Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

Лабораторная работа № 1
по дисциплине «Проектный семинар по информационной безопасности»

Студент гр. БИБ211
_____ А.И. Семененя
«17» декабря 2021 г.

Руководитель
Заведующий кафедрой информационной безопасности киберфизических систем
канд. техн. наук, доцент
_____О.О. Евсютин
«___» _____ 2021 г.

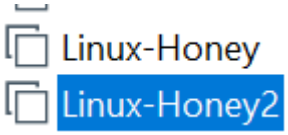
Москва 2021

Цель: получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.

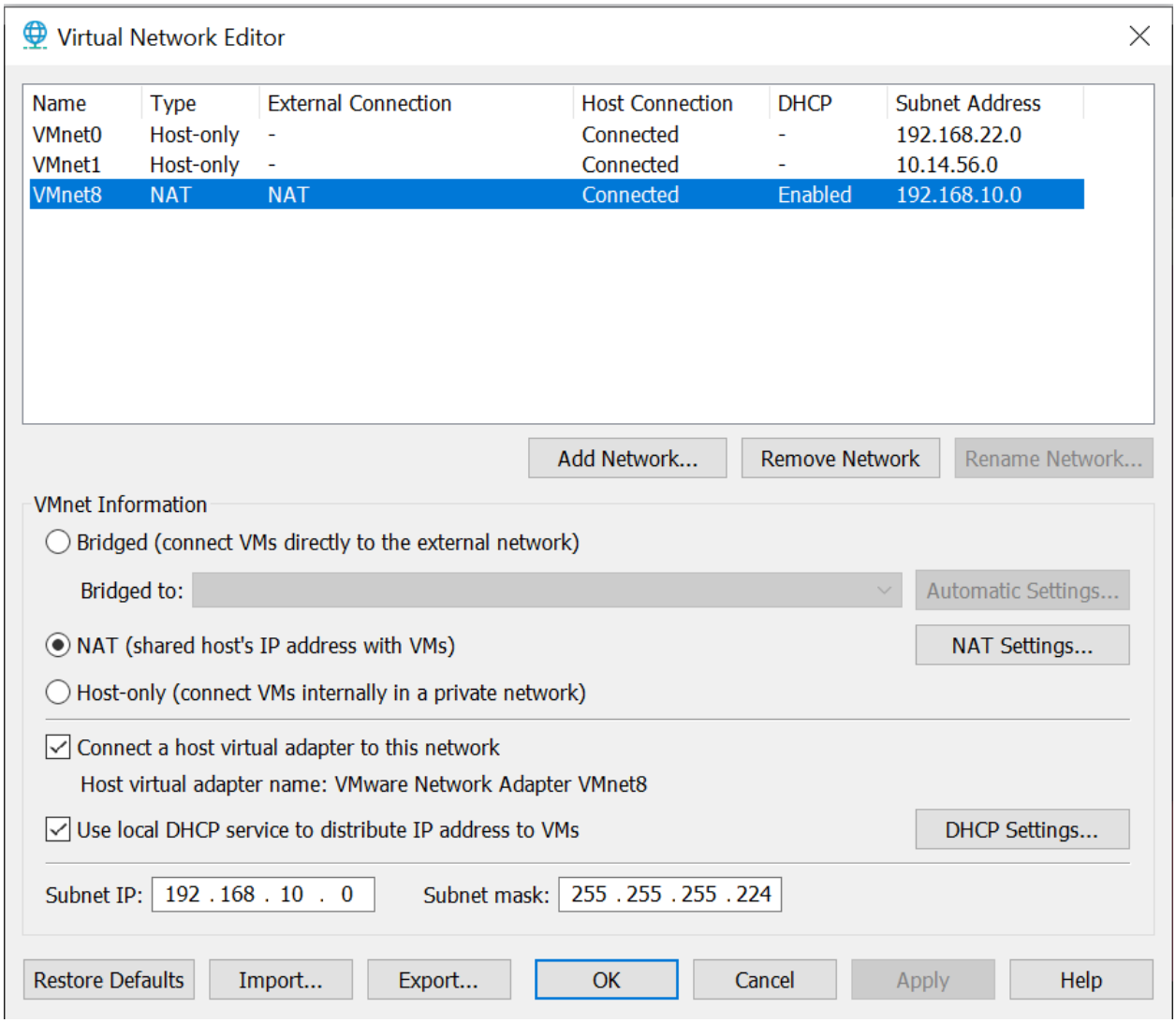
Вариант 1
Параметры:
Сеть NAT 192.168.10.0/27
Gateway 192.168.10.10
DNS 192.168.10.10
DHCP – работает

Ход работы
Часть 1

1. Создаём копию виртуальной машины Linux-honey. Запускаем обе машины в VMWare.



2. Согласно параметрам варианта создаём изолированную сеть. Подключаем обе машины к NAT.

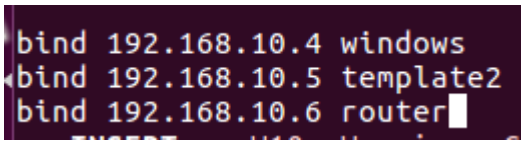


3. С помощью команды *ip a* определяем IP-адреса виртуальных машин.

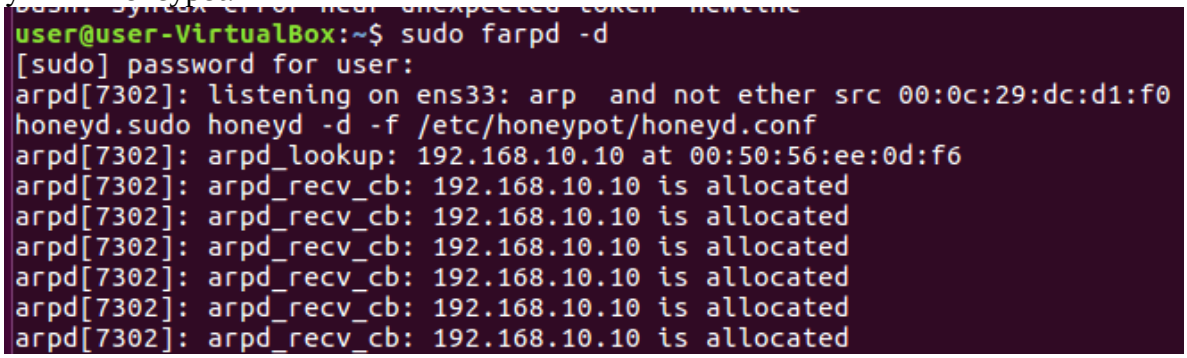
У первой: **192.168.10.16/27**

У второй: **192.168.10.17/27**

4. Меняем IP-адреса ловушек в /etc/honeypot/honeyd.conf на лежащие в заданном диапазоне.

