УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Кашаев М. П., Лущ И. С.
Научный руководитель – ст. преподаватель Гутич И. И.

Информационная безопасность подразумевает под собой комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства. На сегодняшний день самыми распространенными видами сетевых атак являются:

– сетевая разведка;
– IP-spoofing;
– mailbombing;
– DDOS-атака;
– Man-in-the-Middle;
– phishing.

Многие виды атак используются совместно для увеличения вероятности успеха атаки. Теперь поговорим про каждую из перечисленных атак подробнее.

Сетевая разведка

Один из самых распространенных и простых видов атак, когда не требуется специализированное ПО, а лишь устройство с доступом в интернет и браузером. Данные атаки используется в паре с социальной инженерией. Суть сетевой атаки: имея какую-то базовую информацию о человеке, например, ФИО, человека можно найти в социальных сетях, где многие указывают информацию о себе. Многим кажется, что это информацию нельзя использовать в корыстных целях, однако это не так. Для атакующего любая, даже самая незначительная информация об объекте атаки может представлять интерес. Таким образом можно собрать множество информации о человеке, а если нет информации о нужном человеке, то можно начать сбор информации о его друзьях и через них узнать необходимую информацию о цели.

Для предотвращения получения информации о себе в идеальном случае не регистрироваться в социальных сетях. Однако в современном мире такое осуществить крайне сложно, поэтому при регистрации стоит указывать о себе как можно меньше данных, например, оставить только ФИО и почту. Также в организациях, беспокоящихся о сохранности своих данных, следует проводить инструктаж с сотрудниками на предмет нераспространения личной информации о себе и коллегах в интернете.

Социальная инженерия

Социальная инженерия представляет собой способ получения информации от человека используя психологическое воздействие. Социальная инженерия используется в совокупности не только с сетевой разведкой, но и другими видами разведки.

Для получения информации существует множество техник, суть которых сводится к ошибкам, которые допускаются людьми в поведении. Сейчас социальная инженерия приобрела прочную связь с киберпреступностью, но на самом деле это понятие появилось давно и изначально не имело выраженного негативного оттенка. Самой известной личностью в этом направлении является Кевин Митник. В 2001 году вышла книга «Искусство обмана» под его авторством, повествующая о техниках использования и примерами применения социальной инженерии. Кевин Митник заявляет, что намного проще получить пароль путем обмана, нежели пытаться взломать систему безопасности. Социальная инженерия не работает без данных о цели, а для их получения может использоваться, например, сетевая разведка. Самый простой пример – телефонный звонок, где злоумышленник выдает себя за кого-то другого, пытаясь узнать у абонента конфиденциальную информацию, играя на чувствах человека, обманывая или шантажируя его.

Для борьбы с социальной инженерией используются тесты на проникновение. Данный тест состоит из нескольких этапов: разработка плана испытаний, выбор вектора атаки, попытка проникновения и подготовка отчета. В случае успешного проникновения в отчете составляются критерии уязвимости сотрудников и, поскольку атака направлена на людей, проводится инструктаж с сотрудниками для предотвращения подобных ситуаций в будущем.

IP-спуфинг

IP-спуфинг – это создание пакетов интернет-протокола, которые имеют измененный адрес источника, чтобы либо скрыть личность отправителя, либо выдать себя за другую компьютерную систему, либо и то, и другое. Это метод, часто используется для проведения DDoS-атак на конкретное устройство или окружающую инфраструктуру. IP-спуфинг кратко: злоумышленник, отправляет пакет кому-то с неправильным обратным адресом.

Отправка и получение IP-пакетов является основным способом взаимодействия сетевых компьютеров и других устройств и составляет основу современного Интернета. Все IP-пакеты содержат заголовок, который предшествует телу пакета и содержит важную информацию о маршрутизации, включая адрес источника. В обычном пакете IP-адрес источника – это адрес отправителя пакета. Если пакет был подделан, адрес источника будет подделан (рис. 1).

