

## Лабораторная работа. Honeypot, Nmap

Цель работы: получить практические и теоретические навыки работы с honeypot, способами и методами сканирования сети

### Вариант 2

Подсеть 1 машины : 10.10.10.18 / 27

Подсеть 2 машины : 10.10.10.19 / 27

Редактор виртуальной сети

| Имя    | Тип        | Внешнее подключение | Подключение узла | DHCP     | Адрес подсети |
|--------|------------|---------------------|------------------|----------|---------------|
| VMnet0 | Другой     | -                   | -                | -        | 192.168.174.0 |
| VMnet1 | Только ... | -                   | Подключено       | -        | 192.168.56.0  |
| VMnet8 | NAT        | NAT                 | Подключено       | Включено | 10.10.10.0    |

Добавить сеть... Удалить сеть Переименовать сеть...

Информация о VMnet

☐ Мост (подключение виртуальных машин непосредственно к внешней сети)

Мост к: Автонастройка...

☒ NAT (общий IP-адрес узла с виртуальной машиной) Параметры NAT...

☐ Только для узла (подключение виртуальных машин внутри частной сети)

☒ Подключить виртуальный адаптер узла к этой сети

Имя виртуального адаптера узла: Сетевой адаптер VMware VMnet8

☒ Использовать локальную службу DHCP для распространения IP-адресов для виртуальных машин Параметры DHCP...

IP-адрес подсети: 10 . 10 . 10 . 0 Маска подсети: 255 . 255 . 255 . 224

Настраиваю Nat 10.10.10.0

Сеть: vmnet8

IP-адрес подсети: 10.10.10.0

Маска подсети: 255.255.255.224

IP-адрес шлюза: 10 . 10 . 10 . 10

Поразрядный порт

Gateway 10.10.10.10

DNS-сервера

Предпочтительный DNS-сервер: 10 . 10 . 10 . 10

DNS 10.10.10.10

Dhcp включен

```

user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group 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 1141sec preferred_lft 1141sec
    inet6 fe80::bf4f:8c40:2a4:8d5c/64 scope link
        valid_lft forever preferred_lft forever

```

Определяю адрес подсети 2 машины

```

user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group default qlen 1000
    link/ether 00:0c:29:6d:da:09 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.18/27 brd 10.10.10.31 scope global dynamic ens33
        valid_lft 1642sec preferred_lft 1642sec
    inet6 fe80::adf6:cc43:f1b:f3c9/64 scope link
        valid_lft forever preferred_lft forever

```

Определяю адрес подсети 1 машины

```

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"

bind 10.10.10.11 windows
bind 10.10.10.12 template2
bind 10.10.10.13 router

```

```

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"

bind 10.10.10.14 windows
bind 10.10.10.15 template2
bind 10.10.10.16 router

```

Настраиваю ip адреса виртуальных точек в том же диапазоне, что и ip адрес виртуальной машины

```
user@user-VirtualBox:~$ sudo nmap -sT 10.10.10.18

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-22 18:26 MSK
Nmap scan report for 10.10.10.18
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

user@user-VirtualBox:~$ nmap -sR 10.10.10.19
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 2020-12-22 18:59 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00011s 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: 1 IP address (1 host up) scanned in 1.61 seconds
```

Произвожу изучение средств сканирования nmap

```
user@user-VirtualBox:~$ sudo farpd -d
arpd[22410]: listening on ens33: arp and not ether src 00:0c:29:4f:8c:67
arpd[22410]: arpd_lookup: 10.10.10.19 at 00:0c:29:4f:8c:67

user@user-VirtualBox: ~
user@user-VirtualBox:~$ sudo honeyd -d -f /etc/honeypot/honeyd.conf
[sudo] password for user:
Honeyd V1.5c Copyright (c) 2002-2007 Niels Provos
honeyd[22445]: started with -d -f /etc/honeypot/honeyd.conf
honeyd[22445]: listening promiscuously on ens33: (arp or ip proto 47 or (udp and
src port 67 and dst port 68) or (ip )) and not ether src 00:0c:29:4f:8c:67
honeyd[22445]: Demoting process privileges to uid 65534, gid 65534
```

запускаю на 2 виртуальной машине Honeypot для сканирования ip адресов с помощью nmap

