Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Отчёт по лабораторной работе №2
«Идентификация узлов и портов сетевых служб»

Выполнил студент группы МС-42: Казак И.В.

Проверил:

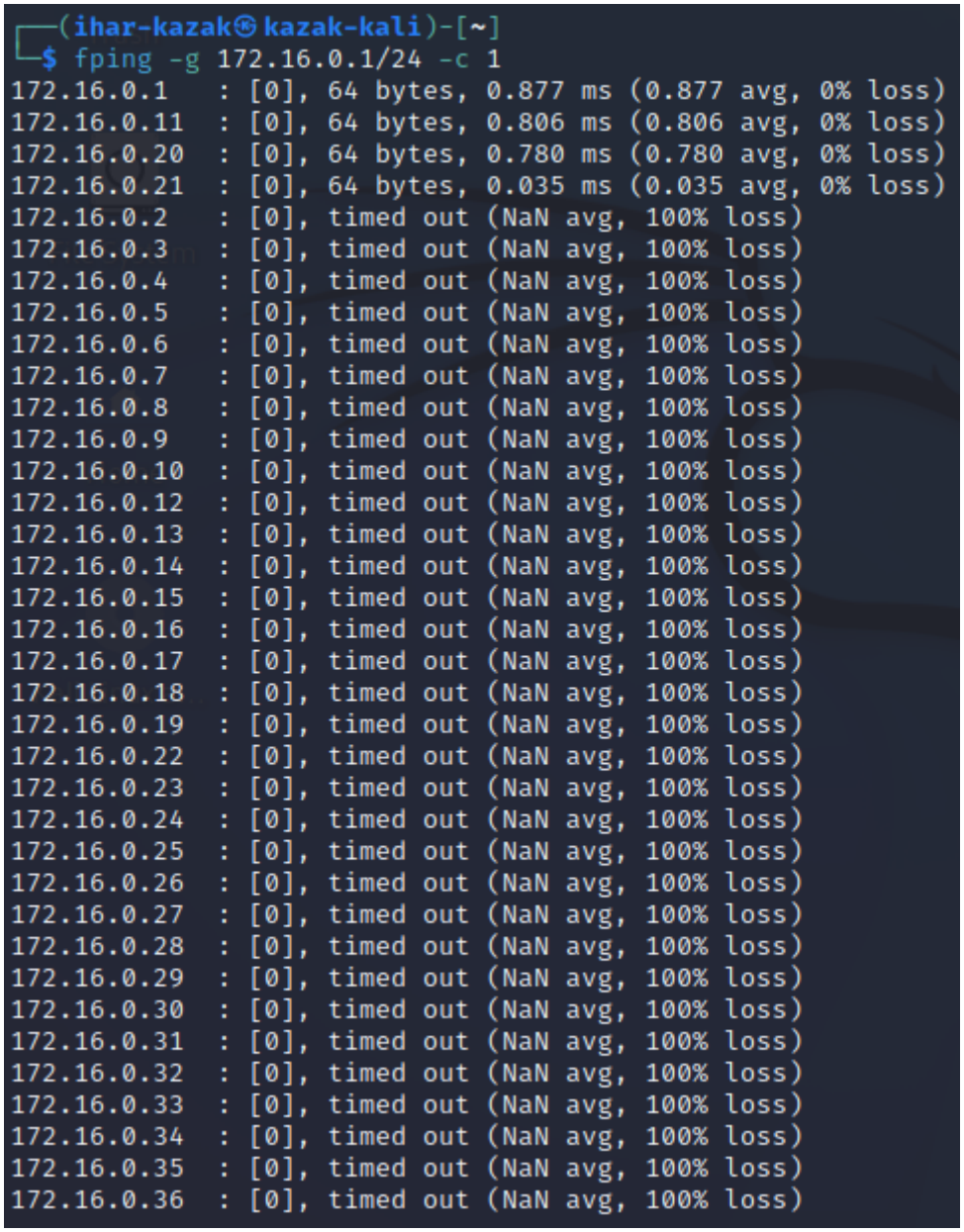
Старший преподаватель Грищенко В.В.

Гомель 2022

Цель работы: обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

Ход работы.

