включительно, но лучше все же использовать WebBrowserPassView.

3. *BulletsPassView* – позволяет восстановить пароли, сохраненные в различных приложениях для Windows, таких как CuteFTP, FileZilla, VNC.

4. *Network Password Recovery* – восстанавливает пароли к папкам общего доступа в сети. Есть поддержка Windows 8 и Windows 10.

5. *PstPassword* – позволяет восстановить пароль из файла PST. Работает с Outlook до версии 2007. PasswordFox, ChromePass, OperaPassView восстанавливают пароли, сохраненные в Firefox, Chrome и Opera соответственно.

6. *WirelessKeyView* – находит сохраненный пароль к Wi-Fi. Хотя в этом, как правило, нет смысла, поскольку Windows этот пароль не скрывает, и в любой момент его можно просмотреть, используя средства ОС.

7. *Remote Desktop PassView* – достает пароли из файлов RDP. RouterPassView – это утилита, которая позволяет восстановить пароли маршрутизаторов и ключи беспроводных сетей, если есть резервная копия конфигурации маршрутизатора, сохраненная как локальный файл.

8. *Nsasoft SpotAuditor* – мощное решение для восстановления паролей и прочей важной информации. Программа работает с внушительным списком приложений, среди которых популярные браузеры, почтовые клиенты, средства общения, FTP-клиенты (рис. 8.16).

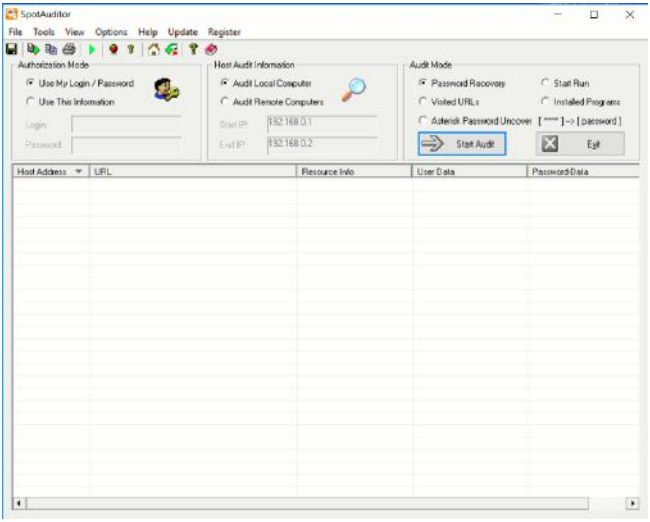


Рис. 8.16. Пример извлечения паролей FTP

9. *Firefox Password Recovery Master* – это удобный инструмент, позволяющий восстанавливать любые закэшированные пароли для популярного браузера Mozilla Firefox. Данная программа предоставляет список паролей к сайтам сразу же после своего запуска.

Программа Firefox Password Recovery Master является очень удобной, так как она предоставляет все пароли сразу же, невзирая на их длину и сложность, данная утилита может восстанавливать пароли, введенные на любом языке, помогает восстанавливать пароли, зашифрованные User Master Password (пароль для доступа к хранилищу паролей).

Интерфейс данной программы (рис. 8.17) является очень простым и обладает такими полезными свойствами, как копирование извлеченных данных в буфер обмена и их сохранение в виде форматированного текста.


Рис. 8.17. Интерфейс Firefox Password Recovery Master

В завершении обзора программного обеспечения для мгновенного извлечения паролей рассмотрим Passware Kit и Advanced IM Password Recovery.

Комплект утилит Passware Kit (рис. 8.18) предназначен для проведения процесса поиска утерянных паролей. Также его можно использовать для проверки криптостойкости паролей на файлы, содержащие ценную информацию.

Passware Kit позволяет находить пароли в следующих типах файлов: Microsoft Access, Backup, Excel, Internet Explorer, Mail, Money, Outlook, Outlook Express, Project, Schedule+, Word; Lotus 1-2-3, Adobe Acrobat, Symantec ACT!, FileMaker, MYOB, Lotus Organizer, Paradox, Peachtree, QuickBooks, Quicken, Visual Basic for Application, Windows XP 2000, NT 4.0, WordPerfect, Lotus WordPro, WinZip, PKZip.

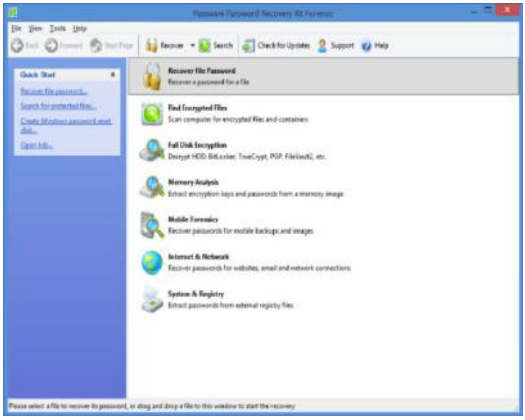

Рис. 8.18. Интерфейс Passware Kit

*Advanced Instant Messengers Password Recovery* полностью восстанавливает логин и пароль к учетным записям в различных коммуникаторах (программах мгновенного обмена сообщениями). Таким образом, Advanced Instant Messengers Password Recovery является самым универсальным продуктом в своем классе. Если на компьютере установлено несколько программ-мессенджеров, то Advanced Instant Messengers Password Recovery восстановит пароли к записям, созданным во всех программах (рис. 8.19).

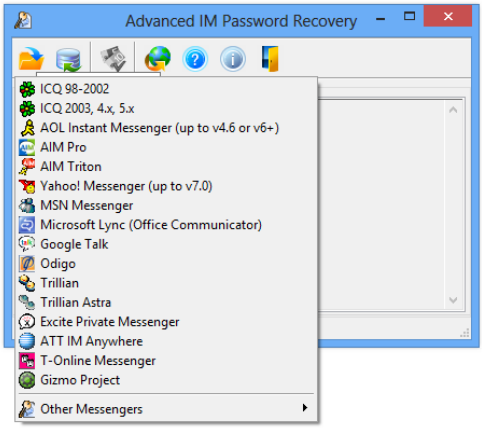


Рис. 8.19. Интерфейс Advanced Instant Messengers Password Recovery

Проблема забытых паролей встает достаточно остро, особенно если зашифрованные данные срочно необходимы, но, к сожалению, никак не удается вспомнить ключевое слово, необходимое для их расшифровки. Следует отметить, что алгоритмы, используемые при шифровании в обычных приложениях Windows, мягко говоря, не слишком криптоустойчивы. Соответственно, это означает, что при достаточно мощном компьютере и наличии определенного отрезка времени практически любой зашифрованный файл может быть раскрыт, особенно если учитывать тот факт, что пользовательские пароли, как правило, являются относительно несложными.

## § 4. Рекурсивный поиск содержимого файлов

В ряде случаев возникает необходимость поиска определенного слова и сочетания символов (номер банковской карты, адреса электронной почты и т. д.) по всем файлам электронного носителя. В Linux все это делается с помощью одной очень простой, но в то же время эффективной утилиты grep или аналогов (ack, rg, ag, pt). С ее помощью можно искать не только строки в файлах, но и фильтровать вывод команд и др.

Команда grep (global regular expression print) одна из самых используемых в терминале Linux, которая входит в состав проекта GNU. Консольная утилита grep решает множество задач, в основном она используется для поиска строк, соответствующих строке в тексте или содержимому файлов. Также она может находить по шаблону или регулярным выражениям. Команда в считанные секунды найдет файл с нужной строчкой, текст в файле или отфильтрует из вывода только пару нужных строк. Синтаксис команды выглядит следующим образом:

$ grep [опции] шаблон [имя файла...],

где опции – это дополнительные параметры, с помощью которых указываются различные настройки поиска и вывода, например, количество строк или режим инверсии; шаблон – это любая строка или регулярное выражение, по которому будет вестись поиск; файл и команда – это то место, где будет вестись поиск; grep позволяет искать в нескольких файлах и даже в каталоге, используя рекурсивный режим.

Основные опции утилиты, которые помогут более эффективно выполнять поиск текста в файлах grep:

- b – показывать номер блока перед строкой;
- c – подсчитать количество вхождений шаблона;
- h – не выводить имя файла в результатах поиска внутри файлов Linux;
- i – не учитывать регистр;
- l – отобразить только имена файлов, в которых найден шаблон;
- n – показывать номер строки в файле;
- s – не показывать сообщения об ошибках;
- v – инвертировать поиск, выдавать все строки кроме тех, что содержат шаблон;
- w – искать шаблон как слово, окруженное пробелами;
- e – использовать регулярные выражения при поиске;
- An – показать вхождение и n строк до него;
- Bn – показать вхождение и n строк после него;
- Cn – показать n строк до и после вхождения.

Когда необходимо найти строку abc, grep будет выводить также kbabc, abc123, aafrabc32 и тому подобные комбинации. Пользователь может уточнить поиск по содержимому файлов в Linux только для тех строк, которые выключают искомые слова с помощью опции -w:

$ grep -w "abc" имя_файла.

При указании grep, с помощью опции l, можно вывести имя файла, в котором было найдено заданное слово, например, следующая команда выведет все имена файлов, при поиске по содержимому, которые были обнаружены с вхождением primary:

$ grep -l 'primary' *.c.

Использование команды grep для поиска и фильтрации вывода команд в операционной системе Linux является одним из самых удобных способов. При правильном применении эта утилита станет эффективным инструментом рекурсивного поиска.

Существуют инструменты рекурсивного поиска с графическим интерфейсом пользователя, которые сканируют образ диска, файл или каталог с файлами и извлекает полезную информацию без анализа файловой системы или структур файловой системы. Ярким примером является Bulk Extractor (рис. 8.20).

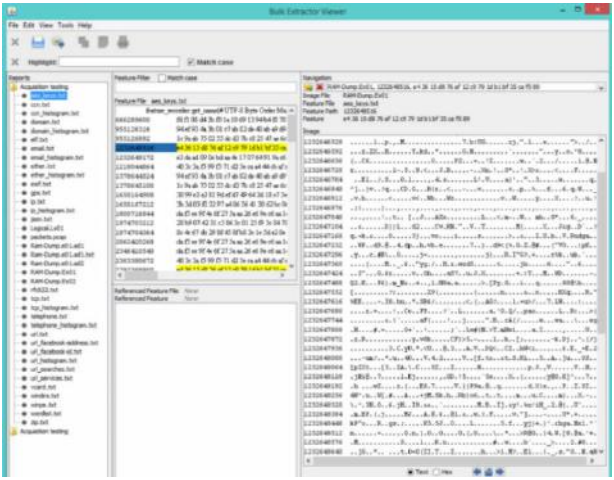

Рис. 8.20. Оконный интерфейс Bulk Extractor

Эта программа отличается от других подобных инструментов своей скоростью и проработкой. Поскольку Bulk Extractor

игнорирует структуру файловой системы, то может обрабатывать разные части диска параллельно. На практике программа разбивает диск на страницы по 16 Мб и обрабатывает по одной из них на каждом доступном ядре. Это означает, что 24-ядерные машины обрабатывают диск примерно в 24 раза быстрее, чем одноядерные. Bulk Extractor автоматически обнаруживает, распаковывает и рекурсивно повторно обрабатывает сжатые данные, которые обрабатываются с помощью различных алгоритмов.

Еще одно преимущество игнорирования файловых систем заключается в том, что Bulk Extractor можно использовать для обработки любых цифровых носителей, например для жестких дисков, твердотельных накопителей, оптических носителей, видеокарт, сотовых телефонов, дампа сетевых пакетов и др.

# ГЛАВА IX. ПОЛУЧЕНИЕ ИНФОРМАЦИИ С ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ

## § 1. Виды информации на разных уровнях OSI

За последнее время можно наблюдать огромный рост пользователей интернета и, соответственно, увеличение трафика телекоммуникационной среде. Значительное влияние оказывают корпоративные сети, которые принимают электронную почту, общаются в чатах, социальных сетях, занимаются веб-серфингом, используют интернет-торговлю, совершают звонки через интернет, и все это обычные средства ежедневного общения и получения информации. Так, даркнет привлекает преступников и террористов с целью совершения различного рода преступлений. Между тем незаконная интернет-деятельность может быть использована для торговли наркотиками или оружием или осуществлять рассылку спама и вирусов по электронной почте.

Получение информации с технических каналов связи может заменить физический доступ к компьютерной системе, поскольку даст такую же информацию, а именно: содержимое электронной почты, свидетельства о просмотре веб-сайтов, о размещении информации в сети, о несанкционированном доступе к удаленным узлам, об использовании контрафактных программ. К тому же перехватить трафик бывает проще, чем найти и изъять в исправном состоянии компьютер.

Выделим основные организационные варианты снятия информации с технических каналов связи:

- получение при помощи имеющейся аппаратуры СОРМ;
- получение средствами оператора связи;
- получение собственными средствами.

В подавляющем большинстве случаев в полученной информации может содержаться тайна частной жизни. Поэтому необходимо иметь судебное решение. Без судебной санкции возможен перехват своего собственного трафика потерпевшим либо с его письменного разрешения. К тому же с технической точки зрения существует ряд проблем при перехвате информации в технических каналах:

– идентификаторы (IP-адреса, MAC-адреса) контролируемого отправителя и получателя находятся в общем потоке данных и должны быть изначально незаметно извлечены;

– контролируемый поток данных проходит в общих битовых потоках на многих узлах сети Интернет. Кроме того, архитектура предоставления доступа к интернету не безупречна. Таким образом, возникают проблемы конфиденциальности других участников информационного обмена, поскольку чужие данные могут быть ошибочно захвачены;

– в транспортировке данных через интернет участвует много посредников, включая операторов основных сетей, поставщиков услуг (например, e-mail) и т. д.;

– получение может блокироваться средствами защиты провайдера (ISP) в интересах безопасности своих клиентов;

– шифрование делает чрезвычайно сложными, если не невозможными, извлечения данных.

Международной организацией по стандартизации в качестве средства для облегчения взаимодействия оборудования пакетной сети от разных производителей используется в качестве эталона модель OSI. Она также поддерживает взаимодействие между приложениями, работающими на сетевой инфраструктуре, поддерживаемой таким оборудованием.

Снятие информации с технических каналов связи в большинстве случаев может быть реализовано на уровнях базовой эталонной модели взаимодействия открытых систем (OSI), как показано на рис. 9.1 [14].

