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: Баль П. М.
Проверил: Грищенко В. В.

2022

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

Цель работы: целью лабораторной работы является 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.

Последовательность действий

Шаг 1. Загрузим виртуальную машину TWS1. Войдём в систему. Настроим сетевые интерфейсы. Запустим анализатор протоколов tcpdump или wireshark.

Шаг 2. Выполним идентификацию узлов с помощью средства fping для сети 192.168.1.0/24:

```
k5-3-29-6@k5-3-29-6:~$ fping -g 192.168.1.0/24 -saq -c 1
192.168.1.1   : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.50/0.50/0.50
192.168.1.35  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.48/0.48/0.48
192.168.1.37  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.53/0.53/0.53
192.168.1.38  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.46/0.46/0.46
192.168.1.45  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.37/1.37/1.37
192.168.1.46  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.49/0.49/0.49
192.168.1.53  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.07/0.07/0.07
192.168.1.62  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 6.72/6.72/6.72
192.168.1.64  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.73/0.73/0.73
192.168.1.69  : xmt/rcv/%loss = 1/1/0%, min/avg/max = 71.3/71.3/71.3

     254 targets
      10 alive
     244 unreachable
       0 unknown addresses

     244 timeouts (waiting for response)
     254 ICMP Echos sent
      10 ICMP Echo Replies received
      44 other ICMP received

 0.07 ms (min round trip time)
 8.27 ms (avg round trip time)
 71.3 ms (max round trip time)
        3.583 sec (elapsed real time)
```

Шаг 3. С помощью сетевого сканера nmap выполним идентификацию узлов методом ARP Scan:

```
k5-3-29-6@k5-3-29-6:~$ nmap -sn 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-05 13:21 +03
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.00055s latency).
```

```
Nmap scan report for 192.168.1.35
Host is up (0.0020s latency).
Nmap scan report for 192.168.1.37
Host is up (0.00098s latency).
Nmap scan report for 192.168.1.38
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.46
Host is up (0.0016s latency).
Nmap scan report for k5-3-29-6 (192.168.1.53)
Host is up (0.00017s latency).
Nmap scan report for 192.168.1.62
Host is up (0.0044s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.35 seconds
```

Шаг 4. С помощью средства hping2 выполним идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request:

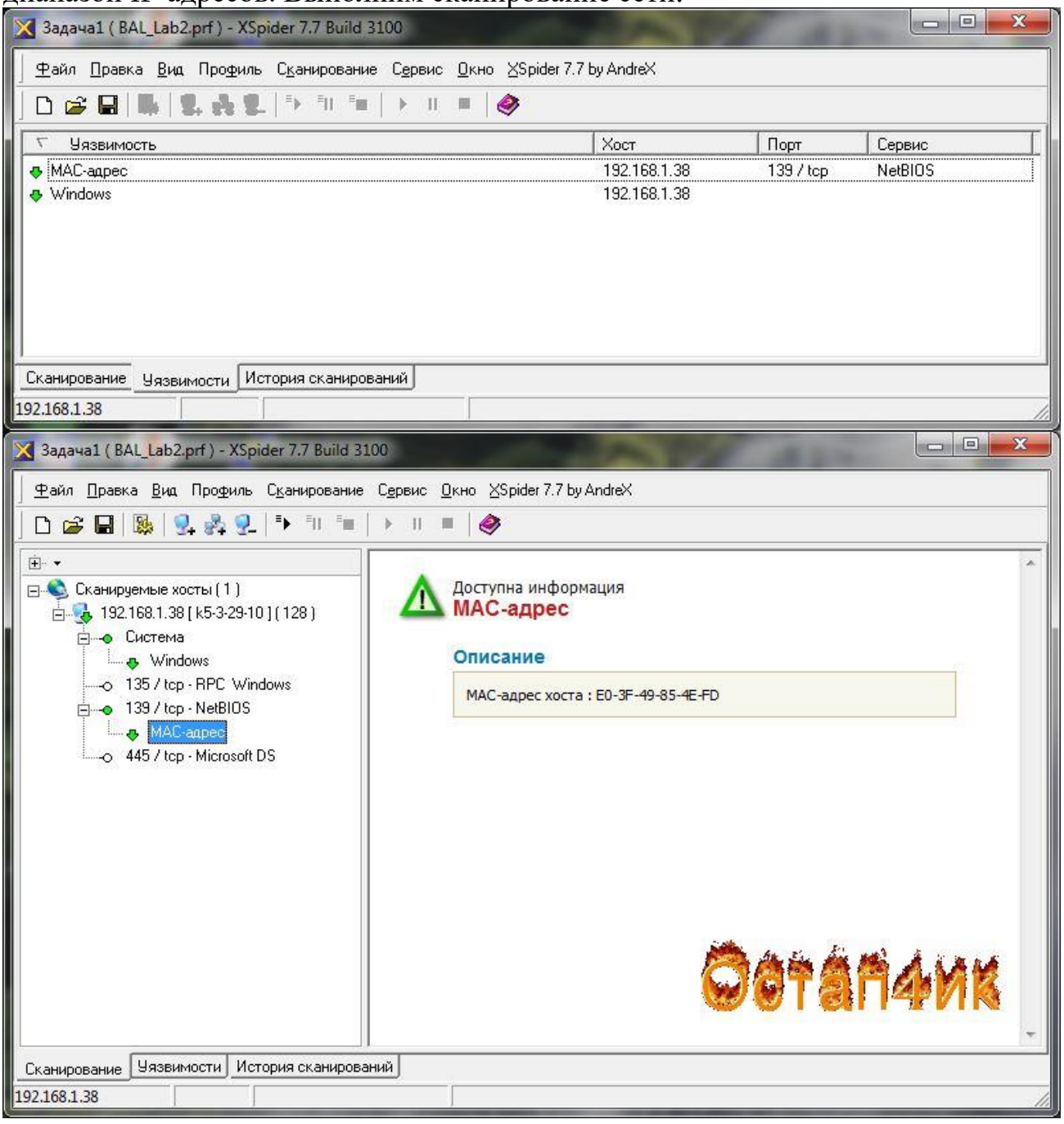
```
k5-3-29-6@k5-3-29-6:~$ sudo hping3 -C 13 192.168.1.38
[sudo] password for k5-3-29-6:
HPING 192.168.1.38 (enp3s0 192.168.1.38): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.38 ttl=128 id=26555 icmp_seq=0 rtt=7.5 ms
ICMP timestamp: Originate=37486641 Receive=3639778305 Transmit=3639778305
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.38 ttl=128 id=26556 icmp_seq=1 rtt=7.3 ms
ICMP timestamp: Originate=37487641 Receive=4042169345 Transmit=4042169345
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.38 ttl=128 id=26557 icmp_seq=2 rtt=7.1 ms
ICMP timestamp: Originate=37488641 Receive=4042169345 Transmit=4042169345
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.38 ttl=128 id=26558 icmp_seq=3 rtt=3.0 ms
ICMP timestamp: Originate=37489641 Receive=149658625 Transmit=149658625
ICMP timestamp RTT tsrtt=4

len=46 ip=192.168.1.38 ttl=128 id=26559 icmp_seq=4 rtt=2.9 ms
ICMP timestamp: Originate=37490642 Receive=149658625 Transmit=149658625
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.38 ttl=128 id=26561 icmp_seq=5 rtt=2.7 ms
ICMP timestamp: Originate=37491642 Receive=552049665 Transmit=552049665
ICMP timestamp RTT tsrtt=3
```

Шаг 5. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.

```
k5-3-29-6@k5-3-29-6:~$ sudo hping3 -d 53 192.168.1.38
HPING 192.168.1.38 (enp3s0 192.168.1.38): NO FLAGS are set, 40 headers + 53 data bytes
len=46 ip=192.168.1.38 ttl=128 DF id=26976 sport=0 flags=RA seq=0 win=0 rtt=7.8 ms
len=46 ip=192.168.1.38 ttl=128 DF id=26977 sport=0 flags=RA seq=1 win=0 rtt=7.7 ms
len=46 ip=192.168.1.38 ttl=128 DF id=26978 sport=0 flags=RA seq=2 win=0 rtt=7.6 ms
len=46 ip=192.168.1.38 ttl=128 DF id=26979 sport=0 flags=RA seq=3 win=0 rtt=7.5 ms

k5-3-29-6@k5-3-29-6:~$ sudo nmap -PS -sU -p 111 192.168.1.38

Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-05 13:36 +03
Nmap scan report for 192.168.1.38
Host is up (0.00031s latency).

PORT    STATE  SERVICE
```

```
111/udp closed rpcbind
MAC Address: E0:3F:49:85:4E:FD (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

Шаг 6. На узле TWS2 запустим сканер безопасности XSpider. Укажем диапазон IP-адресов. Выполним сканирование сети:



Шаг 7. На узле TWS1 с помощью сетевого сканера nmap выполним идентификацию открытых TCP и UDP портов найденных узлов IP-сети 172.168.1.0/24, используя основные методы сканирования:

```
k5-3-29-2@k5-3-29-2:~$ sudo nmap -sS -n 192.168.1.38
[sudo] password for k5-3-29-2:
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-12 09:36 +03
Nmap scan report for 192.168.1.38
Host is up (0.00032s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: E0:3F:49:85:4E:FD (Asustek Computer)
```

Вывод: изучили методы и средства идентификации доступных узлов и сетевых портов в анализируемой КС..