

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
Кнышев Н.В.
Проверил: Грищенко В.В.

2022

Лабораторная работа №2

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

Постановка задачи: выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

Шаг 1. Выполнить идентификацию узлов с помощью средства `fping` для сети 172.16.0.0/24. Просмотреть трассировку сканирования:

```
└─$ fping -g 172.16.0.0/24 -c1
172.16.0.1 : [0], 64 bytes, 0.486 ms (0.486 avg, 0% loss)
172.16.0.17 : [0], 64 bytes, 0.209 ms (0.209 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)
```

Шаг 2. С помощью сетевого сканера `nmap` выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования:

```
└─$ nmap -sn 172.16.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 09:30 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.0017s latency).
Nmap scan report for 172.16.0.17
Host is up (0.0024s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 13.57 seconds
```

Шаг 3. С помощью средства `hping2` выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request, просмотреть трассировку сканирования:

```
└─$ sudo hping3 -C 13 172.16.0.1
[sudo] пароль для nikita:
HPING 172.16.0.1 (eth0 172.16.0.1): icmp mode set, 28 headers + 0 data byte
len=46 ip=172.16.0.1 ttl=128 id=18641 icmp_seq=0 rtt=7.4 ms
ICMP timestamp: Originate=24385390 Receive=2045682947 Transmit=2045682947
ICMP timestamp RTT tsrtt=8

len=46 ip=172.16.0.1 ttl=128 id=18642 icmp_seq=1 rtt=7.8 ms
ICMP timestamp: Originate=24386390 Receive=1660069123 Transmit=1660069123
ICMP timestamp RTT tsrtt=8

len=46 ip=172.16.0.1 ttl=128 id=18643 icmp_seq=2 rtt=6.9 ms
ICMP timestamp: Originate=24387390 Receive=1274455299 Transmit=1274455299
ICMP timestamp RTT tsrtt=7

len=46 ip=172.16.0.1 ttl=128 id=18729 icmp_seq=3 rtt=6.1 ms
ICMP timestamp: Originate=24388391 Receive=905618691 Transmit=905618691
ICMP timestamp RTT tsrtt=6

len=46 ip=172.16.0.1 ttl=128 id=18730 icmp_seq=4 rtt=5.9 ms
ICMP timestamp: Originate=24389391 Receive=520004867 Transmit=520004867
ICMP timestamp RTT tsrtt=6

len=46 ip=172.16.0.1 ttl=128 id=18731 icmp_seq=5 rtt=4.9 ms
ICMP timestamp: Originate=24390392 Receive=134391299 Transmit=134391299
ICMP timestamp RTT tsrtt=5

len=46 ip=172.16.0.1 ttl=128 id=18732 icmp_seq=6 rtt=4.9 ms
ICMP timestamp: Originate=24391393 Receive=4043679235 Transmit=4043679235
ICMP timestamp RTT tsrtt=5
```

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

```

$ sudo hping3 -i 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=2270 seq=0
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2271 seq=1
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2272 seq=2
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2273 seq=3
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2274 seq=4
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2275 seq=5
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2276 seq=6
ICMP Port Unreachable from ip=172.16.0.1 name=server.pms.by
status=0 port=2277 seq=7

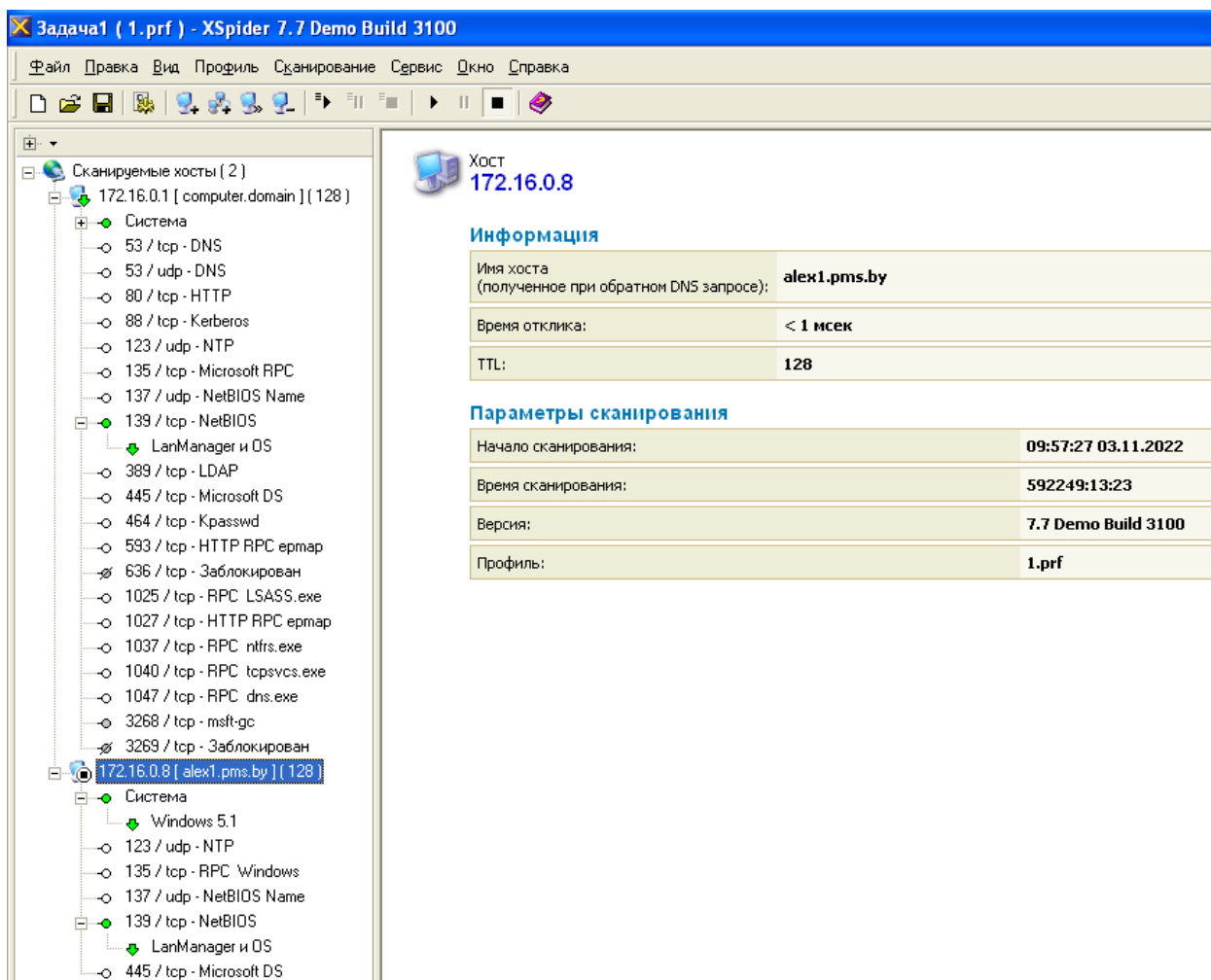
$ sudo hping3 -d 53 172.16.0.1
HPING 172.16.0.1 (eth0 172.16.0.1): NO FLAGS are set, 40 headers + 53 data bytes
len=46 ip=172.16.0.1 ttl=128 id=19295 sport=0 flags=RA seq=0 win=0 rtt=3.1 ms
len=46 ip=172.16.0.1 ttl=128 id=19296 sport=0 flags=RA seq=1 win=0 rtt=2.9 ms
len=46 ip=172.16.0.1 ttl=128 id=19297 sport=0 flags=RA seq=2 win=0 rtt=2.9 ms
len=46 ip=172.16.0.1 ttl=128 id=19298 sport=0 flags=RA seq=3 win=0 rtt=2.0 ms
len=46 ip=172.16.0.1 ttl=128 id=19299 sport=0 flags=RA seq=4 win=0 rtt=1.1 ms
len=46 ip=172.16.0.1 ttl=128 id=19300 sport=0 flags=RA seq=5 win=0 rtt=8.8 ms
len=46 ip=172.16.0.1 ttl=128 id=19301 sport=0 flags=RA seq=6 win=0 rtt=7.8 ms
len=46 ip=172.16.0.1 ttl=128 id=19302 sport=0 flags=RA seq=7 win=0 rtt=8.2 ms
len=46 ip=172.16.0.1 ttl=128 id=19303 sport=0 flags=RA seq=8 win=0 rtt=7.7 ms

$ sudo nmap -PS -sU -p 111 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 09:55 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.00061s latency).

PORT      STATE SERVICE
111/udp   closed rpcbind
MAC Address: 08:00:27:52:64:3A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.26 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 TWS1 с помощью сетевого сканера nmap выполнить идентификацию открытых TCP и UDP портов найденных узлов IP-сети 172.16.8.0/24, используя основные методы сканирования.

```
$ sudo nmap -sS -n 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 10:05 MSK
Nmap scan report for 172.16.0.1
Host is up (0.00029s 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: 08:00:27:52:64:3A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

$ sudo nmap -sS -n 172.16.0.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 10:10 MSK
Nmap scan report for 172.16.0.8
Host is up (0.00062s latency).
All 1000 scanned ports on 172.16.0.8 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B1:21:7C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
```

Вывод: в ходе лабораторной работы были получены знания о методах и средствах идентификации доступных узлов и сетевых портов в анализируемой КС, выполнена идентификация узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.