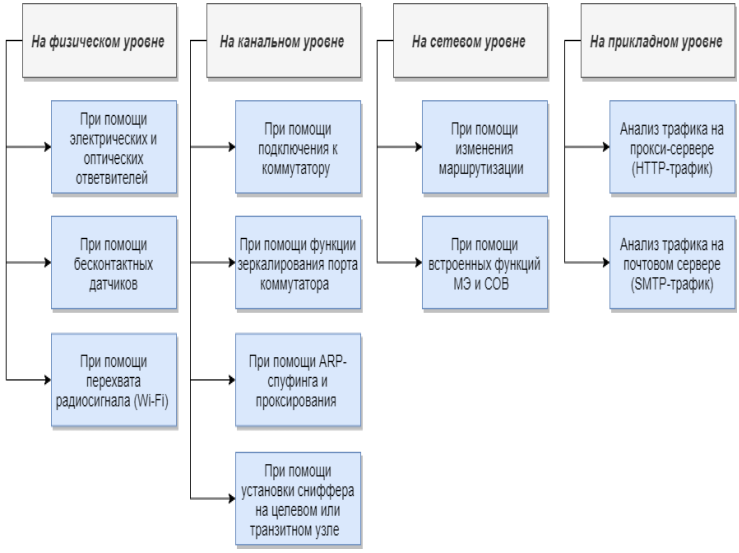


Рис. 9.1. Способы реализации перехвата трафика

Поскольку модель требует независимой работы своих уровней, разработчики приложений и поставщики оборудования могут отдельно использовать каждый уровень в своих технических решениях.

*Уровень приложений (уровень 7)*. Этот уровень определяет, как приложения взаимодействуют друг с другом по сети. Классические приложения позволяют передачу электронной почты, передачу файлов, запросов к удаленным базам данных и доступ к удаленному терминалу. Протоколы, работающие на уровне FTP, Telnet, POP3, SNMP, DHCP, HTTP, NFS и X Windows, имея доступ к серверу приложений, могут перехватить данные этих

приложений, однако эти приложения не всегда доступны на сервере, управляющем такими приложениями.

*Уровень представлений (уровень 6)*. Здесь в основном происходит обмен данными. Формат данных, как правило, текстовый (ASCII), графический (GIF, TIFF, JPEG) и аудиовизуальный (MPEG). Перехват на этом уровне тесно связан с перехватом на предыдущем уровне, т. е. перехваченные форматы данных из конкретных приложений определяются через уровень 6.

*Уровень сеансовый (уровень 5)*. Этот уровень управляет соединением и завершением сеансов связи, а также режимом передачи данных (симплекс, полудуплекс, дуплекс). Когда данные извлекаются из линии связи, необходимо знать режим передачи для перехвата нижнего уровня.

*Уровень транспортный (уровень 4)*. Транспортный уровень устанавливает соединение между двумя узлами, фактически создавая виртуальную линию связи. Наиболее распространенным протоколом этого уровня является TCP, который обеспечивает надежное соединение между хостами посредствам управления потока данных, обнаружения ошибок и подтверждения приема пакетов. Другим популярным протоколом транспортного уровня является протокол универсальной датаграммы (UDP).

UDP намного проще TCP и не имеет возможности подтверждения передачи, поэтому он перемещает пакеты бесконтрольно при доставке в пункт назначения. Тем не менее UDP используется в приложениях, поддерживающих как потоковый звук и видео, где передача должна происходить с минимальной задержкой. Протоколы TCP и UDP имеют важное значение при перехвате трафика.

*Уровень сетевой (уровень 3)*. Этот уровень определяет, как данные между узлами должны передаваться, по одной или нескольким сетям. Наиболее распространенным протоколом этого

уровня является Internet Protocol (IP). Заголовки IP содержит крайне важную информацию для перехвата, например IP-адреса источника и получателя.

*Уровень канальный (уровень 2)*. Этот уровень перемещает IP-пакеты (известные как датаграммы) между хостами. Он описывается рядом протоколов передачи данных, такими как: Ethernet, ATM, frame relay, Token Ring и т. д.

*Уровень физический (уровень 1)*. Первый уровень представляет собой электрические сигналы (провода, контакты, разъема и т. д.), составляющие сетевую инфраструктуру. Прослушивание телефонных переговоров происходит именно на этом уровне с помощью физического подключения.

Каждому из уровней соответствует свое техническое средство. На рис. 9.2 указаны устройства, отвечающие за работу уровня.


Рис. 9.2. Устройства, поддерживающие каждый уровень

Для сетевого представления стека TCP/IP модель OSI можно уменьшить до четырех уровней. Уровни 5, 6 и 7 модели OSI объединяются в один слой приложений, а 1 и 2 уровни объединяются в один слой «канальный» (рис. 9.3). При этом уменьшение уровней покажет принцип перехвата пакетов яснее, ведь уровни

OSI могут показать, какой тип информации можно получить (рис. 9.4) [40].

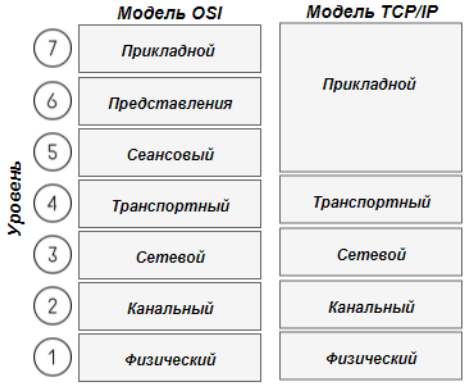


Рис. 9.3. Сокращенный вариант модели OSI

Приложения седьмого уровня позволяют напрямую передавать соответствующую информацию. Но бывает так, что программные продукты не имеют возможности перехвата данных или поставщики услуг не сотрудничают по причине ограниченности юрисдикции.

На шестом уровне циркулирует информация приложений, доступ к нему позволит получать контент (файлы) напрямую [10].

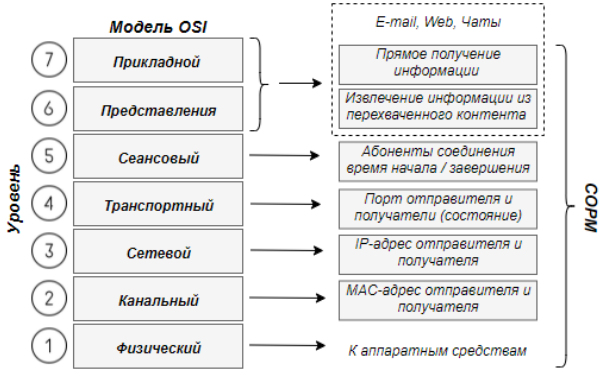


Рис. 9.4. Связь уровней OSI с информацией, получаемой при перехвате и извлечении данных

Снятие информации на данном уровне может проводится с помощью компьютера или устройства, инициирующего, завершающего и управляющего сеансом связи. Классическая конфигурация снятия информации – это хост управления доступом в интернет совместно с сервером RADIUS.

Транспортная информация в датаграмме TCP или UDP может быть извлечена из передающего узла или устройства, управляющего виртуальной схемой связи. Данная информация будет включать в себя номера портов участвующих узлов в обмене данными. Однако на практике может не быть соответствующих интерфейсов для извлечения такой информации, поэтому успешное извлечение, как правило, не гарантированно.

На сетевом уровне происходит прямой перехват IP-пакетов. Такая функция обычно выполняется маршрутизатором с портом, предназначенным для репликации пакетов контролируемых IP-адресов. После этого пакеты отправляется на устройство-посредник, где информация форматируется и анализируется.

Перехват на канальном уровне, теоретически, может быть осуществлен устройствах, поддерживающих ATM-коммутацию, маршрутизацию, ретрансляцию кадров, Ethernet. Однако необходимо приложить значительные усилия для сборки пакетов более высокого уровня для получения конечного содержимого и перехвата связанной информации.

Физический уровень требует прямого подключения к сетевой инфраструктуре, проводу, оптоволокну или радиоканалу. Нужно иметь специальную аппаратуру для извлечения информации при минимальном вмешательстве в производительность сети. После извлечения сигналы должны быть преобразованы в потоки битов. Технологии анализа должны позволять восстанавливать пакеты более высокого уровня из потока битов, что достаточно непросто,

особенно когда это должно проводится в реальном времени или когда на один из более высоких уровней подвергнут шифрованию.

Формулируя техническое задание для снятия информации с технических каналов, следует непременно оценить размер информации. Без точных условий информация может достигнуть большого объема, который достаточно сложно анализировать.

Например, нас интересуют действия пользователя, работающего за домашним компьютером, который подключен к интернету. В его трафике мы хотели бы найти доказательства неправомерного доступа к удаленным узлам. Было бы ошибкой ставить задачу так: «перехват исходящего и входящего трафика компьютера с определенного IP-адреса». Помимо неправомерного доступа подозреваемый также занимается и другой деятельностью. Поскольку современные тарифные планы провайдеров интернета предусматривают безлимитный трафик, а это десятки и даже сотни гигабайт за сутки. Причем большинство задач, связанных с обменом трафика, выполняются в автоматическом режиме (обновление системы, торренты и т. д.). На таком фоне суточные объемы трафика и электронной почты и различных интернет-мессенджеров просто теряются, а интересующая нас информация содержится именно в последних. Перехват всего перечисленного трафика за несколько дней требует диска с очень большой емкостью, который может отсутствовать в распоряжении специалиста. И потом найти в этой куче полезные сведения будет очень сложно.

В описанной ситуации правильная формулировка задания должна сводиться к перехвату исходящего и входящего трафика компьютера с конкретным идентификатором (MAC-адресом, IP-адресом) и указанием конкретных протоколов (например, POP3, IMAP4, SMTP) [14].

К перехваченному трафику для его анализа необходимо прикладывать информацию о конфигурации и состоянии коммуникационного оборудования, чтобы в ходе анализа содержимого трафика можно было интерпретировать данные с меньшим количеством предположений.

Некоторая часть трафика может оказаться зашифрованной. Это касается таких протоколов, как HTTPS, SSH, SMTP/TTS, IPSec и др. В некоторых случаях весь трафик между определенными узлами или сетями подвергается шифрованию (VPN-туннели). Во всех протоколах, даже простейших, сейчас используются стойкие алгоритмы шифрования [14].

Столкнувшись с зашифрованным трафиком, можно узнать немногое: установить сам факт сетевой активности, ее приблизительный объем, а также установить IP-адреса взаимодействующих.

Статистика прошедшего трафика собирается на многих устройствах. Все без исключения маршрутизаторы, а также многие иные коммуникационные устройства имеют встроенные функции для сбора разнообразной статистики. Статистика – это, конечно, не перехват трафика, и она не дает доступа к его содержимому, но отсюда можно получить немало информации.

В простейших случаях на каждом интерфейсе подсчитывается лишь общее количество полученных и отправленных байтов и пакетов. Настройки по умолчанию предполагают более подробную статистику. Полное архивирование всего трафика ведется лишь в редких случаях и не для всех протоколов.

Часто статистика ведется по формату NetFlow. Он предусматривает запись сведений о каждом потоке (Flow), т. е. серии пакетов, объединенных совокупностью IP-адресов, портов и номером протокола. По такой статистике можно установить следу-

ющее: факт обращения определенного узла (компьютера, идентифицированного IP-адресом) к другому узлу; время обращения с точностью до интервала дискретизации (от 5 мин до 1 ч); количество переданного и полученного трафика; протокол; номера портов с обеих сторон (для TCP и UDP) [14].

Еще одна задача, выполняемая при помощи статистики трафика – это обнаружение источника DOS-атаки или иной атаки с подделанными IP-адресами источника. По статистике видно (трассировку), с какого интерфейса пришел на маршрутизатор пакет, т. е. какой был предыдущий узел. Обратившись к статистике этого предыдущего узла, мы можем узнать предпредыдущий узел и т. д. К сожалению, это непростая задача, так как придется устанавливать контакт с несколькими провайдерами. Если один из них откажется сотрудничать или не сохранит статистику, то цепочка оборвется.

Кроме полного перехвата сетевого трафика и анализа его статистики имеют право на существование промежуточные варианты. Полное содержимое трафика может оказаться слишком объемным, что затрудняет анализ или делает его невозможным в реальном времени. Статистика, напротив, слишком скупа. Промежуточные варианты – это перехват сведений о сетевых соединениях (сессиях) или перехват трафика на основе сигнатур.

Сведения о сетевых соединениях или о заголовках пакетов – это, с одной стороны, урезанный перехват трафика (без сохранения сведений о содержимом пакетов, но лишь об их заголовках), с другой – развернутый вариант статистики (когда записывается не агрегированная по времени информация о переданных пакетах).

Перехват по сигнатурам используется для защиты информации в таком техническом средстве, как система обнаружения атак (IDS). Она ищет в передаваемых пакетах заранее предопределен-

ные последовательности байтов, соответствующие попыткам несанкционированного доступа, активности вредоносных программ, иным неразрешенным или подозрительным действиям.

Аналогично можно построить и анализ трафика объекта контроля – предопределить характерные последовательности (сигнатуры), соответствующие подозрительным действиям. И ловить только сессии, в которых встречаются эти сигнатуры. Например, подозреваемый пользуется услугами провайдера коммутируемого доступа и, следовательно, соединение с интернетом происходит с использованием динамического IP-адреса. Наряду с ним IP-адреса из той же сети используют еще несколько сотен пользователей. Требуется проконтролировать переписку подозреваемого по электронной почте. Для этого достаточно записывать все SMTP-сессии, исходящие из сети, где расположен компьютер подозреваемого, в которых встречается последовательность символов: from: <адрес интересующего пользователя>, чтобы выделить письма, направленные от подозреваемого любым адресатам через любые промежуточные узлы. Для такого избирательного перехвата можно использовать почти любую IDS. Многие из них поддерживают довольно сложные сигнатуры со многими условиями.

При перехвате трафика в рамках оперативных мероприятий важно различать доступ сети и доступ к сетевым службам. Доступ к сети обычно организуется интернет-провайдером, который использует инфраструктуру оператора связи. Доступ реализуется на всех уровнях модели OSI, от авторизации доступа до сеансового транспорта, до общего общедоступного интернета. Доступ к сетевым службам (например, электронная почта, чат) могут предоставляться сетевым оператором или сторонней сервисной организацией (поставщиком услуг). Сетевые службы в основном сосредоточены на уровнях 6 и 7, но также могут быть

задействованы более низкие уровни (как в коммерческих, так и частных реализациях VPN на основе IPSec), в данной схеме владелец хоста, крупные сервисы имеют свой хостинг.

## § 2. Перехват трафика в локальной вычислительной сети

Основной особенностью компьютерных сетей, является распределенность в пространстве ее объектов. Эта особенность привела к появлению специфичной для них типовой угрозы безопасности, заключающейся в прослушивании канала связи. Данная угроза безопасности компьютерных сетей получила название «анализ сетевого трафика» (sniffing), сокращенно – «сетевой анализ».

Сетевой анализ позволяет, во-первых, изучить логику работы компьютерной сети, т. е. получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент их появления. Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы, распределенной внутренней сети, позволяет на практике моделировать и осуществлять многие виды типовых удаленных атак.