На 1 виртуальной машине произвожу сканирование ip адресов с помощью nmap

TCP Connect

```

user@user-VirtualBox:~$ sudo nmap -sT 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:13 MSK
Nmap scan report for 10.10.10.19
Host is up (0.0023s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

```

22 порт открыт, остальные 999 закрыты

TCP-SYN

```

user@user-VirtualBox:~$ sudo nmap -sS 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:15 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00022s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5510/tcp  filtered secureidprop
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds

```

22 и 5510 порт открыт и фильтруется соответственно, 998 закрыты

Сканирования FIN, Xmas Tree и NULL

```

user@user-VirtualBox:~$ sudo nmap -sF 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:51 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00058s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 87.73 seconds

```

```

user@user-VirtualBox:~$ sudo nmap -sX 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:53 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00061s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 88.93 seconds

```

```

user@user-VirtualBox:~$ sudo nmap -sN 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:55 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00056s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 88.32 seconds

```

Отправка пакетов с отключенными флагами в заголовке TCP

Сканирование протоколов IP

```

user@user-VirtualBox:~$ sudo nmap -sO 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:45 MSK
Warning: 10.10.10.19 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.19
Host is up (0.00056s latency).
Not shown: 247 closed protocols
PROTOCOL  STATE      SERVICE
1         open      icmp
2         open|filtered igmp
6         open      tcp
17        open      udp
41        open|filtered ipv6
103       open|filtered pim
106       open|filtered qnx
136       open|filtered udplite
255       open|filtered unknown
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 301.57 seconds

```

Хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. 247 недоступных протоколов = не поддерживаются хостом. Остальные — поддерживаются.

ACK-сканирование

```

user@user-VirtualBox:~$ sudo nmap -sA 10.10.10.19
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:41 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00018s latency).
All 1000 scanned ports on 10.10.10.19 are unfiltered
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
user@user-VirtualBox:~$ sudo nmap -sO 10.10.10.19

```

Передаю ACK пакеты на сканируемые порты.  
Порты классифицируются как не фильтруемые.

TCP Window



```

user@user-VirtualBox:~$ sudo nmap -sW 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:57 MSK
Nmap scan report for 10.10.10.19
Host is up (0.0014s latency).
All 1000 scanned ports on 10.10.10.19 are closed
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds

```

Открытых портов нет, все закрыты

## RPC-сканирование

```

user@user-VirtualBox:~$ sudo nmap -sR 10.10.10.19
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 2020-12-25 16:16 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00011s 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:29:4F:8C:67 (VMware)
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: 1 IP address (1 host up) scanned in 2.32 seconds

```

22 обслуживающий порт

ос Ubuntu v 2.10

Сканирование ОС

```

user@user-VirtualBox:~$ sudo nmap -O 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 16:11 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00054s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)
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=12/25%OT=22%CT=1%CU=37389%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=5FE5E508%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10E%TI=Z%CI=Z%TS=
OS:A)SEQ(SP=106%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B
OS:4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W
OS:1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%
OS:O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=
OS:N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.73 seconds

```

сканирование для определения ос на сканируемом хосте ( на данном скрине не определилось)

