Кибератака «человек посередине»

Введение

Изо дня в день компьютерные системы и приложения постоянно развиваются, но параллельно с этим развиваются и технологии кибератак. Одной из популярных атак на сегодняшний день является атака "человек посередине" (Man-in-the-Middle). В данном случае злоумышленник вмешивается в соединение между двумя пользователями, при этом оставаясь незамеченным. Вредоносное программное обеспечение, применяемое в осуществлении этих атак, способно отслеживать и изменять информацию, которой обмениваются пользователи. Злоумышленник имеет возможность не только получать доступ к конфиденциальной информации, но и изменять ее, будучи при этом необнаруженным. Ввиду сильной распространённости данного вида атак важную роль играет понимание того, как они устроены. В данном эссе приведена суть атак "человек по середине", их проявления, а также представлены несколько методов противодействия данным угрозам.

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.

ARP-спуфинг

Приведем пример атаки, основанной на ARP-спуфинге. Когда один пользователь общается с другим в зашифрованной сети, если он не знает MAC-адреса получателя, то он 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.

Допустим, существует сеть, в которой находятся три пользователя: Жертва №1 (Ж1) с IP-адресом 10.0.0.v1, MAC-адресом СС:СС:СС:СС:СС:V1; Жертва №2 (Ж2) с IP-адресом 10.0.0.v2, MAC-адресом DD:DD:DD:DD:DD: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 Ж1, 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 Ж1
2. Аналогично З отправляет ответ на ARP-запрос Ж2, 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 Ж2

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.

DNS-спуфинг

DNS-сервер - это система позволяющая сопоставлять доменные имена с их IP-адресами. Вся система DNS организована в соответствии с иерархией. При обработке доменных имен резольвер локального DNS-сервера последовательно обращается к различным серверам, до того момента, пока не обнаружит нужный сервер в соответствующем домене. Локальный DNS-сервер принимает ответы откуда угодно, при условии, что формат ответа соответствует запросу. Злоумышленники могут вмешаться в этот процесс, изменяя ответы, получаемые от найденных ранее DNS-серверов. В результате, локальный DNS-сервер может использовать DNS-записи злоумышленника, вместо подлинного ответа от уполномоченного сервера, так как он не способен отличить фальшивый ответ от правильного. Для взлома DNS-сервера, обычно используются две стратегии: атака с использованием подделки ответов с помощью атаки "дней рождения" и эксплойт Каминского.

**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 атак на DNS, использующих «парадокс дней рождения». Обычно для успешной атаки требовалось около 256 попыток, чтобы угадать идентификатор транзакции. Для успешной атаки фальшивый DNS-ответ должен был прийти на целевой резольвер раньше, чем ответ от реального DNS-сервера. Если оригинальный ответ приходит 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.

**Эксплойт Каминского**

Данный метод атаки представляет собой своего рода измененную атаку «дней рождения». Атакующий отправляет резольверу запрос для несуществующего домена. После получения запроса резольвер перенаправляет его на корневой сервер, чтобы получить IP-адрес ложного домена. В это время злоумышленник отправляет большое количество поддельных ответов на резольвер, рассчитывая на то, что у какого-то из этих ответов идентификатор транзакции совпадет с идентификатором транзакции исходного запроса. В случае успеха злоумышленник подменит в кэше DNS-сервера IP-адрес. В таком случае резольвер будет направлять всех пользователей на поддельный IP-адрес до тех пор, пока не истечет жизненный цикл записи DNS.

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 «DHCP Starvation» атаку 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 легитимный 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 мошеннический DHCP-сервер.

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. Операция происходит на уровне сети, что делает внешние признаки манипуляции незаметными. Существует два вида атаки данного типа: «Неслепой IP-спуфинг» и «Слепой IP-спуфинг».

**Неслепой IP-спуфинг**