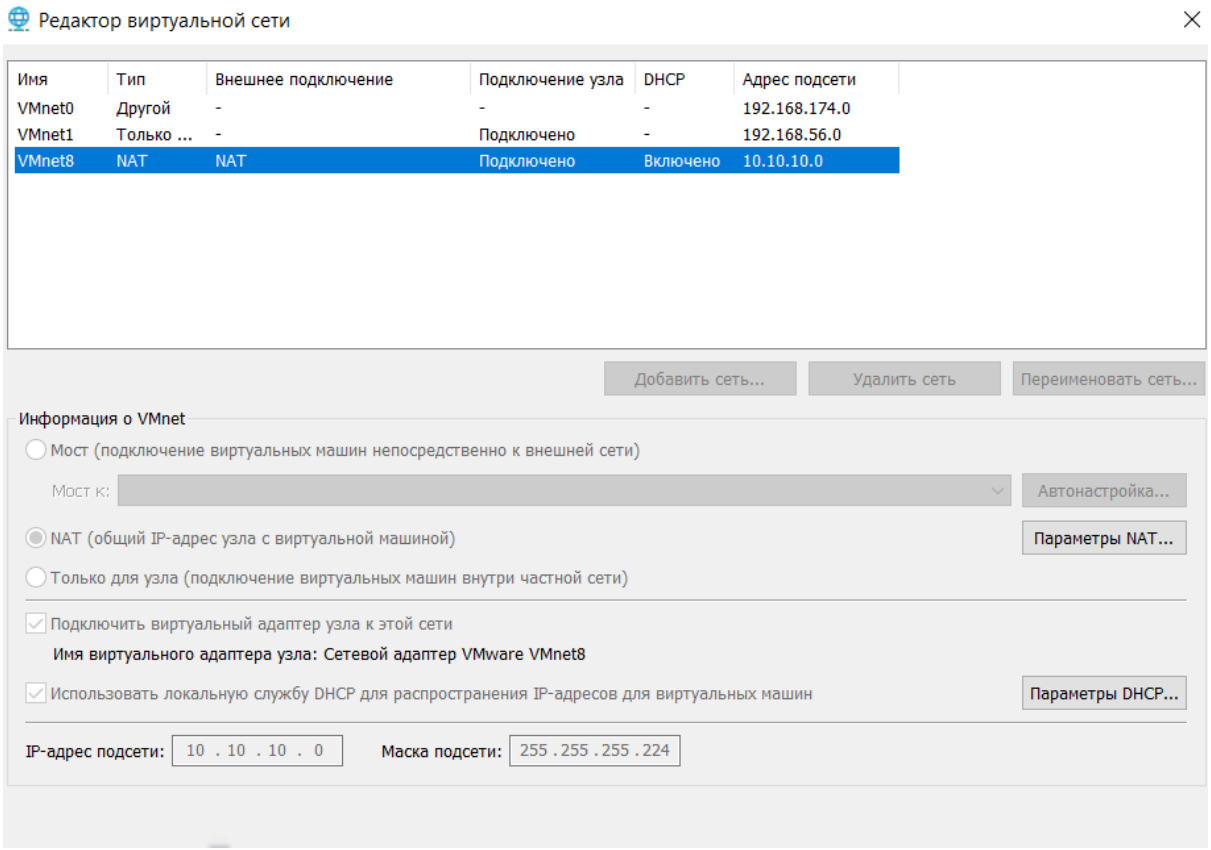
Лабораторная работа. Honeypot, Nmap

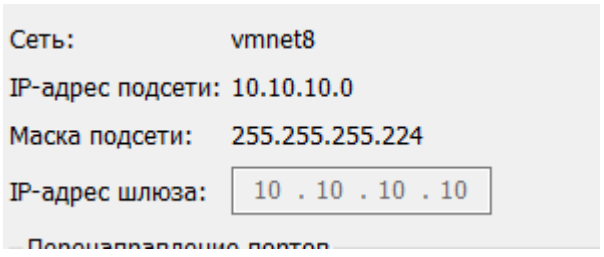
Цель работы: разобраться с локальными атаками типа человек посередине (Man in the middle “MITM”). Закрепить принципы работы протоколов ARP и DHCP и протестировать работу пакета ettercap.

Вариант 2

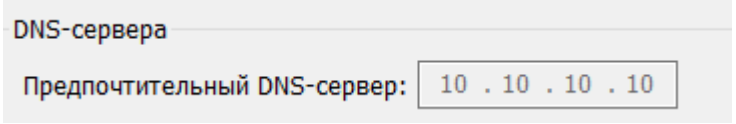
Настройка NAT



Настройка gateway4



Настройка DNS



DHCP включен

Часть 1.

