УДК 339.138

Студ. Д.Д. Летковский
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СЕТЕВАЯ БЕЗОПАСНОСТЬ: СНИФФИНГ И СПУФИНГ

В контексте информационной безопасности и защиты данных в компьютерных сетях [1-2] важную роль играет сниффинг и спуфинг.

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 [3]. 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 применяются как в деструктивных, так и 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 используют 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) — ситуация, в которой один человек или программа успешно маскируется под другую путём фальсификации данных и позволяет получить незаконные преимущества [4].

Спуферы электронной почты делают так, что кажется, будто сообщение пришло от кого-то еще, а не от фактического отправителя. Спуферы электронной почты часто являются спамерами, но технику спуфинга используют сталкеры (stalkers) и флеймеры (flamers), а также те, кто скрывает себя при отправке сообщений. Спуфинг электронной почты является формой обмана, схожей с подделкой чей-то подписи на документе.

Самая простая форма спуфинга электронной почты — изменение поля «От» в клиенте электронной почты отправителя. Вместо своего имени вы можете ввести там имя кого угодно, так что когда адресат получает сообщение, это выглядит как послание от «Президента США», «Джона Доу» или от кого-либо еще, чье имя вы написали в области для конфигурирования (configuration field). Более изощренные формы спуфинга включают изменение заголовков сообщения.

Спуферы могут также отсылать свои сообщения через открытые релей (почтовые SMTP-серверы, которые сконфигурированы для разрешения третьим лицам, не являющимся пользователями местной сети, отправлять почту через них), чтобы замаскировать источник этих сообщений.

Спуферы сайтов устанавливают их на своих собственных серверах. Эти веб-узлы кажутся другими, законными, сайтами на других серверах. Например, спуфер может создать сайт, который делает вид, что он сайт Министерства обороны США или сайт Microsoft.

Спуфинг IP-адресов часто используется для запуска таких атак, как DoS. IP-спуфинг может обходить механизмы защиты, которые требуют аутентификации на основании адресов IP. Например, пакет

изменяется так, что кажется, будто он пришел с компьютера в местной сети, хотя на самом деле он пришел из Интернета.

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. Интернет-портал [Электронный ресурс]/ IT-безопасность. – Режим доступа: http://elims2.blogspot.com.by/2008/03/sniffer.html. – Дата доступа: 20.03.1017.

4. Интернет-портал [Электронный ресурс]/ Определение направления на спуфер с помощью ГНСС-приемника. – Режим доступа: http:// secure.tradition.ru/2018/02/09/. – Дата доступа: 20.03.1017.

УДК004.056

Студ. В.Н. Долговечный
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

УЯЗВИМОСТИ И МЕТОДЫ ЗАЩИТЫ БАЗ ДАННЫХ НА МОБИЛЬНОЙ ПЛАТФОРМЕ

В соответствии с последними данными исследовательской компании eMarketer [1], специализирующейся на анализе рынка высоких технологий, смартфонами уже пользуется больше четверти мирового населения. Это около 2,5 млрд. человек. И тенденция роста пользователей мобильных устройств продолжается.

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные: номера кредитных карт, электронную почту, геолокационные сведения, профили в социальных сетях, средства удалённого доступа и управления предприятием, фотографии, видео и т. д. Несанкционированный доступ к таким чувствительным данным может привести к критической ситуации [2]. Между тем, рынок мобильных приложений растёт с большой скоростью, а пользователи особенно не задумываются о том, какие разрешения они предоставляют при-