Во-вторых, разрешает непосредственно перехватить поток данных, которыми обмениваются объекты сети. То есть удаленная атака этого типа заключается в получении несанкционированного доступа к информации, которой обмениваются два сетевых абонента. При реализации данной угрозы нельзя модифицировать трафик, а сам анализ возможен только внутри одного сегмента сети. Примером информации, перехваченной при помощи такой типовой атаки, могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети и т. д.

В качестве наиболее популярных областей практического применения можно выделить следующее: анализ трафика с целью выявления проблем в работе сети (в том числе несанкционированной активности); восстановление потоков данных («прослушивание»); предотвращение различного рода сетевых атак; сбор статистики.

Компьютеры, подключенные к сети Ethernet, имеют возможность перехватывать информацию, адресованную своим соседям. В сетях Ethernet основной причиной является принятый широковещательный механизм обмена сообщениями. Широковещательные рассылки нужны в том случае, если узлам нужно найти информацию, не зная точно, на каком узле она находится, или если узлу нужно своевременно предоставить информацию всем остальным узлам в той же сети. Когда узел получает сообщение на адрес широковещательной рассылки, он его принимает и обрабатывает так же, как и те, что адресованы ему. Когда узел отправляет широковещательное сообщение, концентраторы и коммутаторы его передают всем подключенным к одной локальной сети узлам.

В сети все данные форматируются в пакеты, содержащие данные и служебную информацию связи. Компьютер может иметь одну или несколько карт сетевого интерфейса. Каждая из этих карт имеет уникальный идентификатор оборудования – MAC. Когда два человека устанавливают соединение, каждый пакет содержит адрес двух сетевых карт, и эти адреса используются для маршрутизации пакета на правильный сетевой узел.

Сетевой трафик других компьютеров сети по умолчанию для вас недоступен. Проблема в том, что все сетевые пакеты адресованы кому-то, а ваш сетевой адаптер его проигнорирует, если вы не являетесь получателем пакета. На практике большинство адаптеров имеют возможность принимать чужие пакеты. Для этого нужно просто включить специальный режим работы для вашего

сетевого адаптера, еще его называют беспорядочным (promiscuous). В этом режиме сетевой адаптер принимает все пакеты, входящие в сегмент сети, без разбора. В сети на основе концентратора достаточно переключить адаптер в режим promiscuous, чтобы получить доступ ко всему трафику в локальной сети, поскольку концентратор является примитивным устройством. Когда он получил пакет из некоторого порта, он просто ретранслирует его на другие порты. Таким образом, было бы достаточно просто подключиться к любому порту концентратора для мониторинга сетевого трафика, проходящего через концентратор.

В наши дни большинство локальных сетей основаны на коммутаторе. В отличие от концентратора, коммутатор, получив пакет, ретранслирует его только на один порт, к которому подключен компьютер-получатель согласно построенной заранее таблицы коммутации. Коммутаторы поддерживают таблицу MAC-адресов и портов, связанных с каждым из этих адресов (Content Addressable Memory Table). Когда он получил пакет, коммутатор проверяет MAC-адрес получателя в таблице и выбирает соответствующий порт для маршрутизации пакета. Благодаря этой функции анализ сетевого трафика может быть ограничен: ваш адаптер будет принимать только те пакеты, которые адресованы вам, потому что этот коммутатор не позволит другим пакетам попасть в ваш сегмент сети.

Коммутаторы были созданы для минимизации сетевой нагрузки и максимальной пропускной способности. Кроме того, на рынке доступны специальные управляемые коммутаторы, которые достаточно широко распространены и имеют специальную функцию по упрощению работы систем анализа трафика и решения для мониторинга. Благодаря этой возможности управляемый коммутатор может быть сконфигурирован таким образом, чтобы

все проходящие через него пакеты были реплицированы на определенный порт коммутатора. Производители называют эту функцию по-разному: Port Mirroring, Switched Port Analyzer (SPAN) или Roving Analysis Port (RAP).

Управляемые коммутаторы обладают большим перечнем достоинств, но неуправляемые коммутаторы по-прежнему используются больше по причине их более низкой стоимости. В этом случае, если вы хотите отслеживать трафик, есть два способа доступа к трафику в сети, построенной на неуправляемых коммутаторах, аппаратный и программный.

Аппаратный заключается в подключении управляемого коммутатора или концентратора к интересующему сегменту сети, где вы хотите контролировать трафик (например, до маршрутизатора).

Программный способ для мониторинга трафика в коммутируемой сети основаны на внедрении ложного узла или перенаправлении трафика. Программный перехват сетевого трафика можно разделить на активный и пассивный.

*Активный перехват* трафика, как уже было отмечено, основан на перенаправлении трафика сети. Многие из протоколов стека TCP/IP не обеспечивают механизмы для аутентификации источника или назначения сообщения. Таким образом, они уязвимы для подмены узла сети спуфинга. Наиболее распространенные для локальных сетей: ARP-Spoofing, IP-Spoofing и MAC-Spoofing.

*Пассивный перехват* трафика основан на методе «прослушивания» сетевого интерфейса компьютера. Активный перехват трафика реализуется через атаку на канальном или сетевом уровне, приводящую к перенаправлению трафика.

Перехват трафика осуществляется посредством снифферов – программы, предназначенной для перехвата трафика.

Сниффер работает на уровне сетевого адаптера Network Interface Card (NIC, канальный уровень) и скрытым образом перехватывает весь трафик. Снифферы обходят механизмы фильтрации (адреса, порты и т. д.), а драйверы Ethernet и стек TCP/IP используют для интерпретации данных. Пакетные снифферы захватывают из «провода» все, что по нему приходит. Снифферы могут сохранять кадры в двоичном формате и позже расшифровывать их, чтобы раскрыть информацию более высокого уровня, спрятанную внутри.

Типовой сетевой сниффер имеет следующие компоненты: аппаратное обеспечение, драйвер захвата, буфер, функции анализа в реальном времени, декодер и пакетный редактор.

*Аппаратное обеспечение*. Большинство сетевых снифферов работают со стандартными сетевыми адаптерами, хотя некоторые из них требуют специализированного оборудования, которое обычно имеет больше аналитических возможностей, например, возможность анализировать ошибки.

*Драйвер захвата*. Драйвер захвата является наиболее важным компонентом сетевого сниффера. Он захватывает данные из сети, фильтрует их в соответствии с критериями, заданными пользователем, и сохраняет в буфер.

*Буфер*. Буфер используется для хранения захваченных данных. Он работает в двух режимах. Один предназначен для удаления данных после заполнения буфера. Другой режим основан на циклическом подходе циклический подход, при котором новые данные заменяют устаревшие. Некоторые снифферы могут хранить захваченные данные на жестком диске, позволяя хранить сотни гигабайт данных.

*Анализ в режиме реального времени*. Эта функция анализирует данные сразу после захвата. Она способна обнаружить проблемы с производительностью сети и сбои во время захвата.

*Декодер*. Компонент декодера отображает захваченные сетевые данные с использованием дескриптивного текста, поэтому аналитик сможет понять захваченные данные и выяснить сетевые проблемы.

*Пакетный редактор*. Возможность редактирования позволяет пользователю редактировать захваченные пакеты и повторно передавать их в сеть.

Большинство сетевых снифферов работают одинаково и отображают одну и ту же базовую информацию. Как правило, плата сетевого интерфейса (NIC) на главном компьютере настроена на фильтрацию трафика, который адресован ему. Захваченный трафик передается в декодер драйвера пакетов, который идентифицирует пакеты и разбивает их на соответствующие уровни. Захваченные сетевые данные обычно отображаются в окне с тремя панелями. На верхней панели отображается сводка пакетов данных: дата и время захвата пакета, исходные и целевые IP-адреса и адреса портов, тип протокола и сводка данных пакета. На средней панели указывается логическое содержание выбранного пакета, а на третьей панели отображается пакет в шестнадцатеричном или ASCII форматах.

Одним из самых распространенных снифферов сегодня остается Wireshark – программа, которая поддерживает анализ большого количества разных сетевых протоколов. Этот сниффер позволяет просматривать и сохранять весь проходящий по сети трафик в реальном времени. Для работы сниффера необходимо дополнительно устанавливать библиотеку WinPcap (Packet Capture), которая содержит драйвера и библиотеки для взаимодействия с Network Driver Interface Specification (NIDS). Прямое взаимодействие с NIDS позволяет перехватывать, внедрять и применять фильтрацию сетевых пакетов. На рис. 9.5 представлена сетевая архитектура операционной системы Windows.

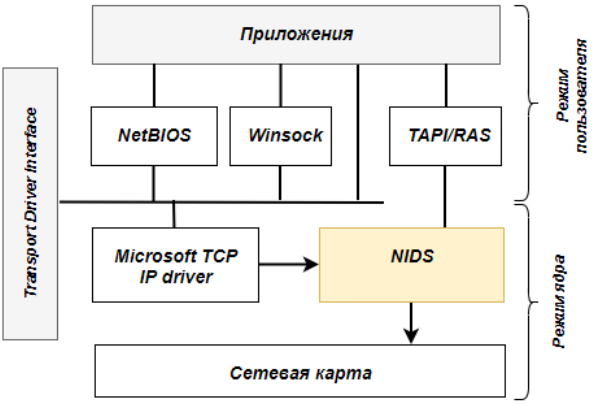


Рис. 9.5. Сетевая архитектура Windows

Библиотека libwiretap предназначена для чтения и записи полученных данных WinPcap. Dumpcap записывает полученные данные на жесткий диск и передает их для анализа. Так libwireshark позволяет анализировать полученный поток данных (рис. 9.6).

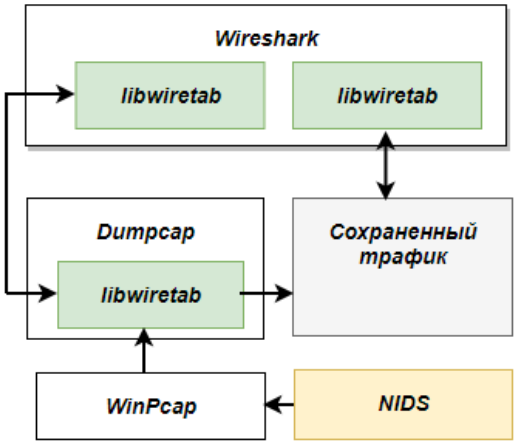


Рис. 9.6. Архитектура Wireshark

Перед использованием любого сетевого снифферa важно определить, под какой платформой он работает.

Практически все сетевые снифферы имеют фильтры захвата и отображения, которые позволяют пользователю захватывать или отображать определенные сетевые пакеты, соответствующие определенным заданным критериям. Также снифферы имеют большой набор фильтров, которые могут использоваться для фильтрации пакетов на основе исходных и/или целевых портов, а также адресов источника и/или назначения.

Чтение собранных данных является важной особенностью сетевых снифферов. Захваченные пакеты могут отображаться разными цветами в зависимости от пользовательских критериев раскраски. Это повышает читаемость захваченных данных. Пользователь может изменить цвет отображения выбранного пакета или группы пакетов. Другим фактором, который повышает разборчивость, является способность декодировать захваченные пакеты данных.

Важной особенностью сетевых снифферов является включение инструментов анализа данных. Эти инструменты предоставляют пользователю статистические отчеты о соединениях, протоколах и использовании сети. Во многих снифферах есть функции редактирования дублирования, удаления, вставки и отправки пакетов.

В дополнение практически все снифферы поддерживают сохранение захваченных данных в файл в разных форматах. Поддерживается экспорт данных в текстовый файл и XML. Эта функция позволяет пользователю импортировать захваченные данные в другие приложения для целей анализа.

В рамках конкретных продуктов могут быть реализованы дополнительные возможности, например, разбор заголовков сетевых протоколов, фильтрация по заданным критериям, восстановление сессий. Снифферы можно разделить на следующие категории:

– анализаторы протоколов (Wireshark, Network Miner, TracePlus Web Detective, CommView);

– пакетные снифферы (RawCap, tcpdump, Network Probe, Etherscan Analyzer).

– снифферы беспроводных сетей (Kismet, airodump-ng, CommView for Wi-Fi) – перехватывают трафик беспроводных сетей даже без подключения к этим сетям;

– password-снифферы (Cain&Abel, Ace Password Sniffer, Intercepter-NG) – перехватывают трафик и извлекают пароли;

– HTTP-снифферы (HTTP Analyzer, IEWatch Professional, EffeTech HTTP Sniffer) – перехватывают HTTP-заголовки;

– print-снифферы (O&K Print Watch, PrintMonitor, Print Inspector) – позволяют контролировать и управлять процессом печати в сети;

– IM-снифферы (MSN Shiffer, ICQ Sniffer, AIM Sniff, IM-Sniffer) – предоставляют перехваченную переписку в виде, удобном для чтения.

Отдельно стоит уделить внимание универсальным инструментам для Windows. Основная цель таких утилит – использование различных методов взлома вместе в программе, ориентированной на восстановление пароля.

*Cain & Abel* – один из самых удобных инструментов безопасности который, вероятно, находится в программном пакете каждого специалиста по безопасности. Согласно официальному сайту, Cain & Abel – это инструмент для восстановления пароля для операционных систем Microsoft. Это позволяет легко восстанавливать различные типы паролей, изучая сеть, взламывая зашифрованные пароли с помощью атак типа «Словарь», «Брутфорс» и «Криптоанализ», записывать VoIP-разговоры, расшифровывая скремблиро-

ванные пароли, восстанавливая ключи беспроводной сети, открывая окна с паролями, кэшированные пароли и анализировать маршрутизацию протоколов (рис. 9.7).

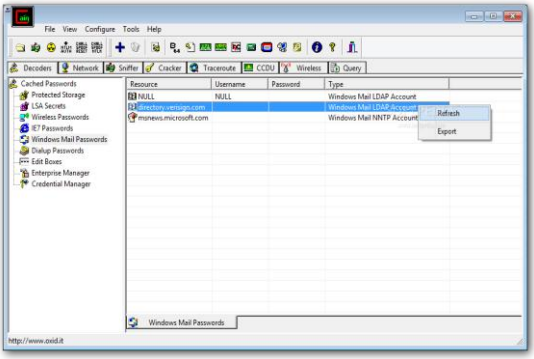


Рис. 9.7. Оконный интерфейс Cain & Abel

Последняя версия работает быстрее и содержит множество новых функций, таких как ARP-Spoofing, которая позволяет перехватывать трафик в коммутируемых локальные сети и реализовывать атаки Man-in-the-Middle. Этот сниффер также может анализировать зашифрованные протоколы, такие как SSH-1 и HTTPS, и содержит фильтры для сбора учетных данных из широкого спектра механизмов аутентификации. Имеется возможность отправки протоколов проверки подлинности протоколов аутентификации.

*Intercepter-NG* – инструмент, который можно использовать для атаки MITM в сети во время теста на проникновение. Он очень удобный для перехвата паролей, зашифрованного трафика, изображений, передаваемых через мессенджеры и многое другое.

Intercepter очень похож на Wireshark при отображении сетевых пакетов и способен перехватывать трафик удаленно на целевом компьютере, захватывая сетевой трафик в этой системе, и передавать захваченные пакеты другому хосту. Инструмент можно

установить на операционную систему Windows, есть консольная версия и смартфоны Android (рис. 9.8).

Рис. 9.8. Оконный интерфейс Intercepter-NG

Кроме перехвата сетевого трафика Intercepter-NG имеет следующие возможности: перехват хешированных паролей (ICQ, IRC, AIM, FTP, IMAP, POP3, SMTP, LDAP, BNC, SOCKS, HTTP, WWW, NNTP, CVS, TELNET, MRA, DC ++ VNC, MYSQL, ORACLE, NTLM); перехват сообщений чата (ICQ, AIM, JABBER, YAHOO, MSN, IRC, MRA); восстановление файлов из HTTP, FTP, IMAP, POP3, SMTP, SMB; промежуточный режим ARP, DHCP; шлюз; интеллектуальное сканирование; удаленный захват трафика с помощью RPCAP-демона; NAT SOCKS DHCP; ARP DNS через ICMP DHCP SSL SSL STRIP WPA DSMBRelay MiTM DNS-Spoofing.

# ГЛАВА X. МОДЕЛИРОВАНИЕ УДАЛЕННЫХ СЕТЕВЫХ АТАК

## § 1. Атаки на канальном уровне

В данной главе будут рассмотрены общие подходы по реализации удаленных сетевых атак, особое внимание уделим работе отдельных протоколов межсетевого взаимодействия и их уязвимостям. В качестве примера будет описано то программное обеспечение, которое позволяет проводить нижеприведенные атаки.

Работа межсетевого взаимодействия компьютерных систем в настоящее время представляется моделью OSI. Данная модель предусматривает семь уровней сетевого взаимодействия, на каждом из которых решаются конкретные задачи.

Осуществить атаку на компьютерные системы в сети можно на физическом, канальном, сетевом и транспортном уровне модели OSI. На физическом уровне основное устройство – это концентратор (Hub) или повторитель (рис. 10.1, 10.2). Атака на данном уровне – это прослушивание трафика, так как производится широковещательная рассылка [2].

Рис. 10.1. Сетевые концентраторы

Рис. 10.2. Сетевые коммутаторы Cisco и D-Link

Развитие сетевых технологий повлияло на появление коммутаторов более сложного устройства по сравнению с концентратором. Коммутатор после подключения к порту компьютера формирует таблицу коммутации, в которой прописаны соответствия порта и MAC-адреса. Получив пакет на один из своих портов, он пересылает его только на тот порт, к которому подключен получатель пакета, идентифицируя его по MAC-адресу.

Далее рассмотрим основные типы атак, которые применимы для коммутаторов. Для реализации описанных сетевых атак важно иметь непосредственный доступ к локальной сети.

*Переполнение таблицы коммутации*. Коммутатор имеет таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста и он работает в режиме обучения. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, и в результате трафик локализуется (рис. 10.3). Таблица коммутации имеет ограниченный размер, например,

для коммутатора Cisco Catalyst 2 960 таблица может хранить до 8 192 MAC-адресов, а Catalyst 6000 серии – до 128 000 MAC-адресов. Content Addressable Memory (далее – CAM) – Cisco термин для обозначения MAC-таблиц, в некоторой литературе упоминается как L2 Forwarding Table [31, 43].

После переполнения таблицы коммутатор превращается в обычный концентратор, рассылая пакеты на все порты.

*VLAN Hopping.* Атака основана на возможности коммутаторов автоматически согласовывать тип своего порта: access или trunk. Следовательно, можно попытаться передать данные в другой VLAN.

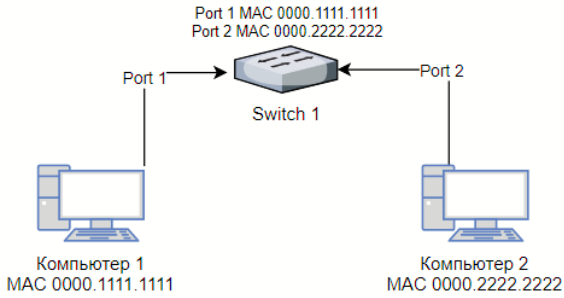


Рис. 10.3. Построение таблицы коммутации

В современных сетях используется протокол 802.1Q, который расширяет кадр, полями VLAN Identifier и VID. Это поле позволяет коммутатору определить, какой группе портов адресован кадр. По сути, 802.1Q – это гибкий механизм для создания необходимой логической топологии, поверх уже существующей физической [31, 43].

PC1 подключен к access-порту fa2/1 коммутатора SW1 в VLAN10. Это означает, что при попадании кадра на порт коммутатора в него будет добавлен 802.1Q header с информацией о принадлежности к VLAN10. SW1 пересылает тегированный кадр на SW2 через trunk-порт. SW2 получает кадр, смотрит в

свою CAM-таблицу и отправляет кадр в соответствующий access-порт, заголовок 802.1Q снимается (рис. 10.4) [43].

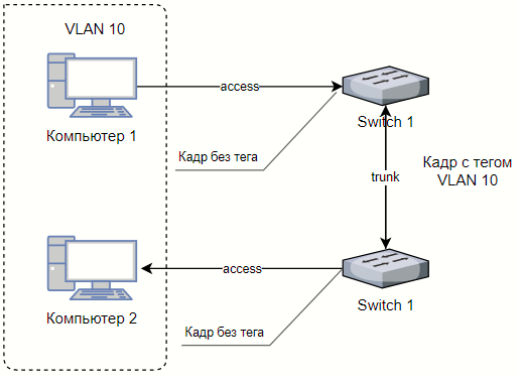


Рис. 10.4. Процесс передачи кадра в сети с протоколом 802.1Q

Как уже было сказано, VLAN hopping основан на том, что коммутаторы имеют возможность автоматически согласовывать тип порта. Для этого используется протокол компании Cisco DTP (Dynamic Trunking Protocol). При его применении (включен по умолчанию) возможны следующие состояния порта: dynamic auto, dynamic desirable, static access, static trunk. Предоставим сводную таблицу о согласовании состояния двух портов, подключенных друг к другу (рис. 10.5) [43].

Порт коммутатора может согласовать свою работу в режиме trunk при определенных условиях, а именно в режимах dynamic auto и dynamic desirable. В том случае, если коммутатор будет вести себя как порт в режиме desirable, он получит доступ к трафику всех VLAN, которыми оперирует коммутатор.

| | Dynamic Auto | Dynamic Desirable | Trunk | Access |
|---|---|---|---|---|
| Dynamic Auto | Access | Trunk | Trunk | Access |
| Dynamic Desirable | Trunk | Trunk | Trunk | Access |
| Trunk | Trunk | Trunk | Trunk | Limited Connectivity |
| Access | Access | Access | Limited Connectivity | Access |

Рис. 10.5. Таблица согласования состояния портов

Проблема заключается в том, что на коммутаторах фирмы Cisco по умолчанию все порты находятся в режиме auto, и, если порт настроен в режиме access/auto, при получении запроса на согласование его состояние может измениться на trunk/auto.

Еще один возможный вектор атаки VLAN hopping – использование native VLAN и добавление второго тега. Работает он только в том случае, если атакующее устройство находится в том VLAN, который является native VLAN для trunk-порта.

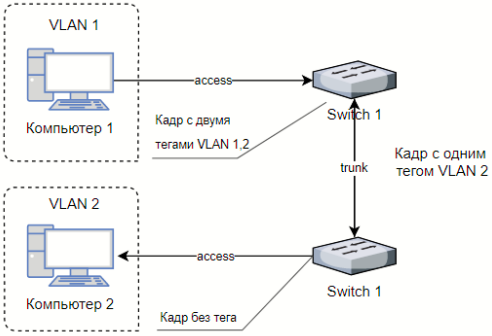


Рис. 10.6. Реализация атаки с использование native VLAN

Исходя из определения native VLAN, кадр, пришедший на порт fa2/1, находящийся в VLAN1, будет передаваться через trunk-порт не тегированным, но, так как атакующий PC1 присвоил ему два заголовка, на выходе он окажется с тегом VLAN2

и дойдет до атакуемого клиента, чего при нормальной ситуации быть не должно (рис. 10.6).

Следует заметить, что такая атака является однонаправленной, так как невозможно по такой же схеме передать кадр обратно.

*Атака на STP*. Протокол STP – предотвращает от зацикливания в мостовой архитектуре локальной сети. Каждая топология STP имеет свой собственный корневой мост (коммутатор), который определяет, как рассчитывается топология STP. Роль корневого коммутатора выбирается таким образом, чтобы все остальные коммутаторы могли определить, насколько много портов от корневого моста. Порт, который имеет самое низкое значение пути, помещается в состояние пересылки. Все остальные порты, которые могут привести к корневому мосту, блокируются. Порты в топологии коммутации, ведущие от корневого моста, продолжают переправляться.

Процесс выбора корневого коммутатора определяется идентификатором моста. Идентификатор моста состоит из настраиваемого приоритета и его MAC-адреса.

Коммутатор с наименьшим идентификатором моста выбирается как корневой мост. Если приоритеты коммутатора равны или если приоритет не настроен, коммутатор с самым низким MAC-адресом выбирается корневым.

Атаки в данном случае направлены на дестабилизацию MAC-таблицы, и удерживать сеть в постоянном состоянии можно, переименовав корневой коммутатор. Добиться этого не сложно, потому что в STP нет механизма аутентификации.

Для этого необходимо создать служебный пакет BPDU несуществующего коммутатора с идентификатором 1, тем самым сделать несуществующий коммутатор корневым мостом. Далее необходимо вызывать постоянное изменение корневого моста,

используя минимальное и максимальное значения в пакетах путем оправки и задержки BPDU.

Повторяя этот процесс, сеть будет находиться в постоянном состоянии переименования корневого моста, и любой широковещательный или многоадресный трафик вызовет широковещательный шторм, насыщая сеть кадрами.

*MAC-Spoofing.* Сетевые узлы могут временно изменять MAC-адрес сетевых интерфейсов на случайные значения для времени рабочего сеанса. Это то, что называется спуфинг MAC-адресов. Метод, используемый коммутаторами для заполнения таблицы MAC-адресов, приводит к уязвимости, известной как спуфинг MAC. Атаки с помощью спуфинга происходят, когда один хост маскирует или позирует как другой, чтобы получать в противном случае недоступные данные или обходить конфигурации безопасности.

В отличие от концентраторов, коммутаторы регулируют поток данных между портами, создавая мгновенные сети, которые содержат только два оконечных устройства, которые общаются друг с другом в тот момент времени. Коммутаторы выполняют это путем пересылки данных из определенных портов на основе MAC-адреса. Коммутаторы поддерживают таблицы MAC-адресов, также называемые таблицами поиска адресной памяти (CAM), для отслеживания MAC-адресов источника, связанных с каждым портом коммутатора. Эти таблицы поиска заполняются процессом адресации на коммутаторе.

Если коммутатор получает входящий фрейм данных, а MAC-адрес назначения не находится в таблице, коммутатор пересылает кадр из всех портов, за исключением порта, на котором он был получен. Когда принимающий узел отвечает, коммутатор записывает MAC-адрес узла в таблицу адресов из поля адреса

источника кадра. Коммутаторы заполняют таблицу MAC-адресов, записывая исходный MAC-адрес кадра и связывая этот адрес с портом, на котором получен кадр.

В сетях с несколькими взаимосвязанными коммутаторами таблицы MAC-адресов записывают несколько MAC-адресов для коммутаторов портов. Эти MAC-адреса отражают удаленные узлы или узлы, которые подключены к другому коммутатору в коммутируемом домене.

*Атака на PVLAN*. Частные виртуальные локальные сети позволяют дополнительно сегментировать участок сети на канальном уровне, ограничивая размер широковещательного домена. Атака на PVLAN использует ожидаемое поведение частной VLAN против самой VLAN. PVLAN – реализуется и ограничивает трафик на канальном уровне. Когда используется PVLAN-коммутатор пересылает весь трафик через маршрутизатор, при этом пересылка происходит, даже если пункт назначения находится в той же локальной сети, что и источник. Однако маршрутизатор является устройством сетевого уровня. Соответственно, имея доступ к маршрутизатору, мы можем перехватить трафик, циркулирующий в PVLAN

Обычно для двух хостов в PVLAN не удается обмениваться данными друг с другом посредством прямой связи второго уровня, это происходит с использованием маршрутизатора в качестве ретрансляции пакетов.

Для реализации данной атаки пользователь может подделать пакет, в котором он укажет в IP-адресе назначения необходимое ему устройство, находящееся на другом порту isolated, источник останется без изменения, а вот в качестве MAC-адреса назначения он укажет MAC-адрес устройства L3. Данное устройство, получив пакет, переправит его по указанному адресу. Принимающая

сторона может сделать то же самое. Таким образом, будет обеспечена передача данных между isolated-портами.

*Атака на DHCP*. DHCP-сервер можно атаковать несколькими различными способами Rogue DHCP Server и DHCP starvation:

1. Можно сформировать и послать DHCP-серверу огромное количество DHCP-запросов с разными MAC-адресами. Сервер будет выделять IP-адреса из пула, и рано или поздно весь DHCP-пул закончится, после чего сервер не сможет обслуживать новых клиентов. По сути, это DoS-атака, так как нарушается работоспособность сети. Метод борьбы с подобными атаками называется DHCP-Snooping. Данный метод заключается в следующем. Когда коммутатор получает пакет, то он сравнивает MAC-адрес, указанный в DHCP-запросе, с MAC-адресом, который был прописан на порту коммутатора. Если адреса совпадают, то коммутатор отправляет пакет дальше, если не совпадают, то пакет отбрасывается.

Действие происходит следующим образом: атакующее устройство запрашивает себе IP-адрес у DHCP-сервера и получает его; MAC-адрес атакующего устройства изменяется, и оно запрашивает следующий, уже другой IP-адрес, маскируясь под нового клиента; такие действия повторяются до тех пор, пока весь пул IP-адресов на сервере не будет исчерпан.

Далее возможны два пути развития событий, в зависимости от того, что является целью атаки:

– отказ в обслуживании. IP-адреса исчерпаны, и новые хосты не могут получить их. Таким образом, их взаимодействие с сетью на этом закончится;

– подмена DHCP-сервера. DHCP starvation отлично комбинируется с предыдущей атакой. Так как на основном DHCP-сервере свободных адресов не осталось, он выбывает из игры,

и 100 % клиентов достается вражескому атакующему DHCP-серверу.

