Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Пакет dsniff

http://www.monkey.org/~dugsong/dsniff/

Пакет dsniff представляет собой набор программ для сетевого аудита и проверок на возможность проникновения Программы dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf и webspy обеспечивают пассивный мониторинг сети для поиска интересующих данных. (пароли, адреса электронной почты, файлы и т. п.), arpspoof, dnsspoof и macof обеспечивают перехват сетевого трафика, в обычных условиях недоступного для анализа (например, в коммутируемой сети), а sshmitm и webmitm обеспечивают возможность организации MITM-атак для перехвата сессий SSH и HTTPS за счет использования недостатков PKI.

Программы требуют аккуратного использования и могут нанести существенный ущерб при их необдуманном применении.

arpspoof

Программа arpspoof обеспечивает возможность сбора пакетов в коммутируемых средах ЛВС.

Синтаксис

```
arpspoof [-i interface] [-t target] host
```

Программа **arpspoof** перенаправляет пакеты от хоста, указанного параметром target, или всех хостов локальной сети, предназначенные для другого хоста ЛВС , с помощью обманных откликов ARP. Такой перехват пакетов обеспечивает эффективный мониторинг трафика в коммутируемых сетях.

Для использования **arpspoof** в ядре ОС (или пользовательской программе, служащей для маршрутизации – например, fragrouter) должен быть включен режим пересылки IP.

Опции

`-i interface`
задает используемый программой интерфейс.

`-t target`
задает хост ЛВС, трафик которого будет перехватывать программа; по умолчанию программа перехватывает весь трафик локальной сети.

`host`
задает хост, на который передается перехваченный трафик (обычно это локальный шлюз).

dnsspoof

Программа dnsspoof обеспечивает передачу обманных откликов на запросы DNS типа A и PTR.

Синтаксис

```
dnsspoof [-i interface] [-f hostsfile] [expression]
```

Программа dnsspoof обеспечивает подмену откликов на запросы DNS типа A (прямое преобразование) и PTR (обратное преобразовани) в локальной сети. Эта программа может оказаться полезной для обхода систем контроля доступа по именам хостов или организации различных MITM-атак.

Опции

`-i interface`
задает используемый программой интерфейс.

`-f hostsfile`
задает полное имя файла, в формате hosts, содержащего список имен, для которых будут передаваться подставные отклики. В каждой строке такого файла должно быть указано одно имя (не псевдоним) хоста или шаблон имен (например, *.domain.net).

`expression`
Задает фильтр tcpdump для отбора интересующего трафика.

Если параметр hostsfile не указан в командной строке, обманные отклики будут генерироваться для всех запросов типа A по отношению к хостам ЛВС с возвратом IP-адреса локальной машины.

dsniff

Программа dsniff обеспечивает возможность сбора различных паролей, передаваемых через локальную сеть.

Синтаксис

```
dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen] [-f services] [-t trigger[,...]]]
[-r|-w savefile] [expression]
```

Используя программу dsniff, можно собрать пользовательские пароли FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase и Microsoft SQL.

Программа dsniff автоматически распознает и выполняет анализ пакетов каждого из прикладных протоколов, сохраняя интересующие байты в формате Berkeley DB и протоколируя уникальные попытки аутентификации пользователей. Полная сборка TCP/IP обеспечивается библиотекой libnids.

Опции

-c
задает выполнение полнодуплексной сборки потоков TCP для обработки трафика с асимметричными маршрутами (например, при использовании arpspoof) для перехвата пользовательского трафика, предназначенного локальному шлюзу.

-d
включает режим отладки.

-m
включает автоматическое детектирование протокола.

-n
отключает преобразование адресов IP в имена хостов.

-i interface
задает используемый программой интерфейс.

-s snaplen
задает анализ не менее snaplen начальных байтов из каждого соединения TCP (по умолчанию просматривается 1024 байта).

-f services
загружает триггеры из файла services.

-t trigger[,...]
загружает триггеры из списка (разделенные запятыми записи виде port/proto=service – например, 80/tcp=http).

-r savefile
задает чтение данных из файла, созданного программой при использовании ее с опцией -w.

-w file
задает запись собранной информации в файл вместо ее разбора и вывода на консоль.

expression
задает фильтр tcpdump для сбора пакетов.

По сигналу hangup программа dsniff будет сохранять текущую таблицу триггеров в файле /etc/dsniff.services.

Файлы

/etc/dsniff.services
используемая по умолчанию таблица триггеров.

/etc/dsniff.magic
список сетевых протоколов.

filesnarf

Программа filesnarf собирает файлы, передаваемые по протоколу NFS, и сохраняет их в текущем каталоге.

