Мачинский Никита Андреевич, курсант,
Московский университет МВД России имени В. Я. Кикотя, г. Москва

Хмирова Елена Аркадьевна,
старший преподаватель кафедры иностранных языков
Московский университет МВД России имени В. Я. Кикотя, г. Москва

ВИДЫ СЕТЕВЫХ АТАК И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ АТАКАМ

Аннотация: Многие люди полагаются на Интернет в своей профессиональной, социальной и личной деятельности. Но есть также люди, которые пытаются нанести ущерб нашим компьютерам, подключенным к Интернету, нарушить нашу конфиденциальность и вывести из строя интернет-сервисы.

Ключевые слова: интернет; мошенничество; фишинг; маркетинг; защита; вредоносные программы;

Насколько уязвимы компьютерные сети? Какие типы атак сегодня наиболее распространены?

Кибератака — это любой тип наступательных действий, нацеленных на компьютерные информационные системы, инфраструктуры, компьютерные сети или устройства персональных компьютеров с использованием различных методов для кражи, изменения или уничтожения данных или информационных систем**.**

Вредоносное ПО – сокращение от вредоносного программного обеспечения, которое специально разработано для нарушения работы, повреждения или получения санкционированного доступа к компьютерной системе. Большая часть современных вредоносных программ являются

самовоспроизводящимися: заразив один хост, с этого хоста они пытаются проникнуть на другие хосты через Интернет, а с вновь зараженных хостов они пытаются проникнуть еще на несколько хостов. Таким образом, самовоспроизводящиеся вредоносные программы могут распространяться экспоненциально быстро.

Вирус – вредоносное ПО, для заражения устройства которым требуется какое-либо взаимодействие с пользователем. Классический пример – вложение электронной почты, содержащее вредоносный исполняемый код. Если пользователь получает и открывает такое вложение, он непреднамеренно запускает вредоносное ПО на устройстве.

Червь – вредоносное ПО, которое может проникнуть на устройство без явного вмешательства пользователя. Например, пользователь может запускать уязвимое сетевое приложение, которому злоумышленник может отправить вредоносное ПО. В некоторых случаях без вмешательства пользователя приложение может принять вредоносное ПО из Интернета и запустить его, создав червя.

Ботнет – сеть частных компьютеров, зараженных вредоносным программным обеспечением и контролируемых, как группа без ведома владельцев, например, для рассылки спама.

DoS (отказ в обслуживании) – DoS-атака делает сеть, хост или другие элементы инфраструктуры непригодными для использования законными пользователями. Большинство DoS-атак в Интернете попадают в одну из трех категорий:

• *Атака через уязвимости*: включает в себя отправку нескольких тщательно продуманных сообщений в уязвимое приложение или операционную систему, работающую на целевом хосте. Если уязвимому приложению или операционной системе будет отправлена правильно подобранная последовательность пакетов, работа может остановиться или, что еще хуже, произойдет сбой хоста.

• *Переполнение пропускной способности*: Злоумышленник отправляет поток пакетов на целевой хост — так много пакетов, что канал доступа целевого объекта забивается, не позволяя законным пакетам достичь сервера.

• *Переполнение соединений*: Злоумышленник устанавливает большое количество полуоткрытых или полностью открытых TCP-соединений на целевом хосте. Хост может настолько увязнуть в этих фиктивных соединениях, что перестанет принимать законные соединения.

DDoS (распределенный DoS) – DDoS – это тип атаки DOS, при которой несколько скомпрометированных систем используются для нацеливания на одну систему, что вызывает атаку типа «отказ в обслуживании» (DoS). DDoS-атаки с использованием бот-сетей с тысячами хостов сегодня являются обычным явлением. Атаки DDoS намного сложнее обнаружить и защититься от них, чем атаки DoS с одного хоста.

Сниффер пакетов. Пассивный приемник, который записывает копию каждого пролетевшего пакета, называется сниффером пакетов. Если поместить пассивный приемник рядом с беспроводным передатчиком, приемник может получать копию каждого передаваемого пакета. Эти пакеты могут содержать все виды конфиденциальной информации, включая пароли, номера социального страхования, коммерческую тайну и личные сообщения. Некоторые из лучших средств защиты от перехвата пакетов включают криптографию.

IP-спуфинг. Возможность вводить пакеты данных в Интернет с ложным исходным адресом известна как IP-спуфинг и является лишь одним из многих способов, с помощью которых один пользователь может маскироваться под другого пользователя. Чтобы решить эту проблему, нам понадобится аутентификация конечной точки, то есть механизм, который позволит нам с уверенностью определить, исходит ли сообщение оттуда, где, по нашему мнению, оно происходит.

Атака «человек посередине» – как следует из названия, атака «человек посередине» происходит, когда кто-то между вами и человеком, с которым вы общаетесь, активно отслеживает, захватывает и прозрачно контролирует ваше общение. Например, злоумышленник может перенаправить обмен данными. Когда компьютеры взаимодействуют на нижних уровнях сетевого уровня, они могут быть не в состоянии определить, с кем они обмениваются данными.

