ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ
КОМПЬЮТЕРНЫЕ СЕТИ

ЛАБОРАТОРНАЯ РАБОТА № 8~~6~~

Атаки MITM~~Honeypot, Nmap~~

Выполнил:
Мосолков Е.Н.
Преподаватель:
~~Евсютин ~~Минченков В~~О~~.О.

Москва 2020 г.

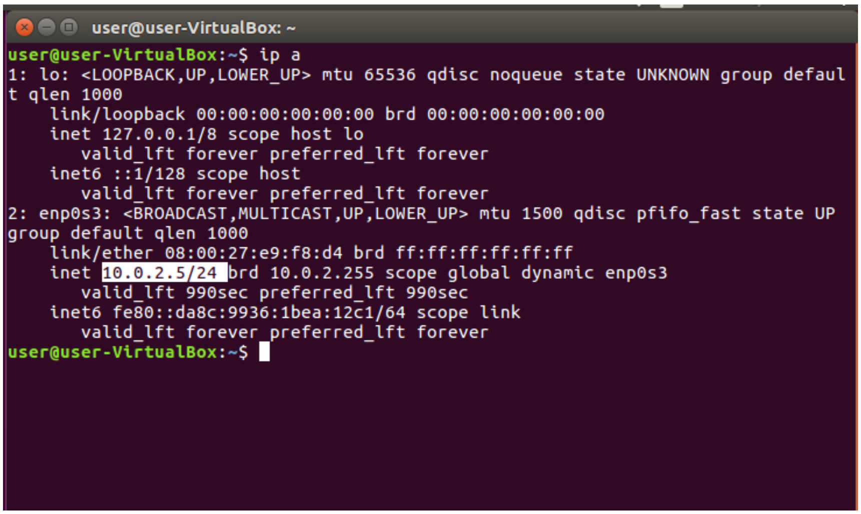
ЦЕЛЬ РАБОТЫ

Цель работы состоит в изучении работы локальных атак типа человек по середине (Man in the middle)
, а также в закреплении
принципа работы ARP и DHCP и тестирование работы пакеты ettercap.

ХОД РАБОТЫ

Часть 1

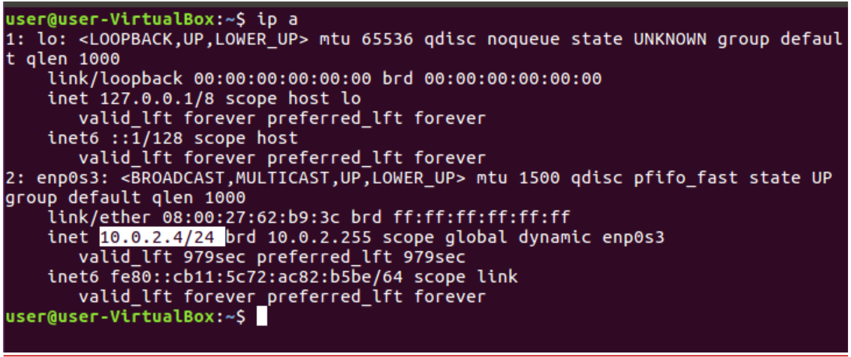
Определяем IP машин



user@user-VirtualBox: ~

```
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:e9:f8:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 990sec preferred_lft 990sec
    inet6 fe80::da8c:9936:1bea:12c1/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$
```

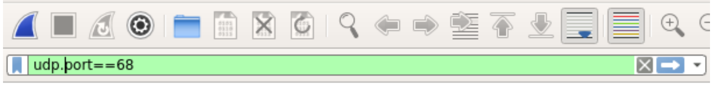
Атакуемая машина



```
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:62:b9:3c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 979sec preferred_lft 979sec
    inet6 fe80::cb11:5c72:ac82:b5be/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$
```