DDoS-атаки часто используют спуфинг с целью перегрузить цель трафиком, маскируя личность вредоносного источника, предотвращая усилия по смягчению последствий и скрывая устройства сети. Если IP-адрес источника фальсифицируется и непрерывно рандомизируется, блокировка вредоносных запросов становится сложной. IP-спуфинг также затрудняет для правоохранительных органов и команд кибербезопасности отслеживание виновного в атаке.

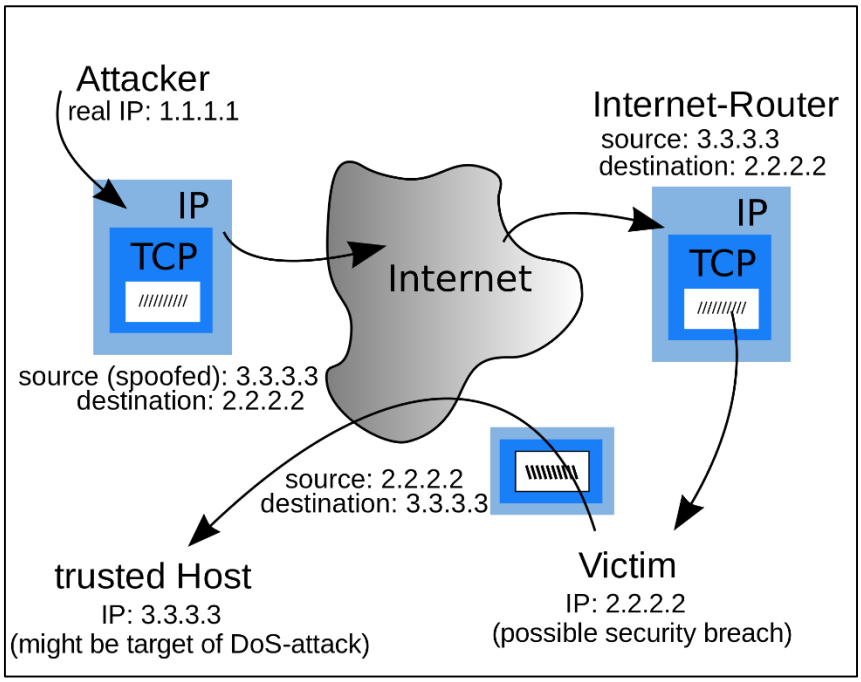

Рис. 1 – Схема IP-спуфинга

Спуфинг также используется для маскировки под другое устройство, так что вместо этого ответы отправляются на это целевое устройство. Также используется при атаке на DNS сервера. Возможность изменения исходного IP-адреса присуща дизайну TCP/IP, что делает его постоянной проблемой безопасности.

Как защититься от IP-спуфинга (фильтрация по карману): вероятность применения IP-спуфинг к сети нельзя предотвратить полностью, однако можно принять меры, чтобы остановить проникновение поддельных пакетов в сеть. Очень распространенной защитой от спуфинга является фильтрация входящего трафика, которая описана в политике безопасности каждой конкретной компании. Фильтрация входящих пакетов – это форма фильтрации пакетов, обычно реализуемая на пограничном устройстве сети, которое проверяет входящие IP-пакеты и проверяет их исходные заголовки. Если исходные заголовки этих пакетов не соответствуют их источнику или они иным образом выглядят подозрительными, пакеты отклоняются. Некоторые сети также реализуют фильтрацию выходов, которая рассматривает IP-пакеты, выходящие из сети, гарантируя, что эти пакеты имеют законные заголовки источника, чтобы кто-то в сети не мог запустить исходящую вредоносную атаку с помощью IP-спуфинга.

DDOS-атака

DDoS-атаки осуществляются с помощью сетей машин, подключенных к Интернету. Эти сети состоят из компьютеров и других устройств (например, устройств IoT), которые были заражены вредоносным ПО, что позволяет злоумышленнику управлять ими удаленно. Эти отдельные устройства называются

ботами, а группа ботов называется ботнетом. После установки ботнета злоумышленник может направить атаку, отправив удаленные инструкции каждому боту.