Шаг 1. Выполним идентификацию узлов с помощью средства fping для сети **172.16.0.1/24**. Просмотрим трассировку сканирования с помощью команды **fping –g 172.16.0.1/24 –c 1**



Шаг 2. С помощью сетевого сканера nmap выполним идентификацию узлов методом **ARP Scan**. Просмотрим трассировку сканирования: **nmap –sn 172.16.0.1/24**

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ nmap -sn 172.16.0.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-26 19:14 +03
Nmap scan report for 172.16.0.1
Host is up (0.0037s latency).
Nmap scan report for 172.16.0.21
Host is up (0.00088s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 20.25 seconds
```

Шаг 3. С помощью средства hping2 выполним идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request.

Например, **hping3 –C 13 172.16.0.20**. Просмотрим трассировку сканирования.

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo hping3 -C 13 172.16.0.20
HPING 172.16.0.20 (eth0 172.16.0.20): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.0.20 ttl=128 id=598 icmp_seq=0 rtt=7.7 ms
ICMP timestamp: Originate=59880075 Receive=1271093763 Transmit=1271093763
ICMP timestamp RTT tsrtt=7

len=46 ip=172.16.0.20 ttl=128 id=599 icmp_seq=1 rtt=13.8 ms
ICMP timestamp: Originate=59881102 Receive=1388796419 Transmit=1388796419
ICMP timestamp RTT tsrtt=14

len=46 ip=172.16.0.20 ttl=128 id=600 icmp_seq=2 rtt=5.7 ms
ICMP timestamp: Originate=59882149 Receive=1691048451 Transmit=1691048451
ICMP timestamp RTT tsrtt=5

len=46 ip=172.16.0.20 ttl=128 id=601 icmp_seq=3 rtt=4.7 ms
ICMP timestamp: Originate=59883149 Receive=1305434627 Transmit=1305434627
ICMP timestamp RTT tsrtt=5

len=46 ip=172.16.0.20 ttl=128 id=602 icmp_seq=4 rtt=7.4 ms
ICMP timestamp: Originate=59884162 Receive=1087592963 Transmit=1087592963
ICMP timestamp RTT tsrtt=8

len=46 ip=172.16.0.20 ttl=128 id=603 icmp_seq=5 rtt=3.1 ms
ICMP timestamp: Originate=59885163 Receive=718756355 Transmit=718756355
ICMP timestamp RTT tsrtt=3

len=46 ip=172.16.0.20 ttl=128 id=604 icmp_seq=6 rtt=3.0 ms
ICMP timestamp: Originate=59886163 Receive=333142531 Transmit=333142531
ICMP timestamp RTT tsrtt=3

len=46 ip=172.16.0.20 ttl=128 id=605 icmp_seq=7 rtt=2.2 ms
ICMP timestamp: Originate=59887164 Receive=4259207683 Transmit=4259207683
ICMP timestamp RTT tsrtt=3

^C
— 172.16.0.20 hping statistic —
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 2.2/6.0/13.8 ms
```

Шаг 4. С помощью средств **hping2** и **nmap** выполним идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.

Например, **nmap –PS –sU –p 111 172.16.0.20**

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo nmap -PS -sU -p 111 172.16.0.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-26 20:52 +03
Nmap scan report for 172.16.0.20
Host is up (0.00065s latency).

PORT    STATE  SERVICE
111/udp closed rpcbind
MAC Address: 08:00:27:9F:62:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.98 seconds
```

Шаг 5. На узле с помощью сетевого сканера nmap выполним идентификацию открытых TCP и UDP портов найденных узлов IP-сети **172.16.0.1/24**, используя основные методы сканирования.
Например: **nmap –sS –n 172.16.0.11,**
nmap –sS –n 172.16.0.20.

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo nmap -sS -n 172.16.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-26 20:41 +03
Nmap scan report for 172.16.0.11
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:6E:60:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo nmap -sS -n 172.16.0.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-26 19:39 +03
Nmap scan report for 172.16.0.20
Host is up (0.00025s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:9F:62:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

Вывод: в ходе лабораторной работы познакомились, а также воспользовались методами и средствами идентификации доступных узлов и сетевых портов в анализируемой КС.