

## **Тема и цель работы**

**Тема лабораторной работы:** «Атаки MITM».

**Цель работы:** Изучение атак с человеком посередине.

## Выполнение

### Часть 1. DHCP-spoofing

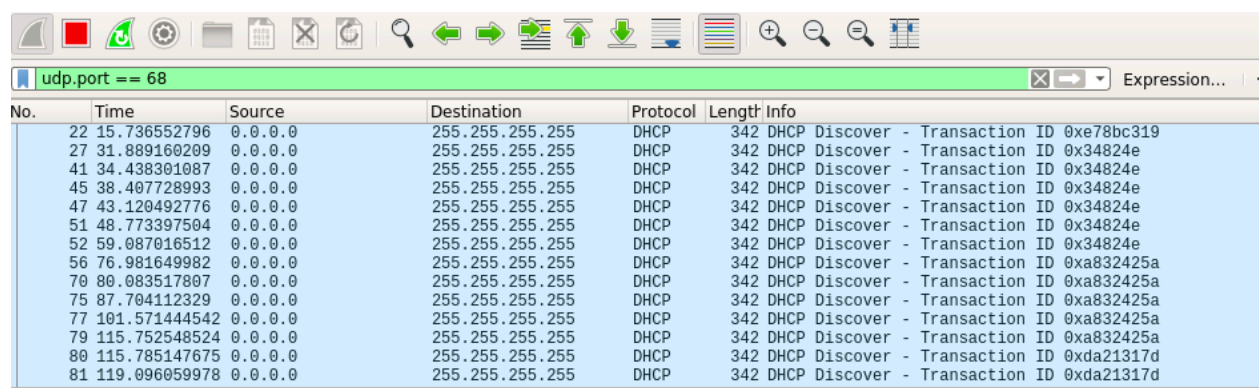
1. Для проведения работы требуется использование двух виртуальных машин на базе Linux-honeyd.
2. Следует настроить сетевые интерфейсы обеих машин для функционирования в режиме NAT.
3. После настройки можно запустить машины (учетная запись: user, пароль: 1234567).
4. Для выполнения атаки определите одну машину как атакующую (Hacker), а другую — как атакуемую (Server).
5. В отчете необходимо зафиксировать сетевые параметры обеих машин (IP и MAC адреса), для чего в терминалах выполните команду `ip a`.
6. На атакующей машине требуется установить дополнительные пакеты, для чего в терминале выполните следующие команды: `sudo apt-get update` `sudo apt-get install` `wireshark -y`

`sudo apt-get install ettercap-graphical -y`

```
root@user-VirtualBox:/home/user# apt-get install ettercap-graphical -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ettercap-common liblua5.1-2 liblua5.1-common libnet1
The following NEW packages will be installed:
  ettercap-common ettercap-graphical liblua5.1-2 liblua5.1-common
  libnet1
0 upgraded, 5 newly installed, 0 to remove and 160 not upgraded.
Need to get 1 246 kB of archives.
After this operation, 3 493 kB of additional disk space will be used.
```

3. Запускаем на атакующей машине в новом терминале программу `wireshark`
4. Для наглядности работы в `wireshark` сразу применяем фильтр DHCP пакетов:

`udp.port == 68`



No.	Time	Source	Destination	Protocol	Length	Info
22	15.736552796	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe78bc319
27	31.889160209	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
41	34.438301087	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
45	38.407728993	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
47	43.120492776	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
51	48.773397504	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
52	59.087016512	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x34824e
56	76.981649982	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa832425a
70	80.083517807	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa832425a
75	87.704112329	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa832425a
77	101.571444542	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa832425a
79	115.752548524	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa832425a
80	115.785147675	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xda21317d
81	119.096059978	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xda21317d

5. На атакуемой машине выполняем сброс `dhcpcd` настроек на сетевых адаптерах. Для этого выполняем в терминале команду:

`sudo dhclient -r` `sudo`

`dhclient`

```
root@user-VirtualBox:/home/user# dhclient -r
root@user-VirtualBox:/home/user# dhclient
```

6. Фиксируем в отчете перехваченные пакеты по протоколу DHCP. И комментируем результат согласно стандартной работе протокола DHCP.