Когда сервер или сеть жертвы становятся мишенью ботнета, каждый бот отправляет запросы на IP-адрес цели, что потенциально приводит к перегрузке сервера или сети, что приводит к отказу в обслуживании нормального трафика. Поскольку каждый бот является законным интернет-устройством, отделить атакующий трафик от обычного трафика может быть сложно.

Признаками атаки являются:

– подозрительное количество трафика, исходящего с одного IP-адреса или IP-диапазона;

– поток трафика от пользователей, которые используют один поведенческий профиль, такой как тип устройства, геолокация или версия веб-браузера;

– необъяснимый всплеск запросов на одну страницу или конечную точку;

– нечетные модели трафика, такие как всплески в нечетные часы дня или шаблоны, которые кажутся неестественными (например, всплеск каждые 10 минут).

Различные типы DDoS-атак нацелены на различные компоненты сетевого соединения. Чтобы понять, как работают различные DDoS-атаки, необходимо знать, как осуществляется сетевое подключение – модель ОСИ (рис. 2).

Семиуровневая модель OSI	
7	Прикладной уровень (application layer)
6	Уровень представления (presentation layer)
5	Сеансовый уровень (session layer)
4	Транспортный уровень (transport layer)
3	Сетевой уровень (network layer)
2	Канальный уровень (data link layer)
1	Физический уровень (physical layer)

Рис. 2 – Модель OSI

Атаки можно произвести на любой из 7 уровней, но в основном проводят атаки трех видов:

1. Атаки на прикладном уровне. Иногда называемая DDoS-атакой уровня 7 (7-й уровень модели OSI), цель этих атак состоит в том, чтобы исчерпать ресурсы цели для создания отказа в обслуживании. Атаки нацелены на уровень, на котором веб-страницы генерируются на сервере и доставляются в ответ на HTTP-запросы. Один HTTP-запрос вычислительно дешев для выполнения на стороне клиента, но ответ на него может быть дорого, так как сервер часто загружает несколько файлов и выполняет запросы к базе данных для создания веб-страницы. От атак уровня 7 трудно защититься, так как может быть трудно отличить вредоносный трафик от законного трафика.

2. HTTP-флуд. Эта атака похожа на нажатие обновления в веб-браузере снова и снова на нескольких разных компьютерах одновременно – большое количество HTTP-запросов наводняет сервер, что приводит к отказу в обслуживании. Этот тип атаки варьируется от простой до сложной. Более простые реализации могут получить доступ к одному URL-адресу с одинаковым диапазоном атакующих IP-адресов, рефереров и пользовательских агентов. Сложные версии могут использовать большое количество атакующих IP-адресов и нацеливаться на случайные URL-адреса с помощью случайных рефереров и пользовательских агентов.

3. Протокольные атаки, также известные как атаки на исчерпание состояния, вызывают перебои в обслуживании из-за чрезмерного потребления ресурсов сервера и/или ресурсов сетевого оборудования, такого как брандмауэры и балансировщики нагрузки. Атаки протокола используют слабые места на уровне 3 и уровне 4 стека протоколов, чтобы сделать цель недоступной.

SYN-флуд. SYN в TCP/IP. Если установлен флаг SYN (идет установление сессии), то поле содержит изначальный порядковый номер – ISN (Initial Sequence Number). В целях безопасности это значение генерируется случайным образом и может быть равно от 0 до $2^{32}-1$ (4294967295). Первый байт полезных данных в устанавливающейся сессии будет иметь номер ISN+1. SYN Flood аналогичен работнику в отделении почты, получающему запросы от оператора отделения. Рабочий получает запрос, идет и забирает посылку с полки и ждет подтверждения, прежде чем выносить посылку в зал. Затем работник получает гораздо больше запросов пакетов без подтверждения, до момента пока он попросту не сможет переносить посылки. Эта атака использует рукопожатие TCP – последовательность связи, с помощью которой два компьютера инициируют сетевое соединение – путем отправки цели большого количества SYN-пакетов TCP «Initial Connection Request» с поддельными IP-адресами источника. Целевая машина отвечает на каждый запрос на подключение, а затем ждет последнего шага в рукопожатии, который никогда не приходит, что истощает ресурсы цели в процессе (рис. 3).