Подсети машин :
атакующая : 10.10.10.19 / 27
атакуемая : 10.10.10.20 / 27

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:4f:8c:67 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.19/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1793sec preferred_lft 1793sec
    inet6 fe80::bf4f:8c40:2a4:8d5c/64 scope link
       valid_lft forever preferred_lft forever
```

атакующая машина

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:6d:da:09 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.20/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1797sec preferred_lft 1797sec
    inet6 fe80::adf6:cc43:f1b:f3c9/64 scope link
       valid_lft forever preferred_lft forever
```

атакуемая машина

Установка обновлений, wireshark и ettercap :

```
user@user-VirtualBox:~$ sudo apt-get update
[sudo] password for user:
Hit:1 http://ru.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metada
ta [93,0 kB]
Get:6 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 DEP-11 Me
tadata [130 kB]
Get:7 http://ru.archive.ubuntu.com/ubuntu xenial-updates/main amd64 DEP-11 Metad
ata [326 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 DEP-11
Metadata [2 468 B]
Get:9 http://ru.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 DEP-11 M
etadata [281 kB]
Get:10 http://ru.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 DEP-1
1 Metadata [5 960 B]
Get:11 http://ru.archive.ubuntu.com/ubuntu xenial-backports/main amd64 DEP-11 Me
tadata [3 328 B]
Get:12 http://ru.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 DEP-1
1 Metadata [6 616 B]
Fetched 1 173 kB in 56s (20,7 kB/s)
Reading package lists... Done
```

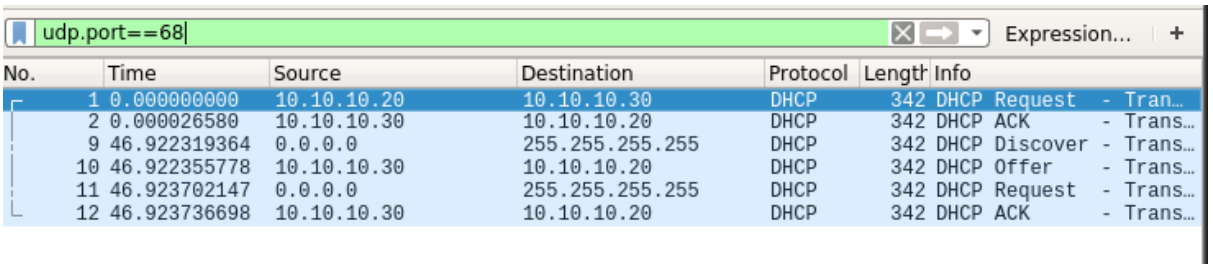
```
user@user-VirtualBox:~$ sudo apt-get install wireshark -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (2.6.10-1~ubuntu16.04.0).
0 upgraded, 0 newly installed, 0 to remove and 30 not upgraded.
```

```
user@user-VirtualBox:~$ sudo 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 libluajit-5.1-2 libluajit-5.1-common libnet1
The following NEW packages will be installed:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common
  libnet1
0 upgraded, 5 newly installed, 0 to remove and 30 not upgraded.
Need to get 1 246 kB of archives.
After this operation, 3 493 kB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu xenial/main amd64 libnet1 amd64 1.1.6+
dfsg-3 [42,1 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libluaji
t-5.1-common all 2.0.4+dfsg-1+deb9u1build0.16.04.1 [35,4 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libluaji
t-5.1-2 amd64 2.0.4+dfsg-1+deb9u1build0.16.04.1 [205 kB]
```

На атакуемой машине выполняю сброс dhcp настроек на сетевых адаптерах :

```
user@user-VirtualBox:~$ sudo dhclient -r
[sudo] password for user:
user@user-VirtualBox:~$ sudo dhclient
RTNETLINK answers: File exists
user@user-VirtualBox:~$
```

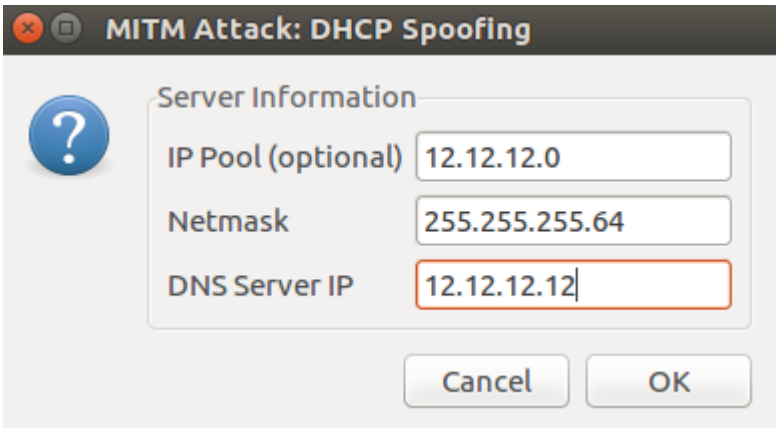
Применяю фильтр DHCP пакетов :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.10.20	10.10.10.30	DHCP	342	DHCP Request - Tran…
2	0.000026580	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Trans…
9	46.922319364	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Trans…
10	46.922355778	10.10.10.30	10.10.10.20	DHCP	342	DHCP Offer - Trans…
11	46.923702147	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Trans…
12	46.923736698	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Trans…

