**Описание**

**Цель**: Данная лабораторная работа поможет Вам разобраться с локальными атаками типа человек посередине (Man in the middle “MITM”). Вы также закрепите принципы работы протоколов ARP и DHCP и протестируете работу пакета ettercap.

**Основные теоретические сведения**

**1.1 Атака ARP – spoofing**

ARP-spoofing (ARP — poisoning) — разновидность сетевой атаки типа MITM (англ. Man in the middle), применяемая в сетях с использованием протокола ARP. В основном применяется в сетях Ethernet. Атака основана на недостатках протокола ARP.

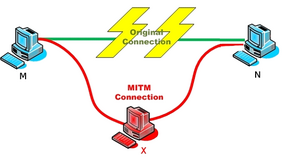
При использовании в распределённой вычислительной сети алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект распределённой вычислительной системы». Анализ безопасности протокола ARP показывает, что, перехватив на атакующем узле внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым узлом (например, маршрутизатором), и в дальнейшем активно контролировать сетевой трафик дезинформированного узла, воздействуя на него.

**1.2 Описание атаки**

Два компьютера (узла) M и N в локальной сети Ethernet обмениваются сообщениями. Злоумышленник X, находящийся в этой же сети, хочет перехватывать сообщения между этими узлами. До применения атаки ARP-spoofing на сетевом интерфейсе узла M ARP-таблица содержит IP- и MAC-адреса узла N. Также на сетевом интерфейсе узла N ARP-таблица содержит IP- и MACадреса узла M.

Во время атаки ARP-spoofing узел X (злоумышленник) отсылает два ARP-ответа (без запроса) — узлу M и узлу N. ARP-ответ узлу M содержит IP-адрес N и MAC-адрес X. ARP-ответ узлу N содержит IP-адрес M и MAC-адрес X.

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



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

**1.3 DHCP-spoofing или подмена**

Несмотря на то, что DHCP является протоколом прикладного уровня модели OSI, основная его работа сосредоточена на канальном уровне. Это означает, что возникновение проблем с его функционированием будет иметь последствия на одном из самых базовых уровней сети.

Первое сообщение DHCP Discover от клиента N является широковещательным, то есть его получат все пользователи сети, в том числе сервер DHCP\_server и злоумышленник X. Они отправят свои ответы DHCP Offer клиенту, из которых он должен выбрать то, что его «устроит». По умолчанию в большинстве систем клиент выбирает первое пришедшее предложение, игнорируя остальные. Таким образом, открывается брешь: если ответ от X придёт раньше, атака окажется успешной. Сервер может быть физически более удалён от клиента, чем злоумышленник, а также быть менее быстрым, поэтому вероятность успешной реализации атаки довольно высока.

Последствия:

• Злоумышленник может в своём ответе клиенту указать неправильные данные о сети, что приведёт к невозможности его дальнейшей работы, то есть будет реализован отказ в обслуживании.

• В большинстве случаев протокол DHCP предоставляет клиенту информацию о шлюзе по умолчанию. Таким образом, злоумышленник имеет возможность указать себя в качестве шлюза, что является реализацией атаки «человек посередине» на сетевом уровне.

Описание атаки

• Злоумышленник настраивает реальный DHCP- сервер в атакуемой сети. В качестве настроек выдает ложные настройки сети

• В сети появляется новый клиент DHCP - N

• Злоумышленник и реальный DHCP посылают свои предложения по настройкам сети

• Клиент N выбирает первое из двух предложений

• В случае успешной атаки клиент не имеет реального доступа к сети

Практическая часть №2. Атаки MITM. Вариант 1.

Изображение выглядит как текст

Автоматически созданное описание

Часть 1. DHCP-spoofing

1. Создаём две виртуальные машины по готовому шаблону, данному в задании:

Изображение выглядит как текст, снимок экрана, экран

Автоматически созданное описание

1. Создаём изолированную сеть “Nat” и задаём значение 192.168.10.0/27:

Изображение выглядит как текст, снимок экрана, монитор, черный

Автоматически созданное описание

1. Подключаем обе виртуальные машины к “Nat” сети:

Изображение выглядит как текст, снимок экрана, монитор, экран

Автоматически созданное описание

1. Определяем IP и MAC адреса виртуальных машин используя команду “ip a”.

Первая машинa – Атакующий (X). IP адрес – 192.168.10.5/27, MAC адрес – 08:00:27:64:47:5e.

Изображение выглядит как текст

Автоматически созданное описание

Вторая машина – Атакуемый (N). IP адрес – 192.168.10.6/27, MAC адрес – 08:00:27:33:6а:с7.

