

Кибератака «человек посередине»

Попов Юрий Б01-004

01.12.2023

Содержание

1	Введение	1
2	Принцип работы атаки	2
3	ARP-спуфинг	2
3.1	Пример атаки	2
4	DNS-спуфинг	3
4.1	Использование атаки «дней рождения»	3
4.2	Эксплойт Каминского	3
5	DHCP-спуфинг	4
6	IP-спуфинг	4
6.1	Неслепой IP-спуфинг	5
6.2	Слепой IP-спуфинг	5
7	Защита от атаки «человек посередине»	5
7.1	Защита от ARP-спуфинга	5
7.2	Защита от DNS-спуфинга	6
7.3	Защита от DHCP-спуфинга	6
7.4	Защита от IP-спуфинга	6
8	Дальнейшая судьба атаки "человек посередине"	6
	Ссылки на источники	8

1 Введение

Изо дня в день компьютерные системы и приложения постоянно развиваются, но параллельно с этим развиваются и технологии проведения нападений. Одной из популярных кибератак на сегодняшний день является

атака «человек посередине» (Man In The Middle, MITM). MITM - это атака, во время которой злоумышленник вмешивается в соединение между двумя пользователями, при этом оставаясь незамеченным. С помощью вредоносного программного обеспечения, применяемого в осуществлении этих нападений, он способен отслеживать и изменять информацию, которой обмениваются пользователи. Из-за сильной распространённости данного вида кибератак важную роль играет понимание того, как они устроены. В эссе приведён принцип работы таких нападений, их проявления, а также представлены несколько методов противодействия угрозам.

2 Принцип работы атаки

Чаще всего атаки данного типа основаны на спуфинге. Спуфинг - технический прием выдачи себя за другое лицо, чтобы обмануть сеть или конкретного пользователя с целью вызвать доверие в надежности источника информации. Злоумышленник внедряется в коммуникацию между двумя пользователями и контролирует входящий и исходящий трафик.

3 ARP-спуфинг

Когда один пользователь общается с другим в зашифрованной сети, если он не знает MAC-адреса получателя, то отправляет широковещательный ARP-запрос, на который ответит тот пользователь, который имеет нужный MAC-адрес, чтобы отправитель заполнил свою ARP-таблицу. В это время ввиду того, что ARP-таблица заполняется динамически, а способов верификации MAC-адресов на данный момент не существует, кэш данной таблицы может быть подделан злоумышленником путем отправки ложных ARP-ответов.

3.1 Пример атаки

Приведем пример атаки, основанной на ARP-спуфинге. Допустим, существует сеть, в которой находятся три пользователя: Жертва №1 (ЖК1) с IP-адресом 10.0.0.v1, MAC-адресом AA:AA:AA:AA:AA:V1; Жертва №2 (ЖК2) с IP-адресом 10.0.0.v2, MAC-адресом BB:BB:BB:BB:BB:V2; Злоумышленник (З) с IP-адресом 10.0.0.v3, MAC-адресом FF:FF:FF:FF:FF:V3. Атака будет происходить следующим образом.

1. З отправляет ответ на ARP-запрос ЖК1, в котором сообщается, что IP-адресу 10.0.0.v2 соответствует MAC-адрес FF:FF:FF:FF:FF:V3. Данная запись появится в ARP-таблице ЖК1
2. З отправляет ответ на ARP-запрос ЖК2, в котором сообщается, что IP-адресу 10.0.0.v1 соответствует MAC-адрес FF:FF:FF:FF:FF:V3. Данная запись появится в ARP-таблице ЖК2

После этого, если Жертва №1 захочет отправить сообщение Жертве №2, она отправит его Злоумышленнику, сама об этом не подозревая. Точно так же это работает и в обратную сторону, Жертва №2 при отправке сообщений будет ненамеренно отправлять их Злоумышленнику.

4 DNS-спуфинг

DNS (Domain Name System) - это система, позволяющая сопоставлять доменные имена с их IP-адресами. Вся система DNS организована в соответствии с иерархией. При обработке доменных имён локальный DNS-резольвер последовательно обращается к различным DNS-серверам, до того момента, пока не обнаружит нужный сервер в соответствующем домене. Резольвер принимает ответы откуда угодно, при условии, что формат ответа соответствует запросу. Хакеры могут вмешаться в этот процесс, подменяя ответы, получаемые от DNS-серверов. В результате, локальный DNS-резольвер может использовать записи злоумышленников, вместо подлинного ответа от уполномоченного сервера, так как он не способен отличить фальшивый ответ от истинного. Для DNS-спуфинга обычно используются две стратегии: подделка ответов с помощью атаки «дней рождения» и эксплойт Каминского.

