Современные хакерские методы

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

1. *Скрипт киддиз*

Скрипт киддиз (script kiddies) – это пользователи, отыскивающие сценарии эксплойтов в интернете и запускающие их против всех систем, которые только можно найти (не требуют специальных знаний или инструкций).

2. *Прослушивание коммутируемых сетей*

Прослушивание коммутируемых сетей или снифинг (sniffing) – используется хакерами для сбора паролей и другой системной информации после взлома системы.

Принцип работы: сетевой адаптер перехватывает все пакеты, перемещающиеся по сети, а не только пакеты, адресованные данному адаптеру или системе после того, как снифер установит плату сетевого интерфейса в режим прослушивания смешанного трафика (promiscuous mode). Данные сниферы работают в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами. В коммутируемой среде используются сниферы, специально разработанные для данной среды.

3. Перенаправление трафика

Для кадра, передаваемого по сети Ethernet, на основании адреса доступа к среде передачи данных (Media Access Control) – MAC-адреса, коммутатор направляет трафик к портам. С учетом того, что каждая плата сетевого интерфейса имеет уникальный MAC-адрес, коммутатор распознает, какие адреса назначены какому порту. Поэтому при передаче кадра с определенным MAC-адресом получателя коммутатор направляет этот кадр к порту, к которому приписан данный MAC-адрес.

Теперь рассмотрим методы, с помощью которых можно заставить коммутатор направлять сетевой трафик к сниферу.

4. ARP-спуфинг (ARP-spoofing)

ARP – это протокол преобразования адресов (Address Resolution Protocol), используемый для получения MAC-адреса, связанного с определенным IP-адресом. При передаче трафика, система-отправитель посылает ARP-запрос по IP-адресу получателя, а система-получатель отвечает на этот запрос передачей своего MAC-адреса, который будет использоваться системой-отправителем для прямой передачи трафика. При перехвате интересующего трафика, снифер ответит на ARP-запрос вместо реальной системы-получателя и предоставит собственный MAC-адрес. В результате система-отправитель будет посылать трафик на снифер. Если трафик на снифер будет переадресован не целиком, то появится вероятность возникновения отказа в доступе к сети. К тому же, снифер должен размещаться в том же самом сегменте локальной сети, где находятся системы отправителя и получателя.

5. Дублирование MAC-адресов

Дублирование MAC-адреса системы-получателя – еще один способ «убеждения» коммутатора посылать трафик на снифер. Достигается это путем изменения MAC-адреса на снифере и размещения в системе, которая находится в том же сегменте локальной сети.

Примечание: MAC-адрес в системе Unix меняется с помощью команды **ipconfig**, в системе Windows с помощью аналогичных утилит.

6. Имитация доменного имени

Имитация доменного имени позволяет сниферу перехватывать DNS-запросы от системы-отправителя и отвечать на них. Снифер передает свой IP-адрес системе-отправителю, тем самым присваивая весь передающийся трафик себе. После чего он перенаправляет этот трафик реальному получателю. Для выполнения данной атаки сниферу необходимо просматривать все DNS-запросы и отвечать на них до того, как это сделает реальный получатель. Поэтому он должен располагаться на маршруте следования трафика от системы-отправителя к DNS-серверу, а еще лучше – в той же локальной подсети, что и отправитель.

7. Отправка всего трафика ко всем портам

Суть данной атаки заключается в следующем. Хакер непосредственно подключается к нужному коммутатору и заставляет его работать в качестве хаба (концентратора). Каждый коммутатор использует определенный объем памяти для хранения таблицы соответствий между MAC-адресом и физическим портом коммутатора. Эта память имеет ограниченный объем. При ее переполнении некоторые коммутаторы могут ошибочно выдавать состояние «открытый», это означает, что коммутатор прекратит передачу трафика по определенным MAC-адресам и начнет пересылать весь трафик ко всем портам. Другими словами коммутатор будет работать подобно сетевому устройству коллективного доступа (хабу), позволяя сниферу выполнять свои функции.

Вывод

Для выполнения выше перечисленных атак, хакер должен установить систему на локальном коммутаторе. Однако для начала он должен войти в систему через известную уязвимость, а затем инсталлировать необходимое для снифинга программное обеспечение.