Изображение выглядит как текст

Автоматически созданное описание

1. Устанавливаем дополнительные пакеты. Выполним в терминале следующие команды:

sudo apt-get update

sudo apt-get install wireshark –y

sudo apt-get install ettercap-graphical –y

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

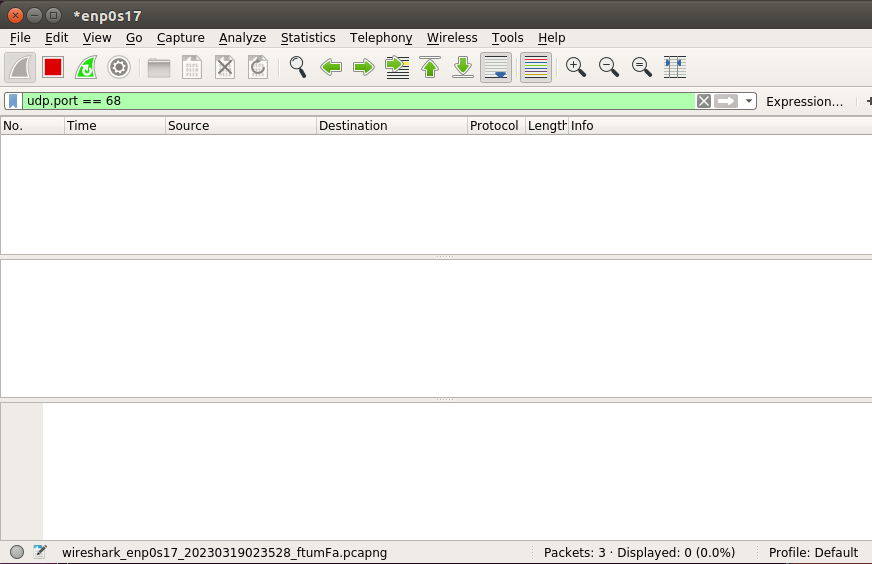
Автоматически созданное описание

1. Запускаем на атакующей машине в новом терминале программу wireshark и запускаем логирование сетевых пакетов на единственном сетевом адаптере:

Изображение выглядит как текст

Автоматически созданное описание

1. Для наглядности работы в wireshark сразу применяем фильтр DHCP пакетов:



1. На атакуемой машине выполняем сброс dhcp настроек на сетевых адаптерах. Для этого выполняем в терминале следующие команды:

“sudo dhclient –r”

“sudo dhclient”

Изображение выглядит как текст

Автоматически созданное описание

1. Фиксируем перехваченные пакеты по протоколу DHCP:

Изображение выглядит как стол

Автоматически созданное описание

Команда “sudo dhclient –r” удаляет текущую аренду IP-адреса для сетевого интерфейса.

Команда “sudo dhclient” запрашивает новую аренду IP-адреса для сетевого интерфейса. Это можно увидеть на 7 (DHCP Discover), 8 (DHCP Offer), 9 (DHCP Request) и 10 кадре (DHCP ACK).

DHCP Discover – широковещательным запрос, отправляемый компьютером для поиска DHCP-сервера в сети, его получают все пользователи сети.

DHCP Offer – это ответ на DHCP Discover, отправленный DHCP-сервером. DHCP-сервер отправляет предложение сетевых параметров, таких как IP-адрес, подсеть и шлюз, которые компьютер может использовать в своей сетевой конфигурации.

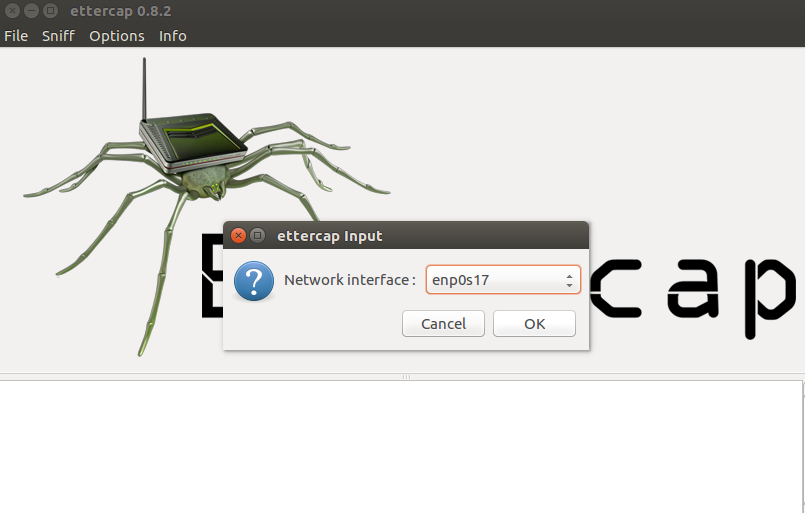
DHCP Request – это запрос от компьютера к DHCP-серверу, в котором он просит у сервера подтверждение предложенных сетевых настроек.