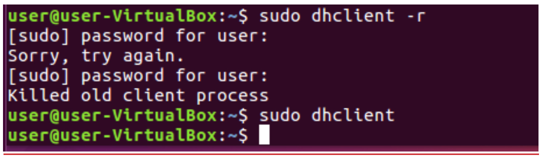
Атакующая машина

Применям фильтр DHCP пакетов на атакующей машине

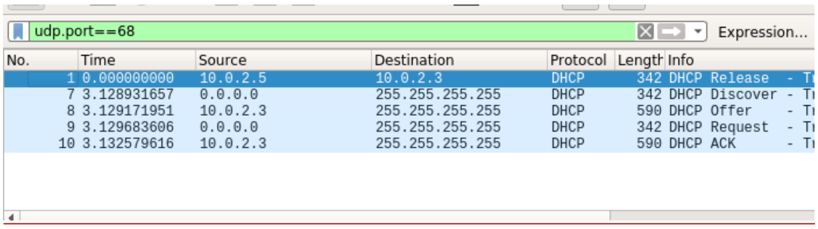


```
udp.port==68
```

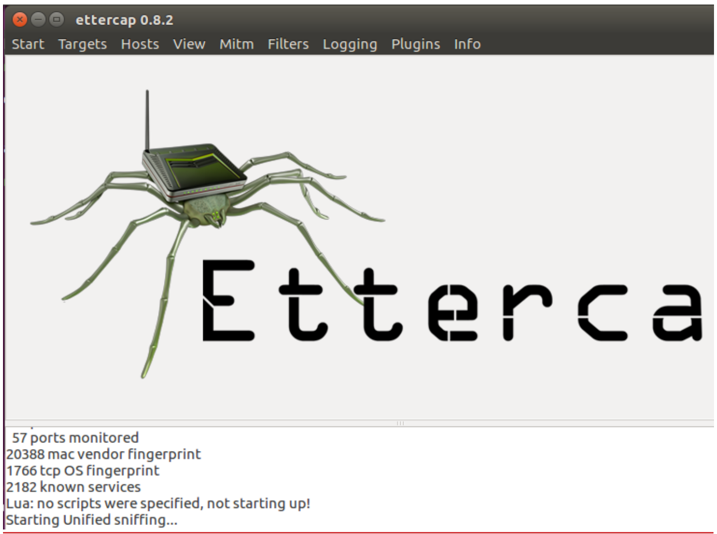
Сбросили dhcp настроек на сетевых адаптерах на атакуемой машине



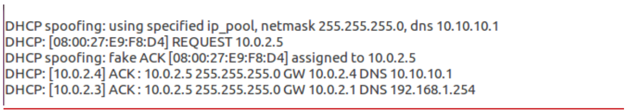
```
user@user-VirtualBox:~$ sudo dhclient -r
[sudo] password for user:
Sorry, try again.
[sudo] password for user:
Killed old client process
user@user-VirtualBox:~$ sudo dhclient
user@user-VirtualBox:~$ 
```



```
No.     Time          Source       Destination        Protocol  Length Info
      1 0.000000000   10.0.2.5     10.0.2.3           DHCP        342 DHCP Release  - T
      7 3.128931657   0.0.0.0      255.255.255.255    DHCP        342 DHCP Discover - T
      8 3.129171951   10.0.2.3     255.255.255.255    DHCP        590 DHCP Offer    - T
      9 3.129683606   0.0.0.0      255.255.255.255    DHCP        342 DHCP Request  - T
     10 3.132579616   10.0.2.3     255.255.255.255    DHCP        590 DHCP ACK      - T
```

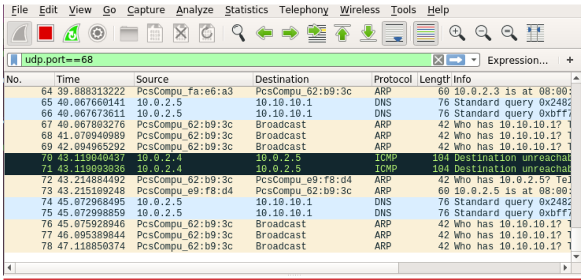


```
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

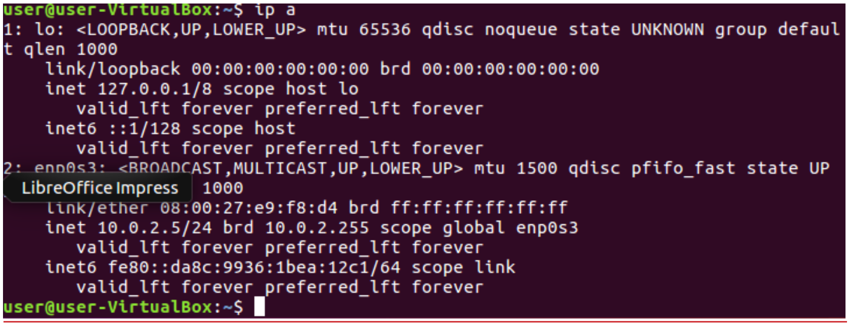