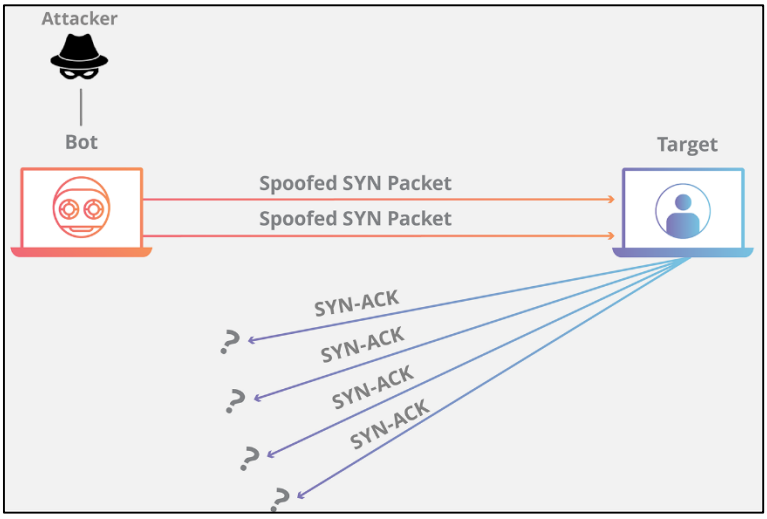

Рис. 3 – Схема атаки Syn-флуд

Объемные атаки пытаются создать перегрузку, потребляя всю доступную пропускную способность между целью и более крупным Интернетом. Большие объемы данных отправляются цели с помощью формы усиления или других средств создания массивного трафика, таких как запросы из ботнета.

Перегрузка DNS похоже на то, когда кто-то позвонит в ресторан и скажет: «У меня будет заказ, – перечислит его содержимое и скажет: пожалуйста, перезвоните мне и повторите весь мой заказ», где номер обратного звонка на самом деле принадлежит жертве. С очень небольшими усилиями генерируется длинный ответ и отправляется жертве. Сделав запрос на открытый DNS-сервер с поддельным IP-адресом (IP-адресом жертвы), целевой IP-адрес получает ответ от сервера.

Для защиты от DDoS-атак используют различные средства защиты, которые можно разделить на локальные, гибридные и облачные. Локальные решения зачастую используются крупными операторами и дата-центрами, которые могут себе позволить собственную службу реагирования, позволяющую справится с мощными атаки. Облачные решения схожи с локальными и предлагают практически такой же функционал. В него может входить защита сайтов от атак, производимых ботами, и сопровождение во время этих самых атак. Гибридное решение представляет собой смесь из двух предыдущих средств: имеется локальное решение, а также облачное, подключаемое автоматически во время крупных атак.

Mailbombing

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами. Для использования данных атак было разработано множество программ, и даже неопытный пользователь мог совершить атаку, указав всего лишь e-mail жертвы, текст сообщения, и количество необходимых сообщений. Многие такие программы позволяли прятать реальный IP-адрес отправителя, используя для рассылки анонимный почтовый сервер. Эту атаку сложно предотвратить, так как даже почтовые фильтры провайдеров не могут определить реального отправителя спама. Провайдер может ограничить количество писем от одного отправителя, но адрес отправителя и тема зачастую генерируются случайным образом.

Также если совместить возможность отправки писем через почту и воздействие на человека, используя социальную инженерию, то запросто можно получить еще один особо опасный вид вирусов. Суть данной атаки заключается в том, что пользователю приходит письмо, возможно от схожего адреса, который он знает, а может и человеческий интерес берет верх. В таком случае пользователь компьютера атакует сам себя, просто загрузив, например, документ из письма. В этом случае его могут остановить антивирусы, но пользователи ввиду интереса могут отключить его. Далее все зависит от того, какие цели преследовал атако-

вавший. В одном случае вирус будет находиться в спящем режиме, но по команде атакующий может «оживить» его и получить доступ к компьютеру или компьютер станет частью ботнет сети, которая может производить DDoS-атаку.