Запускаю ettercap :

Ввожу настройки ложного DHCP сервера :

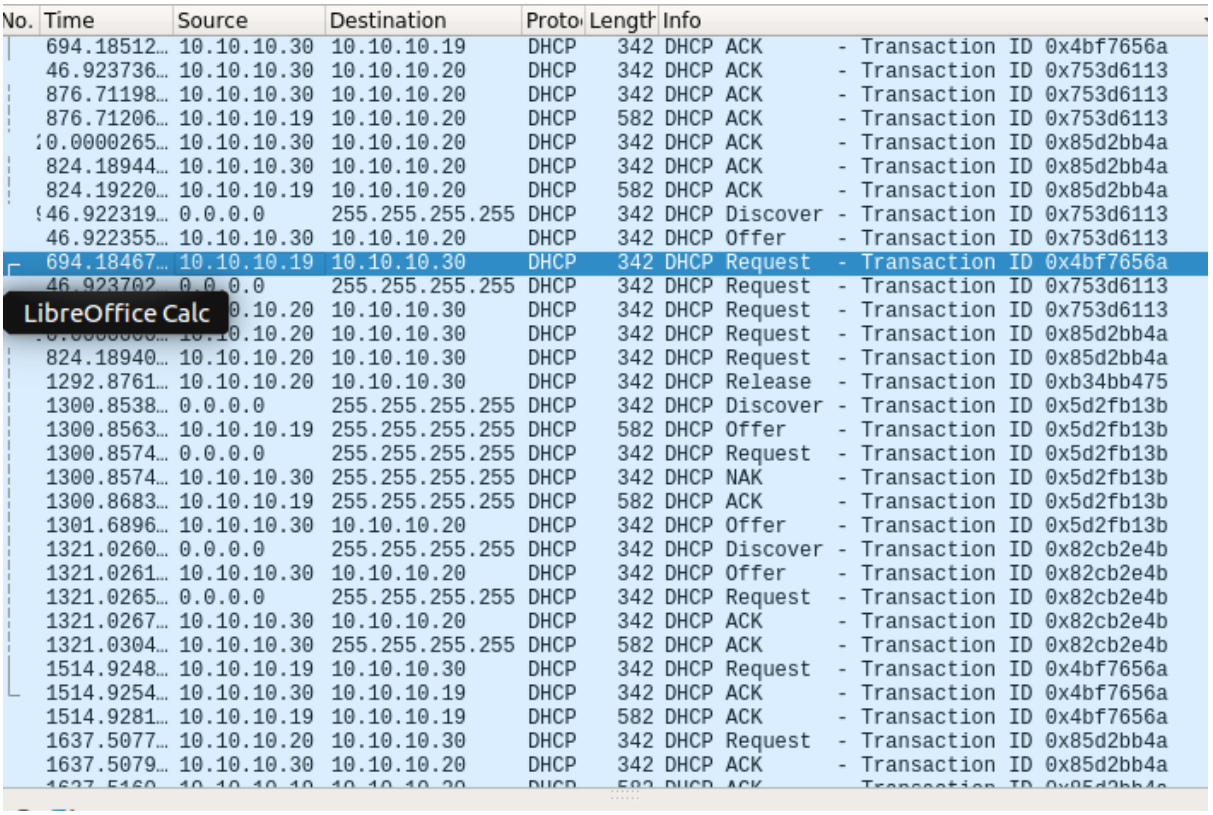


На атакуемой машине вновь делаю сброс DHCP настроек :

```
user@user-VirtualBox:~$ sudo dhclient -r
[sudo] password for user:
Killed old client process
user@user-VirtualBox:~$ sudo dhclient
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:6d:da:09 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.20/27 brd 10.10.10.31 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::adf6:cc43:f1b:f3c9/64 scope link
       valid_lft forever preferred_lft forever
```

