Гомельский Государственный Университет

им. Ф. Скорины

Лабораторная работа №2.
Идентификация узлов и портов сетевых служб

Проверил:

Грищенко В.В.

Студент МС – 42:

Черненок А.В.

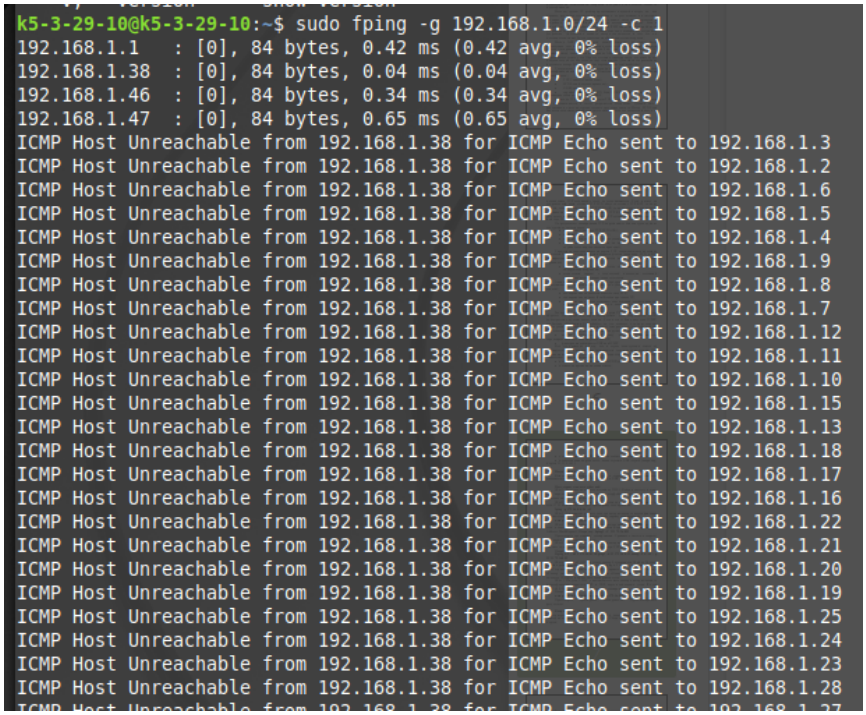
г. Гомель

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

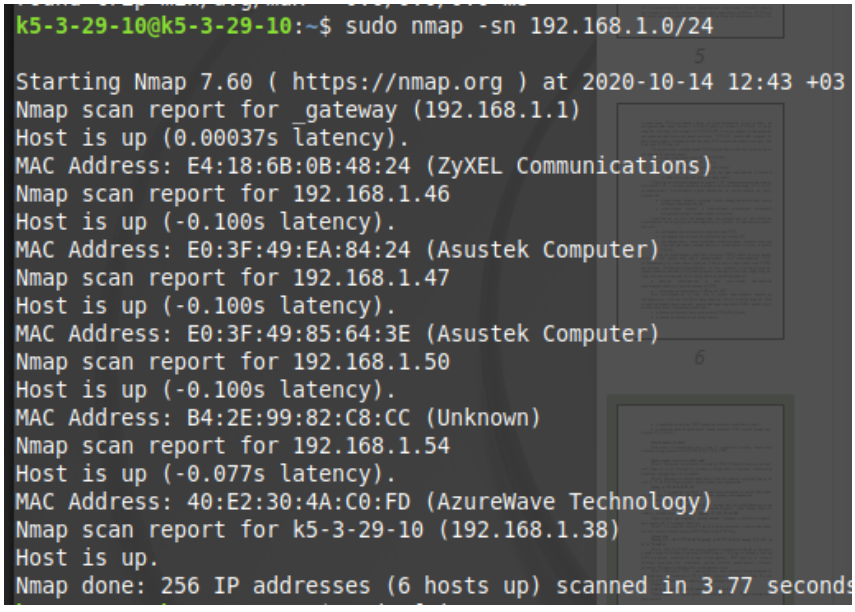
Постановка задачи: выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

Последовательность действий

Шаг 1. Выполнить идентификацию узлов с помощью средства fping для сети 192.168.1.0/24. Просмотреть трассировку сканирования: **fping –g 192.168.1.0/24 –c 1**



Шаг 2. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования: **nmap –sn 192.168.1.0/24**



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

Например: **hping3 –C 13 192.168.1.47** 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 d
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=35325509 Receive=35322113 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=35323113 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
```

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

Например: **nmap –PS –sU –p 111 192.168.1.47**

```
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
```