#### Анализ перехваченных DHCP-пакетов:

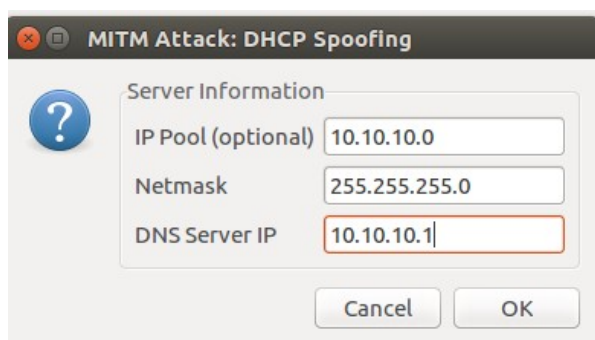
Зафиксирована стандартная последовательность обмена по протоколу DHCP (DORA):

1. **Discover** — клиент отправляет широковещательный запрос в поиске DHCP-серверов.
2. **Offer** — DHCP-сервер предлагает IP-адрес.
3. **Request** — клиент выбирает и запрашивает один из предложенных адресов.
4. **ACK** — сервер подтверждает аренду IP-адреса

На атакующей машине запускаем приложение Ettercap



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



9. На атакуемой машине вновь делаем сброс DHCP настроек:

sudo dhclient -r sudo

dhclient

10. На атакуемой машине проверяем текущие настройки сети (ip a)

```
root@user-VirtualBox:/home/user# ip -br a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s8            UP          10.10.10.0/24
enp0s17           UP          10.0.2.15/24 fd00::4079:43e7:71af:1129/64 fd00::e5f8:9a3:f21d:9f6c/64 fe80::eb48:68d1:8053:ff0d/64
root@user-VirtualBox:/home/user#
```

11.

12. На атакующей машине в логах Ettercap должно быть сообщение “fake OFFER”, обозначающее, что злоумышленник отработал.

```
DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns 10.10.10.1
DHCP: [08:00:27:A2:13:50] DISCOVER
DHCP spoofing: fake OFFER [08:00:27:A2:13:50] offering 10.10.10.0
DHCP: [192.168.1.11] OFFER: 10.10.10.0 255.255.255.0 GW 192.168.1.11 DNS 10.10.10.1
DHCP: [08:00:27:A2:13:50] REQUEST 10.10.10.0
DHCP spoofing: fake ACK [08:00:27:A2:13:50] assigned to 10.10.10.0
DHCP: [192.168.1.11] ACK: 10.10.10.0 255.255.255.0 GW 192.168.1.11 DNS 10.10.10.1
```

13. 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.

17	32.482484996	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
18	38.361221851	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
19	49.405555121	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
24	70.780853545	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
26	89.688679441	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
27	101.391527504	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
28	108.885256687	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
29	123.616241198	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
30	140.522355809	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
31	153.858895257	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3df7fb17
32	169.943295509	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5db7fa34
33	169.943836661	192.168.1.11	255.255.255.255	DHCP	582	DHCP Offer - Transaction ID 0x5db7fa34
34	169.999810722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5db7fa34
35	170.005268030	192.168.1.11	255.255.255.255	DHCP	582	DHCP ACK - Transaction ID 0x5db7fa34

Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

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

**Вывод:** Злоумышленник отработал, но атака не удалась.

## 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”

```

user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
enp0s8            UP            192.168.1.10/24 fe80::a00:27ff:fea2:1350/64

root@user-VirtualBox:/home/user# ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
enp0s8            UP            192.168.1.12/24 fe80::a00:27ff:fe48:30cb/64

user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
enp0s8            UP            192.168.1.11/24 fe80::a00:27ff:febe:2f6e/64

```

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.

```

user@user-VirtualBox:~$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=1.51 ms
^C
--- 192.168.1.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.519/1.519/1.519/0.000 ms
user@user-VirtualBox:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=1.87 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=1.77 ms
^C
--- 192.168.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.772/1.824/1.877/0.067 ms
user@user-VirtualBox:~$

```

```

root@user-VirtualBox:/home/user# ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.991 ms
^C
--- 192.168.1.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.991/0.991/0.991/0.000 ms
root@user-VirtualBox:/home/user# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.951 ms
^C
--- 192.168.1.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.951/0.951/0.951/0.000 ms
root@user-VirtualBox:/home/user#