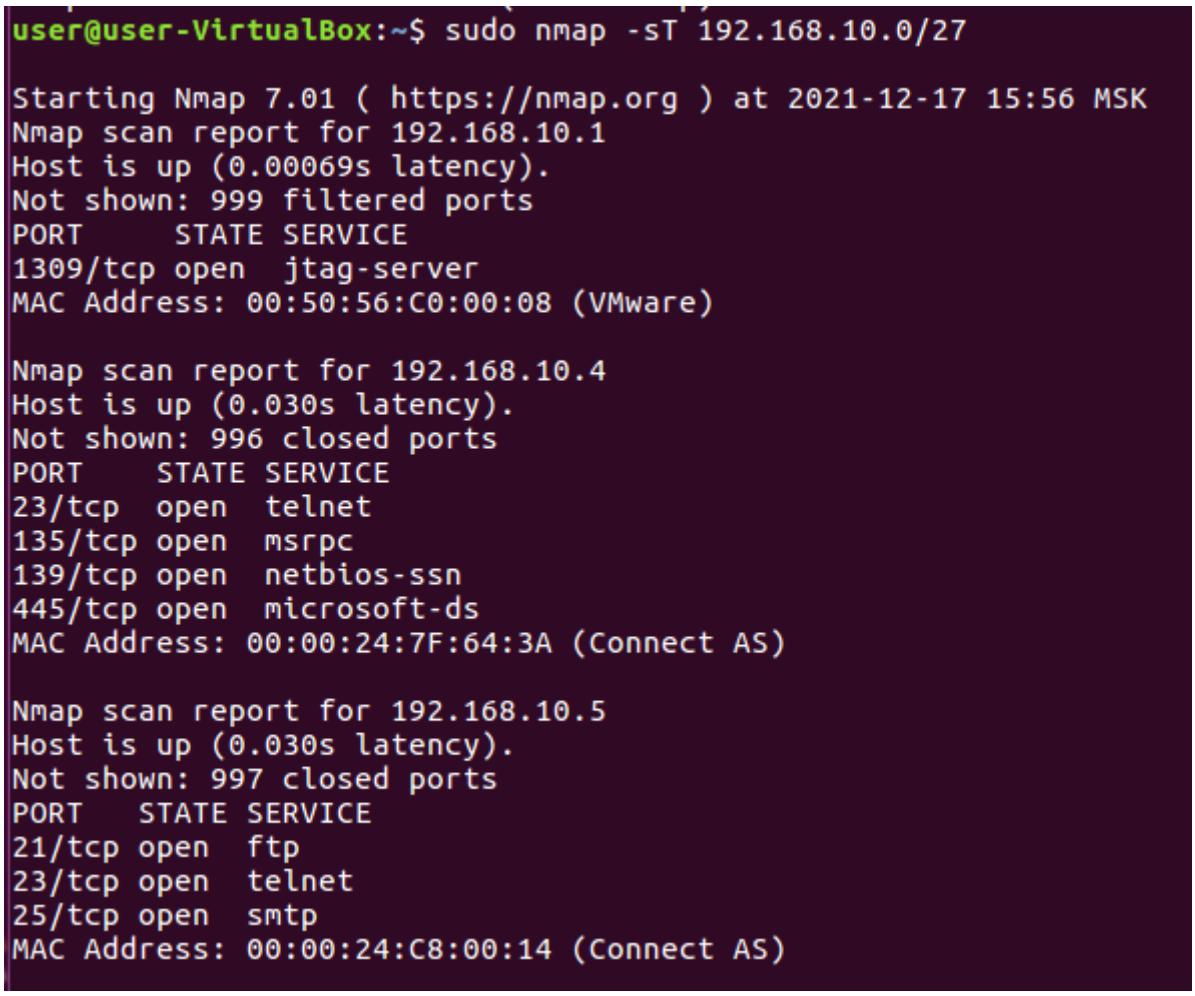


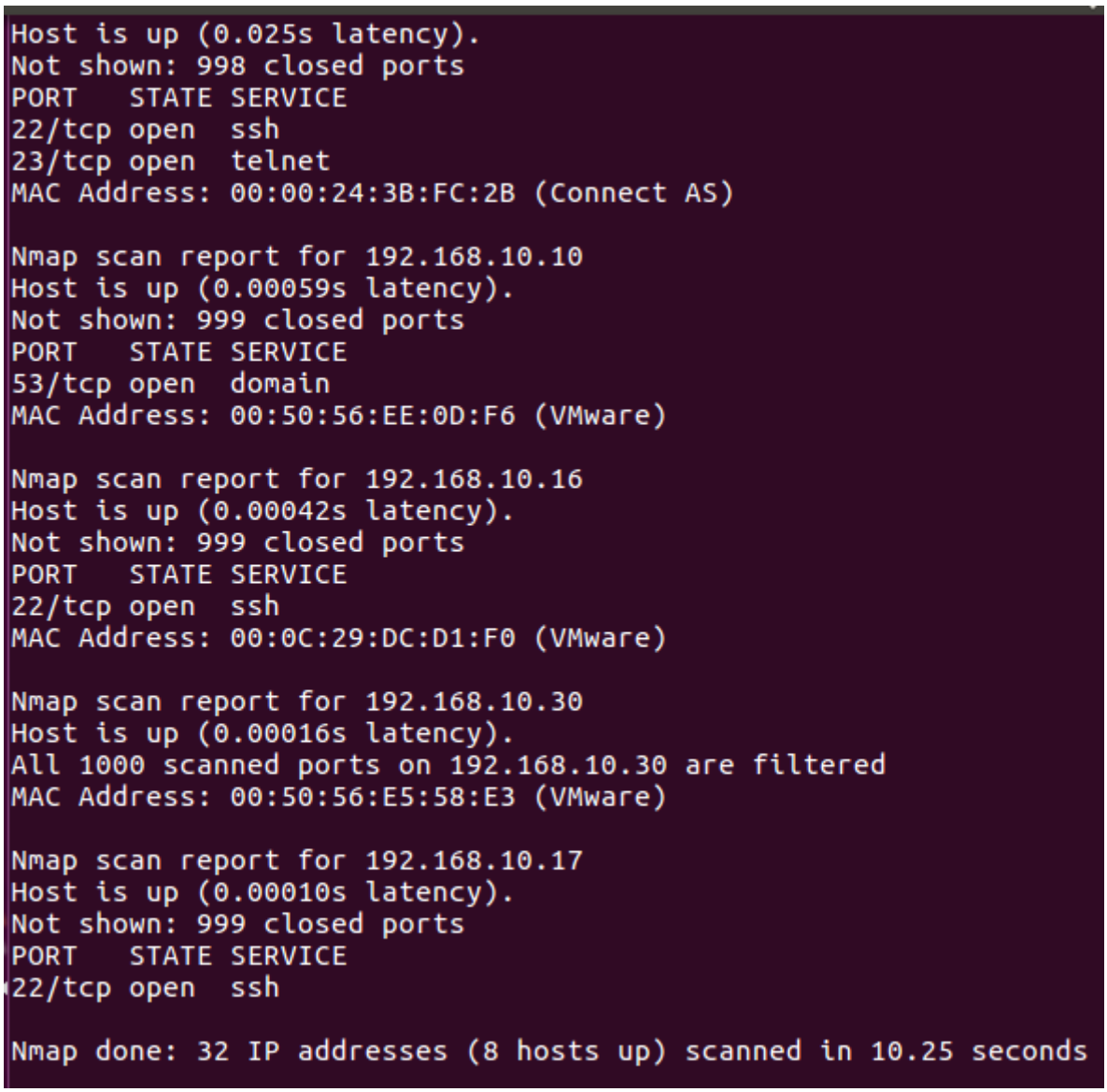
5. Запускаем honeypot.



6. Переключаемся на вторую виртуальную машину. С помощью утилиты nmap всеми способами, описанными в теоретической части, проводим сканирование сети с honeypot.

TCP Connect():


user@user-VirtualBox:~$ sudo nmap -sT 192.168.10.0/27
Starting Nmap 7.01 (https://nmap.org) at 2021-12-17 15:56 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00069s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
1309/tcp open jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.10.4
Host is up (0.030s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
23/tcp open telnet
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 00:00:24:7F:64:3A (Connect AS)
Nmap scan report for 192.168.10.5
Host is up (0.030s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
MAC Address: 00:00:24:C8:00:14 (Connect AS)


Host is up (0.025s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
MAC Address: 00:00:24:3B:FC:2B (Connect AS)
Nmap scan report for 192.168.10.10
Host is up (0.00059s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)
Nmap scan report for 192.168.10.16
Host is up (0.00042s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 00:0C:29:DC:D1:F0 (VMware)
Nmap scan report for 192.168.10.30
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.10.30 are filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)
Nmap scan report for 192.168.10.17
Host is up (0.00010s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
Nmap done: 32 IP addresses (8 hosts up) scanned in 10.25 seconds

TCP-SYN:

```
user@user-VirtualBox:~$ sudo nmap -sS 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 15:57 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00073s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
1309/tcp open  jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.016s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.019s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
25/tcp open  smtp
MAC Address: 00:00:24:C8:00:14 (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 00:00:24:3B:FC:2B (Connect AS)

Nmap scan report for 192.168.10.10
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.16
Host is up (0.00081s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.30
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.10.30 are filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)
```

```
Nmap scan report for 192.168.10.17
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 32 IP addresses (8 hosts up) scanned in 245.22 seconds
```

FIN:

```
user@user-VirtualBox:~$ sudo nmap -sF 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:02 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00085s latency).
All 1000 scanned ports on 192.168.10.1 are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.022s latency).
Not shown: 996 closed ports
PORT    STATE         SERVICE
23/tcp  open|filtered telnet
135/tcp open|filtered msrpc
139/tcp open|filtered netbios-ssn
445/tcp open|filtered microsoft-ds
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.024s latency).
Not shown: 997 closed ports
PORT   STATE         SERVICE
21/tcp open|filtered ftp
23/tcp open|filtered telnet
25/tcp open|filtered smtp
MAC Address: 00:00:24:C8:00:14 (Connect AS)
```

```
Nmap scan report for 192.168.10.6
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
23/tcp open|filtered telnet
MAC Address: 00:00:24:3B:FC:2B (Connect AS)

Nmap scan report for 192.168.10.10
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.16
Host is up (0.00068s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.30
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.10.30 are open|filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)
```

```
Nmap scan report for 192.168.10.17
Host is up (0.000093s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 32 IP addresses (8 hosts up) scanned in 335.12 seconds
```