2. Можно также развернуть свой DHCP-сервер, выдавать свои настройки пользователям сети (можно указать любой DNS, Gateway и т. д.) и воспользоваться этим уже по своему усмотрению, начиная от прослушивания трафика до подделки DNS-ответов и т. д.

Цель данной атаки – подмена DHCP-сервера. При одновременном нахождении в сети двух DHCP-серверов, один из которых «вражеский», некоторая часть клиентов сконфигурирует у себя неправильные адреса и прочие сетевые реквизиты.

Вследствие подмены шлюза по умолчанию неавторизованный DHCP-сервер получит возможность прослушивать весь трафик клиентов, перенаправляя в дальнейшем пакеты по назначению. Таким образом мы имеем простейшую реализацию атаки типа MitM (Man in the Middle), которая может быть осуществлена в большинстве современных сетей.

*ARP-Spoofing* (ARP Cache poisoning) – это атака, используемая для прослушивания сети, построенной на коммутаторах. ARP (англ. Address Resolution Protocol – протокол определения адреса), использующийся в компьютерных сетях протокол низкого уровня, предназначенный для определения адреса канального уровня по известному адресу сетевого уровня.

Суть этой атаки заключается в следующем. Посылает ложные ARP-пакеты, для того чтобы убедить компьютер жертвы в том, что прослушивающий компьютер и есть конечный адресат. Далее пакеты с компьютера жертвы перехватываются и пересылаются реальному получателю, mac-адрес отправителя в них подменяется, чтобы ответные пакеты тоже шли через прослушивающий компьютер. Прослушивающий компьютер становится шлюзом для трафика жертвы.

Стоит отметить, что при попытке прослушать трафик нескольких активно общающихся компьютеров и, соответственно, возникающем при этом переполнении APR-таблиц, возможны перегрузка и, как следствие, падение сети. Помимо прочего, это чревато обнаружением атаки.

Также стоит отметить, что данная атака может быть реализована только при наличии доступа в локальную сеть. За пределами локальной сети, не удастся осуществить ARP-Spoofing. Для реализации этой атаки ему придется сначала захватить контроль над одной из машин, находящейся в одном сегменте локальной сети, а уже потом с этой машины осуществлять «отравление» ARP-кэша.

## § 2. Атаки на сетевом уровне

Атаки на сетевом уровне нацелены на маршрутизаторы и алгоритмы маршрутизации. Маршрутизатором назначается основное устройство сетевого уровня эталонной модели взаимодействия открытых систем (рис. 10.7). Маршрутизаторы связывают многочисленные компьютерные сети, представляющих интернет, и отвечают за определение адресата и выбор наилучшего маршрута, пакета данных до этого пункта назначения (получателя).

Маршрутизаторы могут объединять несколько основных сервисов и утилит сети, это делает их более безопасными и гибкими. Маршрутизаторы могут, например, содержать служебную программу безопасности, такую как брандмауэр. Они также могут помочь повысить функциональность сети, интегрируя сервисы голосовые и видеопотоки данных.

Существует два основных типа маршрутизаторов: статические и динамические. Статический маршрутизатор настраивается вручную администратором сети, в нем программируются

все маршруты, по которым происходят пересылки пакетов данных. Динамический маршрутизатор автоматически управляет маршрутизацией трафика по сети с использованием протоколов маршрутизации.


Рис. 10.7. Профессиональный и домашний маршрутизатор

В средах, использующих статическую маршрутизацию, маршруты и информация о маршруте вводятся вручную в таблицы маршрутизации, что может привести к ошибкам. Кроме того, при изменении макета или топологии сети статически настроенные маршрутизаторы должны быть вручную обновлены с изменениями. По данным причинам статическая маршрутизация подходит только для маленькой среды, где возможны только один или два маршрутизатора. Практичнее использовать динамическую маршрутизацию.

В динамической среде маршрутизации используются специальные протоколы маршрутизации для связи. Цель этих протоколов проста: они позволяют маршрутизаторам передавать информацию о себе другим маршрутизаторам, чтобы они могли создавать таблицы маршрутизации. Существуют два основных типа протоколов маршрутизации: протоколы векторных расстояний (RIP) и протоколы состояния канала (OSPF).

RIP является относительно старым, но все еще широко используемым внутренним протоколом маршрутизации, созданным для использования в небольших однородных сетях. Это

классический протокол маршрутизации на основе расстояния. RIP документируется в RFC 1058.

RIP использует пакеты данных протокола пользовательских дейтаграмм (UDP) для обмена информацией о маршрутизации. Программное обеспечение Cisco IOS отправляет информацию о маршрутизации каждые 30 с, что называется рекламой. Если маршрутизатор не получает обновления от другого маршрутизатора в течение 180 с и более, он отмечает маршруты, обслуживаемые необожженным маршрутизатором, как непригодные для использования. Если обновления по истечении 240 с все еще не происходит, то маршрутизатор удаляет все записи таблицы маршрутизации для незарегистрированного маршрутизатора.

Метрикой, которую RIP использует для оценки стоимости различных маршрутов, является подсчет переходов. Счетчик переходов – это количество маршрутизаторов, которые могут быть пройдены по маршруту. Прямая связь имеет метрику ноль; если количество переходов равно 16, то узел считается не доступным. Если пропускная способность между маршрутизаторами неодинакова, то использование протокола RIP неэффективно. На примере, изображенном на рис. 10.8, видно, что данный протокол выберет маршрут с более низкой пропускной способностью по причине меньшего числа переходов.

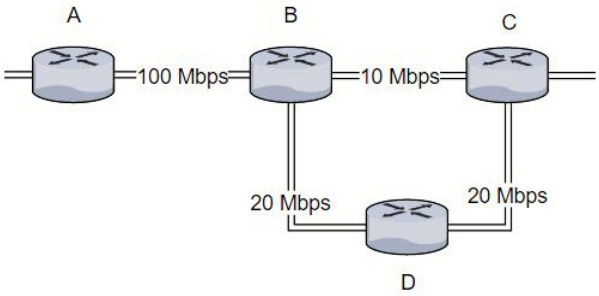


Рис. 10.8. Выбор протокола RIP между точками A-C будет по принципу меньшего количества переходов

Протоколы динамической маршрутизации уязвимы для классических атак, таких как DDoS, прослушивание и модификация трафика. Отказ в обслуживании являются общей угрозой для различных устройств и приложений. Они не специфичны для RIP. Другое дело – прослушивание и модификация трафика. Здесь основными атаками, типичными для протокола маршрутизации RIP, являются следующие: ложные маршруты, понижение версии протокола RIP, взлом хеша MD5 [2].

*Open Shortest Path First (OSPF)* – это протокол внутренних шлюзов (IGP), стандартизованный целевой группой Internet Engineering Task Force (IETF) и широко используемый в крупных корпоративных сетях. OSPF – это протокол маршрутизации состояния канала, обеспечивающий быструю конвергенцию и отличную масштабируемость. Как и все протоколы состояния канала связи, OSPF очень эффективен в использовании полосы пропускания сети.

Cisco является активным членом рабочей группы OSPF в IETF и отвечает за многие из продолжающихся усовершенствований протокола. Протокол маршрутизации (OSPF) не имеет механизма аутентификации, что может позволить атакующему полностью контролировать таблицу маршрутизации и перехватывать трафик.

Атака осуществляется отправкой поддельных пакетов OSPF. Успешная отправка может привести к перестроению таблицы маршрутизации на целевом маршрутизаторе, а также распространению созданного обновления.

Чтобы использовать эту уязвимость, атакующий должен точно определить некоторые параметры в базе данных LSA на целевом маршрутизаторе. Эта уязвимость может быть инициирована только путем отправки обработанных одноадресных или

многоадресных пакетов LSA первого типа. Никакие другие пакеты LSA не могут вызвать эту уязвимость. Эта уязвимость не устранена в протоколе OSPFv3.

Эта уязвимость возможна только на LSA-маршрутизаторах (LSA тип 1). В результате использования этой уязвимости целевой маршрутизатор будет иметь несогласованную информацию в своей базе данных LSA-данных Router Link States, где информация идентификатора ссылки не будет соответствовать идентификатору «рекламного» маршрутизатора в выводе команды show ip ospf database.

BGP – это протокол, позволяющий одной сети интернета сообщать другим о своем существовании и сетях, которые могут быть достигнуты через него. Они также могут узнать, как добраться до других сетей в интернете. Получив информацию BGP, маршрутизаторы выбирают лучший маршрут в целевую сеть и добавляют ее в свои таблицы маршрутизации. BGP использует несколько параметров для определения наилучшего маршрута. Наиболее очевидным является количество сетей до места назначения или длина так называемого AS-Path. Чем короче AS-Path, тем лучше маршрут. Другое общее правило – самое длинное префиксное совпадение. Маршрут с самой длинной, более конкретной маской предпочтительнее при отправке пакета. Другими словами, если вы видите объявления для 130.95.0.0/16 сеть (т. е. 130.95.0.0–130.95.255.255) по пути A и объявления к 130.95.0.0/24 сети (т. е. 130.95.0.0–130.95.0.255) через пути B, трафик, следуя на 130.95.0.0 / 24 будет проходить по пути B несмотря на то, что путь A может быть намного короче.

Протокол пограничного шлюза (BGP, RFC 4271) является широко используемым протоколом маршрутизации между автономными системами. Связь BGP между одноранговыми маршрутизаторами имеет решающее значение для стабильной работы

интернета. Множественные реализации BGP-приложений не обрабатывают специально созданные сообщения BGP UPDATE. Уязвимая реализация BGP может сбрасывать сеансы при обработке обработанных сообщений UPDATE. Постоянная атака может привести к нестабильности маршрутизации (разворот маршрута). Чтобы повлиять на сеанс BGP, атакующему необходимо будет успешно внедрить специально созданный пакет в существующий сеанс BGP или базовый сеанс TCP (179/tcp). Другими словами, необходимо иметь действительный, настроенный сеанс BGP или иметь возможность обманывать трафик TCP.

Данная уязвимость была впервые объявлена как влияющая на маршрутизаторы Juniper, но дальнейшие исследования показали, что маршрутизаторы других производителей имеют такую же уязвимость.

Удаленный атакующий может вызвать отказ в обслуживании, введя специально обработанное сообщение BGP UPDATE в законный сеанс BGP. Атакующий с настроенным сеансом BGP может атаковать цели с удалением BGP или может обмануть TCP-трафик.

## § 3. Атаки на транспортном уровне

Протоколы транспортного уровня предназначены для обеспечения непосредственного информационного обмена между двумя пользовательскими процессами. Существует два типа протоколов транспортного уровня: сегментирующие протоколы и несегментирующие протоколы доставки дейтаграмм.

Сегментирующие протоколы транспортного уровня разбивают исходное сообщение на блоки данных транспортного уровня – сегменты.

Протоколы доставки дейтаграмм не сегментируют сообщение и отправляют его одним целым, называемым дейтаграммой. При этом функции установления и разрыва соединения, управления потоком не нужны. Протоколы доставки дейтаграмм просты для реализации, однако не обеспечивают гарантированной и достоверной доставки сообщений.

В качестве протоколов транспортного уровня в сети Internet могут быть использованы два протокола: UDP и TCP. Рассмотрим, как можно воздействовать на эти протоколы.

*Атаки на TCP*. Протокол TCP используется для обеспечения надежного информационного обмена на транспортном уровне в интернете. Транспортный протокол является наиболее распространенным средством транспортировки трафика. Прежде всего рассмотрим механизм действия протокола. В отличие от протокола UDP, который может сразу же начать передачу пакетов, TCP устанавливает соединения (виртуальный канал), которые должны быть созданы перед передачей данных. TCP-соединение можно разделить на три стадии: установка соединения, передача данных, завершение соединения.

Начало сеанса TCP принято называть трехсторонним рукопожатием (three-way handshake). Это метод, используемый TCP, который устанавливает TCP/IP-соединение через сеть на основе протокола интернет. Технология трехстороннего установления связи TCP часто упоминается как SYN-SYN-AC» (или, более точно, SYN, SYN-ACK, ACK), поскольку три протокола передаются TCP для согласования и запуска сеанса TCP между двумя компьютерами. Механизм handshaking TCP разработан таким образом, чтобы два компьютера при установлении связи могли согласовывать параметры сетевого соединения сокета TCP перед передачей данных, таких как запросы веб-браузера SSH и HTTP.

Данный трехсторонний процесс установления связи разработан таким образом, что оба конца могут инициировать и согласовывать отдельные соединения сокетов TCP одновременно. Возможность одновременного согласования нескольких соединений сокетов TCP в обоих направлениях позволяет объединить один физический сетевой интерфейс, такой как Ethernet, для одновременной передачи нескольких потоков данных TCP.

Ниже приведена упрощенная схема трехстороннего процесса установления связи TCP (рис. 10.9).

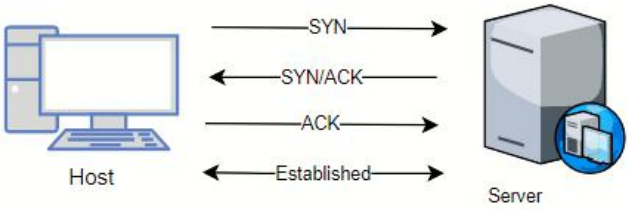


Рис. 10.9. Тройное рукопожатие протокола TCP

Host отправляет пакет хронологии TCP SYN на сервер (или другой компьютер). Server получает Host SYN. Server передает SYNchronize-ACKnowledgement. Host получает Server SYN-ACK. Host отправляет ACKnowledge. Server получает ACK. Соединение сокетов TCP – Established.

SYNchronize и сообщения ACKnowledge обозначаются как SYN-битом, так и ACK-битом внутри заголовка TCP, а сообщение SYN-ACK имеет как бит SYN, так и ACK-бит, включенный в заголовке TCP.

TCP знает, открывается ли соединение сокета сетевого TCP или синхронизируется, устанавливается с помощью сообщений SYNchronize и ACKnowledge при установлении подключения к сети TCP.

Когда связь между двумя компьютерами завершается, выполняется другая трехсторонняя связь для разрыва соединения сокета TCP. Эта настройка и отключение соединения сокетов TCP являются частью того, что квалифицирует TCP как надежный протокол. TCP также подтверждает, что данные успешно получены, и гарантирует, что данные будут повторно определены в правильном порядке.

Обратите внимание, что UDP – протокол без установления соединения. Это означает, что UDP не устанавливает соединения, как TCP, поэтому он не выполняет это трехстороннее рукопожатие, и по этой причине называется ненадежным протоколом. Это не означает, что UDP не может передавать данные, он просто не обсуждает, как будет работать conneciton, а просто передает данные.

