УДК 004.056+003.26

Студ. Е.А. Шпаковский
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СЕТЕВАЯ БЕЗОПАСНОСТЬ: СНИФФИНГ И СПУФИНГ

В настоящее время люди все чаще сталкиваются с терминами «Информационной безопасности и защиты данных в компьютерных сетях» [1,2]. В мире происходит много хакерских атак, давайте рассмотрим такие, как сниффинг и спуфинг [3,4].

Сниффер может анализировать только то, что проходит через «его» сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов — форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Перехват трафика может осуществляться:

• обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);

• подключением сниффера в разрыв канала;

• ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер (Network tap);

• через анализ побочных электромагнитных излучений и восстановление, таким образом, прослушиваемого трафика;

• через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

Снифферы не всегда применяются в плохих целях, они также могут использоваться в благих целях. Анализ прошедшего через сниффер трафика позволяет:

• обнаружить паразитный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны; как правило, для этих целей ис-

пользуют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ);

• выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов — мониторов сетевой активности);

• перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации;

• локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами).

Спуфинг (англ. spoofing — подмена) — вид сетевой атаки, при которой злоумышленник стремиться выдать себя за другое лицо. Мошенник стремится обмануть сеть или конкретного пользователя, чтобы убедить его в надежности информации.

ARP-спуфинг осуществляет перехват трафика за счет уязвимости api-протокола из-за отсутствия проверок подлинности запросов и ответов. Протоколы пропускают исходящий трафик на сервер злоумышленника, в результате хакер получает секретные сведения логин, пароль и т. д.

Рассмотрим пример, приведенный на рисунке 1.

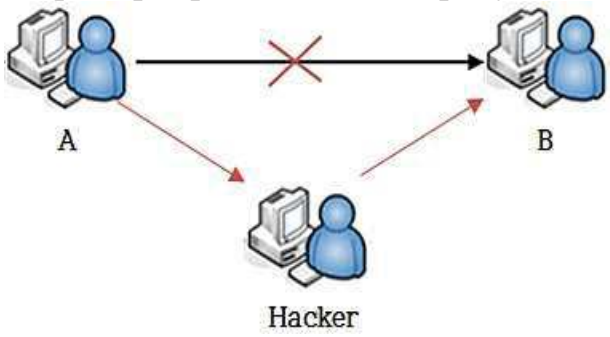

Рисунок 1 – Принцип реализации ARP-атаки

Связь между A и B до применения ARP-spoofing производилась напрямую между двумя компьютерами. В случае, когда произошла ARP-spoofing атака на связь между A и B, все пакеты проходят сперва через H-хакера.

1. Два компьютера (узла) A и B в локальной сети Ethernet обмениваются сообщениями. Злоумышленник H, находящийся в этой же сети, хочет перехватывать сообщения между этими узлами. До применения атаки ARP-spoofing на сетевом интерфейсе узла A ARP-таблица содержит IP- и MAC-адреса [2] узла B. Также на сетевом интерфейсе узла B ARP-таблица содержит IP- и MAC-адреса узла A.

2. Во время атаки ARP-spoofing узел H (злоумышленник) отсылает два ARP-ответа (без запроса) — узлу A и узлу B. ARP-ответ узлу A содержит IP-адрес B и MAC-адрес H. ARP-ответ узлу B содержит IP-адрес A и MAC-адрес B.

3. Так как компьютеры A и B поддерживают самопроизвольный ARP, то, после получения ARP-ответа, они изменяют свои ARP-таблицы, и теперь ARP-таблица A содержит MAC адрес H, привязанный к IP-адресу B, а ARP-таблица B содержит MAC адрес H, привязанный к IP-адресу A.

4. Тем самым атака ARP-spoofing выполнена, и теперь все пакеты (трафик) между A и B проходят через H. К примеру, если A хочет передать пакет компьютеру B, то A «смотрит» в свою ARP-таблицу, находит запись с IP-адресом узла B, выбирает оттуда MAC-адрес (а там уже MAC-адрес узла H) и передает пакет. Пакет поступает на интерфейс H, анализируется им, после чего перенаправляется узлу B.

Чтобы предотвратить ARP-атаку можно использовать несколько методов, каждый из которых имеет свои плюсы и минусы. К ним относятся статические ARP записи, шифрование, VPN и анализ пакетов.

Статические ARP записи – это решение связано с большими административными затратами и рекомендуется только для небольших сетей. Он включает добавление ARP записи для каждого компьютера в сети на каждый отдельный компьютер.

Сопоставление компьютеров с наборами статических IP-адресов и MAC-адресов помогает предотвратить спуфинговые атаки (spoofingattacks), поскольку компьютеры могут игнорировать ответы ARP. К сожалению, это решение может защитить вас только от простых атак.

Шифрование[1, 5]: протоколы, такие как HTTPS и SSH, также могут помочь уменьшить вероятность успешной атаки отравления ARP. Когда трафик зашифрован, злоумышленнику придется предпринять дополнительный шаг, чтобы обмануть браузер цели и заставить его принять незаконный сертификат. Однако любые данные, передаваемые за пределы этих протоколов, будут по-прежнему уязвимы.

VPN может быть разумной защитой для частных лиц, но данный вариант обычно не подходят для крупных организаций. Если только один человек устанавливает потенциально опасное соединение, например, использует публичный Wi-Fi в аэропорту, то VPN зашифрует все данные, которые передаются между клиентом и сервером выхода. Это помогает обеспечить их безопасность, потому что злоумышленник сможет увидеть только зашифрованный текст.

Тем не менее, это менее осуществимое решение на организационном уровне, поскольку между каждым компьютером и каждым сервером должны быть установлены VPN-соединения. Это будет не только сложно настроить и поддерживать, но шифрование и дешифрование в таких масштабах также будет влиять на производительность сети.

Фильтры пакетов. Эти фильтры анализируют каждый пакет, отправляемый по сети. Они могут отфильтровывать и блокировать вредоносные пакеты, а также те, чьи IP-адреса являются подозрительными. Фильтры пакетов также могут сообщать о том, поступает ли пакет из внутренней сети, когда он фактически исходит извне, что, в свою очередь помогает снизить вероятность успеха атаки.

Если вы хотите, чтобы ваша сеть была защищена от угрозы «отравления» ARP, лучший вариант для вас – это комбинация вышеупомянутых инструментов предотвращения и обнаружения. Методы предотвращения, как правило, имеют недостатки в определенных ситуациях, поэтому даже самая безопасная среда может оказаться под угрозой.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск : БГТУ, 2016, – 220 с.

2. Урбанович, П. П. Компьютерные сети : учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. - Минск: БГТУ, 2011. - 399с.

3. IT-безопасность. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/ARP-spoofing. – Дата доступа: 17.04.2019.

4. Сниферы. [Электронный ресурс]. – Режим доступа: https://www.avast.ru/c-sniffer. – Дата доступа: 17.04.2019.

5. Урбанович, П. П. Информационная безопасность и надежность систем: учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007. – 87 с.