Xmas Tree:

```
user@user-VirtualBox:~$ sudo nmap -sX 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:08 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.10.1 are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.10.4 are closed
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.10.5 are closed
MAC Address: 00:00:24:C8:00:14 (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.10.6 are closed
MAC Address: 00:00:24:3B:FC:2B (Connect AS)

Nmap scan report for 192.168.10.10
Host is up (0.00045s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)
```

```
Nmap scan report for 192.168.10.16
Host is up (0.0019s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.30
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.10.30 are open|filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)

Nmap scan report for 192.168.10.17
Host is up (0.000098s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 32 IP addresses (8 hosts up) scanned in 333.42 seconds
```

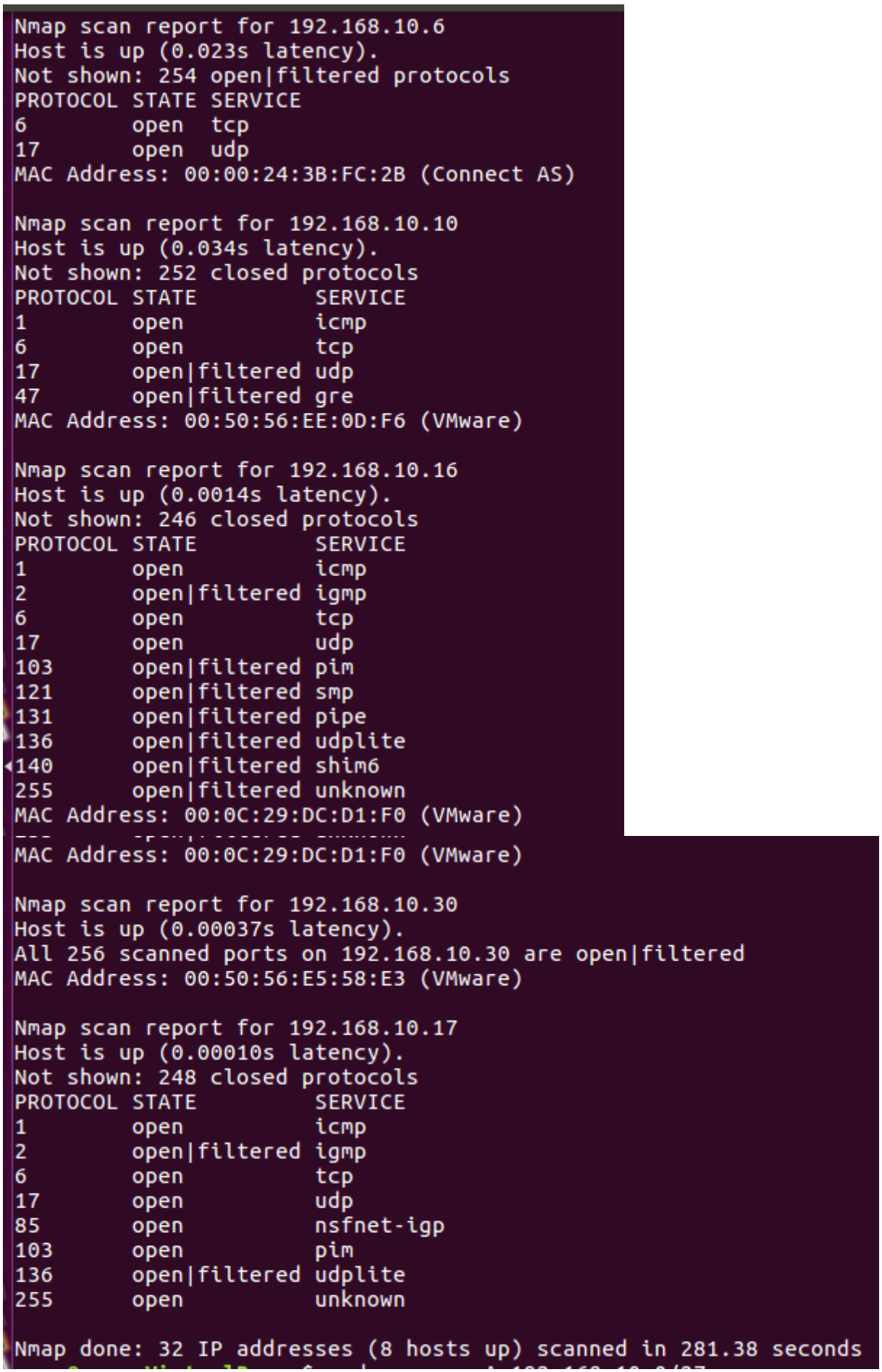
NULL:

```
user@user-VirtualBox:~$ sudo nmap -sN 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:13 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.10.1 are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.10.4 are closed
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.023s latency).
Not shown: 997 closed ports
PORT   STATE         SERVICE
21/tcp open|filtered ftp
23/tcp open|filtered telnet
25/tcp open|filtered smtp
MAC Address: 00:00:24:C8:00:14 (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.10.6 are closed
MAC Address: 00:00:24:3B:FC:2B (Connect AS)
```

```
Nmap scan report for 192.168.10.10
Host is up (0.00044s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.16
Host is up (0.00066s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.30
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.10.30 are open|filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)

Nmap scan report for 192.168.10.17
Host is up (0.000088s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 32 IP addresses (8 hosts up) scanned in 348.27 seconds
```

Сканирование протокола IP:

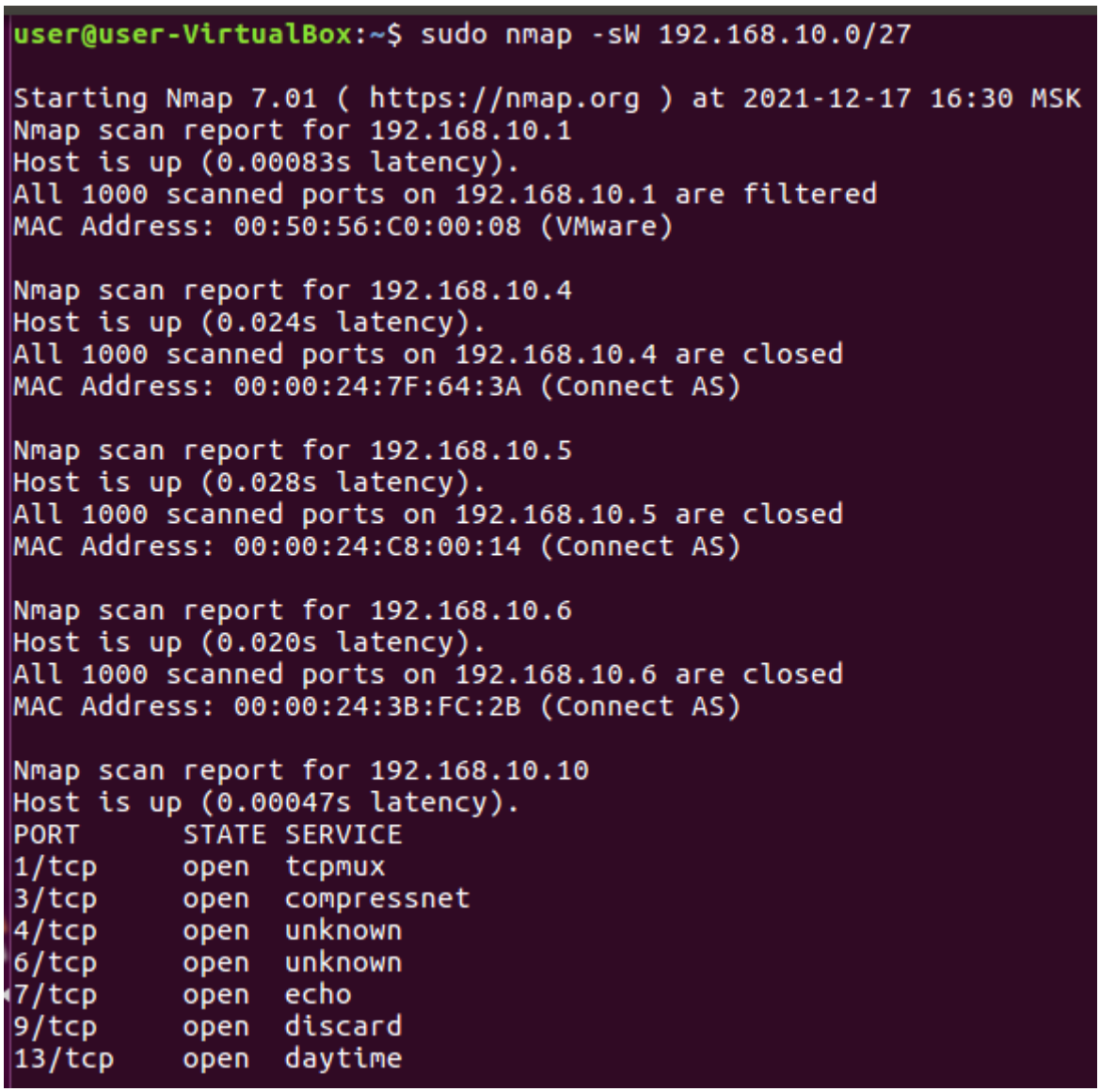
```
user@user-VirtualBox:~$ sudo nmap -sO 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:19 MSK
Warning: 192.168.10.16 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.10.1
Host is up (0.00056s latency).
All 256 scanned ports on 192.168.10.1 are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.027s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
17       open  udp
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.023s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
17       open  udp
MAC Address: 00:00:24:C8:00:14 (Connect AS)
```