Обратите внимание, что FTP, Telnet, HTTP, HTTPS, SMTP, POP3, IMAP, SSH и любой другой протокол, проходящий через TCP, тоже используют трехстороннее рукопожатие, выполняемое при открытии соединения. HTTP-запросы в интернете, SMTP-сообщения электронной почты, передача файлов FTP – все управляют сообщениями, которые они отправляют. TCP обрабатывает передачу этих сообщений.

TCP отправляется поверх протокола интернета (IP) в стеке протоколов, поэтому комбинированные пары интернет-протоколов называются TCP/IP (TCP через IP). Сегменты TCP передаются внутри раздела полезной нагрузки IP-пакетов. IP обрабатывает IP-адресацию и маршрутизацию и получает пакеты из одного места в другое, но TCP управляет фактическими сокетами связи между конечными точками (компьютеры из каждой точки сети или интернет-соединения).

Протокол TCP является ориентированным на соединение и надежным протоколом, но рассмотрим подробней как работает

TCP. Предположим, есть два хоста (A и B), которые хотят общаться друг с другом. Предположим, что хост A начинает общение. Теперь с точки зрения TCP хост A отправляет SYN-пакет в узел B. Пакет SYN представляет собой пакет TCP с флагом SYN. В этом пакете также упоминается начальный порядковый номер (sequence number), который является значением, генерируемым TCP-сервером хоста A исходным портом (целевым портом). Когда этот пакет принимается на уровне TCP хоста B, этот хост отвечает TCP-пакетом с флагами SYN и ACK, начальным порядковым номером и другой информацией. Когда хост A принимает этот пакет, он проверяет некоторую информацию, такую как флаг SYN, номер подтверждения Acknowledgment Number (который равен sequence number + 1), чтобы убедиться, что это ожидаемый пакет из Host B. В ответ хост A отправляет пакет с флагом ACK. И номером подтверждения, установленным для sequence number B + 1.

Таким образом, можно увидеть, что порядковые номера играют важную роль в TCP-связи. Номер последовательности – это номер, который TCP связывает с начальным байтом данных в определенном пакете. Таким образом, принимающий TCP отслеживает полученные данные и подтверждает их. Номер подтверждения всегда является следующим ожидаемым порядковым номером. Все атаки основаны на угадывании TCP-последовательности и атаки сброса TCP соединения.

Рассмотрим техники сетевых атак.

*Атака прогноза последовательности TCP (IP-Spoofing).* Предположим, что хост A и хост B соединены друг с другом, атакующий, находящийся между ними, может контролировать пакеты между A и B. Так, при атаке Host A он наводнит Host B новыми запросами, вызывающими атаку Denial of Service, чтобы остановить общение Host B с A. Теперь он может предсказать

порядковый номер пакета, который ожидает А от В. Атакующий готовит такой пакет и отправляет его в Host А. Так как его поддельный номер упакованный, так что хозяин А думает, что его выход из Б. Теперь он представляет собой пакет, завершающий соединение или запрашивающий Host А для запуска некоторых вредоносных команд, скриптов и т. д. Таким образом, соединение может быть захвачено.

Другим способом может быть предсказание ISN (начальный порядковый номер): когда создаются новые соединения, используется генератор ISN, который выбирает новый 32-битный ISN. Генератор связан с 32-битными тактами (возможно, фиктивными), бит младшего порядка которых увеличивается примерно каждые четыре микросекунды. Таким образом, ISN-цикл завершает свой круг примерно каждые 4,55 часов. Поскольку мы предполагаем, что сегменты останутся в сети менее 4,55 часов (приравнивается к максимальной продолжительности жизни сегмента MSL), то можно предположить, что ISN будет уникальным.

Стеки TCP/IP BSD отключаются от вышеуказанного механизма. Стеки BSD TCP/IP увеличивают порядковый номер на 128 000 с и на 64 000 с для каждого нового TCP-соединения.

*Атака сброса TCP соединения*. Если атакующий может захватить TCP-сессию (как сказано выше), то данная атака может быть запущена. Необходимо отправить пакеты с RST Flag ON на А и В или на любой из хостов. А, и В не знают, что пакеты, отправлены злоумышленником и обрабатывают эти пакеты. Если они сбрасывают пакеты, то соединение между А и В прекращается. Таким образом, атаки TCP-сброса нацелены на прекращение действительного TCP-соединения между двумя хостами.

Создание пакетов (packet crafting) – это техника, которая позволяет сетевым инженерам или пентестерам исследовать

сети, проверять правила межсетевых экранов и находить уязвимые места. Делается это обычно вручную, отправляя пакеты на различные устройства в сети.

Создание пакетов вручную не означает, что нужно писать код на каком-либо высокоуровневом языке программирования, можно воспользоваться готовым инструментом, например Scapy.

*Атака SYN-flood.* Этот тип атаки, по сути, «отказ в обслуживании» (DDoS), целью которого сделать сервер недоступным, используя все доступные серверные ресурсы. Повторно отправляя пакеты начального запроса на соединение (SYN), атакующий может перегружать все доступные порты на целевом сервере, что приводит к тому, что целевое устройство реагирует медленно или вообще не работает. SYN-flood может проводиться тремя различными способами:

– *прямая атака* – это поток SYN, где IP-адрес не подделан. В этой атаке атакующий не маскирует свой IP-адрес. В результате атакующий использует одно исходное устройство с реальным IP-адресом для создания атаки. На практике этот метод используется редко (если вообще используется), в этой атаке нужно просто заблокировать IP-адрес каждой вредоносной системы;

– *spoofed attack* – при этом способе атакующий может также подделывать IP-адрес в каждом отправляемом SYN-пакете, чтобы препятствовать усилиям по отслеживанию и затруднять их идентификацию. Хотя пакеты могут быть подделаны, их можно проследить обратно к источнику.

*Распределенная атака* (DDoS). Если атака создается с использованием бот-сети, вероятность отслеживания атаки очень низка. Для дополнительного уровня анонимности атакующий может иметь каждое распределенное устройство, которое также подменяет IP-адреса, с которых он отправляет пакеты.

*Атака Teardrop*. Это тоже атака «отказ в обслуживании» (DoS), которая включает отправку фрагментированных пакетов на целевую машину. Так как машина, получающая такие пакеты, не может их собрать из-за ошибки в повторной сборке фрагментации TCP/IP, пакеты перекрываются друг с другом, происходит сбой целевого сетевого устройства. Обычно это возникает в более старых операционных системах, таких как Windows 3.1x, Windows 95, Windows NT и версиях ядра Linux до 2.1.63.

Одним из полей в заголовке IP является поле «смещение фрагмента», указывающее начальную позицию или смещение данных, содержащихся в фрагментированном пакете, относительно данных в исходном пакете. Если сумма смещения и размер одного фрагментированного пакета отличается от суммы следующего фрагментированного пакета, они перекрываются. Когда это происходит, сервер, уязвимый для атак teardrop, не может собрать пакеты, что приведет к условию отказа в обслуживании.

*TCP Session Hijacking*. Цель атаки на захват TCP-сессии заключается в том, чтобы захватить существующее TCP-соединение (сеанс) между двумя жертвами, введя вредоносное содержимое в этот сеанс. Если это соединение является сеансом telnet, атакующие могут вводить вредоносные команды в этот сеанс, заставляя жертвы выполнять вредоносные команды.

*Атаки на ICMP*. Основное назначение протокола обмена управляющими сообщениями ICMP – это обнаружение ошибок и передача информации о таких ошибках. Протокол транспортного уровня (в частности, TCP), получая сообщения ICMP об ошибках в сети, может выполнять те или иные действия для преодоления возникших проблем.

ICMP-сообщения также могут использоваться для атаки на TCP. Для этого атакующий отправляет сообщение об ошибке ICMP, которое указывает на ошибку в любой из двух конечных

точек TCP-соединения. Соединение должно быть немедленно разорвано, поскольку RFC 1122 предусматривает, что хост должен прервать соответствующее соединение при получении такого сообщения об ошибке ICMP. RFC 1122 определяет такие ошибки, как сообщения об ошибках ICMP типа 3 (Destination Unreachable) с кодом 2 (недопустимый протокол), 3 (порт недоступен) или 4 (требуется фрагментация и бит DF).

Сообщение об отключении источника ICMP используется перегруженными маршрутизаторами, чтобы сообщить TCP-отправителям о необходимости замедления работы. Необходимо отметить, что некоторые системы могут разумно игнорировать этот тип ICMP-ошибок в определенном состоянии TCP.

*ICMP-Tunneling*. ICMP может содержать данные о времени и маршрутах. Пакет может использоваться для хранения информации, отличной от предполагаемой информации. Это позволяет использовать ICMP-пакет в качестве канала связи между двумя системами. Канал можно использовать для отправки троянского коня или другого вредоносного пакета. Показателем счетчика является отказ в трафике ICMP в вашей сети.

*Smurf*. Эта атака использует IP-спуфинг и трансляцию для отправки ping группе хостов в сети. Когда хост пингует, он отправляет информацию о трафике сообщений ICMP. Если широковещательная передача отправляется в сеть, все хосты ответят на пинг. Результатом является перегрузка сети и целевой системы. Единственный способ предотвратить эту атаку – запретить трафик ICMP на маршрутизаторе.

Атаки, приводящие к снижению скорости передачи данных, в отдельных случаях решаются гораздо сложнее чем полный разрыв соединений.

*Атаки на UDP*. Протокол пользовательских дейтаграмм предлагает только минимальную транспортную услугу (не гарантированную доставку дейтаграмм) и предоставляет приложениям прямой доступ к службе дейтаграмм IP-уровня. UDP использует приложения, которые не требуют уровня обслуживания TCP или которые хотят использовать службы связи (например, многоадресную или широковещательную доставку), недоступные из TCP.

UDP – это почти нулевой протокол. Единственными услугами, которые он предоставляет по IP, являются контрольные суммы данных и мультиплексирование по номеру порта. Поэтому прикладная программа, работающая поверх UDP, должна иметь дело непосредственно со сквозными проблемами связи, с которыми мог бы справиться протокол, ориентированный на соединение, например повторная передача для надежной доставки, пакетирования и повторной сборки, управления потоком, предотвращения перегрузки и т. д., когда это необходимо. Достаточно сложная связь между IP и TCP будет отражена в связи между UDP и многими приложениями, использующими UDP.

*UDP Flood Attack.* Подобно потоку ICMP, наводнение UDP происходит, когда атакующий отправляет IP-пакеты, содержащие датаграммы UDP, с целью замедления жертвы до такой степени, что она больше не может обрабатывать действительные соединения. Атака на UDP представляет собой сетевой поток и попрежнему является одним из наиболее распространенных отказов сегодня. Атакующий отправляет UDP-пакеты, обычно большие, на один пункт назначения или на случайные порты. В большинстве случаев атакующие обманывают SRC IP, что легко сделать, поскольку протокол UDP является бесконтактным и не имеет какого-либо механизма рукопожатия или сеанса.

Основной целью потока UDP является насыщение интернет-канала и оказание влияния на сеть и элементы безопасности, а чаще всего на брандмауэры, на пути к целевому серверу.

## § 4. Атаки на беспроводные устройства и технологии

Сегодня беспроводные сети стали уязвимей кабельных – в проводной сети пакеты информации передаются по физическому носителю, например, используется медный кабель или оптоволокно, между тем злоумышленники способны перехватить сигнал, находясь в зоне действия сети и не имея физического доступа. Готовясь к обеспечению безопасности беспроводных сетей, следует изучить беспроводные атаки и установить, что может им угрожать в той или иной ситуации.

Беспроводные атаки могут осуществляться разными способами. Одни методы полагаются на обман пользователей, другие используют брутфорс, а некоторые ищут людей, которые не защищают свою сеть. Многие из этих атак тесно связаны друг с другом. Ниже рассмотрим некоторые виды этих атак:

1. *Обнаружение пакетов.* Когда информация отправляется туда и обратно по сети, она отправляется пакетами. Поскольку трафик передается по радиоканалу, сделать это очень легко. Довольно много трафика (FTP, HTTP, SNMP и т. д.) отправляется в открытом виде, что означает отсутствие шифрования. Поэтому использование такого инструмента, как Wireshark, позволяет читать данные в виде простого текста. Это может привести к легкому похищению паролей или утечке конфиденциальной информации. Зашифрованные данные также могут быть захвачены, но

атакующему гораздо труднее расшифровать защищенные пакеты данных.

2. *Точка доступа Rouge.* Когда в сети появляется неавторизованная точка доступа (AP), она считается точкой доступа к сети. Такие точки могут быть доступны неопытному пользователю. Эти точки доступа представляют собой уязвимость для сети, поскольку они оставляют ее открытой для различных атак. К ним относятся сканирование уязвимостей для подготовки атак, отравления ARP, захвата пакетов и атак типа «отказ в обслуживании».

3. *Кража пароля*. При передаче данных по беспроводным сетям пользователи часто заходят на сайт и отправляют пароли, и, если сайт не использует SSL или TLS, этот пароль находится в обычном тексте для чтения. Есть способы обойти эти методы шифрования, чтобы украсть пароль.

4. *«Человек посередине» (MITM).* Можно обмануть коммуникационные устройства, которые могут записывать трафик для просмотра позже (например, при обрыве пакетов) и даже изменять содержимое файлов. В эти пакеты можно вставлять различные типы вредоносных программ, изменять содержимое электронной почты или отбросить трафик, чтобы связь была заблокирована DOS-атакой.

5. *Подавление.* Существует множество способов обрыва беспроводной сети. Один из методов – отправка точке доступа кадров деаутентификации. Это эффективно подавляет сеть и предотвращает прохождение легального трафика. Эта атака немного необычна, потому что не приносит никакой пользы. Один из немногих примеров того, как можно ее использовать – это подавление сигналов Wi-Fi конкурентов, что является незаконным (как и все эти атаки), поэтому компании будут стремиться их не использовать.

6. *WarDriving.* Термин происходит от старого понятия «военный» набор, где люди набирают случайные телефонные номера в поисках доступных модемов. Суть атаки в объезде окрестностей, в попытках найти уязвимые точки доступа. Можно использовать беспилотные летательные аппараты, чтобы попытаться взломать точки доступа на более высоких этажах здания.

7. *Атаки на протоколы шифрования WEP/WPA*. Атаки на беспроводные маршрутизаторы могут быть огромной проблемой. Старые стандарты шифрования чрезвычайно уязвимы. В этом случае довольно легко получить ключ доступа. Далее рассмотрим более подробно уязвимости WEP, WPA и WPA2.