Еще один распространен вид вирусов, называемый «шифровальщик». Загрузившись в компьютер при выключении, включении, перезагрузке они могут «вшить» себя в низшие слои системы или, например, в БИОС, и провести шифрование. Обычно такие атаки быстро устраняют, выпуская специальные утилиты под конкретный вирус. И из-за того, что их быстро устраняют все они имеют таймер, обычно ограниченный 24 часами. После этого данные попросту стираются, иногда без возможности восстановления. Если обычный пользователь потеряет какую-то малую часть своих данных, то организации, например, больницы, попросту парализуются.

У всех вирусов, передаваемых по почте также есть общая черта – каждый из них пытается распространится по сети и на конкретной системе. Распространение по сети подразумевает что как только ваш компьютер будет захвачен, то с него можно вести рассылку, что повысит результативность, ввиду того что все, с кем вы ранее вели переписку откроют «посылку» и также заразятся, распространяя вредоносные письма далее по сети.

Для борьбы с данным видом атак следует фильтровать входящие письма. На рабочей почте можно создать так называемый «белый» лист почтовых адресов – в него входят известные пользователю почтовые адреса, которым можно доверять и не опасаться заразить систему.

MITM

Атака «человек посередине» (Man-in-the-Middle) – это форма кибератаки, при которой для перехвата данных используются методы, позволяющие внедриться в существующее подключение или процесс связи. Злоумышленник может быть пассивным слушателем в вашем разговоре, незаметно крадущим какие-то сведения, или активным участником, изменяя содержание ваших сообщений или выдавая себя за человека или систему, с которыми Вы, по вашему мнению, установили подключение.

Еще недавно были популярны стационарные телефоны с несколькими трубками, и один член семьи мог взять трубку во время разговора другого. Вы могли даже не подозревать, что вас слушает кто-то еще, пока он не начнет вклиниваться в разговор. В этом и заключается принцип атаки «человек посередине».

Многофакторная аутентификация может быть эффективной защитой от кражи учетных данных. Даже если злоумышленник узнает ваше имя пользователя и пароль, ему понадобится ваш второй аутентификатор, чтобы их использовать. К сожалению, в некоторых случаях многофакторную защиту можно обойти, например, создав страницу-копию, с которой трафик будет перенаправляться при вводе паролей.

Brute force

Брутфорсом называется метод взлома учетных записей путем подбора паролей к ним. Термин образован от англоязычного словосочетания «brute force», означающего в переводе «грубая сила». Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью найти правильную. Недавно появилась статистика о скорости взлома паролей за 2021 год (рис. 4). В своем отчете специалисты утверждают, что при создании пароля важна не только его длина, но и сложность (сочетание цифр, букв разных регистров и спецсимволов). К примеру, используя современные методы подбора, комбинацию из 11 цифр хакеры подберут практически мгновенно, а из того же количества строчных букв – за пару часов. Зато при добавлении к ним заглавных букв время брутфорса вырастет до 5 месяцев, а в связке с цифрами – до трех лет. Судя по опубликованной таблице, оптимальным вариантом для защиты важной информации выглядит 12-значный пароль из цифр и букв разных регистров. На взлом такого сочетания путем перебора современным ПК потребуется примерно 200 лет. А если подстраховаться при помощи 18-значного комбинирования с добавлением еще и специальных символов, то время подбора станет просто астрономическим – 438 триллионов лет. Поэтому данный метод используют все реже и используя специализированные словари, в которые вносятся «ключевые слова», которые могут относится к атакуемой цели.

Рис. 4 – Статистика скорости взлома

Устройства для взлома

Помимо программных средств можно получить физический доступ к устройству. Для этого используются различные устройства, позволяющие совершать нежелательные операции над устройствами пользователей.