Nmap scan report for 192.168.10.6
Host is up (0.023s latency).
Not shown: 254 open|filtered protocols
PROTOCOL STATE SERVICE
6 open tcp
17 open udp
MAC Address: 00:00:24:3B:FC:2B (Connect AS)
Nmap scan report for 192.168.10.10
Host is up (0.034s latency).
Not shown: 252 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
6 open tcp
17 open|filtered udp
47 open|filtered gre
MAC Address: 00:50:56:EE:0D:F6 (VMware)
Nmap scan report for 192.168.10.16
Host is up (0.0014s latency).
Not shown: 246 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
121 open|filtered smp
131 open|filtered pipe
136 open|filtered udplite
140 open|filtered shim6
255 open|filtered unknown
MAC Address: 00:0C:29:DC:D1:F0 (VMware)
MAC Address: 00:0C:29:DC:D1:F0 (VMware)
Nmap scan report for 192.168.10.30
Host is up (0.00037s latency).
All 256 scanned ports on 192.168.10.30 are open|filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)
Nmap scan report for 192.168.10.17
Host is up (0.00010s latency).
Not shown: 248 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
85 open nsfnet-igp
103 open pim
136 open|filtered udplite
255 open unknown
Nmap done: 32 IP addresses (8 hosts up) scanned in 281.38 seconds

ACK-сканирование:

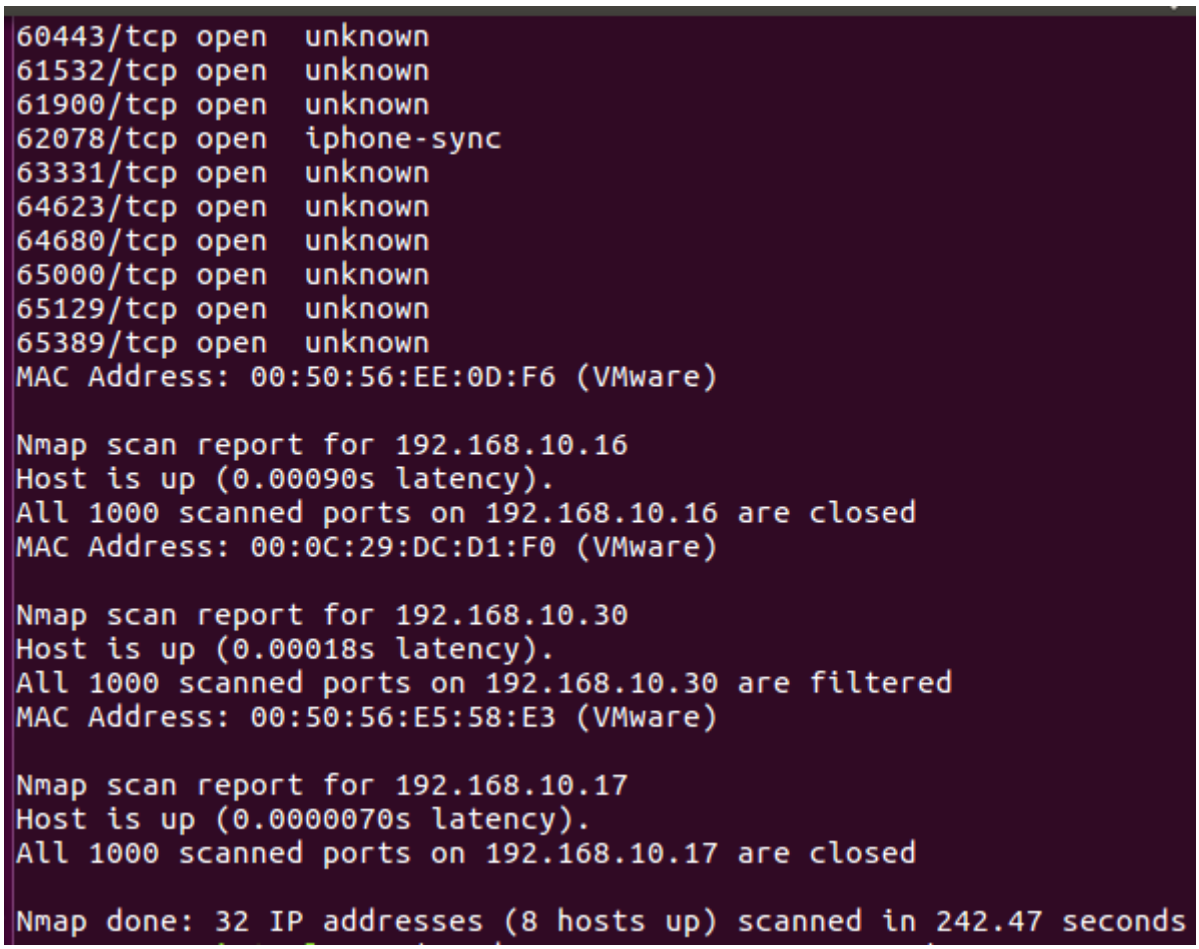
```
user@user-VirtualBox:~$ sudo nmap -sA 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:25 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00090s latency).
All 1000 scanned ports on 192.168.10.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.10.4 are unfiltered
MAC Address: 00:00:24:7F:64:3A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.024s latency).
All 1000 scanned ports on 192.168.10.5 are unfiltered
MAC Address: 00:00:24:C8:00:14 (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.017s latency).
All 1000 scanned ports on 192.168.10.6 are unfiltered
MAC Address: 00:00:24:3B:FC:2B (Connect AS)

Nmap scan report for 192.168.10.10
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.10.10 are unfiltered
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.16
Host is up (0.00076s latency).
All 1000 scanned ports on 192.168.10.16 are unfiltered
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.30
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.10.30 are filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)

Nmap scan report for 192.168.10.17
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.10.17 are unfiltered

Nmap done: 32 IP addresses (8 hosts up) scanned in 240.18 seconds
```

TCP Window:

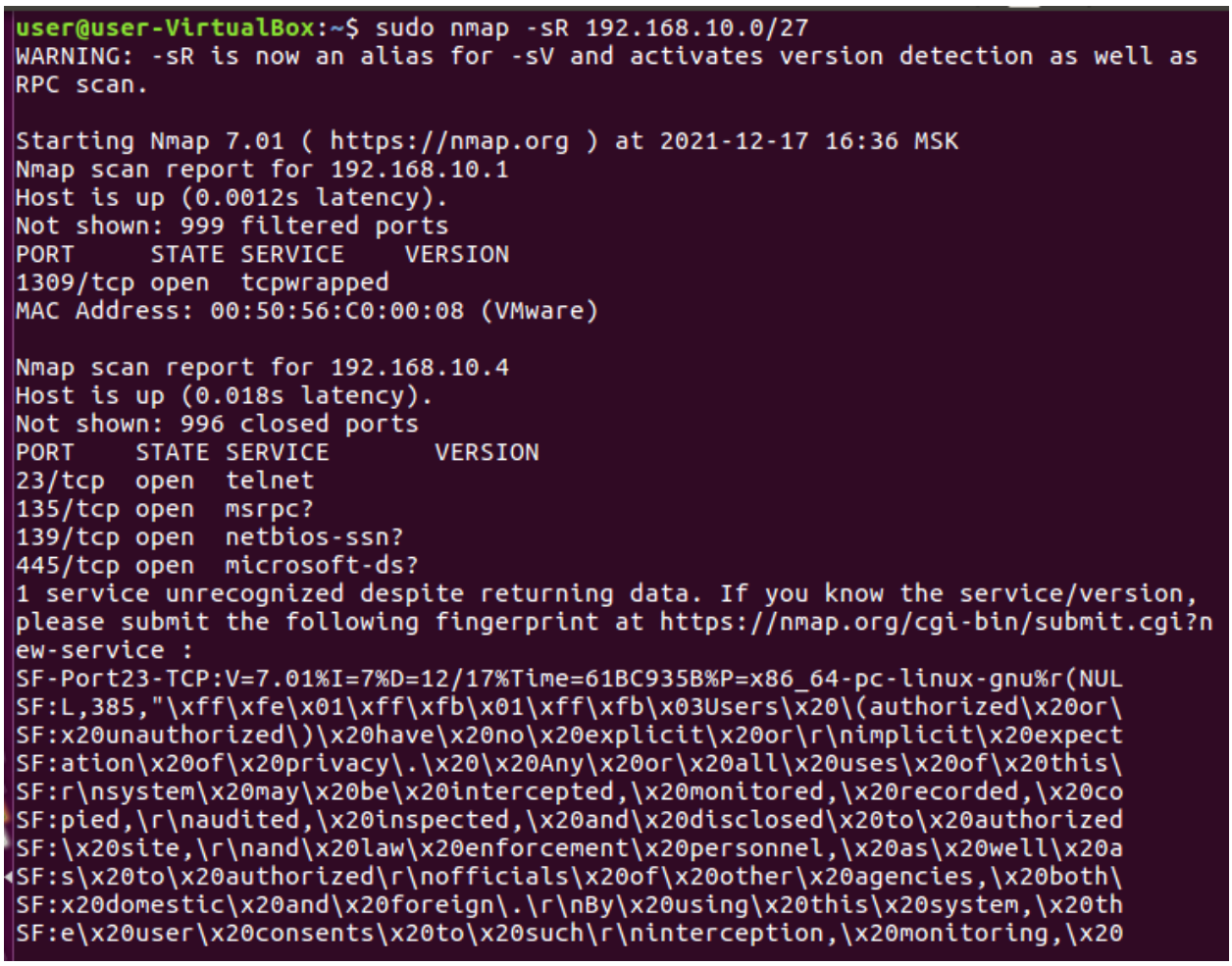

user@user-VirtualBox:~$ sudo nmap -sW 192.168.10.0/27
Starting Nmap 7.01 (https://nmap.org) at 2021-12-17 16:30 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00083s latency).
All 1000 scanned ports on 192.168.10.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.10.4
Host is up (0.024s latency).
All 1000 scanned ports on 192.168.10.4 are closed
MAC Address: 00:00:24:7F:64:3A (Connect AS)
Nmap scan report for 192.168.10.5
Host is up (0.028s latency).
All 1000 scanned ports on 192.168.10.5 are closed
MAC Address: 00:00:24:C8:00:14 (Connect AS)
Nmap scan report for 192.168.10.6
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.10.6 are closed
MAC Address: 00:00:24:3B:FC:2B (Connect AS)
Nmap scan report for 192.168.10.10
Host is up (0.00047s latency).
PORT STATE SERVICE
1/tcp open tcpmux
3/tcp open compressnet
4/tcp open unknown
6/tcp open unknown
7/tcp open echo
9/tcp open discard
13/tcp open daytime

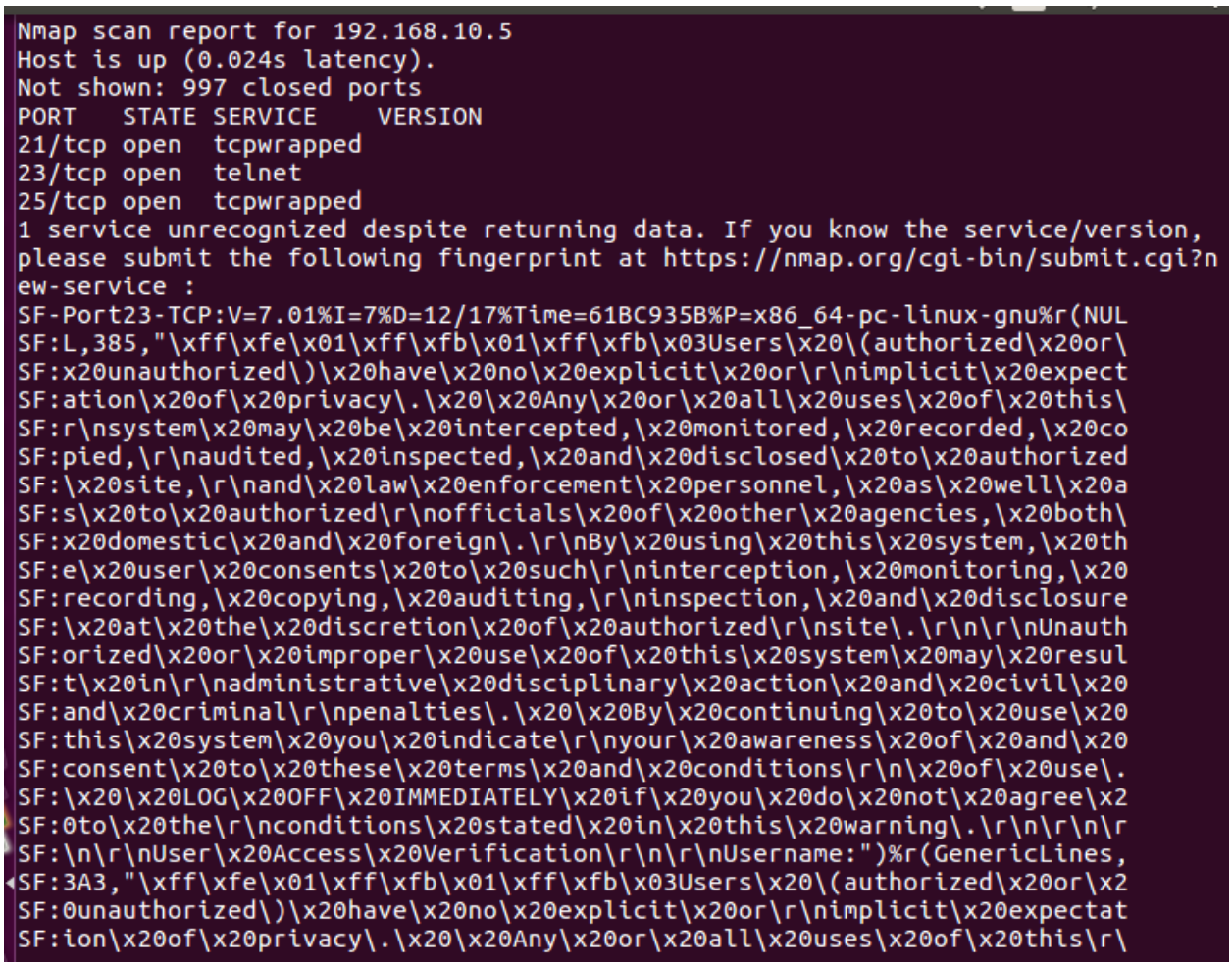

17/tcp open qotd
19/tcp open chargen
20/tcp open ftp-data
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp open smtp
26/tcp open rsftp
30/tcp open unknown
32/tcp open unknown
33/tcp open dsp
37/tcp open time
42/tcp open nameserver
43/tcp open whois
49/tcp open tacacs
53/tcp open domain
70/tcp open gopher
79/tcp open finger
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev
84/tcp open ctf
85/tcp open mit-ml-dev
88/tcp open kerberos-sec
89/tcp open su-mit-tg
90/tcp open dnsix
99/tcp open metagram
100/tcp open newacct
106/tcp open pop3pw
109/tcp open pop2