Добавляю 2 дополнительные ловушки

```
create CatchMe2
set CatchMe2 personality "Linux 1.0.9"
set CatchMe2 default tcp action reset
add CatchMe2 tcp port 28 "/usr/share/honeyd/scripts/router-telnet.pl"
add CatchMe2 tcp port 24 "/usr/share/honeyd/scripts/ftp.sh"
```

```
create CatchMe1
set CatchMe1 personality "Microsoft Windows 98SE"
set CatchMe1 default tcp action reset
add CatchMe1 tcp port 15 "/usr/share/honeyd/scripts/test.sh"
add CatchMe1 tcp port 18 "/usr/share/honeyd/scripts/router-telnet.pl"
```

```
create CatchMe1
set CatchMe1 personality "Microsoft Windows 98SE"
set CatchMe1 default tcp action reset
add CatchMe1 tcp port 15 "/usr/share/honeyd/scripts/test.sh"
add CatchMe1 tcp port 18 "/usr/share/honeyd/scripts/router-telnet.pl"
```

```
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 CatchMe2 ethernet "00:00:24:ab:8c:40"
set CatchMe1 ethernet "00:00:24:ab:8c:50"
```

```
bind 10.10.10.11 windows
bind 10.10.10.12 template2
bind 10.10.10.13 router
bind 10.10.10.17 CatchMe2
bind 10.10.10.18 CatchMe1
```

```
user@user-VirtualBox:~$ sudo honeyd -d -f /etc/honeypot/honeyd.conf
Honeyd V1.5c Copyright (c) 2002-2007 Niels Provos
honeyd[26889]: started with -d -f /etc/honeypot/honeyd.conf
honeyd[26889]: listening promiscuously on ens33: (arp or ip proto 47 or (udp and
src port 67 and dst port 68) or (ip )) and not ether src 00:0c:29:4f:8c:67
honeyd[26889]: Demoting process privileges to uid 65534, gid 65534
```

```
user@user-VirtualBox: ~
```

```
user@user-VirtualBox:~$ sudo farpd -d
[sudo] password for user:
arpd[26634]: listening on ens33: arp and not ether src 00:0c:29:4f:8c:67
arpd[26634]: arpd_lookup: 10.10.10.19 at 00:0c:29:4f:8c:67
arpd[26634]: arpd_lookup: no entry for 10.10.10.30
arpd[26634]: arpd_send: who-has 10.10.10.30 tell 10.10.10.19
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_send: who-has 10.10.10.30 tell 10.10.10.19
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.30 at 00:50:56:e2:19:70
arpd[26634]: arpd_rcv_cb: 10.10.10.19 is allocated
```

```
user@user-VirtualBox:~$ sudo nmap -sT 10.10.10.19
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:13 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00047s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sS 10.10.10.19

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:13 MSK
Nmap scan report for 10.10.10.19
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```



```
user@user-VirtualBox:~$ sudo nmap -sF 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:14 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00054s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 8.75 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sX 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:14 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00038s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sN 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:14 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00033s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sO 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:15 MSK
Warning: 10.10.10.19 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.19
Host is up (0.00061s latency).
Not shown: 249 closed protocols
PROTOCOL  STATE      SERVICE
1         open       icmp
2         open|filtered igmp
6         open       tcp
17        open       udp
103       open|filtered pim
136       open|filtered udplite
255       open|filtered unknown
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 289.51 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sA 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:26 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00027s latency).
All 1000 scanned ports on 10.10.10.19 are unfiltered
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sW 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:27 MSK
Nmap scan report for 10.10.10.19
Host is up (0.00022s latency).
All 1000 scanned ports on 10.10.10.19 are closed
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -sR 10.10.10.19
```

```
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 2020-12-25 23:27 MSK
```

```
Nmap scan report for 10.10.10.19
```

```
Host is up (0.0014s 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:29:4F:8C:67 (VMware)
```

```
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: 1 IP address (1 host up) scanned in 2.83 seconds
```

```
user@user-VirtualBox:~$ sudo nmap -O 10.10.10.19
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-25 23:27 MSK
```

```
Nmap scan report for 10.10.10.19
```

```
Host is up (0.00054s latency).
```

```
Not shown: 999 closed ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
MAC Address: 00:0C:29:4F:8C:67 (VMware)
```

```
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=12/25%OT=22%CT=1%CU=39041%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=5FE64B4F%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=101%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=FC%GCD=1%ISR=101%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4S
OS:T11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=
OS:FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=
OS:M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

```
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
```

После изменения конфиг. файла при повторном сканировании изменилось только отсутствие интернет-протокола ipv6

Part 2

```
C:\Users\HONOR>nmap -T4 -A -v 195.208.245.253
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-26 00:39 RTZ 2 (ceia)
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating Ping Scan at 00:39
```

Провожу сканирование ip адреса 195.208.245.253

| ftp  |            |                 |                 |          |    |
|------|------------|-----------------|-----------------|----------|----|
| No.  | Time       | Source          | Destination     | Protocol | Le |
| 7033 | 116.746691 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7397 | 130.570606 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7398 | 130.572039 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7399 | 130.574490 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7405 | 130.617062 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7409 | 130.618878 | 192.168.1.52    | 195.208.245.253 | FTP      |    |
| 7410 | 130.619024 | 192.168.1.52    | 195.208.245.253 | FTP      |    |
| 7412 | 130.619234 | 192.168.1.52    | 195.208.245.253 | FTP      |    |
| 7413 | 130.623894 | 192.168.1.52    | 195.208.245.253 | FTP      |    |
| 7420 | 130.666417 | 195.208.245.253 | 192.168.1.52    | FTP      |    |
| 7422 | 130.666417 | 195.208.245.253 | 192.168.1.52    | FTP      |    |