На многих предприятиях для доступа к помещениям используются RFID-карты. Существует отдельный класс устройств, позволяющий считывать данные

с оригинальной карты и дублировать их на карту злоумышленника. Примером такого устройства может быть Proxmark 3. Устройство считывает себе в память данные с карточки, которая далее может быть записана на другую карту. Но Proxmark 3 доработан, позволяя хранить в памяти несколько карт и не записывать их на физическую карту, а сразу прикладывать к считывателю.

Многие устройства в системах «умный дом» используют протокол ZigBee. У этого протокола, как и у любого другого имеются свои уязвимости, которые злоумышленник может использовать. ApiMote – это исследовательский аппарат для обеспечения безопасности ZigBee, предназначенный для исследователей, студентов, коммунальных компаний и т. д. для изучения и оценки безопасности систем ZigBee в соответствии с разрешениями. Однако его можно отнести к устройство двойного назначения, поскольку с его помощью злоумышленник может получить нежелательный доступ к системе. ApiMote предварительно оборудован прошивкой KillerBee, поэтому все, что вам нужно сделать, это просто подключиться к системе и использовать утилиты KillerBee, чтобы начать исследование. Он поставляется с антенной, в основном перехватывает пакеты, расшифровка которых не занимает много времени.

USB Rubber Ducky – выглядит и ведет себя как обычная флешка, но ее можно запрограммировать на очень быстрый ввод клавиш с клавиатуры. Она способна взломать любую систему за несколько секунд. Единственный недостаток – вам понадобится физический доступ к компьютеру. Она содержит в автозагрузке флешки скрипт, написанный на языке Ruby, что позволяет ей очень быстро выполнять различные команды, сохранять файлы на флешку. Также имеется версия с WiFi, что позволяет уже установить полноценное удаленное управление. O.MG cable – является разновидностью, внешне представляет обычный кабель для зарядки телефона, но внутри также имеет Rubber Ducky.

В 2019 году на рынке появилось гаджет под названием Hunter Cat. Это устройство, наоборот, помогает пользователям Его разработали для поиска банковских и других скиммеров. Суть его проста: вставляем его в картоприемник, вытаскиваем и смотрим на светодиод. Если он светится зеленым, то скиммер не обнаружен, в противном случае этим банкоматом лучше не пользоваться. Размер Hunter Cat чуть больше банковской карты.

Throwing Star LAN Tap – устройство для атак на локальные Ethernet сети. Подключив устройство в разрез сети или к оконечному устройству сети, оно сможет прослушивать и сохранять весь проходящий трафик, а это могут быть зашифрованные файлы, кэши, cookie-файлы.

Также есть еще куча различных устройств, но абсолютно все из них может заменить одно – Raspberry Pi. За счет того, что большинство ПО для устройств запускается на Linux и не требует много мощности, данные программы можно запустить практически где угодно. Однако зачастую требуются внешние модули и малый форм-фактор. Raspberry Pi имеют в на себе коннекторы GPIO, что позволяет создавать и подключать различные внешние модули.

Итоги

Подводя итог, стоит сказать, что антивирусы являются лишь помощниками в обнаружении и устранении вредоносного ПО, полагаться исключительно на него не стоит. Всегда существует что-то, что антивирус не сможет обнаружить или что сможет этот антивирус обойти. Также не стоит скачивать вложения с электронных писем, от неизвестных пользователей. Также стоит выстраивать физическую защиту устройств, например, отключать USB-разъемы не программным путем, а физически, отключив их от материнской платы, если они не требуются. Различные кабели стоит по возможности прятать от пользователей, устанавливать защищенные короба. Компаниям следует уделять большое внимание защите информации от несанкционированного доступа, например, усиливая свои отделы информационной безопасности. С пользователями стоит проводить регулярные инструктажи, рассказывая им о различных видах атак, которые могут к ним применяться и о способах противодействия им.

Литература

1. Информационная безопасность и зашита информации в современном обществе [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-i-zaschita-informatsii-v-sovremennom-obschestve-1/viewer (дата обращения: 19.04.2022).

2. Искусство обмана – Митник, Кевин [Электронный ресурс]. URL: https://royallib.com/book/mitnik_kevin/iskusstvo_obmana.html (дата обращения: 19.04.2022).