Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №2

«Идентификация узлов и портов сетевых служб»

Выполнил:
Студент группы МС-42
Созинов Л.В.
Проверил:
Грищенко В.В.

2022

Лабораторная работа №2
Идентификация узлов и портов сетевых служб

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

Ход работы

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

```
┌──(skali㉿kali)-[~]
└─$ fping -g 172.16.0.1/24 -c 1
172.16.0.1   : [0], 64 bytes, 0.447 ms (0.447 avg, 0% loss)
172.16.0.11  : [0], 64 bytes, 0.051 ms (0.051 avg, 0% loss)
172.16.0.2   : [0], timed out (NaN avg, 100% loss)
172.16.0.3   : [0], timed out (NaN avg, 100% loss)
172.16.0.4   : [0], timed out (NaN avg, 100% loss)
172.16.0.5   : [0], timed out (NaN avg, 100% loss)
172.16.0.6   : [0], timed out (NaN avg, 100% loss)
172.16.0.7   : [0], timed out (NaN avg, 100% loss)
172.16.0.8   : [0], timed out (NaN avg, 100% loss)
172.16.0.9   : [0], timed out (NaN avg, 100% loss)
172.16.0.10  : [0], timed out (NaN avg, 100% loss)
172.16.0.12  : [0], timed out (NaN avg, 100% loss)
172.16.0.13  : [0], timed out (NaN avg, 100% loss)
172.16.0.14  : [0], timed out (NaN avg, 100% loss)
172.16.0.15  : [0], timed out (NaN avg, 100% loss)
172.16.0.16  : [0], timed out (NaN avg, 100% loss)
172.16.0.17  : [0], timed out (NaN avg, 100% loss)
172.16.0.18  : [0], timed out (NaN avg, 100% loss)
172.16.0.19  : [0], timed out (NaN avg, 100% loss)
172.16.0.20  : [0], timed out (NaN avg, 100% loss)
172.16.0.21  : [0], timed out (NaN avg, 100% loss)
172.16.0.22  : [0], timed out (NaN avg, 100% loss)
172.16.0.23  : [0], timed out (NaN avg, 100% loss)
172.16.0.24  : [0], timed out (NaN avg, 100% loss)
172.16.0.25  : [0], timed out (NaN avg, 100% loss)
```

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

```
┌──(skali㉿kali)-[~]
└─$ nmap -sn 172.16.0.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 00:59 MSK
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.0.1
Host is up (0.0031s latency).
Nmap scan report for 172.16.0.11
Host is up (0.0041s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.56 seconds
```

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

```
┌──(skali㉿kali)-[~]
└─$ sudo hping3 -c 13 172.16.0.1
[sudo] пароль для skali:
HPING 172.16.0.1 (eth0 172.16.0.1): NO FLAGS are set, 40 headers + 0 data byt
es
len=46 ip=172.16.0.1 ttl=128 id=3980 sport=0 flags=RA seq=0 win=0 rtt=7.4 ms
len=46 ip=172.16.0.1 ttl=128 id=3985 sport=0 flags=RA seq=1 win=0 rtt=7.1 ms
len=46 ip=172.16.0.1 ttl=128 id=3986 sport=0 flags=RA seq=2 win=0 rtt=7.0 ms
len=46 ip=172.16.0.1 ttl=128 id=3987 sport=0 flags=RA seq=3 win=0 rtt=6.1 ms
len=46 ip=172.16.0.1 ttl=128 id=3988 sport=0 flags=RA seq=4 win=0 rtt=6.0 ms
len=46 ip=172.16.0.1 ttl=128 id=3989 sport=0 flags=RA seq=5 win=0 rtt=5.5 ms
len=46 ip=172.16.0.1 ttl=128 id=3990 sport=0 flags=RA seq=6 win=0 rtt=5.1 ms
```