На атакующей машине в логах Ettercap появилось сообщение “fake OFFER”, обозначающее, что злоумышленник отработал :

```
DHCP: [00:0C:29:4F:8C:67] REQUEST 10.10.10.19
DHCP: [10.10.10.30] ACK : 10.10.10.19 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
DHCP spoofing: using specified ip_pool, netmask 255.255.255.64, dns 12.12.12.12
DHCP: [00:0C:29:6D:DA:09] REQUEST 10.10.10.20
DHCP spoofing: fake ACK [00:0C:29:6D:DA:09] assigned to 10.10.10.20
DHCP: [10.10.10.30] ACK : 10.10.10.20 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
DHCP: [10.10.10.19] ACK : 10.10.10.20 255.255.255.64 GW 10.10.10.19 DNS 12.12.12.12
DHCP: [00:0C:29:6D:DA:09] REQUEST 10.10.10.20
DHCP spoofing: fake ACK [00:0C:29:6D:DA:09] assigned to 10.10.10.20
DHCP: [10.10.10.30] ACK : 10.10.10.20 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
DHCP: [10.10.10.19] ACK : 10.10.10.20 255.255.255.64 GW 10.10.10.19 DNS 12.12.12.12
DHCP: [00:0C:29:6D:DA:09] DISCOVER
DHCP spoofing: fake OFFER [00:0C:29:6D:DA:09] offering 12.12.12.0
DHCP: [10.10.10.19] OFFER : 12.12.12.0 255.255.255.64 GW 10.10.10.19 DNS 12.12.12.12
DHCP: [00:0C:29:6D:DA:09] REQUEST 12.12.12.0
DHCP spoofing: fake ACK [00:0C:29:6D:DA:09] assigned to 12.12.12.0
DHCP: [10.10.10.19] ACK : 12.12.12.0 255.255.255.64 GW 10.10.10.19 DNS 12.12.12.12
DHCP: [10.10.10.30] OFFER : 10.10.10.20 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
DHCP: [00:0C:29:6D:DA:09] DISCOVER
DHCP: [10.10.10.30] OFFER : 10.10.10.20 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
DHCP: [00:0C:29:6D:DA:09] REQUEST 10.10.10.20
DHCP spoofing: fake ACK [00:0C:29:6D:DA:09] assigned to 10.10.10.20
DHCP: [10.10.10.30] ACK : 10.10.10.20 255.255.255.224 GW 10.10.10.10 DNS 10.10.10.10 "localdomain"
```



No.	Time	Source	Destination	Proto	Length	Info
	694.18512…	10.10.10.30	10.10.10.19	DHCP	342	DHCP ACK - Transaction ID 0x4bf7656a
	46.923736…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x753d6113
	876.71198…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x753d6113
	876.71206…	10.10.10.19	10.10.10.20	DHCP	582	DHCP ACK - Transaction ID 0x753d6113
	0.0000265…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x85d2bb4a
	824.18944…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x85d2bb4a
	824.19220…	10.10.10.19	10.10.10.20	DHCP	582	DHCP ACK - Transaction ID 0x85d2bb4a
	46.922319…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x753d6113
	46.922355…	10.10.10.30	10.10.10.20	DHCP	342	DHCP Offer - Transaction ID 0x753d6113
	694.18467…	10.10.10.19	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x4bf7656a
	46.923702…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x753d6113
		10.10.20	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x753d6113
		10.10.20	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x85d2bb4a
	824.18940…	10.10.10.20	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x85d2bb4a
	1292.8761…	10.10.10.20	10.10.10.30	DHCP	342	DHCP Release - Transaction ID 0xb34bb475
	1300.8538…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5d2fb13b
	1300.8563…	10.10.10.19	255.255.255.255	DHCP	582	DHCP Offer - Transaction ID 0x5d2fb13b
	1300.8574…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5d2fb13b
	1300.8574…	10.10.10.30	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x5d2fb13b
	1300.8683…	10.10.10.19	255.255.255.255	DHCP	582	DHCP ACK - Transaction ID 0x5d2fb13b
	1301.6896…	10.10.10.30	10.10.10.20	DHCP	342	DHCP Offer - Transaction ID 0x5d2fb13b
	1321.0260…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x82cb2e4b
	1321.0261…	10.10.10.30	10.10.10.20	DHCP	342	DHCP Offer - Transaction ID 0x82cb2e4b
	1321.0265…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x82cb2e4b
	1321.0267…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x82cb2e4b
	1321.0304…	10.10.10.30	255.255.255.255	DHCP	582	DHCP ACK - Transaction ID 0x82cb2e4b
	1514.9248…	10.10.10.19	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x4bf7656a
	1514.9254…	10.10.10.30	10.10.10.19	DHCP	342	DHCP ACK - Transaction ID 0x4bf7656a
	1514.9281…	10.10.10.19	10.10.10.19	DHCP	582	DHCP ACK - Transaction ID 0x4bf7656a
	1637.5077…	10.10.10.20	10.10.10.30	DHCP	342	DHCP Request - Transaction ID 0x85d2bb4a
	1637.5079…	10.10.10.30	10.10.10.20	DHCP	342	DHCP ACK - Transaction ID 0x85d2bb4a