DHCP ACK – это подтверждение от DHCP-сервера о том, что настройки были приняты компьютером. В ответ на запрос на DHCP Request, DHCP-сервер отправляет DHCP ACK с подтверждением настроек сети.

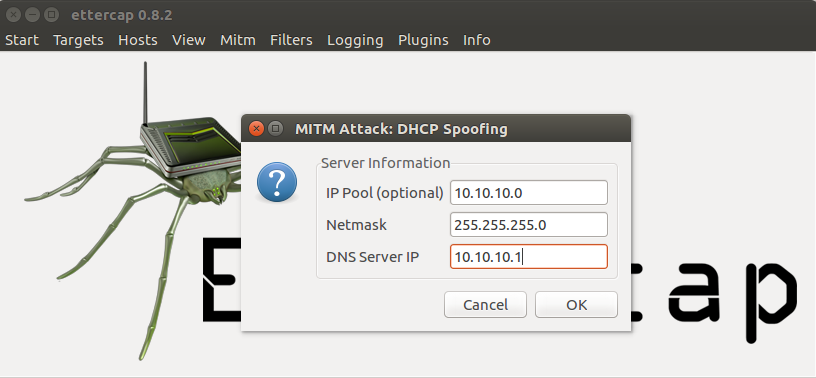
1. Далее на атакующей машине запускаем приложение Ettercap:



1. Затем переводим приложение в режим сниффинга. В меню выбираем “sniff” и потом “Unified sniffing”:



1. Далее в меню “MITM” выбираем пункт “DHCP spoofing” и вводим настройки ложного DHCP сервера:



1. На атакуемой машине вновь делаем сброс DHCP настроек:

Изображение выглядит как текст

Автоматически созданное описание

1. Далее на атакуемой машине проверяем текущие настройки сети и фиксируем это в отчете:

Изображение выглядит как текст

Автоматически созданное описание

1. На атакующей машине в логах Ettercap видим сообщение “fake OFFER”, обозначающее, что злоумышленник сработал:

Изображение выглядит как текст

Автоматически созданное описание

1. В логах wireshark фиксируем измененения:

Изображение выглядит как стол

Автоматически созданное описание

Видим, что кадров стало больше в связи с выполненными раннее действиями. Можно сделать вывод, что все действия были совершены верно, атаку можно считать успешной.

1. Теперь перезагружаем обе виртуальные машины и переходим к выполнению второй части работы.

Часть 2. ARP-spoofing.

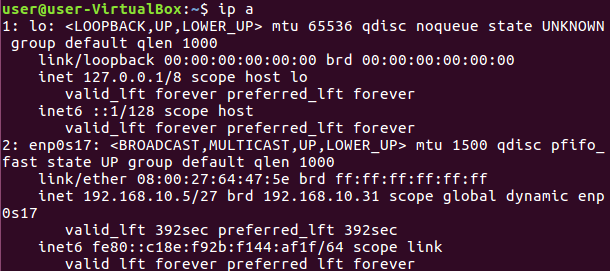
1. Создаём ещё одну копию виртуальной машины:

Изображение выглядит как текст

Автоматически созданное описание

1. Зафиксируем в отчете сетевые настройки данных всех 3 машин.

Первая машинa – Атакующий (X). IP адрес – 192.168.10.5/27, MAC адрес – 08:00:27:64:47:5e.



Вторая машина – Атакуемый (N). IP адрес – 192.168.10.6/27, MAC адрес – 08:00:27:33:6а:с7.

Изображение выглядит как текст

Автоматически созданное описание

Третья машина ещё один Атакуемый (M). IP адрес – 192.168.10.7/27, MAC адрес – 08:00:27:d6:2a:1c.

Изображение выглядит как текст

Автоматически созданное описание

1. Проверяем, что все 3 машины доступны друг для друга. Выполняем перекрестный ping во всех трех машинах:

На первой машине:

Изображение выглядит как календарь

Автоматически созданное описание

На второй машине:

Изображение выглядит как календарь

Автоматически созданное описание

На третьей машине:

Изображение выглядит как календарь

Автоматически созданное описание

1. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда:

“sudo arp –an”

Для первой машины:

Изображение выглядит как текст

Автоматически созданное описание

Для второй машины:

Изображение выглядит как текст

Автоматически созданное описание

Для третьей машины:

Изображение выглядит как текст

Автоматически созданное описание

1. Далее на атакующей машине (на первой) запускаем приложение Ettercap:



1. Запускает на атакующей машине в новом терминале программу wireshark:

