МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»

В. В. Сафронов, С. Л. Кенин, С. А. Рыков

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие

Воронеж
Издательский дом ВГУ
2019

Содержание

ŋqdqyeY bɆ debɆbY3e d eaɑqcy ɟqdqYqyè

только предназначенных MAC-адресу сетевой карты и широковещательных, как это происходит в обычном режиме.

Применение снифферов на разных сетевых уровнях

Важно помнить о том, что атаки с использованием сниффера могут затрагивать диапазон от 1 до 7 уровня OSI. Если говорить о физическом соединении, кто-либо, уже имеющий доступ к внутренней локальной сети (чаще всего это работник компании), может использовать программы для прямого захвата сетевого трафика. Применяя техники спуфинга, взломщик, находящийся за пределами атакуемой сети, может вести перехват пакетов на уровне межсетевого экрана и похищать данные. В последнее время все чаще используется атака, направленная на перехват данных беспроводных сетей, при которой задача атакующего упрощается, так как нужно всего лишь находиться в радиусе действия сети для сбора информации о ней и проникновения в нее.

Использование сниффера в сетях, работающих по протоколу TCP/IP подразумевает захват, декодирование, исследование и интерпретацию данных, передающихся в пакетах по сети.

Для понимания того, для чего взломщики используют снифферы, нам следует знать о том, какие данные они могут получить из сети. Таблица 1.1 иллюстрирует уровни OSI и ту информацию, которой взломщик может завладеть на каждом уровне, успешно использовав сниффер.

Таблица 1.1. Распределение уровней OSI

Уровень	Действие
Прикладной	Захват имен пользователей и паролей
Представительский	Захват трафика сессий SSL/TLS
Сеансовый	Захват трафика Telnet/FTP
Транспортный	Захват TCP-сессий и UDP-трафика
Сетевой	Захват IP-адресов и номеров портов
Канальный	Захват MAC-адресов и ARP-запросов
Физический	Получение сведений о сети

Пакет TCP/IP содержит информацию, необходимую для соединения двух сетевых интерфейсов. Он содержит такие поля с информацией об исходном и целевом IP-адресах, номерах портов, номере пакета и типе протокола. Каждое из этих полей является необходимым для функционирования различных уровней сетевого стека и особенно приложений, относящихся к прикладному уровню (уровню 7 OSI), обрабатывающих принятые данные.

По своей природе протокол TCP/IP занимается только тем, что проверяет, сформирован ли пакет, добавлен ли он в Ethernet-фрейм и доставлен ли он от отправителя по сети к адресату. Однако, в этом протоколе не имеется механизмов для контроля безопасности данных. Таким образом, задача по установлению того, не произошло ли вмешательство в передачу данных, перекладывается на высшие уровни сетевого стека.

Способы перехвата траффика

В зависимости от того, каково нахождение взломщиков в сети, где производится перехват данных, они используют программы для захвата или программы для исследования пакетов.

В отношении технической стороны захвата пакетов следует помнить о том, что программы, осуществляющие захват пакетов, всегда работают в promiscous-режиме, что делает возможным захват и сохранение всех данных, передающихся по сети, с их помощью. Это также означает то, что даже если пакет не предназначается для сетевого интерфейса, на котором работает сниффер, он все равно будет захвачен, сохранен и проанализирован.

В ходе атак, заключающихся в захвате пакетов, используются снифферы, являющиеся либо программным обеспечением с открытым исходным кодом, либо коммерческим программным обеспечением. В целом, существуют три пути перехвата трафика в сети:

– использование внешней сети для перехвата траффика;

– использование внутренней сети для перехвата траффика;

– использование беспроводной сети для перехвата траффика.

Похищение паролей (Web password sniffing)

Как становится ясно из названия, в ходе атаки перехватываются данные HTTP-сессий и из них выделяются идентификаторы пользователей и пароли, которые похищаются. Хотя для защиты HTTP-сессий от таких атак и разработан протокол SSL, существует множество сайтов во внутренних сетях, использующих стандартное менее безопасное шифрование. Достаточно просто перехватить данные зашифрованные по алгоритмам Base64 или Base128 и получить пароль, применив специальное программное обеспечение. В современных снифферах присутствует функция захвата и получения информации, передаваемой в рамках SSL-сессий, но использовать эту функцию непросто.