4.1 Использование атаки «дней рождения»

Протокол DNS не содержит механизмов аутентификации ответов на рекурсивные и итеративные запросы. При проверке ответов используются только 16-битный идентификатор транзакции, IP-адрес отправителя и целевой порт. До 2008 года все DNS-резольверы использовали стандартный порт 53, что делало всю информацию кроме идентификатора транзакции предсказуемой для подделки ответа. Эта особенность послужила основой для DNS-атак, использующих «парадокс дней рождения». Обычно требовалось около 256 попыток (оценка сложности атаки приведена здесь [12]), чтобы угадать идентификатор транзакции. Для успешной атаки фальшивый DNS-ответ должен был прийти на целевой резольвер раньше, чем реальный ответ от DNS-сервера. Если оригинальный ответ придёт первым, он будет записан в кэше, и резольвер перестанет отправлять запросы с тем же доменным именем до истечения срока жизни записи в кэше (TTL). Таким образом, злоумышленник не сможет изменить кэш для этого домена в течение всего периода TTL.

4.2 Эксплойт Каминского

Уязвимость, обнаруженная Дэном Каминским, впервые была им представлена на конференции BlackHat в 2008 году. Данный метод атаки представляет собой своего рода измененную атаку «дней рождения». Суть его заключается в том, что атакующий отправляет DNS-резольверу запрос для

несуществующего поддомена. После получения запроса резольвер перенаправляет его на корневой сервер, так как данный поддомен, очевидно, отсутствует в его кэше. В это время злоумышленник отправляет большое количество поддельных ответов на резольвер, рассчитывая на то, что у какого-то из них идентификатор транзакции совпадет с идентификатором транзакции исходного запроса. В случае успеха злоумышленник подменит в кэше DNS-резольвера IP-адрес целого домена, к которому относился поддельный поддомен. В результате резольвер будет направлять пользователей на поддельный IP-адрес при попытке обращения к компрометированному домену до тех пор, пока не истечет TTL.

5 DHCP-спуфинг

Протокол DHCP (Dynamic Host Configuration Protocol) используется для автоматической настройки параметров сети на новых узлах. Эти параметры, такие как IP-адрес, маска подсети, адрес DNS-сервера и шлюз по умолчанию, предоставляются хосту DHCP-сервером. Протокол DHCP основан на клиент-серверной архитектуре, где клиенты отправляют запросы DHCP-серверу для получения необходимых сетевых параметров. Уязвимость заключается в том, что в DHCP-сообщениях отсутствует аутентификация источника сообщения. Для начала злоумышленник проводит атаку «DHCP Starvation» на реальный DHCP-сервер, суть которой заключается в отправке огромного количества сообщений DHCPDISCOVER, на которые сервер будет отвечать, тем самым постепенно истощая своё адресное пространство. После того, как злоумышленник выводит из строя реальный DHCP-сервер, он может создать его ложный аналог и заявить пользователям, что теперь именно он является шлюзом по умолчанию. В результате все пользовательские запросы будут проходить через хакерский DHCP-сервер.

6 IP-спуфинг

При использовании IP-спуфинга злоумышленник модифицирует IP-адрес отправителя в заголовке пакета таким образом, чтобы пакет был принят устройством-получателем как исходящий от надежного источника, например, от другого компьютера в сети с разрешенным доступом. При соединении двух устройств в сети с использованием TCP/IP сначала необходимо установить TCP-соединение. Во время его установления устройства отправляют друг другу специальные сообщения, которые содержат в себе последовательности цифр (TCP-последовательности). Номера таких последовательностей позволяют устройствам определить порядок последующих пакетов данных. Атакующий использует TCP-последовательности для изменения IP-пакета. Существует два вида атаки данного типа: «Неслепой IP-спуфинг» и «Слепой IP-спуфинг».

6.1 Неслепой IP-спуфинг

Неслепой IP-спуфинг работает, когда злоумышленник находится в одной подсети с жертвой и может напрямую видеть номера TCP-последовательностей других подключений, например, между жертвой и её маршрутизатором. Сначала злоумышленник перехватывает такое соединение с помощью специального программного обеспечения для мониторинга сети. Проанализировав заголовки перехваченных TCP-пакетов, хакер может узнать номера TCP-последовательностей, основываясь на них, предсказать номер следующей и отправить поддельный IP-пакет, делая вид, что он - оригинальный отправитель. Если этот пакет достигнет места назначения раньше, чем реальный ответ, злоумышленник перехватит соединение.