LibreOffice Calc

Discover, Offer, Request, ACK используются для назначения ip-адреса

Часть 2

Перезагрузил виртуальные машины
Подсети машин :
1 машина : 10.10.10.19/27
2 машина : 10.10.10.21/27
3 машина : 10.10.10.22/27

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:4f:8c:67 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.19/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1488sec preferred_lft 1488sec
    inet6 fe80::bf4f:8c40:2a4:8d5c/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$
```

Атакующая машина 1

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:02:ec:16 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.21/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1770sec preferred_lft 1770sec
    inet6 fe80::21f2:b6cc:a23c:3253/64 scope link
       valid_lft forever preferred_lft forever
```

Атакуемая машина 2

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:64:0e:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.22/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1779sec preferred_lft 1779sec
    inet6 fe80::c652:aad2:3c3a:1d27/64 scope link
       valid_lft forever preferred_lft forever
```

Атакуемая машина 3

Ping от 1 машины , состояние arp таблицы :

```
user@user-VirtualBox:~$ ping 10.10.10.22
PING 10.10.10.22 (10.10.10.22) 56(84) bytes of data.
64 bytes from 10.10.10.22: icmp_seq=1 ttl=64 time=1.35 ms
64 bytes from 10.10.10.22: icmp_seq=2 ttl=64 time=0.696 ms
64 bytes from 10.10.10.22: icmp_seq=3 ttl=64 time=0.709 ms
64 bytes from 10.10.10.22: icmp_seq=4 ttl=64 time=0.723 ms
64 bytes from 10.10.10.22: icmp_seq=5 ttl=64 time=0.647 ms
64 bytes from 10.10.10.22: icmp_seq=6 ttl=64 time=0.738 ms
```

```
user@user-VirtualBox:~$ ping 10.10.10.21
PING 10.10.10.21 (10.10.10.21) 56(84) bytes of data.
64 bytes from 10.10.10.21: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 10.10.10.21: icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from 10.10.10.21: icmp_seq=3 ttl=64 time=0.654 ms
64 bytes from 10.10.10.21: icmp_seq=4 ttl=64 time=0.657 ms
```

```
user@user-VirtualBox:~$ sudo arp -an
[sudo] password for user:
? (10.10.10.22) at 00:0c:29:64:0e:d0 [ether] on ens33
? (10.10.10.21) at 00:0c:29:02:ec:16 [ether] on ens33
? (10.10.10.10) at 00:50:56:ff:da:b3 [ether] on ens33
```

Ping от 2 машины , состояние arp таблицы :

```
user@user-VirtualBox:~$ ping 10.10.10.19
PING 10.10.10.19 (10.10.10.19) 56(84) bytes of data.
64 bytes from 10.10.10.19: icmp_seq=1 ttl=64 time=0.759 ms
64 bytes from 10.10.10.19: icmp_seq=2 ttl=64 time=0.657 ms
64 bytes from 10.10.10.19: icmp_seq=3 ttl=64 time=0.812 ms
```

```
user@user-VirtualBox:~$ ping 10.10.10.22
PING 10.10.10.22 (10.10.10.22) 56(84) bytes of data.
64 bytes from 10.10.10.22: icmp_seq=1 ttl=64 time=1.16 ms
64 bytes from 10.10.10.22: icmp_seq=2 ttl=64 time=0.701 ms
64 bytes from 10.10.10.22: icmp_seq=3 ttl=64 time=0.718 ms
64 bytes from 10.10.10.22: icmp_seq=4 ttl=64 time=0.679 ms
```

