

Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №2.
Идентификация узлов и портов сетевых служб

Проверил:

Грищенко В.В.

Студент МС – 42:

Кузнецов Ю.В.

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. Выполнить идентификацию узлов с помощью средства `fping` для сети 192.168.1.0/24. Просмотреть трассировку сканирования: `fping -g 192.168.1.46/24 -c 1`

```
k5-3-29-10@k5-3-29-10:~$ sudo fping -g 192.168.1.0/24 -c 1
192.168.1.1 : [0], 84 bytes, 0.42 ms (0.42 avg, 0% loss)
192.168.1.38 : [0], 84 bytes, 0.04 ms (0.04 avg, 0% loss)
192.168.1.46 : [0], 84 bytes, 0.34 ms (0.34 avg, 0% loss)
192.168.1.47 : [0], 84 bytes, 0.65 ms (0.65 avg, 0% loss)
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.3
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.6
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.5
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.4
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.9
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.8
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.7
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.12
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.11
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.10
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.15
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.13
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.18
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.17
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.16
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.22
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.21
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.20
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.19
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.25
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.24
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.23
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.28
ICMP Host Unreachable from 192.168.1.38 for ICMP Echo sent to 192.168.1.27
```

Шаг 2. С помощью сетевого сканера `nmap` выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования: `nmap -sn 192.168.1.46/24`

```
k5-3-29-10@k5-3-29-10:~$ sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-14 12:43 +03
Nmap scan report for gateway (192.168.1.1)
Host is up (0.00037s latency).
MAC Address: E4:18:6B:0B:48:24 (ZyXEL Communications)
Nmap scan report for 192.168.1.46
Host is up (-0.100s latency).
MAC Address: E0:3F:49:EA:84:24 (Asustek Computer)
Nmap scan report for 192.168.1.47
Host is up (-0.100s latency).
MAC Address: E0:3F:49:85:64:3E (Asustek Computer)
Nmap scan report for 192.168.1.50
Host is up (-0.100s latency).
MAC Address: B4:2E:99:82:C8:CC (Unknown)
Nmap scan report for 192.168.1.54
Host is up (-0.077s latency).
MAC Address: 40:E2:30:4A:C0:FD (AzureWave Technology)
Nmap scan report for k5-3-29-10 (192.168.1.38)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.77 seconds
```

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

Например: `hping3 -C 13 192.168.1.59` Просмотреть трассировку сканирования.

```

k5-3-29-10@k5-3-29-10:~$ sudo hping3 -C 13 192.168.1.47
HPING 192.168.1.47 (enp3s0 192.168.1.47): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.47 ttl=64 id=23079 icmp seq=0 rtt=7.8 ms
ICMP timestamp: Originate=35324509 Receive=35321113 Transmit=35321113
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.47 ttl=64 id=23194 icmp seq=1 rtt=7.8 ms
ICMP timestamp: Originate=35325909 Receive=35321113 Transmit=35322113
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.47 ttl=64 id=23243 icmp seq=2 rtt=3.6 ms
ICMP timestamp: Originate=35326509 Receive=35321113 Transmit=35323113
ICMP timestamp RTT tsrtt=4

len=46 ip=192.168.1.47 ttl=64 id=23255 icmp seq=3 rtt=7.5 ms
ICMP timestamp: Originate=35327509 Receive=35324113 Transmit=35324113
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.47 ttl=64 id=23295 icmp seq=4 rtt=7.4 ms
ICMP timestamp: Originate=35328509 Receive=35325113 Transmit=35325113
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.1.47 ttl=64 id=23421 icmp seq=5 rtt=3.3 ms
ICMP timestamp: Originate=35329509 Receive=35326114 Transmit=35326114
ICMP timestamp RTT tsrtt=4

len=46 ip=192.168.1.47 ttl=64 id=23425 icmp seq=6 rtt=3.1 ms
ICMP timestamp: Originate=35330510 Receive=35327114 Transmit=35327114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=23525 icmp seq=7 rtt=3.0 ms
ICMP timestamp: Originate=35331510 Receive=35328114 Transmit=35328114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=23620 icmp seq=8 rtt=2.9 ms
ICMP timestamp: Originate=35332510 Receive=35329114 Transmit=35329114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=23659 icmp seq=9 rtt=2.8 ms
ICMP timestamp: Originate=35333510 Receive=35330114 Transmit=35330114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=23663 icmp seq=10 rtt=2.7 ms
ICMP timestamp: Originate=35334510 Receive=35331114 Transmit=35331114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=23837 icmp seq=11 rtt=2.6 ms
ICMP timestamp: Originate=35335510 Receive=35332114 Transmit=35332114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=24007 icmp seq=12 rtt=2.5 ms
ICMP timestamp: Originate=35336510 Receive=35333114 Transmit=35333114
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.1.47 ttl=64 id=24029 icmp seq=13 rtt=2.3 ms

```

Шаг 4. С помощью средств `hping2` и `nmap` выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.
Например: **`nmap -PS -sU -p 111 192.168.1.59`**

```

k5-3-29-10@k5-3-29-10:~$ sudo nmap -PS -sU -p 111 192.168.1.47

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-14 12:53 +03
Nmap scan report for 192.168.1.47
Host is up (0.00032s latency).

PORT      STATE SERVICE
111/udp   closed rpcbind
MAC Address: E0:3F:49:85:64:3E (Asustek Computer)

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

```

Шаг 5. 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.
Например: **`nmap -sS -n 192.168.1.59,`**
`nmap -sS -n 192.168.1.37,`
`nmap -sS -n 192.168.1.41`
Просмотреть трассировки сканирований. Проанализировать результаты.

```
Nmap done: 1 IP address (1 host up) scanned in 0.157 seconds
k5-3-29-10@k5-3-29-10:~$ sudo nmap -sS -n 192.168.1.47

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-14 12:55 +03
Nmap scan report for 192.168.1.47
Host is up (0.00039s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: E0:3F:49:85:64:3E (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
k5-3-29-10@k5-3-29-10:~$ |
```