На данный момент WPA, Wi-Fi Protected Access – новый, самый современный механизм защиты беспроводных сетей от неавторизованного доступа. WPA, и его дальнейшее развитие WPA2 пришли на замену механизму WEP, был не безопасен.

Кадр данных при использовании WEP состоит из зашифрованной и незашифрованной части. Зашифрованная часть содержит в себе данные и контрольные суммы (CRC32), незашифрованная – *вектор инициализации (IV)* и идентификатор ключа. Каждый кадр данных шифруется поточным шифром RC4, используя в качестве ключа шифрования вектор инициализации с присоединенным к нему ключом WEP.

Таким образом, для каждого кадра данных генерируется свой ключ шифрования, однако в то же время каждый новый ключ шифрования отличается от другого всего лишь на вектор инициализации (24 бита, когда длина ключа может быть 40 либо 104 бит).

Если перехватить много пакетов, то также можно получить большое количество зашифрованных данных и векторов инициализации. Как мы выяснили, ключ шифрования для каждого последующего кадра отличается от предыдущего всего на 24 бита

(длина вектора инициализации). Следовательно, есть возможность извлечения ключа путем выполнения математических операций над пакетами.

Практика показывает, что для того, чтобы успешно получить ключ WEP, необходимо захватить около 100–200 тыс. векторов инициализации, в зависимости от длины ключа (WEP-40 или WEP-104). Обычно, для этого нужно перехватить 25–50 Мб трафика, передающегося в сети. При наличии высокой сетевой активности (загрузка файлов или видеоконференции) для захвата необходимого объема трафика хватит 5–10 мин. Так как технология безопасности WEP была взломана довольно давно, то в сети можно найти утилиты, которые в автоматическом режиме извлекают ключ из CAP-файла (дампа трафика), самой распространенной среди них является Aircrack-NG. Поэтому сейчас довольно редко можно встретить беспроводные сети с безопасностью на WEP, к тому же современные маршрутизаторы (роутеры) в настройках безопасности уже не предусматривают настройку WEP. Сегодняшние корпоративные сети защищены WPA и WPA2.

Первые модификации WPA представляли собой усовершенствованный WEP. В нем используется 48-битный вектор инициализации, изменены правила построения вектора, также для подсчета контрольной суммы применяется MIC (Message Integrity Code), который пришел на смену устаревшему и менее надежному CRC32.

Самым главным усовершенствованием является то, что длина ключа шифрования теперь составляет 128 бит, вместо 40. Для управления ключами существует специальная иерархия, которая призвана предотвратить предсказуемость ключа шифрования для каждого кадра. Благодаря протоколу целостности временного

ключа (TKIP) ключ шифрования для каждого кадра данных генерируется таким образом, чтобы они не повторяли друг друга. Это сделало WPA-сети полностью защищеными от атак replay (повторение ключей) и forgery (подмена содержимого пакетов).

Кроме того, в WPA были интегрированы механизмы проверки подлинности: EAP, а также осуществляется полная поддержка 802.1X-стандартов.

8. *Extensible Authentication Protocol* (EAP) – один из самых распространенных протоколов проверки подлинности. Используется для аутентификации в проводных сетях, поэтому WPA-беспроводная сеть легко интегрируема в уже имеющуюся инфраструктуру. Обязательным условием аутентификации является предъявление пользователем маркера доступа, подтверждающего его право на доступ в сеть. Для получения маркера выполняется запрос к специальной базе данных, а без аутентификации работа в сети для пользователя будет запрещена. Система проверки расположена на специальном RADIUS-сервере, а в качестве базы данных используется Active Directory (в системах Windows). Таким образом, WPA является комбинацией технологий и стандартов 802.1X + EAP + TKIP + MIC.

Тем не менее TKIP-защита была частично взломана в 2008 г. Для ее успешного обхода необходимо, чтобы в беспроводном маршрутизаторе использовался QoS. Есть возможность перехватывать и расшифровывать данные, а также подделывать пакеты, передаваемые в сети. Поэтому был разработан механизм WPA2, представляющий собой усовершенствованный WPA.

Нахождение уязвимостей в WPA привело к тому, что были создан метод защиты WPA2. Существенным отличием его от WPA является то, что трафик в сети шифруется не только от устройств, не подключенных к этой сети, но и друг от друга.

Иными словами, каждое устройство имеет свои ключи шифрования для обмена данными с точкой доступа. В сети существует несколько ключей шифрования:

– Pairwise Transient Key (PTK) – при помощи данного типа ключа шифруется личный трафик каждого клиента. Таким образом обеспечивается защита сети «изнутри», чтобы один клиент, авторизованный в сети, не мог перехватить трафик другого;

– Group Temporal Key (GTK) – данный ключ шифрует широковещательные данные.

WPA2 используется в качестве алгоритма шифрования CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) – протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика – протокол шифрования для сети WPA2, использующий алгоритм AES как основу для шифрования данных. В соответствии со стандартом FIPS-197 используется 128-битный ключ шифрования.

Основное отличие от TKIP и WEP – это централизованное управление целостностью пакетов, которое выполняется на уровне AES. Структура пакета, зашифрованного CCMP, увеличена на 16 октетов. Заголовок CCMP состоит из трех частей: PN (номер пакета, 48-разрядный), ExtIV (вектор инициализации), и идентификатора ключа (рис. 10.10) [74].

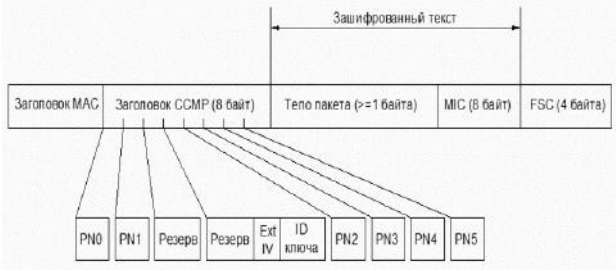


Рис. 10.10. Структура пакета, зашифрованного CCMP

Инкапсуляция данных с использованием CCMP (рис. 10.11):

1) номер пакета увеличивается на некое число, чтобы избежать повторения пакетов;

2) создаются дополнительные аутентификационные данные;

3) создается служебное поле nonce;

4) номер пакета и идентификатор ключа помещаются в заголовок пакета;

5) поле nonce и дополнительные аутентификационные данные шифруются с использованием временного ключа.

Еще одной особенностью WPA и WPA2 является усиленная аутентификация. Для этого в классическую реализацию WAP/WPA2 включена поддержка 802.11 и EAP. На практике это выглядит следующим образом: пользователю предлагается ввести логин и пароль для доступа в сеть. Проверка учетных данных выполняется на RADIUS-сервере, который, в свою очередь, связывается с сервером аутентификации. В качестве сервера аутентификации используется контроллер домена Windows Server 2008R2, его же используют как RADIUS-сервер [74].

Подобный подход к реализации WPA/WPA2 называется WPA-Enterprise. Он используется в крупных производственных сетях, где уже развернута инфраструктура Active Directory.

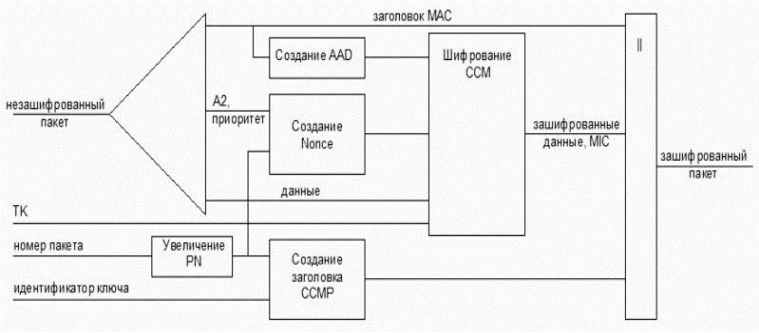


Рис. 10.11. Инкапсуляция данных с использованием CCMP

Декапсуляция данных с использованием CCMP:

1) создаются поля дополнительных идентификационных данных и поле nonce с использованием данных пакета;

2) поле дополнительных идентификационных данных извлекается из заголовка зашифрованного пакета;

3) извлекается поле A2, номер пакета и поле приоритета;

4) извлекается поле MIC;

5) выполняется расшифровка пакета и проверка его целостности с использованием шифротекста пакета, дополнительных идентификационных данных, временного ключа и, собственно, MIC;

6) выполняется сборка пакета в расшифрованном виде;

7) пакеты с повторяющимся номером отбрасываются.

Очевидно, что развертывание Active Directory и RADIUS в условиях малого бизнеса либо же в домашних условиях практически невозможно. Поэтому, чтобы стандарты WPA/WPA2 могли использоваться в домашних условиях, организацией Wi-Fi Alliance была разработана упрощенная реализация, называемая WPA-PSK (Pre-Shared Key). Он использует те же протоколы шифрования, однако схема аутентификации пользователей в нем сильно упрощена. Для того чтобы устройство получило маркер доступа в сеть, на устройстве необходимо ввести специальную парольную фразу, называемую Pre-Shared Key. Длина должна быть от 8 до 32 символов, при этом можно использовать специальные символы, а также символы национальных алфавитов. После ввода парольной фразы она помещается в специальный пакет ассоциации (пакет обмена ключами, handshake), который передается на точку доступа. Если парольная фраза верна, то устройству выдается маркер доступа в сеть. Данный подход в разы проще, чем WPA-Enterprise, и поэтому нашел широкое применение среди малого бизнеса и домашних пользователей.

При всех своих достоинствах WPA/WPA2 не лишены уязвимостей. Еще в 2006 г. TKIP-шифрование в WPA было взломано. Эксплоит позволяет прочитать данные, передаваемые от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. Для реализации этой атаки необходимо, чтобы в сети использовался QoS.

Использовать WPA для защиты беспроводной сети тоже не безопасно. Конечно, взломать его сложнее, нежели WEP, и WPA защитит от простейшей атаки с Aircrack-NG, однако он не устоит против целенаправленной атаки.

В 2008 г. была обнаружена уязвимость, позволяющая провести MITM-атаку. Она позволяла участнику сети перехватить и расшифровать данные, передаваемые между другими участниками сети с использованием их Pairwise Transient Key. Поэтому при работе в такой сети имеет смысл использовать дополнительные средства шифрования передаваемой информации. В то же время для того, чтобы воспользоваться этой уязвимостью, необходимо быть авторизованным и подключенным к сети.

В WPA-PSK упрощена схема авторизации: таким «узким» местом в нем является сам Pre-Shared Key, поскольку ввод этого ключа дает устройству полный доступ в сеть (если не задействована фильтрация по MAC-адресу).

Сам ключ хранится в точке доступа. В зависимости от модели и микропрограммного обеспечения устройства реализуются методы его защиты. В некоторых случаях достаточно получить доступ к веб-интерфейсу управления и Pre-Shared Key, который хранится там открыто.

Последней уязвимостью является возможность перехвата пакетов handshake, в которых передается Pre-Shared Key при подключении устройства к сети. Поскольку Pre-Shared key шифру-

ется, то остается только одна возможность – атака методом «грубой силы» (либо словарная) на захваченные ассоционные пакеты. С одной стороны, это нерационально, но стоит понимать, что для этого совсем не нужно находиться рядом с точкой доступа можно задействовать большие вычислительные ресурсы.

Также стоит обратить внимание, что для того, чтобы перехватить handshake, совсем необязательно ждать того момента, когда в сети будет подключено новое устройство. На некоторых беспроводных адаптерах, при использовании нестандартных драйверов, есть возможность посылки в сеть реассоционных пакетов, которые будут прерывать сетевые соединения и инициировать новый обмен ключами в сети между клиентами и точкой доступа. В таком случае для того, чтобы захватить требуемые пакеты, необходимо, чтобы к сети был подключен хотя бы один клиент. Также необходимо находиться близко от точки доступа, чтобы мощности его адаптера (а такие адаптеры обычно низкочувствительны и маломощны, и сильно перегреваются при работе) хватило для инжекта пакетов реассоциации (вспомните WEP, где нужно было всего лишь «наловить» достаточный объем трафика). Конечно, атака методом «грубой силы» занимает много времени, однако использование вычислительного кластера существенно упрощает задачу.

9. *Уязвимость WPS (защищенная беспроводная сеть)*. В декабре 2011 г. Стефан Фибек и Крейг Хеффнер рассказали о серьезных прорехах в протоколе WPS. Оказалось, что если в точке доступа активирован WPS с PIN (который по умолчанию включен в большинстве роутеров), то подобрать PIN-код для подключения можно за считанные часы.

PIN-код WPS чувствителен к атаке брутфорс. Спецификация WPS для аутентификации PIN-кода позволяет атакующему

узнать половину восьмизначного PIN-кода. Отсутствие правильной политики блокировки после некоторого количества неудачных вводов PIN-код на многих беспроводных маршрутизаторах позволяет использовать атаку полным перебором.

Wi-Fi Protected Setup (WPS) – это вычислительный стандарт, созданный альянсом Wi-Fi для упрощения настройки и обеспечения безопасности домашней небольшой сети. WPS содержит метод аутентификации под названием внешний регистратор, для которого требуется только PIN-код маршрутизатора. Этот метод безопасности подвержен атакам грубой силы.

Когда аутентификация PIN-кода не удастся, точка доступа отправит сообщение EAP-NACK обратно клиенту. Сообщения EAP-NACK отправляются таким образом, что атакующий может определить правильность первой половины PIN-кода. Кроме того, последняя цифра PIN-кода известна, поскольку она является контрольной суммой для PIN-кода. Эта особенность значительно уменьшает количество попыток, необходимых для перебора PIN-кода. Количество попыток идет от 108 до 104 + 103, что составляет 11 000 попыток.

Известно, что многие беспроводные маршрутизаторы не реализуют политику блокировки большого количества попыток ввода PIN-кода. Это значительно сокращает время, необходимое для успешной атаки «грубой силы». Некоторые беспроводные маршрутизаторы в результате такой атаки перестают работать что можно отнести к атаке «отказ в обслуживании» с использованием брутфорс.

Для реализации атаки на беспроводные технологии используют комплексы, состоящие из программной и аппаратной части.

Программные средства тестирования безопасности беспроводных сетей базируются, как правило, на ОС Kali Linux. В нее

входит большой набор различных утилит. Кроме того, существуют операционные системы, предназначенные только для аудита безопасности Wi-Fi с годовыми автоматизированными алгоритмами атаки, например ОС Wifislax.

Так как программная часть построена в основном на Linux, то необходимо внимательно отнестись к выбору сетевого адаптера. Конечно, ядро Linux поддерживает очень большое количество сетевых адаптеров, поэтому можно столкнутся с проблемой поддержки определенных чипсетов. Большинство источников рекомендуют сетевые адаптеры Alfa (рис. 10.12).