```
user@user-VirtualBox:~$ sudo arp -an
[sudo] password for user:
? (10.10.10.30) at 00:50:56:fa:9b:ce [ether] on ens33
? (10.10.10.22) at 00:0c:29:64:0e:d0 [ether] on ens33
? (10.10.10.19) at 00:0c:29:4f:8c:67 [ether] on ens33
? (10.10.10.10) at 00:50:56:ff:da:b3 [ether] on ens33
```

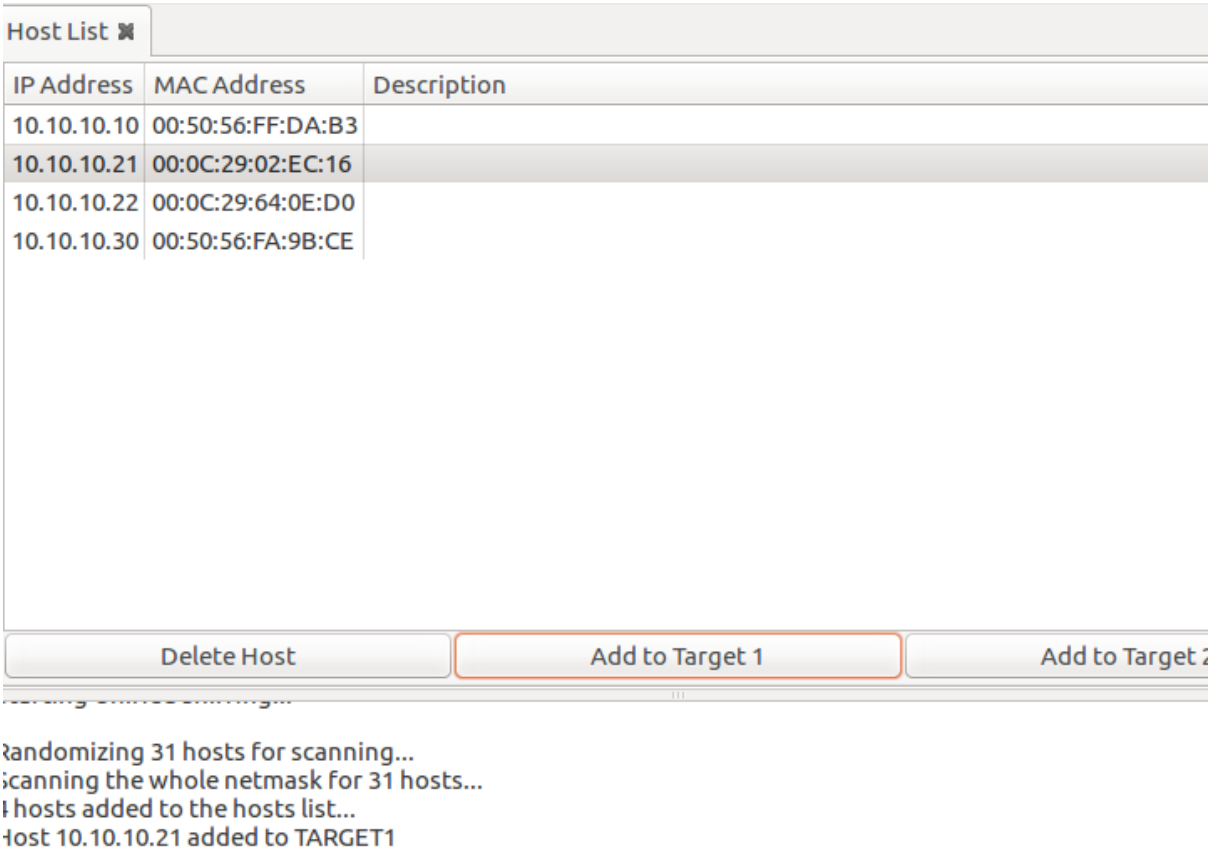
Ping от 3 машины , состояние arp таблицы :

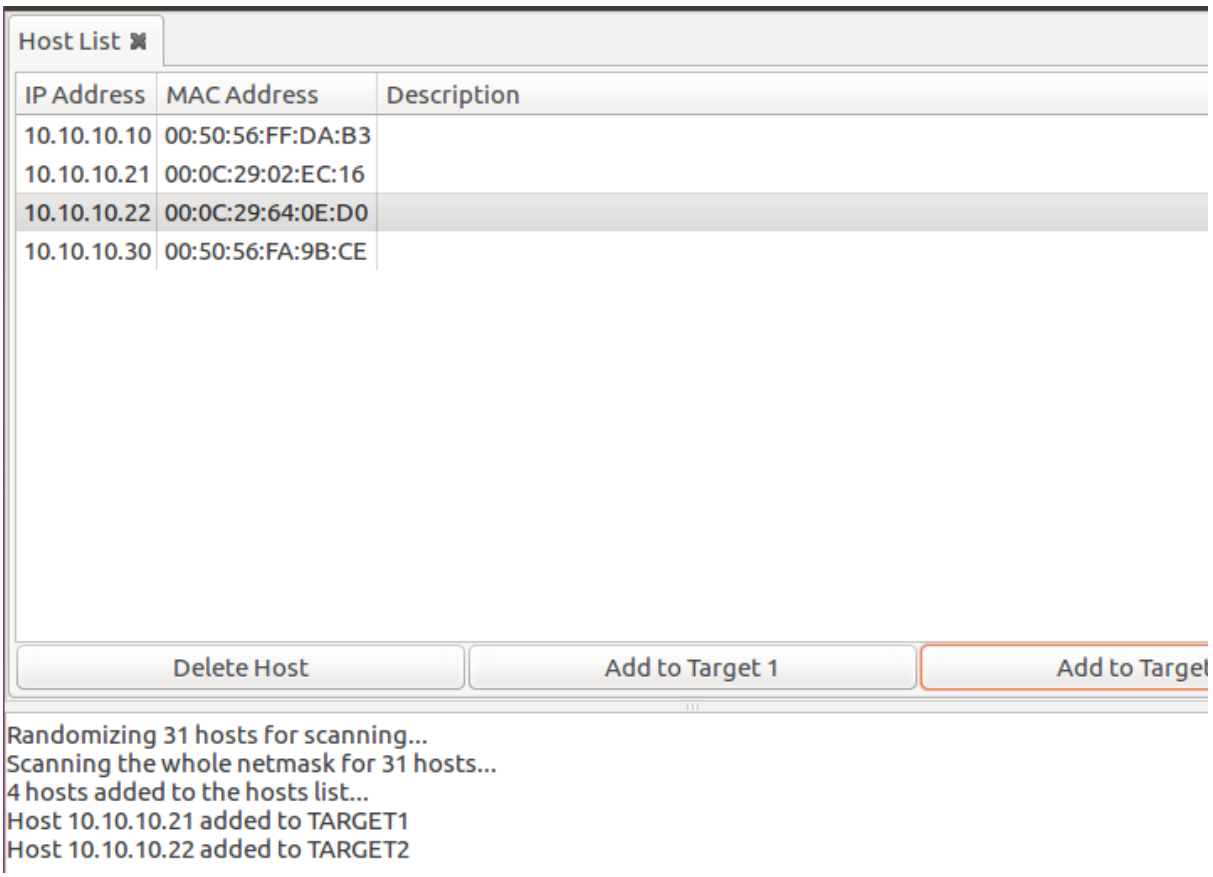
```
user@user-VirtualBox:~$ ping 10.10.10.19
PING 10.10.10.19 (10.10.10.19) 56(84) bytes of data.
64 bytes from 10.10.10.19: icmp_seq=1 ttl=64 time=0.554 ms
64 bytes from 10.10.10.19: icmp_seq=2 ttl=64 time=0.679 ms
64 bytes from 10.10.10.19: icmp_seq=3 ttl=64 time=0.649 ms
64 bytes from 10.10.10.19: icmp_seq=4 ttl=64 time=0.722 ms
```