```
DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns 10.10.10.1
DHCP: [08:00:27:E9:F8:D4] REQUEST 10.0.2.5
DHCP spoofing: fake ACK [08:00:27:E9:F8:D4] assigned to 10.0.2.5
DHCP: [10.0.2.4] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.4 DNS 10.10.10.1
DHCP: [10.0.2.3] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
```

Запустили ettercap и начали unfilled sniffing и настроили ложный DHCP сервер

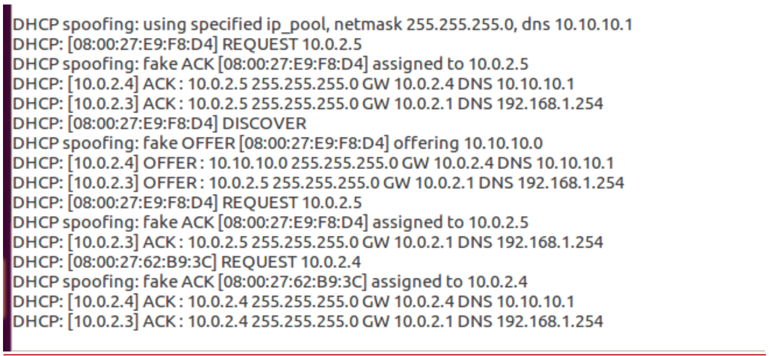

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
udp.port==68

No.   Time          Source              Destination         Protocol Length Info
   64 39.888313222  PcsCompu_fa:e6:a3   PcsCompu_62:b9:3c   ARP        60 10.0.2.3 is at 08:00:
   65 40.067660141  10.0.2.5            10.10.10.1          DNS        76 Standard query 0x2482
   66 40.067673611  10.0.2.5            10.10.10.1          DNS        76 Standard query 0xbff7
   67 40.067803276  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
   68 41.070940989  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
   69 42.094965292  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
   70 43.119040437  10.0.2.4            10.0.2.5            ICMP      104 Destination unreachab
   71 43.119093036  10.0.2.4            10.0.2.5            ICMP      104 Destination unreachab
   72 43.214884492  PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 Who has 10.0.2.5? Tel
   73 43.215109248  PcsCompu_e9:f8:d4   PcsCompu_62:b9:3c   ARP        60 10.0.2.5 is at 08:00:
   74 45.072968495  10.0.2.5            10.10.10.1          DNS        76 Standard query 0x2482
   75 45.072998859  10.0.2.5            10.10.10.1          DNS        76 Standard query 0xbff7
   76 45.075928946  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
   77 46.095389844  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
   78 47.118850374  PcsCompu_62:b9:3c   Broadcast           ARP        42 Who has 10.10.10.1? T
```



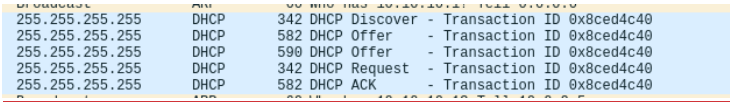
```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
                   1000
    link/ether 08:00:27:e9:f8:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::da8c:9936:1bea:12c1/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$
```