6.2 Слепой IP-спуфинг

Этот тип атаки намного сложнее выполнить, но он не ограничен одной подсетью, поэтому его можно попытаться осуществить, находясь вне локальной сети. Однако он работает только со старыми операционными системами. Ранее протоколы TCP/IP операционных систем использовали предсказуемые алгоритмы для генерации начальных номеров TCP-последовательностей. Иногда номера увеличивались на определенное значение для каждого нового соединения, в каких-то случаях - на определенное значение за единицу прошедшего времени. Чтобы узнать, какой алгоритм используется в конкретном случае, злоумышленник отправляет несколько SYN-запросов жертве и рассматривает начальные номера TCP-последовательностей, полученных от неё. Если он видит определенные закономерности в их генерации, он может попытаться угадать начальный номер последовательности для других соединений. Данная атака больше не работает с современными операционными системами (все современные Unix/Linux/Windows/Mac), потому что современное программное обеспечение в протоколах TCP/IP использует генераторы случайных чисел для создания начальных номеров TCP-последовательностей.

7 Защита от атаки «человек посередине»

7.1 Защита от ARP-спуфинга

Сейчас большинство коммутаторов оснащены функциями DAI (Dynamic ARP Inspection), предотвращающими атаки, основанные на ARP-спуфинге. Они позволяют оценивать достоверность каждого ARP-сообщения и отсеивать подозрительные или выглядящие вредоносными пакеты. Эти функции настраиваются вручную на коммутаторах. Обычно рекомендуется включать DAI на всех портах, за исключением тех, которые подключены к другим коммутаторам.

7.2 Защита от DNS-спуфинга

Чтобы защититься от DNS-спуфинга можно использовать зашифрованные DNS-запросы с помощью протокола DNSSEC (Domain Name System Security Extensions). Он использует подписанные запросы для предотвращения их подмены. Во время использования DNSSEC DNS-резольвер проверяет подпись на уполномоченном DNS-сервере, что замедляет процесс обмена сообщениями, ввиду чего данный протокол пока не получил широкого распространения. В дополнение к представленной мере безопасности следует пользоваться технологией VPN (Virtual Private Network), если это возможно. Она шифрует интернет-подключение и передачу данных в сети. Это защитит трафик и DNS-запросы от локального отслеживания.

7.3 Защита от DHCP-спуфинга

Для защиты от DHCP-спуфинга существует технология DHCP Snooping. Она позволяет осуществить две важные настройки на коммутаторе. Во-первых, с помощью данной технологии можно назначить «доверенные» и «недоверенные» порты. Чаще всего доверенным делается тот, что напрямую подключен к DHCP-серверу или же «смотрит» в его сторону, остальные порты делаются недоверенными. Коммутатор отбрасывает DHCP-ответы, пришедшие с недоверенных портов и не отбрасывает те, что пришли с доверенных. Во-вторых, можно настроить, так называемый, Limit Rate - это ограничение на количество отправленных DHCP-сообщений через порт в секунду. Как только это количество превышает, порт «падает» и более не работает, пока кто-либо вручную не «поднимет» его.

7.4 Защита от IP-спуфинга

Чтобы защититься от атак, основанных на IP-спуфинге, нужно соблюдать ряд мер безопасности. В первую очередь, стоит настроить на маршрутизаторах анти-спуфинг фильтры, которые блокируют входящие сообщения с поддельными IP-адресами. Помимо этого, стоит использовать файрволы (по-другому сетевые экраны), они помогают контролировать входящий и исходящий трафик и не пропускают межсетевые пакеты с недопустимыми источниками. Также очень полезно использовать VPN (данная технология описана в пункте 7.2) для защиты от IP-спуфинга.

8 Дальнейшая судьба атаки "человек посередине"

Данная атака будет актуальной для киберпреступников до тех пор, пока они будут иметь возможность завладеть с её помощью чужой ценной информацией, как, например, различные пароли или пин-коды банковских карт. Разработчики программного обеспечения постоянно работают над устранением

уязвимостей, которые злоумышленники используют для осуществления нападений. На данный момент наблюдается стремительный рост количества сетей и устройств, подключенных к ним, что, несомненно, увеличивает число возможностей для хакеров использовать данную атаку.

Ссылки на источники

- [1] <https://habr.com/ru/companies/varonis/articles/526632/>
- [2] <https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM>
- [3] <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
- [4] <https://www.kaspersky.ru/resource-center/threats/ip-spoofing>
- [5] <https://www.kaspersky.ru/resource-center/threats/ip-spoofing>
- [6] <https://blog.skillfactory.ru/glossary/dns/>
- [7] <https://www.securitylab.ru/analytics/499199.php>
- [8] <https://developer.mozilla.org/ru/docs/Web/HTTP/Overview>
- [9] <https://www.javatpoint.com/cyber-security-mitm-attacks>
- [10] <https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-20-ru>
- [11] <https://community.fs.com/ru/article/what-is-dhcp-snooping-and-how-it-works.html>
- [12] <https://www.geeksforgeeks.org/birthday-attack-in-cryptography/>
- [13] <https://freenvpnplanet.com/ru/blog/cto-takoe-ip-spufing-i-kak-predotvrashhat-spufing-ataki/>