Атака со скомпрометированным ключом. Ключ – это секретный код или число, необходимое для доступа к защищенной информации. Хотя получение ключа – сложный и ресурсоемкий процесс для злоумышленника, он возможен. После того, как злоумышленник получает ключ, этот ключ называется скомпрометированным ключом. Злоумышленник использует скомпрометированный ключ, чтобы получить доступ к защищенной связи без уведомления отправителя или получателя об атаке.

Фишинг – мошенническая практика отправки электронных писем якобы от авторитетных компаний с целью побудить людей раскрыть личную информацию, такую как пароли и номера кредитных карт.

Подмена DNS – также называемая отравлением кэша DNS, представляет собой форму взлома компьютерной безопасности, при которой поврежденные данные системы доменных имен вводятся в кэш преобразователя DNS, в результате чего сервер имен возвращает неверный IP-адрес.

Руткит – руткиты – это скрытые пакеты, предназначенные для использования административных прав и получения права доступа к инструменту сообщества. После установки хакеры имеют полное и неограниченное право доступа к инструменту и, следовательно, могут беспрепятственно выполнять любые действия, включая слежку за клиентами или кражу эксклюзивных данных.

Методами противодействия сетевым атакам являются: контроль доступа, обновление всего программного обеспечения, стандартизация

программного обеспечения, использования мер обеспечения сети и обучение сотрудников. Все эти методы в совокупности смогут обеспечить целостное противодействие сетевым атакам. Разберем их в деталях.

1. Контроль доступа.

Контроль доступа является важной частью безопасности. Слабый контроль доступа делает данные и системы уязвимыми для несанкционированного доступа.

Повысьте меры контроля доступа, используя надежную систему паролей. У вас должно быть сочетание прописных и строчных букв, цифр и специальных символов. Кроме того, всегда сбрасывайте все пароли по умолчанию, а также создайте надежную политику контроля доступа.

2. Обновление всего программного обеспечение.

Какими бы надоедливыми ни были эти предупреждения об обновлениях, они жизненно важны для целостного функционирования сети.

От антивирусного программного обеспечения до компьютерных операционных систем, стоит убедиться, что программное обеспечение обновлено. Когда выпускается новая версия программного обеспечения, она обычно включает исправления для уязвимостей системы безопасности.

Ручное обновление программного обеспечения может занять много времени. Используйте автоматические обновления программного обеспечения для максимально возможного количества программ.

3. Стандартизация программного обеспечения.

Защитите систему, стандартизировав программное обеспечение. Надо убедиться, что пользователи не могут устанавливать программное обеспечение в систему без разрешения.

Незнание того, какое программное обеспечение находится в сети, является огромной уязвимостью системы безопасности. Для этого надо понимать, что все компьютеры используют одно и то же:

- Операционная система
- Браузер
- Медиа плеер
- Плагины

Стандартизация также упрощает обновление системы.

4. Использование мер защиты сети.

Защита сети имеет решающее значение для обеспечения безопасность сети и ее трафика. Для этого необходимо:

- Установить брандмауэр
- Обеспечить надлежащий контроль доступа
- Использовать IDS/IPS для отслеживания потенциального потока пакетов
- Использовать сегментацию сети
- Использовать виртуальную частную сеть (VPN)
- Проводить надлежащее техническое обслуживание

5. Обучение сотрудников.

Иногда внешние угрозы успешны благодаря внутренней угрозе. Самым слабым звеном в защите данных могут быть собственные сотрудники компаний.

У сотрудников компаний должно быть понимание безопасности сети. Сотрудники должны уметь выявлять угрозы. Они также должны знать, с кем связаться, чтобы избежать нарушения безопасности.

Надо проводить обучение по безопасности в течение года и обязательно обновлять его. Каждый день появляются новые угрозы безопасности.

Таким образом, создание хорошей защиты требует понимания способов нападения. В этой статье были рассмотрены наиболее распространенные кибератаки, которые хакеры используют для нарушения работы и взлома информационных систем. У злоумышленников есть много вариантов, таких как DDoS-атаки, заражение вредоносным ПО, перехват «человек посередине» и

подбор пароля методом грубой силы, чтобы попытаться получить несанкционированный доступ к критически важным инфраструктурам и конфиденциальным данным.

Меры по смягчению этих угроз различаются, но основы безопасности остаются прежними: обновление системы и антивирусных баз данных, обучение сотрудников компаний, настройка брандмауэра, сохранение надежных паролей, использование моделей с минимальными привилегиями в вашей ИТ-среде, регулярное составление резервных копий и постоянная проверка ИТ-системы на наличие подозрительной активности.

Список литературы:

1. Анорбоев А. Преступление киберпреступности: уголовно-правовая и криминологическая характеристика. -Т.: 2020, Журнал правовых исследований. 2- специальный номер. - Б. 300-309 с.

2. Турдиева Г.С., Шойимов А.С.Основные особенности и функции использования современных облачных служб в системе образования// Вестник науки и образования 2021. № 17 (120).Часть 3. 52-55 с.

3. Турдиева Г.С. Исползование информационных технологий в сфере туризма // Шойимов А. Научно-методический журнал "ACADEMY" Российский-импакт фактор:0.19. №6 (57). 2020 г. 22-24 с.