Alfa AWUS036NH

Alfa AWUS036ACH

Рис. 10.12. Примеры сетевых адаптеров Alfa

Для того, чтобы прослушивать трафик, нужно перевести наш беспроводной адаптер (сетевую карту) в хакерский режим – monitor mode. Каждый адаптер Wi-Fi на физическом уровне улавливает любые сигналы, пересылаемые устройствами в радиусе действия. Антенна не может не принимать посторонние пакеты. А вот драйвер может работать в трех основных режимах:

1. *Managed mode* – пакеты, не предназначенные этому адаптеру, отбрасываются, а остальные передаются внутрь ОС как «полученные». В этом режиме поврежденные пакеты также отбрасываются. Нормальный режим работы «без свистелок».

2. *Monitor mode* – драйвер не фильтрует пакеты и передает все, что улавливает антенна, в ОС. Пакеты с неверной контрольной суммой не отбрасываются, и их можно видеть, к примеру, в Wireshark.

3. *Promiscuous mode* («беспорядочный» режим) – режим монитора «наполовину». Драйвер будет передавать в ОС пакеты, полученные в рамках сети, к которой мы сейчас подключены (associated), но в отличие от обычного режима не будут отбрасываться пакеты, предназначенные другим клиентам этой сети. Пакеты других сетей будут игнорироваться. Понятно, что это работает только тогда, когда вы можете успешно подключиться и авторизоваться в некоторой сети (открытой или нет). В отличие от монитора этот режим поддерживается меньшим числом адаптеров. При работе в «беспорядочном» режиме, равно как и в режиме клиента, драйвер будет убирать из переданных в ОС пакетов низкоуровневые заголовки канала.

Самым распространенным инструментом для комплексного аудита и полного анализа сетей Wi-Fi (соответственно сетевого трафика) остается Aircrack-ng. Этот набор, кстати, входит в инструментарий Kali Linux, что говорит о его практичности и высокой эффективности. Кроме того, программное обеспечение достаточно функционально и позволяет реализовать большинство описанных сценариев атак. Перечень инструментов, входящих в пакет Aircrack-ng, представлен в табл. 10.1.

*Таблица 10.1*

**Инструменты, входящие в Aircrack-ng**

| № | Название пакета | Функциональные возможности |
|---|---|---|
| 1. | Aircrack-ng | Взламывает ключи WEP и WPA («Перебор по словарю») |
| 2. | Airdecap-ng | Расшифровывает перехваченный трафик при известном ключе |
| 3. | Airmon-ng | Выставление различных карт в режим мониторинга |
| 4. | Aireplay-ng | Пакетный инжектор (Linux и Windows) |
| | Airodump-ng | Анализатор трафика: помещает трафик в файлы PCAP или IVS и показывает информацию о сетях |
| 5. | Airtun-ng | Создает виртуальный интерфейс туннелирования |

*Окончание табл. 10.1*

| | | |
|---|---|---|
| 6. | Packetforge-ng | Создает шифрованные пакеты для инъекции |
| 7. | Ivstools | Инструменты для слияния и конвертирования |
| 8. | Airbase-ng | Предоставляет техники для атаки клиента |
| 9. | Airdecloak-ng | Убирает WEP-маскировку с файлов pcap |
| 10. | Airolib-ng | Хранит и управляет списками ESSID и паролей, вычисляет парные мастер-ключи |
| 11. | Airserv-ng | Открывает доступ к беспроводной сетевой карте с других компьютеров |
| 12. | Buddy-ng | Сервер-помощник для easside-ng, запущенный на удаленном компьютере |
| 13. | Easside-ng | Инструмент для коммуникации с точкой доступа без наличия WEP-ключа |
| 14. | Tkiptun-ng | Атака WPA/TKIP |
| 15. | Wesside-ng | Автоматический инструмент для восстановления WEP-ключа |

Aircrack-ng – это пакет программ, который включает в себя инструменты для следующих задач:

1) *мониторинг* – это инструменты, разработанные специально для захвата трафика с целью последующего анализа. Захваченный беспроводной трафик можно изучить, используя другое программное обеспечение, например Wireshark;

2) *атаки* – инструменты для атаки целевых сетей. В их состав входят средства, которые выполняют атаку во время проверки данных пользователя (аутентификации). Кроме того, Aircrack-ng в момент атаки способен проводить инъекции пакетов, отправляемых в беспроводной поток данных как клиентам, так и точке доступа;

3) *тестирование* – эти инструменты позволяют тестировать беспроводные карты;

4) *взлом* – Aircrack-ng также может взламывать предварительные беспроводные ключи, найденные в WEP, WPA и WPA2.

Пакет программ постоянно совершенствуется и обновляется разработчиками. С помощью Aircrack-ng можно смоделировать различные атаки на беспроводные устройства и выявить слабые места в настройках безопасности.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

*Основная литература*

1. Бабин, С. А. Лаборатория хакера / С. А. Бабин. – СПб. : БХВ-Петербург, 2016. – 240 с.

2. Бирюков, А. А. Информационная безопасность. Защита и нападение / А. А. Бирюков. – 2-е изд., перераб. и доп. – М. : ДМК Пресс, 2017. – 434 с.

3. Введенская, О. Ю. Особенности следообразования при совершении преступления посредством сети Интернет / О. Ю. Введенская // Юридическая наука и правоохранительная практика. – 2015. – № 4. – С. 209–216.

4. Зорин, Е. Л. Стеганография и стегоанализ [Электронный ресурс] : учебное пособие по дисциплине «Обнаружение и распознавание сигналов» / Е. Л. Зорин, Н. В. Чичварин. – М. : МГТУ имени Н. Э. Баумана, 2013. – 1 электрон. опт. диск (CD-ROM).

5. Камский, В. А. Защита личной информации в Интернете, смартфоне и компьютере / В. А. Камский. – СПб. : Наука и Техника, 2017. – 272 с.

6. Мовчан, А. В. Отдельные аспекты применения компьютерной разведки в оперативно-разыскной деятельности / А. В. Мовчан // Проблемы правоохранительной деятельности. – 2014. – № 2. – С. 107–112.

7. Павлюков, В. В. Компьютерная разведка как оперативно-разыскное мероприятие / В. В. Павлюков // Вестник Нижегородской академии МВД России. – 2016. – № 4. – С. 236–240.

8. Пахомова, А. С. Анализ применяемости классификации шаблонов атак CAPEC для описания угроз компьютерного шпионажа / А. С. Пахомова, О. А. Остапенко // Информация и безопасность. – 2014. – № 3. – С. 472–475.

9. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели компьютерной разведки / [А. С. Пахомова и др.] // Информация и безопасность. – 2013. – № 3. – С. 115–118.

10. К вопросу о разработке структурной модели угрозы компьютерной разведки / [А. С. Пахомова и др.] // Информация и безопасность. – 2013. – № 1. – С. 81–86.

11. Райтман, М. А. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета / М. А. Райтман. – СПб. : БХВ-Петербург, 2017. – 624 с.

12. Сизоненко, А. Б. Особенности раскрытия преступлений в сфере компьютерной информации : курс лекций / А. Б. Сизоненко, В. Н. Шишкин. – Краснодар : КрУ МВД России, 2011. – 205 с.

13. Степанов, В. В. Правовые основы оперативно-розыскной деятельности : учебное пособие / В. Ю. Алферов, А. И. Гришин, Н. И. Ильин ; под общ. ред. В. В. Степанова. – 3-е изд., испр. и доп. – Саратов : Саратовский социально-экономический институт (филиал) РЭУ имени Г. В. Плеханова, 2016. – 296 с.

14. Федотов, Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М. : Юридический Мир, 2007. – 432 с.

15. Чечетин, А. Е. Основы оперативно-розыскной деятельности органов внутренних дел : учебное пособие / А. Е. Чечетин. – Хабаровск : Дальневосточный юридический институт МВД России, 2014. – 264с.

16. Язов, Ю. К. Организация защиты информации в информационных системах от несанкционированного доступа : монография / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2018. – 558 с.

17. Кибервойны 2017: баланс сил в мире : аналитический обзор. – Zecurion Analytics, 2017. – 7 с.

18. NATO Handbook Open Source Intelligence. – 2001. – 49 с.

19. Open Source Intelligence (OSINT) 2oolKit On The Go. – 2012. – 168 с.

20. The Evolution of Open Source Intelligence (OSINT). – The Intelligencer. – vol. № 3 – 2013. – С. 56–53.

21. Simmons, C. Avoidit: A Cyber Attack Taxonomy / C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, Qishi Wu. – Annual Symposium on Information Assurance (ASIA'14). – 2014. – Albany, NY.

22. WebKnacKer, A. Быстро и легко. Хакинг и антихакинг: защита и нападение : учебное пособие / A. WebKnacKer – M. : Лучшие книги, 2004. – 400 с.

23. Weidman, G. Penetration testing: A Hands-On Introduction to Hacking / Georgia Weidman. – San Francisco : No Starch Press, 2014. – 531 p.

24. Sanghvi, H. P. Cyber Reconnaissance: An Alarm before Cyber Attack / H. P. Sanghvi, M. S. Dahiya – International Journal of Computer Applications (0975 – 8887). – Vol. 63. – 2013. – № 6.

*Нормативные правовые акты*

25. Федеральный закон «О внешней разведке» от 10 января 1996 г. № 5-ФЗ.

26. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

27. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

28. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ.

29. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (ред. от 18.01.2017).

30. ГОСТ 7.73-96 СИБИД. Поиск и распространение информации. Термины и определения.

31. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

32. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (изд. с поправкой).

33. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

34. ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики.

35. ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.

36. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

37. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.

38. ГОСТ Р 57429-2017 Судебная компьютерно-техническая экспертиза. Термины и определения.

39. ГОСТ Р 58143-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии

с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения.

40. Aqsacom Document No. 040451 Lawful Interception for IP Networks White Paper. – 2010. – 40 p.

*Электронные ресурсы*

41. Seifried, K. Утилиты сканирования системы // URL: http://emanual.ru/download/8826.html.

42. Волков, А. Определение операционной системы удаленного хоста // URL: https://nmap.org/nmap-fingerprinting-article-ru.

43. Лукацкий, А. Сетевая контрразведка: как обнаружить сканирование узлов и портов // URL: http://www.i2r.ru/static/450/out_8940.shtml.

44. I2P: принцип работы // URL: http://www.spy-soft.net/i2p/.

45. Раскрываем секреты сети I2P // URL: https://xakep.ru/2014/09/04/i2p-secrets/.

46. Методы анонимности в сети. Просто о сложном. Часть 1 // URL: https://habrahabr.ru/post/190396.

47. Фингерпринтинг конкретного ПК с точностью 99,24 %: не спасает даже смена браузера // URL: https://geektimes.ru/post/284604/.

48. Бунин, О. Browser Fingerprint – анонимная идентификация браузеров // URL: https://habrahabr.ru/company/olegbunin/blog/321294/.

49. Подмена MAC: атака и защита, теория и практика // URL: https://xakep.ru/2002/01/24/14341/.

50. Фингерпринтинг браузера. Как отслеживают пользователей в сети // URL: https://xakep.ru/2015/01/30/user-web-tracking-howto/.

51. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // URL: https://fstec.ru/component/attachments/download/289.

52. Reasons for Converting File System and 4 Ways to Change File System // URL: https://www.partitionwizard.com/convertpartition/convert-file-system-without-data-loss.html.

53. Krombholz, K. Advanced Social Engineering Attacks / K. Krombholz, H. Hobel, M. Huber, E. Weippl // URL: https://publications.sba-research.org/publications/jisa_revised.pdf.

54. Утилиты для локального поиска // URL: http://compress.ru/Article.aspx?id=21547.

55. Извлечение всех паролей (веб-браузеры, почтовые программы и пр.) в Windows и Linux // URL: https://hackware.ru/?p=1553.

56. Защищаем сеть L2 коммутаторами // URL: https://habrahabr.ru/post/231491/.

57. Защита внутри периметра // URL: https://xakep.ru/2013/08/23/safe-among-perimetr/.

58. Сканирование отображения: атаки на TCP без возможности подмены трафика Часть 1 // URL: https://www.securitylab.ru/analytics/420306.php.

59. Никому ни кабельность: TCP/IP спуфинг // URL: https://xakep.ru/2001/08/07/13264/.

60. Что важно знать об IP-телефонии // URL: https://www.iptc.ru/content/view/18/61/.

61. Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика / Ю. В. Маркин, А. С. Санаров // URL: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf.

62. Макаренко, С. И. Информационное оружие в технической сфере: терминология, классификация, примеры. Системы управления, связи и безопасности / С. И. Макаренко // URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf.

63. Мандиа, К. Защита от вторжений расследование компьютерных преступлений / К. Мандиа // URL: http://compu-

tersbooks.net/index.php?id1=4&category=rukovodstvo-po-po&author=mandia-k&book=2005.

64. Аутентификация в системах Windows. Часть 1 – NTLM // URL: https://interface31.ru/tech_it/2015/03/autentifikaciya-v-sistemah-windows-chast-1-ntlm.html.

65. Знакомство с клавиатурными шпионами // URL: https://www.securitylab.ru/analytics/216399.php.

66. Обзор клавиатурных шпионов: лучшие кейлоггеры // URL: https://xakep.ru/2006/12/04/35563/.

67. Дешифрация существующего пароля BIOS // URL: http://comp0.ru/biospass.html.

68. Способы обхода паролей BIOS // URL: https://habrahabr.ru/post/128466/.

69. Клавиатурные шпионы // URL: http://z-oleg.com/secur/articles/keylogger.php

70. Принципы восстановления данных // URL: http://www.rtt.com/ru/Articles/File_Recovery_Basics/.

71. Best Operating Systems for Anonymity: Comparing Titans // URL: https://hackernoon.com/best-operating-systems-for-anonymity-\-comparing-titans-3501fd5cba3b.

72. Как общаются в даркнете // URL: https://book.cyberyozh.com/ru/xmpp-jabber-kak-obshayutsya-v-darknete/ XMPP (Jabber).

73. Общий обзор реестров и классификаций уязвимостей информационных систем // URL: https://safe-surf.ru/specialists/article/5228/607311/.

74. Теоретические основы защиты WPA\WPA2 // URL: http://mgupi-it.ru/Tech/wireless/wifisecurity_part2-.html.

Учебное пособие

**Поликарпов Евгений Сергеевич**,
кандидат технических наук

# ОСНОВЫ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Редактор *Абилова Ф. А.*
Корректор *Лосева О. С.*
Компьютерная верстка *Абилова Ф. А., Лосева О. С.*

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12

| | | |
|---|---|---|
| Подписано в печать 18.12.2020 | Формат 60×84 1/16 | Тираж 67 экз. |
| Заказ № 258 | Цена договорная | Объем 11,18 уч.-изд. л.<br>19,7 усл. печ. л. |