перехватываю пакеты ftp с помощью wireshark

```
Response: 220 ProFTPD 1.3.5b Server (FTP Server of Rostov State University - only anonymous logins are allowed) [195.208.245.253]
Response: 220 ProFTPD 1.3.5b Server (FTP Server of Rostov State University - only anonymous logins are allowed) [195.208.245.253]
Response: 220 ProFTPD 1.3.5b Server (FTP Server of Rostov State University - only anonymous logins are allowed) [195.208.245.253]
Response: 220 ProFTPD 1.3.5b Server (FTP Server of Rostov State University - only anonymous logins are allowed) [195.208.245.253]
Request: USER anonymous
Request: AUTH TLS
Request: USER anonymous
Request: SYST
Response: 500 AUTH not understood
Response: 331 Anonymous login ok, send your complete email address as your password
Response: 331 Anonymous login ok, send your complete email address as your password
Response: 215 UNIX Type: L8
Request: PASS IEUser@
Request: QUIT
Request: PASS IEUser@
Request: STAT
Response: 221 Goodbye.
Response: 230 Anonymous access granted, restrictions apply
Response: 230 Anonymous access granted, restrictions apply
Response: 530 Please login with USER and PASS
Request: PORT 45,33,32,156,80,80
Request: PASV
Request: QUIT
Response: 501 Illegal PORT command
Response: 227 Entering Passive Mode (195,208,245,253,171,203).
Response: 221 Goodbye.
```

Сервер пишет, что могут быть только анонимные пользователи  
заходим от анонимного пользователя  
вводим пароль  
Пользователь заканчивает работу с сервером  
Потом пользователь пытается войти, но не удается  
(Используя анонимного пользователя ,пароль IEUser@)

Вопросы:

- 1) Статический IP-адрес — это IP-адрес, который был вручную настроен для устройства, а не тот, который был назначен через DHCP — сервер.  
Динамический IP-адрес — это IP-адрес, который автоматически назначается каждому соединению или узлу сети, например вашему смартфону, настольному ПК или беспроводному планшету. Это автоматическое назначение IP-адресов выполняется так называемым DHCP— сервером.  
Динамические IP-адреса куда безопаснее для начинающих пользователей.  
Например, если кто-нибудь примется взламывать мой сетевой узел для получения доступа к компьютеру, после такой элементарной процедуры, как перезагрузка роутера, злоумышленник будет вынужден заново узнавать мой IP-адрес и заниматься взломом фактически с нуля.  
При авторизации на сайтах интернет-банков и в других ресурсах, требующих максимальной защиты информации, существует возможность привязки логина (учетной записи) к определенному IP. И если даже сторонние лица узнают мой пароль, они вряд ли смогут получить доступ к секретным данным, поскольку это будет возможно исключительно с моего IP.
- 2) Метод сканирование протоколов IP заключается в получении информации о машине.
- 3) На пакеты FIN, Xmas Tree и NULL большинство ОС должны ответить флагом RST.
- 4) Основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.  
Хакер сканирует сервер, не зная, что подключённые к нему машины всего лишь ловушки, тем самым получая неверную информацию об устройстве. Поэтому процесс взлома затрудняется.
- 5) Целью злоумышленников является получение информации (для продажи).
- 6) Большое количество открытых портов является подозрением на ловушку для злоумышленника.
- 7) Основные методы сканирования : TCP Connect (сканирующая машина пытается установить соединение со сканируемой), TCP-SYN (посылает SYN-пакет, как бы ради того, чтобы установить новое соединение), сканирования FIN, Xmas Tree и NULL (альтернатива TCP SYN), сканирование протоколов IP (хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста), ACK-сканирование (передача ACK пакетов на сканируемый порт), TCP Window (аналогично ACK-сканированию), RPC-сканирование (для определения

программы, обслуживающей порт и её версии), Сканирование ОС (для определения ОС на сканируемом хосте).

Вывод : изучил средства сканирования nmap, научился создавать ловушки, научился перенимать логин и пароль по протоколу ftp.