Проверили IP атакуемой машиины, ее IP изменился



```
DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns 10.10.10.1
DHCP: [08:00:27:E9:F8:D4] REQUEST 10.0.2.5
DHCP spoofing: fake ACK [08:00:27:E9:F8:D4] assigned to 10.0.2.5
DHCP: [10.0.2.4] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.4 DNS 10.10.10.1
DHCP: [10.0.2.3] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
DHCP: [08:00:27:E9:F8:D4] DISCOVER
DHCP spoofing: fake OFFER [08:00:27:E9:F8:D4] offering 10.10.10.0
DHCP: [10.0.2.4] OFFER : 10.10.10.0 255.255.255.0 GW 10.0.2.4 DNS 10.10.10.1
DHCP: [10.0.2.3] OFFER : 10.0.2.5 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
DHCP: [08:00:27:E9:F8:D4] REQUEST 10.0.2.5
DHCP spoofing: fake ACK [08:00:27:E9:F8:D4] assigned to 10.0.2.5
DHCP: [10.0.2.3] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
DHCP: [08:00:27:62:B9:3C] REQUEST 10.0.2.4
DHCP spoofing: fake ACK [08:00:27:62:B9:3C] assigned to 10.0.2.4
DHCP: [10.0.2.4] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.4 DNS 10.10.10.1
DHCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
```

Злоумышленник отработал

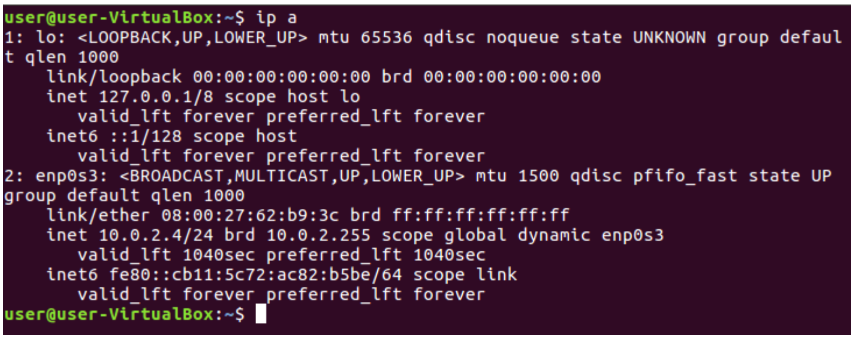


```
255.255.255.255     DHCP      342 DHCP Discover - Transaction ID 0x8ced4c40
255.255.255.255     DHCP      582 DHCP Offer    - Transaction ID 0x8ced4c40
255.255.255.255     DHCP      590 DHCP Offer    - Transaction ID 0x8ced4c40
255.255.255.255     DHCP      342 DHCP Request  - Transaction ID 0x8ced4c40
255.255.255.255     DHCP      582 DHCP ACK      - Transaction ID 0x8ced4c40
```

Лог wireshark

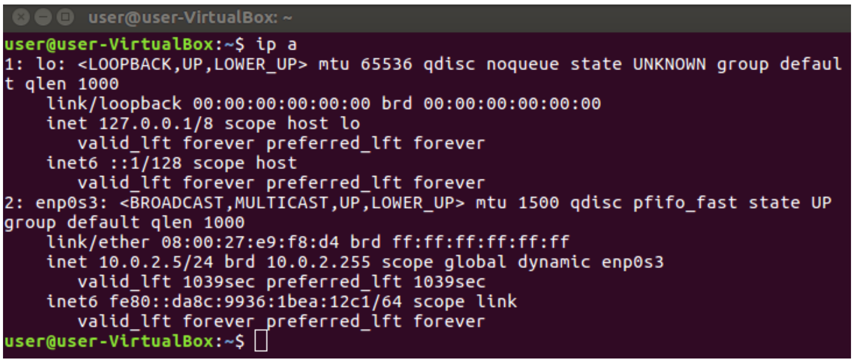
Часть 2

Фиксируем информацию о машинах

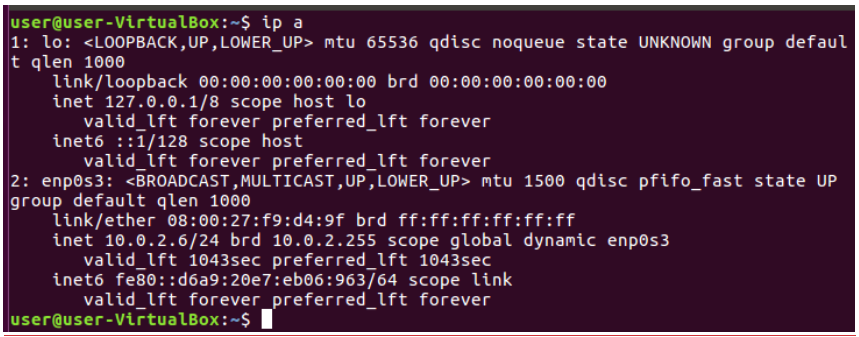


```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:62:b9:3c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1040sec preferred_lft 1040sec
    inet6 fe80::cb11:5c72:ac82:b5be/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$ 
```

Атакующая

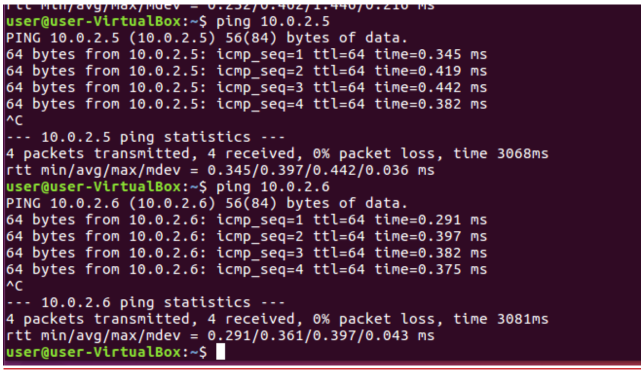


```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:e9:f8:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1039sec preferred_lft 1039sec
    inet6 fe80::da8c:9936:1bea:12c1/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$ 
```

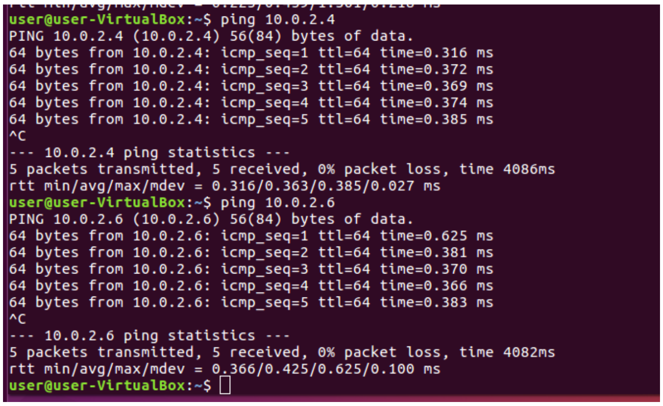


```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:f9:d4:9f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1043sec preferred_lft 1043sec
    inet6 fe80::d6a9:20e7:eb06:963/64 scope link
       valid_lft forever preferred_lft forever
user@user-VirtualBox:~$ 
```

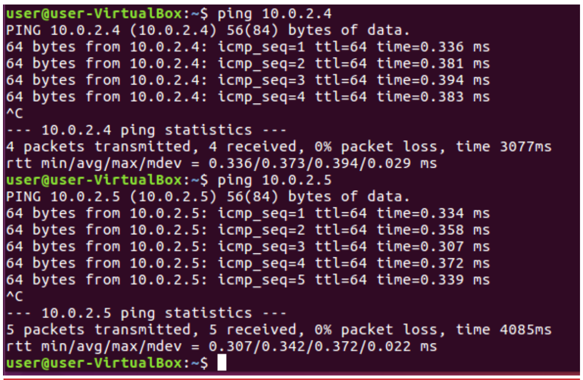
Выполняем перекрестный пинг



```
rtt min/avg/max/mdev = 0.232/0.462/1.440/0.210 ms
user@user-VirtualBox:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.345 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.419 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.442 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.382 ms
^C
--- 10.0.2.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.345/0.397/0.442/0.036 ms
user@user-VirtualBox:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.291 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.397 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.382 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.375 ms
^C
--- 10.0.2.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.291/0.361/0.397/0.043 ms
user@user-VirtualBox:~$
```

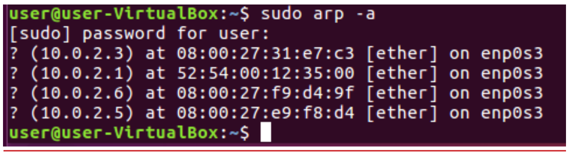


```
rtt min/avg/max/mdev = 0.225/0.439/1.361/0.210 ms
user@user-VirtualBox:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.316 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.372 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.369 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.374 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.385 ms
^C
--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4086ms
rtt min/avg/max/mdev = 0.316/0.363/0.385/0.027 ms
user@user-VirtualBox:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.625 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.381 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.370 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.366 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.383 ms
^C
--- 10.0.2.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.366/0.425/0.625/0.100 ms
user@user-VirtualBox:~$
```

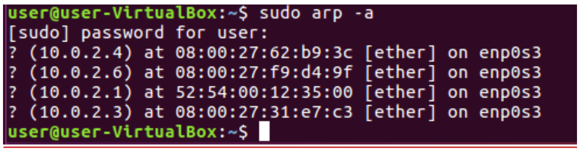


```
user@user-VirtualBox:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.336 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.381 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.394 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.383 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.336/0.373/0.394/0.029 ms
user@user-VirtualBox:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.334 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.358 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.307 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.372 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.339 ms
^C
--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4085ms
rtt min/avg/max/mdev = 0.307/0.342/0.372/0.022 ms
user@user-VirtualBox:~$
```

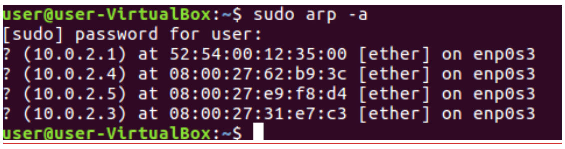
Все пингуется



```
user@user-VirtualBox:~$ sudo arp -a
[sudo] password for user:
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.6) at 08:00:27:f9:d4:9f [ether] on enp0s3
? (10.0.2.5) at 08:00:27:e9:f8:d4 [ether] on enp0s3
user@user-VirtualBox:~$
```

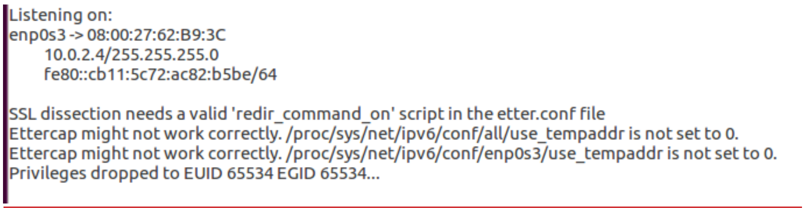


```
user@user-VirtualBox:~$ sudo arp -a
[sudo] password for user:
? (10.0.2.4) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.6) at 08:00:27:f9:d4:9f [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
user@user-VirtualBox:~$
```

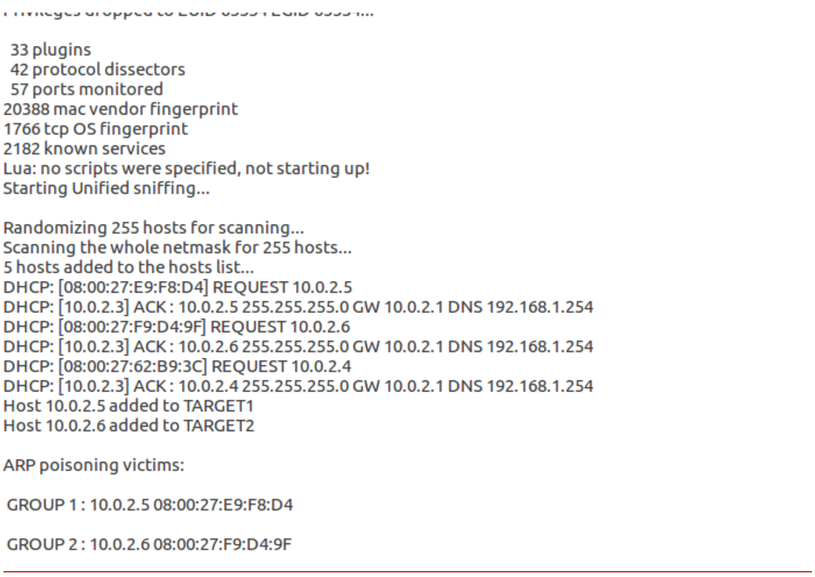


```
user@user-VirtualBox:~$ sudo arp -a
[sudo] password for user:
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.4) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.5) at 08:00:27:e9:f8:d4 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
user@user-VirtualBox:~$
```

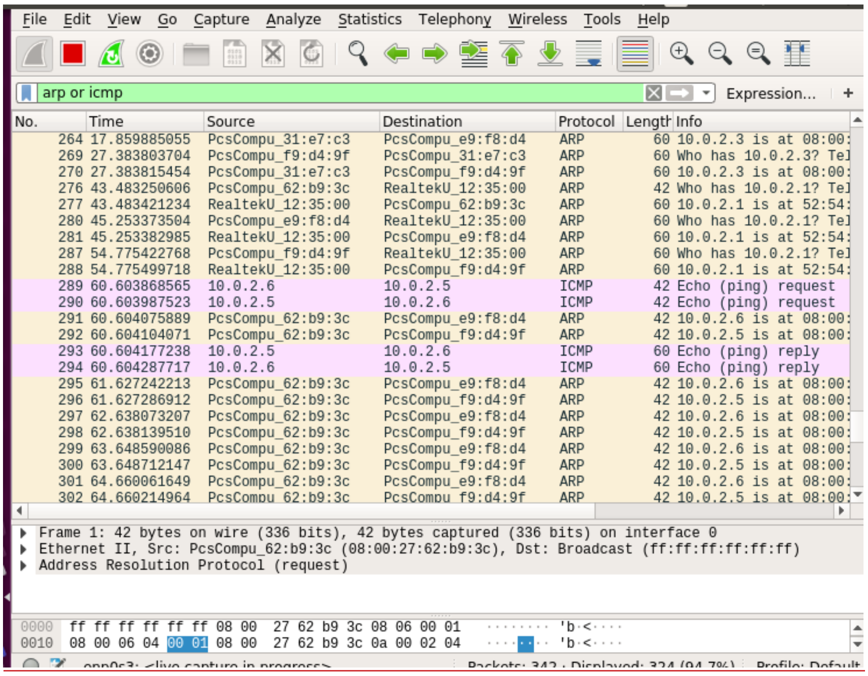
Зафиксировали все таблицы



```
Listening on:
enp0s3 -> 08:00:27:62:B9:3C
      10.0.2.4/255.255.255.0
      fe80::cb11:5c72:ac82:b5be/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempaddr is not set to 0.
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/enp0s3/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...
```



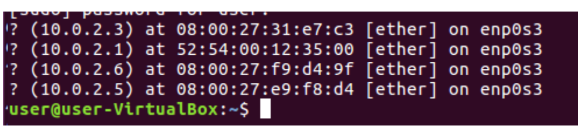
```
Privileges dropped to EUID 65534 EGID 65534...

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
DHCP: [08:00:27:E9:F8:D4] REQUEST 10.0.2.5
DHCP: [10.0.2.3] ACK : 10.0.2.5 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
DHCP: [08:00:27:F9:D4:9F] REQUEST 10.0.2.6
DHCP: [10.0.2.3] ACK : 10.0.2.6 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
DHCP: [08:00:27:62:B9:3C] REQUEST 10.0.2.4
DHCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
Host 10.0.2.5 added to TARGET1
Host 10.0.2.6 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 10.0.2.5 08:00:27:E9:F8:D4

 GROUP 2 : 10.0.2.6 08:00:27:F9:D4:9F
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

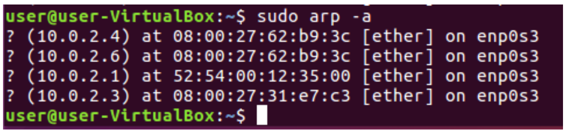
```
arp or icmp
```