```
user@user-VirtualBox:~$ ping 10.10.10.21
PING 10.10.10.21 (10.10.10.21) 56(84) bytes of data.
64 bytes from 10.10.10.21: icmp_seq=1 ttl=64 time=0.601 ms
64 bytes from 10.10.10.21: icmp_seq=2 ttl=64 time=0.623 ms
64 bytes from 10.10.10.21: icmp_seq=3 ttl=64 time=0.603 ms
64 bytes from 10.10.10.21: icmp_seq=4 ttl=64 time=0.717 ms
```

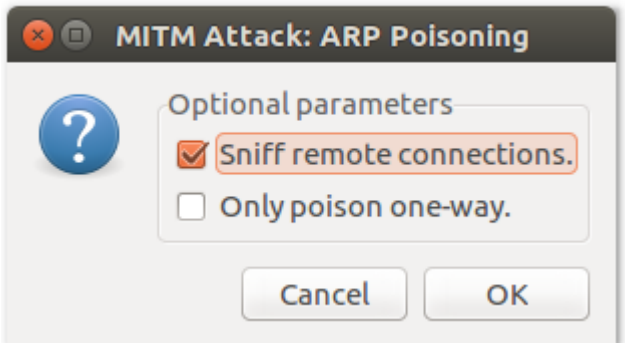
```
user@user-VirtualBox:~$ sudo arp -an
[sudo] password for user:
? (10.10.10.30) at 00:50:56:fa:9b:ce [ether] on ens33
? (10.10.10.10) at 00:50:56:ff:da:b3 [ether] on ens33
? (10.10.10.21) at 00:0c:29:02:ec:16 [ether] on ens33
? (10.10.10.19) at 00:0c:29:4f:8c:67 [ether] on ens33
```

Перевожу Ettercap в режим сниффинга. Делаю сканирование сети. Выбираю ip первой и второй жертвы 2 и 3 машины соответственно и добавляю цель 1 и 2 .

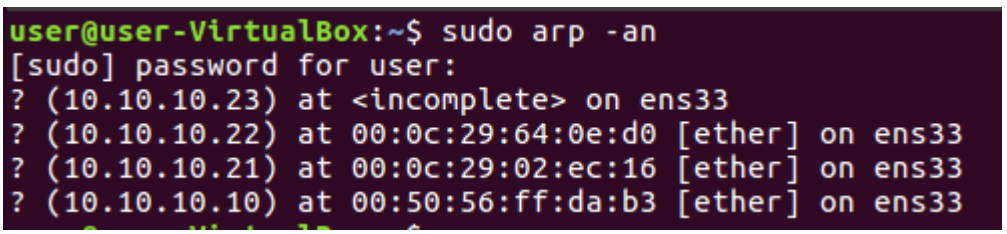




Запускаю процесс атаки на 2 и 3 машины :



Состояние arp таблицы 1 машины :



Появилась подсеть 10.10.10.23 к которому нет доступа и о нём неизвестен mac-адрес

Состояние arp таблицы 2 машины :

