

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
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

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 **172.16.0.0/24**. Просмотрим трассировку сканирования с помощью команды `fping -g 172.16.0.0/24 -c 1`

```
(alex@kali)-[~]
$ fping -g 172.16.0.0/24 -c1
172.16.0.1 : [0], 64 bytes, 1.47 ms (1.47 avg, 0% loss)
172.16.0.10 : [0], 64 bytes, 0.023 ms (0.023 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)
172.16.0.11 : [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)
172.16.0.26 : [0], timed out (NaN avg, 100% loss)
172.16.0.27 : [0], timed out (NaN avg, 100% loss)
172.16.0.28 : [0], timed out (NaN avg, 100% loss)
172.16.0.29 : [0], timed out (NaN avg, 100% loss)
172.16.0.30 : [0], timed out (NaN avg, 100% loss)
```

Шаг 2. С помощью сетевого сканера `nmap` выполним идентификацию узлов методом ARP Scan. Просмотрим трассировку сканирования:
`nmap -sn 172.16.0.0/24`

```
(alex@kali)-[~]
$ nmap -sn 172.16.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 00:54 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.0022s latency).
Nmap scan report for 172.16.0.10
Host is up (0.00012s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.74 seconds
```

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

Например: **hping3 -C 13 172.16.0.1.**

```
(alex@kali)-[~]
$ sudo hping3 -C 13 172.16.0.1
HPING 172.16.0.1 (eth0 172.16.0.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.0.1 ttl=128 id=5023 icmp_seq=0 rtt=3.6 ms
ICMP timestamp: Originate=79047717 Receive=690664964 Transmit=690664964
ICMP timestamp RTT tsrtt=3

len=46 ip=172.16.0.1 ttl=128 id=5024 icmp_seq=1 rtt=3.9 ms
ICMP timestamp: Originate=79048717 Receive=305051140 Transmit=305051140
ICMP timestamp RTT tsrtt=4

len=46 ip=172.16.0.1 ttl=128 id=5025 icmp_seq=2 rtt=3.8 ms
ICMP timestamp: Originate=79049717 Receive=4231116292 Transmit=4231116292
ICMP timestamp RTT tsrtt=4

len=46 ip=172.16.0.1 ttl=128 id=5026 icmp_seq=3 rtt=3.1 ms
ICMP timestamp: Originate=79050718 Receive=3845502468 Transmit=3845502468
ICMP timestamp RTT tsrtt=3

^C
— 172.16.0.1 hping statistic —
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 3.1/3.6/3.9 ms
```

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

Например: **Hping3 -2 -d 53 172.16.0.1, nmap -PS -sU -p 111 172.16.0.1**

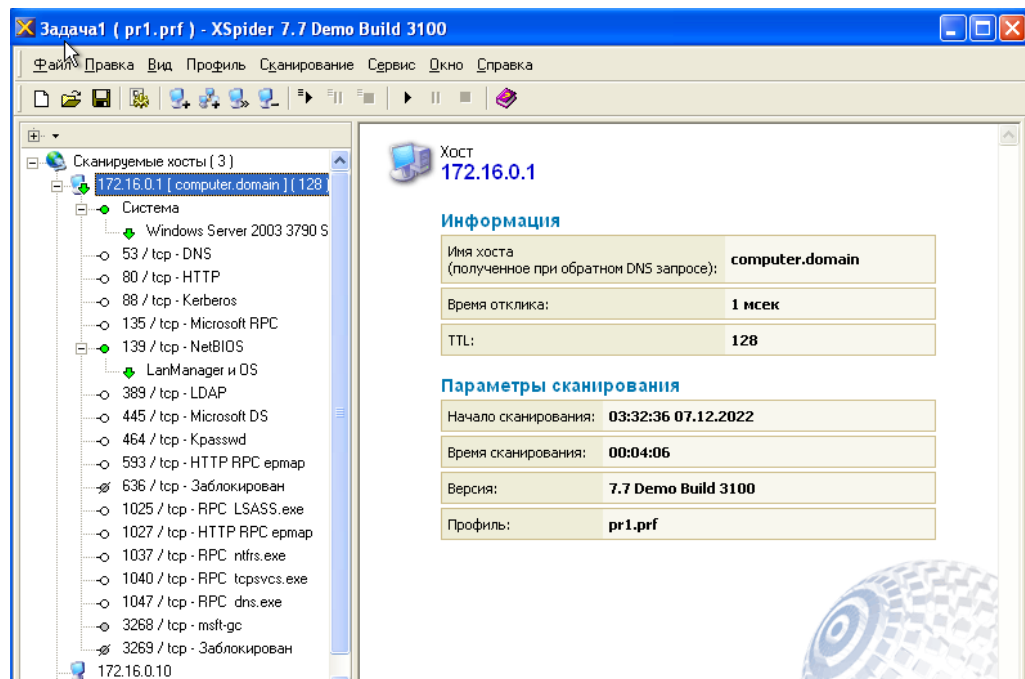
```
(alex@kali)-[~]
$ sudo hping3 -2 -d 53 172.16.0.1
HPING 172.16.0.1 (eth0 172.16.0.1): udp mode set, 28 headers + 53 data bytes
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1968 seq=0
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1969 seq=1
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1970 seq=2
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1971 seq=3
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1972 seq=4
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1973 seq=5
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1974 seq=6
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=1975 seq=7
^C
— 172.16.0.1 hping statistic —
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 1.3/5.2/9.1 ms

(alex@kali)-[~]
$ sudo nmap -PS -sU -p 111 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 01:05 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.00073s latency).

PORT      STATE SERVICE
111/udp   closed rpcbind
MAC Address: 08:00:27:A5:DC:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Шаг 5. На узле TWS2 запустить сканер безопасности XSpider. Создать новый профиль, выбрав параметры ICMP ping и TCP ping, в секции «Сканер UDP сервисов» отключить опцию «Сканировать UDP порты», в секции «Сканер уязвимостей» отключить опцию «Искать уязвимости». Указать диапазон IP-адресов. Выполнить сканирование сети.



Шаг 6. На узле с помощью сетевого сканера nmap выполним идентификацию открытых TCP и UDP портов найденных узлов IP-сети 172.16.0.0/24, используя основные методы сканирования.

Например: **nmap -sS -n 172.16.0.1**

```
(alex@kali)-[~]
$ sudo nmap -sS -n 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 01:08 MSK
Nmap scan report for 172.16.0.1
Host is up (0.00048s 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
1048/tcp  open  neod2
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 08:00:27:A5:DC:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

Вывод: в ходе лабораторной работы ознакомились с методами и средствами идентификации доступных узлов и сетевых портов в анализируемой КС.