…



RPC-сканирование:


user@user-VirtualBox:~$ sudo nmap -sR 192.168.10.0/27
WARNING: -sR is now an alias for -sV and activates version detection as well as
RPC scan.
Starting Nmap 7.01 (https://nmap.org) at 2021-12-17 16:36 MSK
Nmap scan report for 192.168.10.1
Host is up (0.0012s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
1309/tcp open tcpwrapped
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.10.4
Host is up (0.018s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet
135/tcp open msrpc?
139/tcp open netbios-ssn?
445/tcp open microsoft-ds?
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port23-TCP:V=7.01%I=7%D=12/17%Time=61BC935B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,385,"\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\(authorized\x20or\
SF:x20unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expect
SF:ation\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\
SF:r\nsystem\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20co
SF:pied,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized
SF:\x20site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x20a
SF:s\x20to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\
SF:x20domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20th
SF:e\x20user\x20consents\x20to\x20such\r\ninterception,\x20monitoring,\x20



```
Nmap scan report for 192.168.10.5
Host is up (0.024s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
23/tcp open  telnet
25/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port23-TCP:V=7.01%I=7%D=12/17%Time=61BC935B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,385,"\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\(authorized\x20or\
SF:x20unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expect
SF:ation\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\
SF:r\nsystem\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20co
SF:pied,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized
SF:\x20site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x20a
SF:s\x20to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\
SF:x20domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20th
SF:e\x20user\x20consents\x20to\x20such\r\ninterception,\x20monitoring,\x20
SF:recording,\x20copying,\x20auditing,\r\ninspection,\x20and\x20disclosure
SF:\x20at\x20the\x20discretion\x20of\x20authorized\r\nsite\.\r\n\r\nUnauth
SF:orized\x20or\x20improper\x20use\x20of\x20this\x20system\x20may\x20resul
SF:t\x20in\r\nadministrative\x20disciplinary\x20action\x20and\x20civil\x20
SF:and\x20criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x20
SF:this\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x20
SF:consent\x20to\x20these\x20terms\x20and\x20conditions\r\n\x20of\x20use\.
SF:\x20\x20LOG\x20OFF\x20IMMEDIATELY\x20if\x20you\x20do\x20not\x20agree\x2
SF:0to\x20the\r\nconditions\x20stated\x20in\x20this\x20warning\.\r\n\r\n\r
SF:\n\r\nUser\x20Access\x20Verification\r\n\r\nUsername:")%r(GenericLines,
SF:3A3,"\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\(authorized\x20or\x2
SF:0unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expectat
SF:ion\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\r\
```

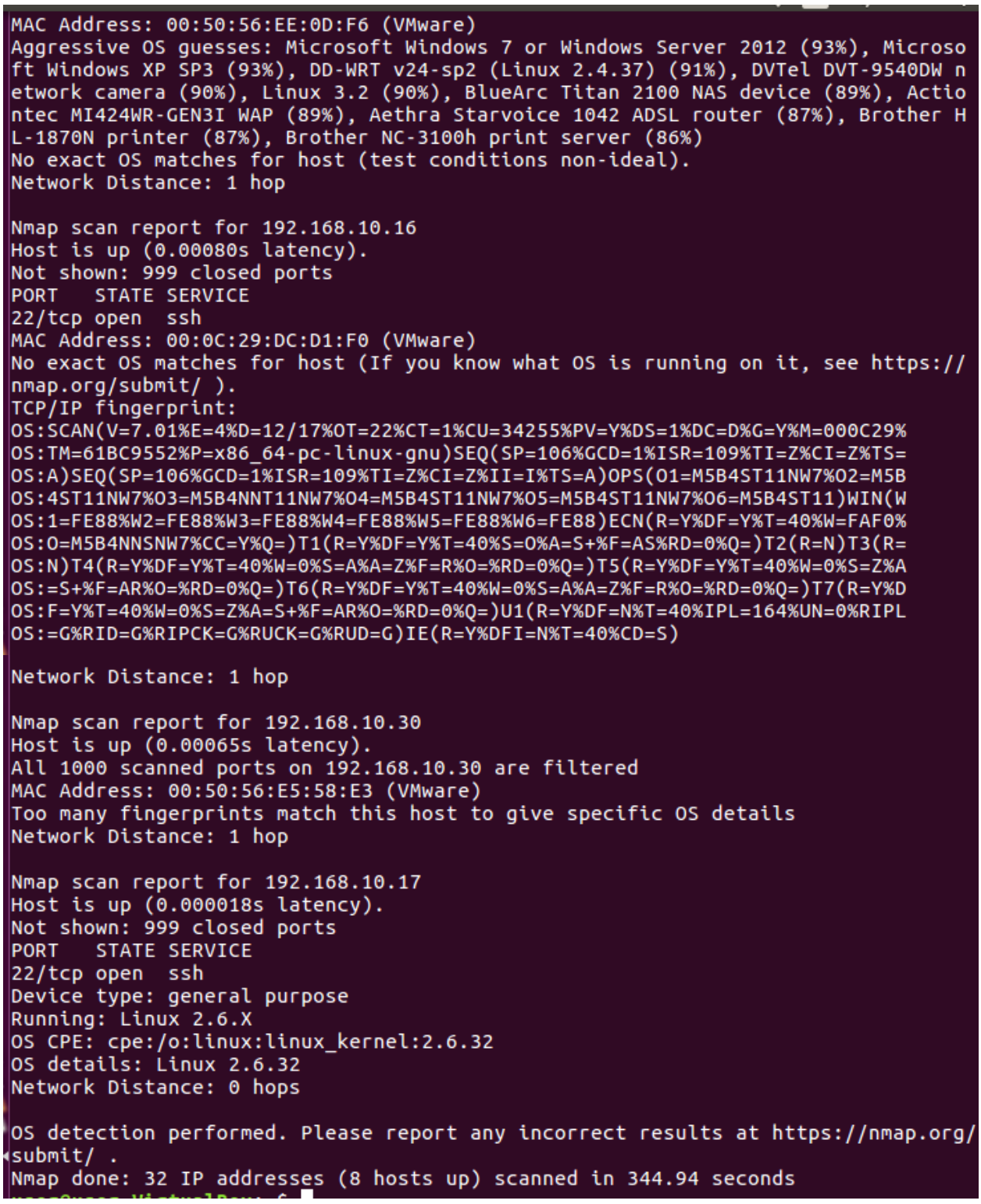
```
SF:\r\nUser\x20Access\x20Verification\r\n\r\nUsername:");
MAC Address: 00:00:24:C8:00:14 (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 1.5)
23/tcp open  telnet
2 services unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi
?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.01%I=7%D=12/17%Time=61BC935B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,D,"SSH-1\.5-2\.40\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port23-TCP:V=7.01%I=7%D=12/17%Time=61BC935B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,385,"\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\(authorized\x20or\
SF:x20unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expect
SF:ation\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\
SF:r\nsystem\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20co
SF:pied,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized
SF:\x20site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x20a
SF:s\x20to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\
SF:x20domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20th
SF:e\x20user\x20consents\x20to\x20such\r\ninterception,\x20monitoring,\x20
SF:recording,\x20copying,\x20auditing,\r\ninspection,\x20and\x20disclosure
SF:\x20at\x20the\x20discretion\x20of\x20authorized\r\nsite\.\r\n\r\nUnauth
SF:orized\x20or\x20improper\x20use\x20of\x20this\x20system\x20may\x20resul
SF:t\x20in\r\nadministrative\x20disciplinary\x20action\x20and\x20civil\x20
SF:and\x20criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x20
SF:this\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x20
SF:consent\x20to\x20these\x20terms\x20and\x20conditions\r\n\x20of\x20use\.
```

```
Nmap scan report for 192.168.10.10
Host is up (0.00043s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND dnsmasq-
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.16
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.
0)
MAC Address: 00:0C:29:DC:D1:F0 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.10.30
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.10.30 are filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)

Nmap scan report for 192.168.10.17
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.
0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 32 IP addresses (8 hosts up) scanned in 385.12 seconds
```