```

```

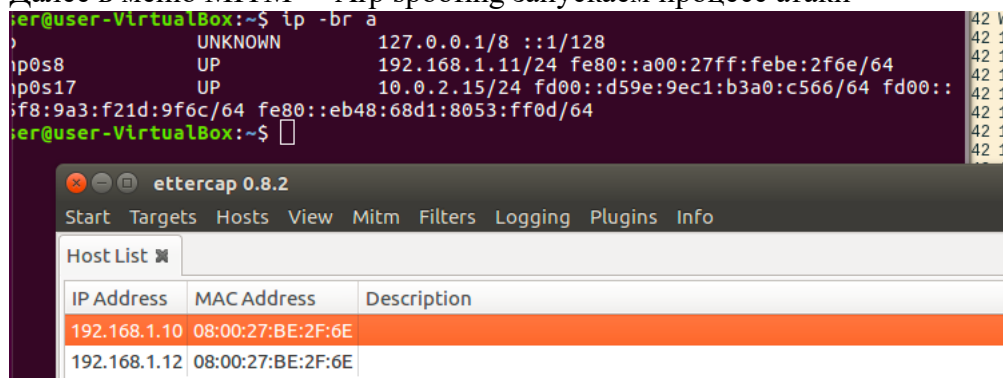
user@user-VirtualBox:~$ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=1.37 ms
^C
--- 192.168.1.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.377/1.377/1.377/0.000 ms
user@user-VirtualBox:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.626 ms
^C
--- 192.168.1.12 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.626/0.626/0.626/0.000 ms
user@user-VirtualBox:~$

```

4. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда:  
sudo arp -an

5. На атакующей машине запускаем приложение Ettercap

6. Запускает на атакующей машине в новом терминале программу wireshark sudo wireshark
7. И запускаем логирование сетевых пакетов на единственном сетевом адаптере.
8. Для наглядности работы в wireshark сразу применяем фильтр пакетов: arp or icmp
9. Переводим приложение Ettercap в режим sniffинга. В меню выбираем “sniff” -> “Unified sniffing”
10. Делаем сканирование сети: меню “Hosts” -> “Scan for hosts”
11. 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).
12. Ip второй жертвы добавляем к цели 2 (Add to target 2).
13. Далее в меню MITM -> Arp spoofing запускаем процесс атаки



14. Фиксируем в отчете состояние arp таблиц каждой из машин. В терминале команда: sudo arp -an



```

root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
? (192.168.1.10) at 08:00:27:a2:13:50 [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
? (192.168.1.10) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
root@user-VirtualBox:/home/user#

```

```

root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (192.168.1.12) at 08:00:27:48:30:cb [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (192.168.1.12) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (192.168.1.12) at 08:00:27:48:30:cb [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
root@user-VirtualBox:/home/user#

```

```

root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
? (192.168.1.10) at 08:00:27:a2:13:50 [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
? (192.168.1.10) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
root@user-VirtualBox:/home/user# arp -an
? (192.168.1.11) at 08:00:27:be:2f:6e [ether] on enp0s8
? (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s17
? (192.168.1.10) at 08:00:27:a2:13:50 [ether] on enp0s8
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on enp0s17
root@user-VirtualBox:/home/user#

```

## 15. Анализируем пакеты, захваченные wireshark

No.	Time	Source	Destination	Protocol	Length	Info
282	101.920437284	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
283	101.920670185	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
284	111.931147019	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
285	111.931372575	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
286	121.941888985	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
287	121.942123266	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
288	131.952616090	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
289	131.952881070	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
290	141.963359460	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
291	141.963534416	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
292	151.973987526	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
293	151.974243774	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e
294	161.986310918	PcsCompu_be:2f:6e	PcsCompu_a2:13:50	ARP	42	192.168.1.12 is at 08:00:27:be:2f:6e
295	161.986893324	PcsCompu_be:2f:6e	PcsCompu_48:30:cb	ARP	42	192.168.1.10 is at 08:00:27:be:2f:6e

## 16. В приложении Ettercap останавливаем процесс атаки: MITM -> Stop mitm attacks

## 17. Фиксируем состояние arp таблиц каждой из машин. В терминале команда: sudo arp -an

## 18. Делаем в отчете выводы по состоянию ARP таблиц в каждый момент времени

(Сравниваем мас адреса записей).

Атака прошла успешно, так как ARP таблицы атакуемых машин изменены





## **Вывод**

Мы научились работать с атаками типа ‘человек посередине’