Похищение TCP-сессий (TCP session stealing)

Этот метод заключается в простом захвате трафика между IP-адресом отправителя и адресата, проходящего через сетевой интерфейс в promiscous-режиме. Такие подробности, как номера портов, типы служб, порядковые номера TCP и сами данные интересуют взломщиков в первую очередь. После захвата достаточного количества пакетов, опытные взломщики могут самостоятельно создавать TCP-сессии, вводя в заблуждение узлы, являющиеся источником и адресатом пакетов, а также осуществлять атаку перехвата с участием человека (man-in-the-middle) в отношении активной TCP-сессии.

Захват данных приложений (Application-level sniffing)

Обычно из захваченных пакетов данных можно получить некоторое количество информации относительно приложений, осуществляющих обмен данными, и на основе этой информации провести другие атаки или просто похитить эту информацию. Например, протокол захвата данных может быть исследован с целью идентификации операционной системы, анализа SQL-за-

просов, получения информации о TCP-портах, специфических для приложения и т. д. С другой стороны, создание списка приложений, исполняющихся на сервере является хорошим началом атаки в отношении этих приложений.

Захват данных в локальной сети (LAN sniff)

Сниффер, работающий во внутренней сети может захватывать данные со всего диапазона IP-адресов. Это помогает злоумышленнику получить данные о функционировании сети, такие, как список активных узлов, список открытых портов, данные об оборудовании серверов и другие. Как только получен список открытых портов, становится возможной атака на основе эксплуатации уязвимостей отдельных служб, работающих на определенных портах [11].

Захват информации об используемых протоколах (Protocol sniff)

Этот метод подразумевает захват данных, относящихся к различным протоколам, используемым в сети. Сначала создается список протоколов, на основе захваченных данных. Этот список в будущем может использоваться для захвата данных, относящихся к отдельным протоколам. Например, если данных, относящихся к протоколу ICMP не было обнаружено во время захвата, считается, что этот протокол заблокирован. Однако, если при захвате обнаружены UDP-пакеты, отдельный сниффер для UDP-трафика начинает использоваться для захвата и расшифровки трафика, относящегося к Telnet, PPP, DNS и другим приложениям.

Захват ARP-трафика (ARP sniff)

В ходе этого популярного метода атаки злоумышленник захватывает как можно больший объем данных для создания таблицы соответствия IP-адресов MAC-адресам. Эта таблица впоследствии может быть использована для подмены ARP-записей (APR poisoning), спуфинг-атак или для эксплуатации уязвимостей маршрутизатора [10].

Роль снифферов

Использование сниффера считается типом "пассивной" атаки, при котором атакующие не могут быть замечены в сети. Это обстоятельство затрудняет определение наличия данной атаки и, поэтому, этот тип атаки является опасным.

Использование сниффера помогает взломщикам либо получить информацию непосредственно из сетевого трафика, либо получить данные о работе сети, которые могут быть использованы для подготовки последующих атак. Взломщики очень часто прибегают к использованию сниффера, так как возможно длительное его использование без риска быть разоблаченным.

Современные снифферы предназначаются для диагностики сетей, но при этом также могут быть использованы и для взлома. В таблице 1.2 приведены основные примеры, описывающую законные и незаконные примеры использования снифферов.

Таблица 1.2. Цели использования снифферов

Примеры законного использования	Примеры незаконного использования
1. Захват пакетов. 2. Анализ использования трафика в сети. 3. Преобразования пакетов для анализа данных. 4. Диагностика сетей.	1. Похищение пользовательских паролей и идентификаторов. 2. Похищение данных, относящихся к сообщениям электронной почты и служб мгновенных сообщений. 3. Похищение данных с применением спуфинга. 4. Похищение средств и причинение ущерба репутации.

Сниффер Wireshark

Утилита Wireshark является широко известным инструментом перехвата и интерактивного анализа сетевого трафика, фактически, стандартом в промышленности и образовании. К ключевым особенностям Wireshark можно отнести: многоплатформенность (Windows, Linux, Mac OS, FreeBSD,