Синтаксис

filesnarf [-i interface] [[-v] pattern [expression]]

Опции

-i interface
задает используемый программой интерфейс.

-v
обращает “знак соответствия” для файлов, заданных параметром pattern.

pattern
задает регулярное выражение для отбора файлов по именам.

expression
задает фильтр tcpdump для сбора пакетов.

macof

Программа macof позволяет создать в локальной сети лавину пакетов со случайными MAC-адресами, в результате которой некоторые коммутаторы могут переходить в режим повторителя (хаба), обеспечивая возможность сбора пакетов. Программа написана на основе Perl-сценария Ian Vitek (ian.vitek@infosec.se) Net::RawIP.

Синтаксис

macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

Опции

-i interface
задает используемый программой интерфейс.

-s src
задает IP-отправителя.

-d dst
задает IP-получателя.

-e tha
задает аппаратный адрес получателя.

-x sport
задает TCP-порт отправителя.

-y dport
задает TCP-порт получателя.

-n times
задает число передаваемых пакетов.

По умолчанию для всех опций используются случайные значения.

mailsnarf

Программа mailsnarf собирает почтовые сообщения в формате Berkeley mbox, перехватывая трафик SMTP и POP. Формат вывода удобен для последующего просмотра с помощью стандартных почтовых клиентов.

Синтаксис

mailsnarf [-i interface] [[-v] pattern [expression]]

Опции

-i interface
задает используемый программой интерфейс.

-v
обращает "знак соответствия" для выражений, заданных параметром pattern.

pattern
задает регулярное выражение для поиска в заголовках и содержимом почтовых сообщений.

expression
задает фильтр tcpdump для сбора пакетов.

msgsnarf

Программа msgsnarf обеспечивает перехват сообщений chat и может работать с форматами обмена сообщениями AOL Instant Messenger, ICQ 2000, IRC, MSN Messenger, Yahoo Messenger.

Синтаксис

msgsnarf [-i interface] [[-v] pattern [expression]]

Опции

-i interface
задает используемый программой интерфейс.

-v
обращает "знак соответствия" для выражений, заданных параметром pattern.

pattern
задает регулярное выражение для поиска в сообщениях.

expression
задает фильтр tcpdump для сбора пакетов.

urlsnarf

Программа urlsnarf перехватывает запросы HTTP и выводит их в формате CLF[1], используемом в большинстве web-серверов. Собранную информацию об URL можно впоследствии обрабатывать с помощью привычного анализатора журнальных файлов.

Синтаксис

urlsnarf [-n] [-i interface] [[-v] pattern [expression]]

Опции

-n
отключает преобразование адресов IP в имена хостов.

-i interface
задает используемый программой интерфейс.

-v
обращает "знак соответствия" для выражений, заданных параметром pattern.

pattern
задает регулярное выражение для поиска URL.

expression
задает фильтр tcpdump для сбора пакетов.

webspy

Программа webspy обеспечивает передачу URL, из перехваченных пользовательских запросов в программу Netscape в реальном масштабе времени. Таким образом обеспечивается возможность синхронного просмотра страниц. Для работы программы должен быть загружен браузер Netscape.

Синтаксис

[1]Common Log Format

webspy [-i interface] host

Опции

-i interface

задает используемый программой интерфейс.

host

задает хост клиента, для которого осуществляется перехват.

sshmitm

Программа sshmitm обеспечивает возможность перехвата данных SSH[2], реализуя функции прокси-сервера и сборщика трафика, перенаправленного с помощью dnsspoof (стр. 1). Программа позволяет перехватывать сеансы подключения по протоколу SSH, а также обмен данными в таких сессиях. В настоящее время программа поддерживает только версию 1 протокола SSH.

Синтаксис

sshmitm [-d] [-I] [-p port] host [port]

Опции

-d

включает расширенный вывод информации (например, для отладки).

-I

включает мониторинг/перехват сеансов обмена данными.

-p port

задает порт для прослушивания.

host

задает удаленный хост, подключения к которому будут перехватываться.

port

задает номер порта на удаленном хосте.

webmitm

Программа webmitm обеспечивает перехват сессий HTTP/HTTPS[3], реализуя функции прозрачного прокси-сервера и захватывая трафик HTTP/HTTPS, перенаправленный с помощью программы dnsspoof (стр. 1). Программа может перехватывать сессии, использующие шифрование SSL.

Синтаксис

webmitm [-d]

Опции

-d

включает режим отладки, обеспечивающий вывод дополнительной информации.

Программа хранит сертификат SSL в файле **webmitm.crt**.

[2]SSH monkey-in-the-middle
[3]HTTP/HTTPS monkey-in-the-middle