Сканирование ОС:

```
user@user-VirtualBox:~$ sudo nmap -O 192.168.10.0/27

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 16:43 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00089s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
1309/tcp open  jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), FreeBSD 6.X (86%), Microsoft Win
dows XP (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.3 cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), FreeBS
D 6.3-RELEASE (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.10.4
Host is up (0.019s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:00:24:7F:64:3A (Connect AS)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=12/17%OT=23%CT=1%CU=32702%PV=Y%DS=1%DC=D%G=Y%M=000024%
OS:TM=61BC9552%P=x86_64-pc-linux-gnu)SEQ(SP=A1%GCD=1%ISR=A8%TI=I%CI=I)OPS(O
OS:1=M5B4NW0NNT11%O2=M5B4NW0NNT11%O3=M5B4NW0NNT11%O4=M5B4NW0NNT11%O5=M5B4NW
OS:0NNT11%O6=M5B4NW0NNT11)WIN(W1=6270%W2=6270%W3=6270%W4=6270%W5=6270%W6=62
OS:70)ECN(R=Y%DF=Y%T=40%W=6270%O=M5B4NW0NNT10%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=40%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF
OS:=Y%T=40%W=6270%S=O%A=S+%F=AS%O=M5B4NW0NNT11%RD=0%Q=)T4(R=Y%DF=N%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=A%A=S+%F=AR%O=%RD=0%Q=)T6
OS:(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=A%A=S+%
OS:F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=Y%T=80%CD=Z)

Network Distance: 1 hop

Nmap scan report for 192.168.10.5
Host is up (0.018s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
25/tcp open  smtp
MAC Address: 00:00:24:C8:00:14 (Connect AS)
No OS matches for host (If you know what OS is running on it, see https://nmap.o
rg/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=12/17%OT=21%CT=1%CU=39858%PV=Y%DS=1%DC=D%G=Y%M=000024%
OS:TM=61BC9552%P=x86_64-pc-linux-gnu)SEQ(SP=D2%GCD=1%ISR=D9%TI=I%CI=I)OPS(O
OS:1=M5B4NNT11NW0%O2=M5B4NNT11NW0%O3=M5B4NNT11NW0%O4=M5B4NNT11NW0%O5=M5B4NN
OS:T11NW0%O6=M5B4NNT11NW0)WIN(W1=7C38%W2=7C38%W3=7C38%W4=7C38%W5=7C38%W6=7C
OS:38)ECN(R=Y%DF=Y%T=40%W=7C38%O=M5B4NNT10NW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=7C38%S=O%A=S+%F=AS%O=M5B4NNT
```

```
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=I)IE(R=Y%DFI=N%T=FF%CD=1)

Network Distance: 1 hop

Nmap scan report for 192.168.10.6
Host is up (0.020s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 00:00:24:3B:FC:2B (Connect AS)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=12/17%OT=22%CT=1%CU=42474%PV=Y%DS=1%DC=D%G=Y%M=000024%
OS:TM=61BC9552%P=x86_64-pc-linux-gnu)SEQ(SP=40%GCD=1%ISR=47%TI=Z%CI=Z%TS=U)
OS:OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=1020%W2=1020%
OS:W3=1020%W4=1020%W5=1020%W6=1020)ECN(R=Y%DF=N%T=40%W=1020%O=M5B4%CC=N%Q=)
OS:T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=40%W=0%S=A%A=S%F=AR
OS:%O=%RD=0%Q=)T3(R=Y%DF=N%T=40%W=1020%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%
OS:DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=A%A=S+%F=AR%
OS:O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%
OS:W=0%S=A%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=Z)

Network Distance: 1 hop

Nmap scan report for 192.168.10.10
Host is up (0.0024s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EE:0D:F6 (VMware)
```



По результату сканирования, а именно отображаемым портам и их количеству, мы можем заметить, что все вышеописанные способы сканирования nmap успешно попадаются на расставленные на первой виртуальной машине ловушки.

7. Добавляем две новых ловушки, настраиваем их параметры.

```
create additional
set additional personality "HP LaserJet 5"
set additional default tcp action reset
add additional tcp port 22 "/usr/share/honeyd/scripts/test.sh"
add additional tcp port 99 open

create additional_2
set additional_2 personality "Hitachi HI-UX/MPP"
set additional_2 default tcp action reset
add additional_2 tcp port 23 "/usr/share/honeyd/scripts/ftp.sh"
add additional_2 tcp port 72 "/usr/share/honeyd/scripts/smtp.sh"
add additional_2 tcp port 31 open

set template2 ethernet "00:00:24:ab:8c:22"
set windows ethernet "00:00:24:ab:8c:12"
set router ethernet "00:00:24:ab:8c:33"
set additional ethernet "00:00:24:ab:8c:15"
set additional_2 ethernet "00:00:24:ab:8c:19"

bind 192.168.10.4 windows
bind 192.168.10.5 template2
bind 192.168.10.6 router
bind 192.168.10.11 additional
bind 192.168.10.20 additional_2
```

8. После добавления новых ловушек запускаем повторное сканирование.

```
user@user-VirtualBox:~$ sudo nmap -sA 192.168.10.0/27
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 21:48 MSK
Nmap scan report for 192.168.10.1
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.10.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.10.4
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.10.4 are unfiltered
MAC Address: 00:00:24:0C:A5:8A (Connect AS)

Nmap scan report for 192.168.10.5
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.10.5 are unfiltered
MAC Address: 00:00:24:5F:ED:DE (Connect AS)

Nmap scan report for 192.168.10.6
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.10.6 are unfiltered
MAC Address: 00:00:24:54:CA:E3 (Connect AS)

Nmap scan report for 192.168.10.10
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.10.10 are unfiltered
MAC Address: 00:50:56:EE:0D:F6 (VMware)

Nmap scan report for 192.168.10.11
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.10.11 are unfiltered
MAC Address: 00:00:24:E5:0D:CD (Connect AS)

Nmap scan report for 192.168.10.16
Host is up (0.00090s latency).
All 1000 scanned ports on 192.168.10.16 are unfiltered
MAC Address: 00:0C:29:DC:D1:F0 (VMware)

Nmap scan report for 192.168.10.20
Host is up (0.019s latency).
All 1000 scanned ports on 192.168.10.20 are unfiltered
MAC Address: 00:00:24:BC:7C:92 (Connect AS)

Nmap scan report for 192.168.10.30
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.10.30 are filtered
MAC Address: 00:50:56:E5:58:E3 (VMware)

Nmap scan report for 192.168.10.17
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.10.17 are unfiltered

Nmap done: 32 IP addresses (10 hosts up) scanned in 250.35 seconds
```

Мы можем увидеть, что nmap видит IP-адреса новых ловушек (192.168.10.11, 192.168.10.20). Это означает, что изменения конфигурации вошли в силу.

Часть 2

1. Утилитой ping проверяем доступ в интернет.
2. Запускаем Wireshark.
3. Сканируем IP-адрес 195.208.245.253:

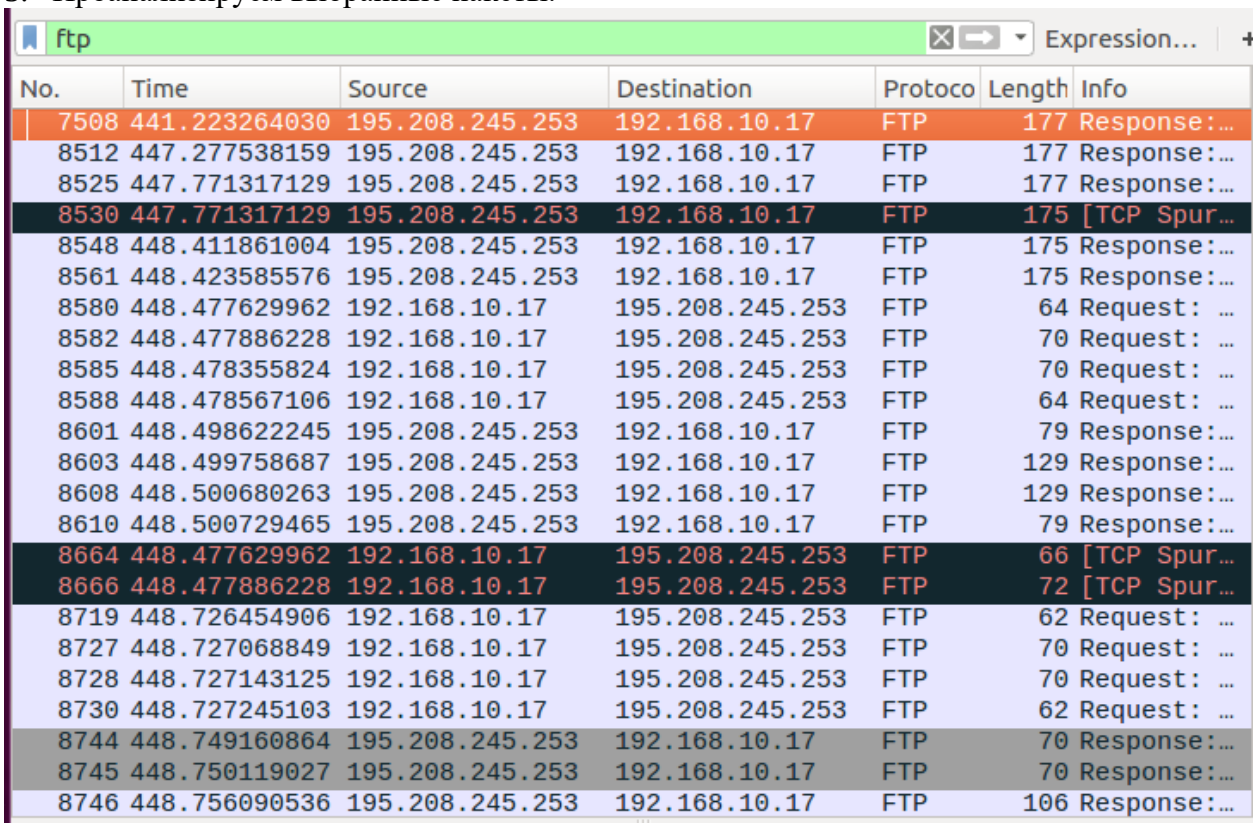
```
user@user-VirtualBox:~$ nmap -T4 -A -v 195.208.245.253 -Pn

Starting Nmap 7.01 ( https://nmap.org ) at 2021-12-17 22:54 MSK
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:54
Completed Parallel DNS resolution of 1 host. at 22:54, 0.16s elapsed
Initiating Connect Scan at 22:54
Scanning fileserv.r61.net (195.208.245.253) [1000 ports]
Discovered open port 22/tcp on 195.208.245.253
Discovered open port 21/tcp on 195.208.245.253
Discovered open port 111/tcp on 195.208.245.253
Discovered open port 139/tcp on 195.208.245.253
Discovered open port 445/tcp on 195.208.245.253
Completed Connect Scan at 22:54, 9.63s elapsed (1000 total ports)
Initiating Service scan at 22:54
Scanning 5 services on fileserv.r61.net (195.208.245.253)
Completed Service scan at 22:55, 6.10s elapsed (5 services on 1 host)
```

```
NSE: Script scanning 195.208.245.253.
Initiating NSE at 22:55
Completed NSE at 22:55, 15.78s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Nmap scan report for fileserv.r61.net (195.208.245.253)
Host is up (0.027s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5b
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x   3 ftp      ftp          4096 Sep 24  2011 Edu_tools
| drwxr-xr-x   2 ftp      ftp          4096 Feb 14  2020 FreeBSD
| drwxr-xr-x   2 ftp      ftp          4096 Mar 31  2020 Solaris
| drwxr-xr-x   4 ftp      ftp          4096 Sep 24  2011 archivers
| drwxr-xr-x   2 ftp      ftp          4096 Sep 21  2015 bacula
| drwxr-xr-x   2 ftp      ftp          4096 Sep 24  2011 ccm
| drwxr-xr-x   3 ftp      ftp          4096 Jan 27  2012 databases
| drwxr-xr-x   3 ftp      ftp          4096 Dec  5  2013 desktop
| drwxr-xr-x   7 ftp      ftp          4096 Jan 27  2012 development
| drwxr-xr-x   5 ftp      ftp          4096 Aug  1  2016 docsvisionclient
| drwxr-xr-x   3 ftp      ftp          4096 Sep 11  2017 fujitsu
| drwxr-xr-x   2 ftp      ftp          4096 Sep 16  2014 gparted
| drwxr-xr-x  17 ftp      ftp          4096 Sep 24  2011 hardware
| drwxr-xr-x   7 ftp      ftp          4096 Apr 20  2018 linux
| drwxr-xr-x   3 ftp      ftp          4096 Sep 24  2011 local
| drwxr-xr-x   3 ftp      ftp          4096 Sep 24  2011 media
| drwxr-xr-x   5 ftp      ftp          4096 Jan 27  2012 net
| drwxr-xr-x   3 ftp      ftp          4096 Jan 27  2012 office
| drwxr-xr-x   3 ftp      ftp          4096 Jul 31 07:04 patches
| drwxr-xr-x   5 ftp      ftp          4096 Jan 27  2012 publishing
| drwxr-xr-x   2 ftp      ftp          4096 Jan 27  2012 security
| drwxr-xr-x   5 ftp      ftp          4096 Sep 24  2011 shells
| drwxr-xr-x   5 ftp      ftp          4096 Sep 24  2011 sysutils
| drwxr-xr-x   7 ftp      ftp          4096 Sep 24  2011 telephony
| drwxr-xr-x   3 ftp      ftp          4096 Sep 24  2011 terminal
| drwxr-xr-x   3 ftp      ftp          4096 Sep 24  2011 text
|_drwxr-xr-x   3 ftp      ftp          4096 Mar 12  2014 video
|_ftp-bounce: bounce working!
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|_  2048 28:0e:4e:46:17:d6:f6:3c:20:0a:52:f7:1d:71:3f:4c (RSA)
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
```

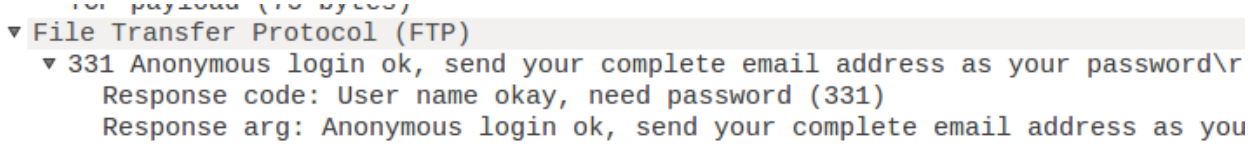
```
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      39633/tcp  mountd
|   100005  1,2,3      49106/udp  mountd
|   100021  1,3,4      36362/udp  nlockmgr
|   100021  1,3,4      45867/tcp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
139/tcp open  netbios-ssn Samba smbd
445/tcp open  netbios-ssn Samba smbd
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| nbstat: NetBIOS name: FILESERV, NetBIOS user: <unknown>, NetBIOS MAC: <unknown
> (unknown)
| Names:
|   FILESERV<00>         Flags: <unique><active>
|   FILESERV<03>         Flags: <unique><active>
|   FILESERV<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   SFEDU<00>            Flags: <group><active>
|   SFEDU<1d>            Flags: <unique><active>
|_  SFEDU<1e>            Flags: <group><active>

NSE: Script Post-scanning.
```

```
NSE: Script Post-scanning.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.83 seconds
```

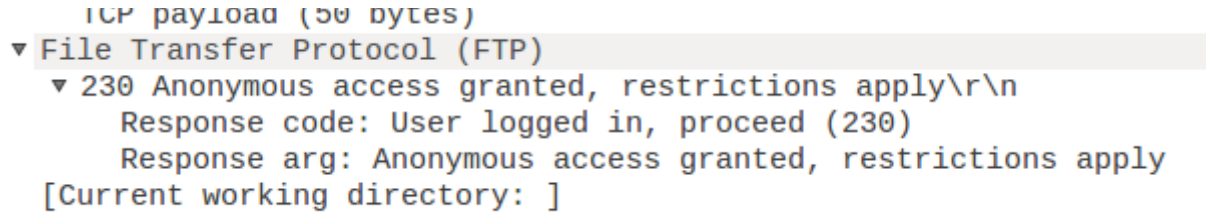
4. Фильтруем пакеты, чтобы отображались только связанные с протоколом FTP.
5. Проанализируем выбранные пакеты.



Производится обмен пакетами между IP-адресом 195.208.245.253 и второй виртуальной машиной, сканирующей этот адрес. Каждый из этих двух адресов переменно как отправляет, так и получает пакеты.



Логин анонимный, но для пароля нужно использовать адрес электронной почты.



Таким образом мы получили анонимный доступ к FTP-серверу.

Выводы по выполненной работе: мы получили практические и теоретические навыки работы с Honeypot, способами и методами сканирования сети.