```
user@user-VirtualBox:~$ sudo arp -an
[sudo] password for user:
? (10.10.10.10) at 00:50:56:ff:da:b3 [ether] on ens33
```

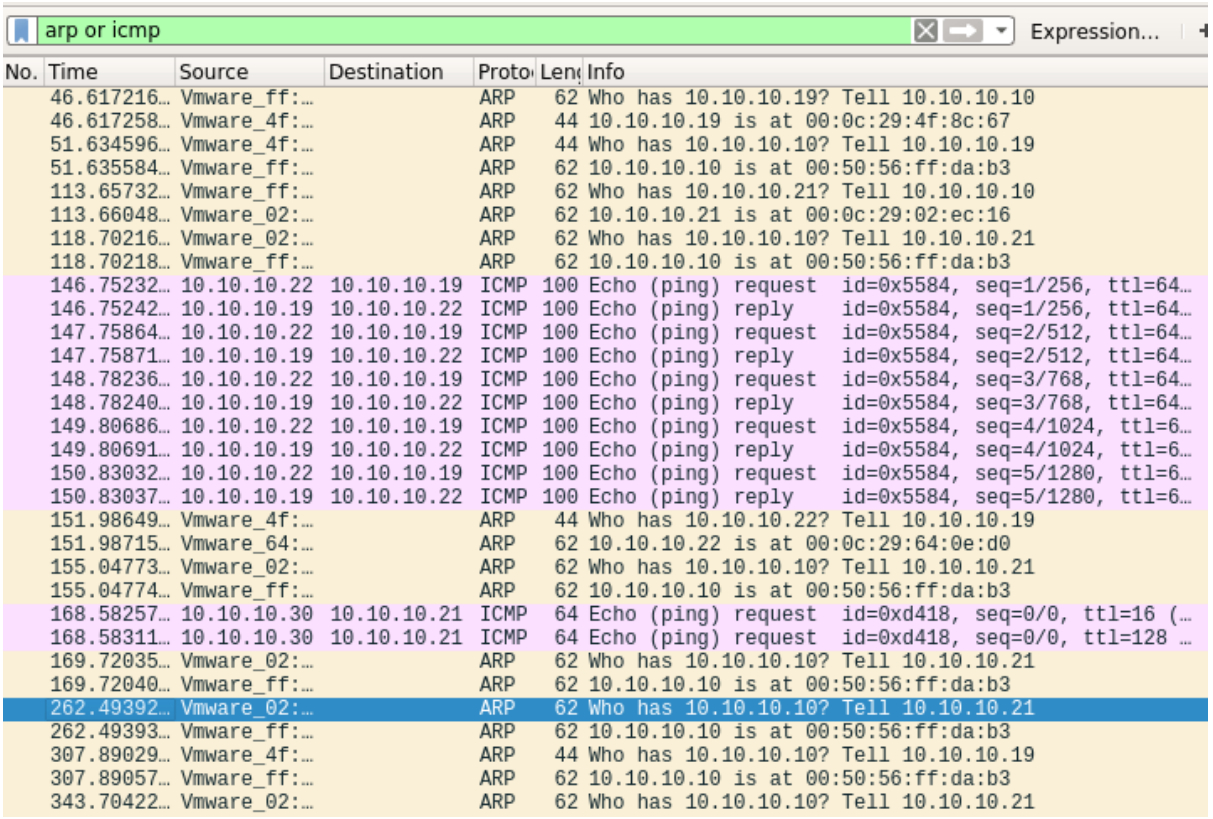
mac-адрес 10.10.10.10 не изменился, все остальные пропали

Состояние arp таблицы 3 машины :

```
user@user-VirtualBox:~$ sudo arp -an
? (10.10.10.30) at 00:50:56:fa:9b:ce [ether] on ens33
? (10.10.10.10) at 00:50:56:ff:da:b3 [ether] on ens33
? (10.10.10.19) at 00:0c:29:4f:8c:67 [ether] on ens33
```

mac-адресы не изменились
пропала подсеть 10.10.10.21

Производился захват arp or icmp пакетов в wireshark :



Протокол icmp говорит, что утилита ping посылала эхозапросы между 3 машинами и получала на них ответы
По протоколу arp видно, что 3 машины передавали пакеты и спрашивали, у кого есть какой адрес, и получали на запросы ответ Mac-адресом
Атакующая машина тем самым с помощью запросов получала ответ от атакуемых машин (mac-адреса)

Вывод : научился работать с протоколами dhcp и arp, узнал, как злоумышленник может подменивать mac-адреса атакуемых машин, выдавая себя за них.