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

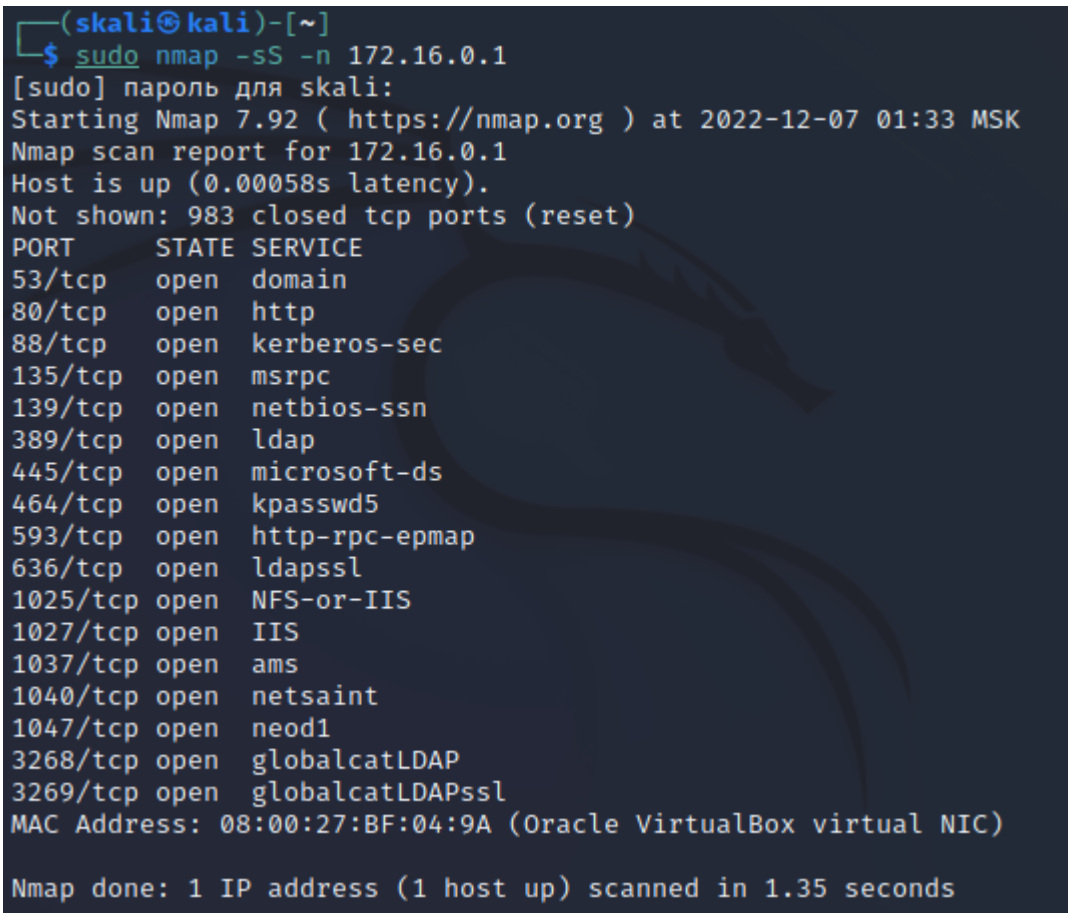
```
┌──(skali㉿kali)-[~]
└─$ sudo hping3 -2 -d 53 172.16.0.1
HPING 172.16.0.1 (eth0 172.16.0.1): udp mode set, 28 headers + 53 data bytes
ICMP Port Unreachable from ip=172.16.0.1 name=UNKNOWN
status=0 port=1459 seq=0
ICMP Port Unreachable from ip=172.16.0.1 name=UNKNOWN
status=0 port=1460 seq=1
ICMP Port Unreachable from ip=172.16.0.1 name=UNKNOWN
status=0 port=1461 seq=2
ICMP Port Unreachable from ip=172.16.0.1 name=UNKNOWN
status=0 port=1462 seq=3
```

```
┌──(skali㉿kali)-[~]
└─$ sudo nmap -PS -sU -p 111 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 01:15 MSK
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.0.1
Host is up (0.00056s latency).

PORT    STATE  SERVICE
111/udp closed rpcbind
MAC Address: 08:00:27:BF:04:9A (Oracle VirtualBox virtual NIC)

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

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.


┌──(skali㉿kali)-[~]
└─$ sudo nmap -sS -n 172.16.0.1
[sudo] пароль для skali:
Starting Nmap 7.92 (https://nmap.org) at 2022-12-07 01:33 MSK
Nmap scan report for 172.16.0.1
Host is up (0.00058s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1025/tcp open NFS-or-IIS
1027/tcp open IIS
1037/tcp open ams
1040/tcp open netsaint
1047/tcp open neod1
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
MAC Address: 08:00:27:BF:04:9A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds