Лабораторная работа. Атаки MITM

Оглавление

[Описание 1](#_Toc58865498)

[Основные теоретические сведения 1](#_Toc58865499)

[Атака ARP – spoofing 1](#_Toc58865500)

[DHCP-spoofing или подмена 2](#_Toc58865501)

[Задания к лабораторной работе 3](#_Toc58865502)

[Часть 1. DHCP-spoofing 3](#_Toc58865503)

[Часть 2. ARP-spoofing 5](#_Toc58865504)

[Содержание отчета по лабораторной работе 6](#_Toc58865505)

[Варианты работ 6](#_Toc58865506)

# 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

## 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.

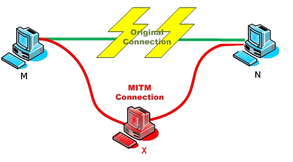
При использовании в распределённой вычислительной сети алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект распределённой вычислительной системы». Анализ безопасности протокола ARP показывает, что, перехватив на атакующем узле внутри данного 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.

**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 MAC-адреса 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.

## 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**

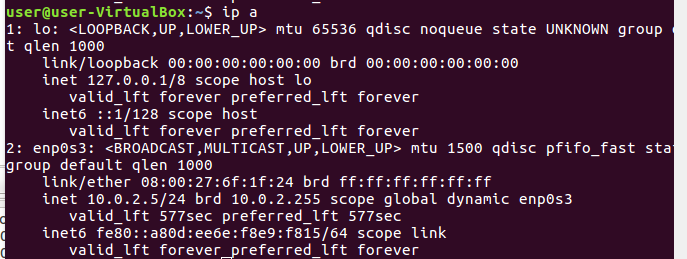
* Злоумышленник настраивает реальный DHCP- сервер в атакуемой сети. В качестве настроек выдает ложные настройки сети
* В сети появляется новый клиент DHCP - N
* Злоумышленник и реальный DHCP посылают свои предложения по настройкам ети
* Клиент N выбирает первое из двух предложений
* В случае успешной атаки клиент не имеет реального доступа к сети.

# Задания к лабораторной работе

## Часть 1. DHCP-spoofing

1. Для выполнения работы вам необходимы 2 виртуальные машины Linux-honeyd
2. Необходимо настроить сетевые адаптеры данных машин для работы в режиме NAT (Встроенный в системы виртуализации DHCP сервер должен быть включен и настроен согласно заданию).
3. Далее можно запустить машины (логин **user**, пароль **1234567).**
4. Для проведения работы выберите одну из машин как Атакующую (X), а вторую машину, как Атакуемую (N).
5. Зафиксируйте в отчете сетевые настройки данных машин (IP и MAC адреса)

Для того чтобы посмотреть сетевые настройки выполните в терминалах машин команду “ip a”



1. Далее на атакующую машину необходимо установить дополнительные пакеты. Выполним в терминале следующие команды:

sudo apt-get update

sudo apt-get install wireshark –y

sudo apt-get install ettercap-graphical –y

1. Запускает на атакующей машине в новом терминале программу wireshark

sudo wireshark

И запускаем логирование сетевых пакетов на единственном сетевом адаптере.

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

udp.port == 68

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

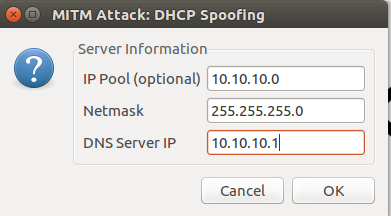
sudo dhclient –r

sudo dhclient

1. Фиксируем в отчете перехваченные пакеты по протоколу DHCP. И комментируем результат согласно стандартной работе протокола DHCP.
2. На атакующей машине запускаем приложение Ettercap



1. Переводим приложение в режим сниффинга. В меню выбираем “sniff” -> “Unified sniffing”
2. Далее в меню “MITM” выбираем пункт “DHCP spoofing” и вводим настройки ложного DHCP сервера.

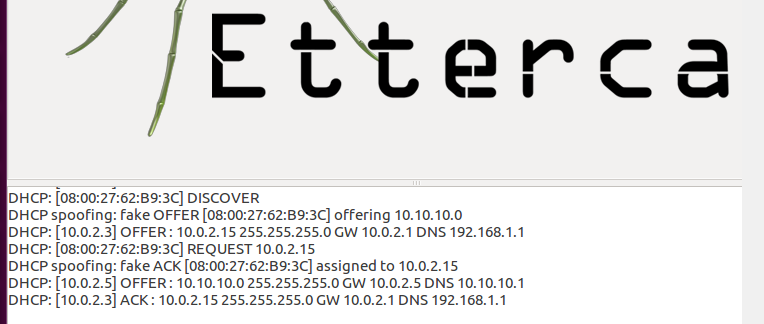


1. На атакуемой машине вновь делаем сброс DHCP настроек:

sudo dhclient –r

sudo dhclient

1. На атакуемой машине проверяем текущие настройки сети (ip a) и фиксируем это в отчете.
2. На атакующей машине в логах Ettercap должно сообщение “fake OFFER”, обозначающее, что злоумышленник отработал.