Изображение выглядит как текст

Автоматически созданное описание

1. Запускаем логирование сетевых пакетов на единственном сетевом адаптере:

Изображение выглядит как текст

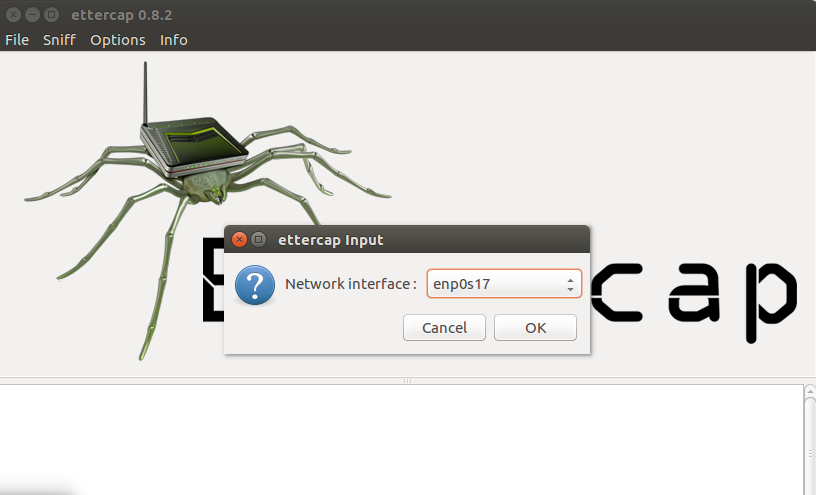
Автоматически созданное описание

1. Для наглядности работы в wireshark сразу применяем фильтр пакетов: “arp or icmp”.

Изображение выглядит как текст

Автоматически созданное описание

1. Переводим приложение Ettercap в режим сниффинга. Выбираем “sniff”, затем “Unified sniffing”



1. Делаем сканирование сети: меню “Hosts” и “Scan for hosts”:

Изображение выглядит как текст, Веб-сайт

Автоматически созданное описание

1. Переходим в меню “Hosts list”. Выбираем в списке ip первой жертвы (192.168.10.6) и через меню правой кнопки мыши добавляем его цель 1 (“Add to target 1”):

Изображение выглядит как текст

Автоматически созданное описание

1. Ip второй жертвы (192.168.10.7) добавляем к цели 2 (“Add to target 2”):

Изображение выглядит как текст

Автоматически созданное описание

1. Далее переходим в меню “MITM”, затем “Arp spoofing” и запускаем процесс атаки:

Изображение выглядит как текст

Автоматически созданное описание

1. Фиксируем в отчете состояние arp таблиц каждой из машин:

Для первой машины:

Изображение выглядит как текст

Автоматически созданное описание

Для второй машины:

Изображение выглядит как текст

Автоматически созданное описание

Для третьей машины:

Изображение выглядит как текст

Автоматически созданное описание

1. Анализируем пакеты, захваченные wireshark:

Изображение выглядит как стол

Автоматически созданное описание

Видим, что атака ARP-spoofing прошла успешно, и теперь все пакеты (трафик) между атакуемыми машинами(M и N) проходят через злоумышленника. К примеру, если M хочет передать пакет компьютеру N, то M смотрит в свою ARP-таблицу, находит запись с IP-адресом узла N, выбирает оттуда MAC-адрес (а там уже MAC-адрес узла X) и передает пакет. Пакет поступает на интерфейс X, анализируется им, после чего перенаправляется узлу N.

1. В приложении Ettercap останавливаем процесс атаки: “MITM” и “Stop mitm attaks”:

Изображение выглядит как текст

Автоматически созданное описание

1. Фиксируем в отчете состояние arp таблиц каждой из машин:

Для первой машины:

Изображение выглядит как текст

Автоматически созданное описание

Для второй машины:

Изображение выглядит как текст

Автоматически созданное описание

Для третьей машины:

Изображение выглядит как текст

Автоматически созданное описание

Проанализировав каждую ARP таблицу, можно идентифицировать каждое устройство, “общающихся” через сеть. ARP таблицы содержат информацию об IP-адресах и соответствующих им MAC-адресах.

На основе полученных раннее результатов, можно заметить, что во время атаки всем IP-адресам атакуемых машин соответствовал один и тот же MAC-адрес, что означает успешную атаку вида ARP-spoofing, но после приостановки процесса атаки, все значения вернулись MAC-адресов вернулись в исходное состояние.

Выводы по выполненной работе:

В результате выполнения данной лабораторной работы был произведён анализ некоторых видов атак типа человек посередине (Man in the middle “MITM”) таких как DHCP-spoofing и ARP-spoofing. Также были освоены принципы работы протоколов ARP и DHCP, а также была протестирована работа пакета ettercap.