```
No.   Time         Source              Destination         Protocol Length Info
  264 17.859885055 PcsCompu_31:e7:c3   PcsCompu_e9:f8:d4   ARP        60 10.0.2.3 is at 08:00:
  269 27.383803704 PcsCompu_f9:d4:9f   PcsCompu_31:e7:c3   ARP        60 Who has 10.0.2.3? Tel
  270 27.383815454 PcsCompu_31:e7:c3   PcsCompu_f9:d4:9f   ARP        60 10.0.2.3 is at 08:00:
  276 43.483250606 PcsCompu_62:b9:3c   RealtekU_12:35:00   ARP        42 Who has 10.0.2.1? Tel
  277 43.483421234 RealtekU_12:35:00   PcsCompu_62:b9:3c   ARP        60 10.0.2.1 is at 52:54:
  280 45.253373504 PcsCompu_e9:f8:d4   RealtekU_12:35:00   ARP        60 Who has 10.0.2.1? Tel
  281 45.253382985 RealtekU_12:35:00   PcsCompu_e9:f8:d4   ARP        60 10.0.2.1 is at 52:54:
  287 54.775422768 PcsCompu_f9:d4:9f   RealtekU_12:35:00   ARP        60 Who has 10.0.2.1? Tel
  288 54.775499718 RealtekU_12:35:00   PcsCompu_f9:d4:9f   ARP        60 10.0.2.1 is at 52:54:
  289 60.603868565 10.0.2.6            10.0.2.5            ICMP       42 Echo (ping) request
  290 60.603987523 10.0.2.5            10.0.2.6            ICMP       42 Echo (ping) request
  291 60.604075889 PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 10.0.2.6 is at 08:00:
  292 60.604104071 PcsCompu_62:b9:3c   PcsCompu_f9:d4:9f   ARP        42 10.0.2.5 is at 08:00:
  293 60.604177238 10.0.2.5            10.0.2.6            ICMP       60 Echo (ping) reply
  294 60.604287717 10.0.2.6            10.0.2.5            ICMP       60 Echo (ping) reply
  295 61.627242213 PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 10.0.2.6 is at 08:00:
  296 61.627286912 PcsCompu_62:b9:3c   PcsCompu_f9:d4:9f   ARP        42 10.0.2.5 is at 08:00:
  297 62.638073207 PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 10.0.2.6 is at 08:00:
  298 62.638139510 PcsCompu_62:b9:3c   PcsCompu_f9:d4:9f   ARP        42 10.0.2.5 is at 08:00:
  299 63.648590086 PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 10.0.2.6 is at 08:00:
  300 63.648712147 PcsCompu_62:b9:3c   PcsCompu_f9:d4:9f   ARP        42 10.0.2.5 is at 08:00:
  301 64.660061649 PcsCompu_62:b9:3c   PcsCompu_e9:f8:d4   ARP        42 10.0.2.6 is at 08:00:
  302 64.660214964 PcsCompu_62:b9:3c   PcsCompu_f9:d4:9f   ARP        42 10.0.2.5 is at 08:00:

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_62:b9:3c (08:00:27:62:b9:3c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 62 b9 3c 08 06 00 01   ········ 'b·<····
0010  08 00 06 04 00 01 08 00  27 62 b9 3c 0a 00 02 04   ········ 'b·<····

enp0s3: <live capture in progress>      Packets: 342 · Displayed: 324 (94.7%)      Profile: Default
```

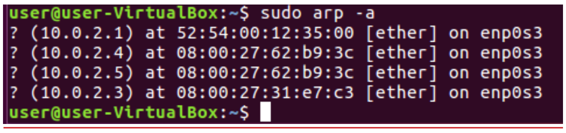
Зафиксировали log wireshark



```
[sudo] password for user:
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.6) at 08:00:27:f9:d4:9f [ether] on enp0s3
? (10.0.2.5) at 08:00:27:e9:f8:d4 [ether] on enp0s3
user@user-VirtualBox:~$
```



```
user@user-VirtualBox:~$ sudo arp -a
? (10.0.2.4) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.6) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
user@user-VirtualBox:~$
```



```
user@user-VirtualBox:~$ sudo arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.4) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.5) at 08:00:27:62:b9:3c [ether] on enp0s3
? (10.0.2.3) at 08:00:27:31:e7:c3 [ether] on enp0s3
user@user-VirtualBox:~$
```

Зафиксировали состояния таблиц

На атакующей машине таблицы не поменялись, а на атакуемых машинах МАС адреса изменились