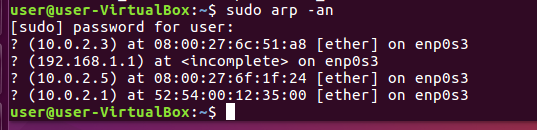
1. В логах wireshark фиксируем изменения и комментируем в отчете результат атаки.

**Атака имеет право быть не до конца успешной, т.к. встроенный DHCP сервер отвечает на запросы очень быстро.**

1. Для завершения работы и перехода к выполнению второй части перезагрузите обе виртуальные машины.

## Часть 2. ARP-spoofing

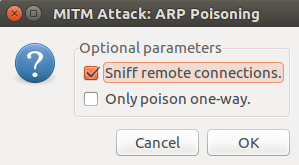
1. Для выполнения данной части вам необходимо сделать еще одну копию атакуемой виртуальной машины.
2. Зафиксируйте в отчете сетевые настройки данных 3 машин (IP и MAC адреса). Для того чтобы посмотреть сетевые настройки выполните в терминалах всех машин команду “ip a”
3. Проверяем, что все 3 машины доступны друг для друга. Выполняем перекрестный ping во всех трех машинах, т.е. по 2 команды ping на каждой из машин.
4. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда: sudo arp –an



1. На атакующей машине запускаем приложение Ettercap
2. Запускает на атакующей машине в новом терминале программу wireshark

sudo wireshark

1. И запускаем логирование сетевых пакетов на единственном сетевом адаптере.
2. Для наглядности работы в wireshark сразу применяем фильтр пакетов: arp or icmp
3. Переводим приложение Ettercap в режим сниффинга. В меню выбираем “sniff” -> “Unified sniffing”
4. Делаем сканирование сети: меню “Hosts” -> “Scan for hosts”
5. Переходим в меню “Hosts list”. Выбираем в списке ip первой жертвы и через меню правой кнопки мыши добавляем его цель 1 (Add to target 1).
6. Ip второй жертвы добавляем к цели 2 (Add to target 2).
7. Далее в меню MITM -> Arp spoofing запускаем процесс атаки



1. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда: sudo arp –an
2. Анализируем пакеты, захваченные wireshark
3. В приложении Ettercap останавливаем процесс атаки: MITM -> Stop mitm attaks
4. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда: sudo arp –an
5. Делаем в отчете выводы по состоянию ARP таблиц в каждый момент времени (Сравниваем ip и mac адреса записей).

# Содержание отчета по лабораторной работе

1. **За копирование отчета другого студента (вами или вашего отчета) автоматом 0 балов без возможности пересдачи**

1. Название (титульная страница) и цель работы.
2. Номер вашего варианта с параметрами подсетей.

4. Поэтапное описание процесса работы со скринами и комментариями

5. Выводы по выполненной работе.

# Варианты работ

1. Сеть NAT 192.168.10.0/27

Gateway 192.168.10.10

DNS 192.168.10.10

DHCP – работает

1. Сеть NAT 10.10.10.0/27

Gateway 10.10.10.10

DNS 10.10.10.10

DHCP – работает

1. Сеть NAT 10.10.10.0/26

Gateway 10.10.10.10

DNS 10.10.10.10

DHCP – работает

1. Сеть NAT 10.11.10.0/25

Gateway 10.11.10.10

DNS 10.11.10.10

DHCP – работает

1. Сеть NAT 10.12.10.0/24

Gateway 10.12.10.10

DNS 10.12.10.10

DHCP – работает

1. Сеть NAT 10.13.10.0/24

Gateway 10.13.10.10

DNS 10.13.10.10

DHCP – работает

1. Сеть NAT 10.13.10.0/24

Gateway 10.13.10.10

DNS 10.13.10.10

DHCP – работает

1. Сеть NAT 10.14.10.0/25

Gateway 10.14.10.10

DNS 10.14.10.10

DHCP – работает

1. Сеть NAT 10.15.10.0/26

Gateway 10.15.10.10

DNS 10.15.10.10

DHCP – работает

1. Сеть NAT 10.16.10.0/27

Gateway 10.16.10.10

DNS 10.16.10.10

DHCP – работает

1. Сеть NAT 10.17.10.0/28

Gateway 10.17.10.10

DNS 10.17.10.10

DHCP – работает

1. Сеть NAT 10.18.10.0/27

Gateway 10.18.10.10

DNS 10.18.10.10

DHCP – работает