Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №2

«Идентификация узлов и портов сетевых служб»

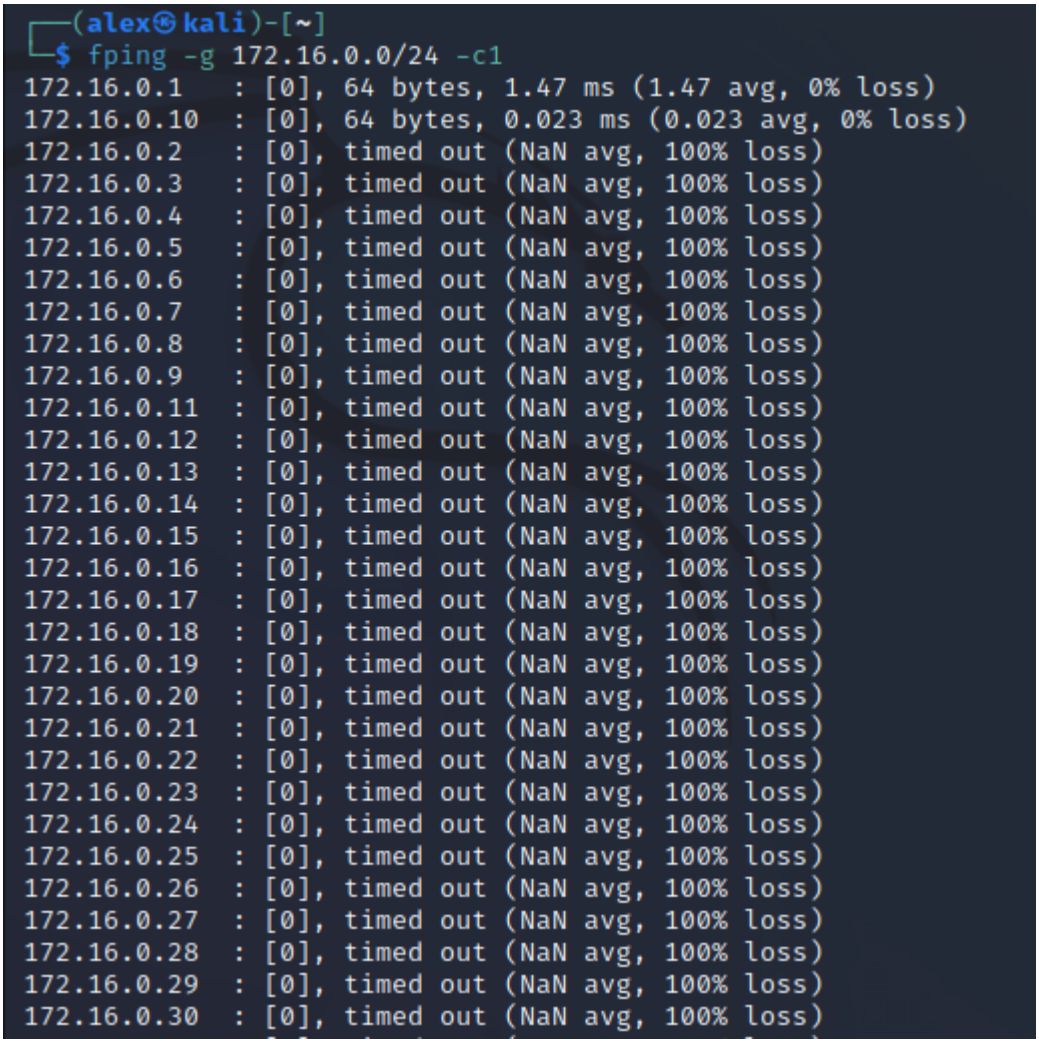
Выполнил:
Студент группы МС-42
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

2022

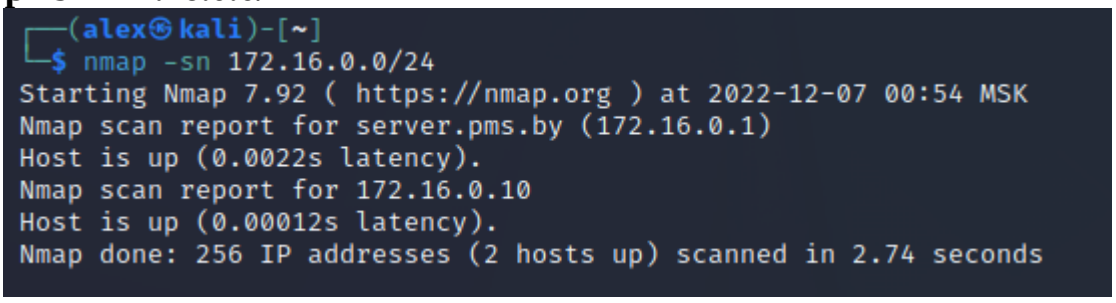
Цель работы: обучение методам и средствам идентификации доступныхузлов и сетевых портов в анализируемой КС.

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**

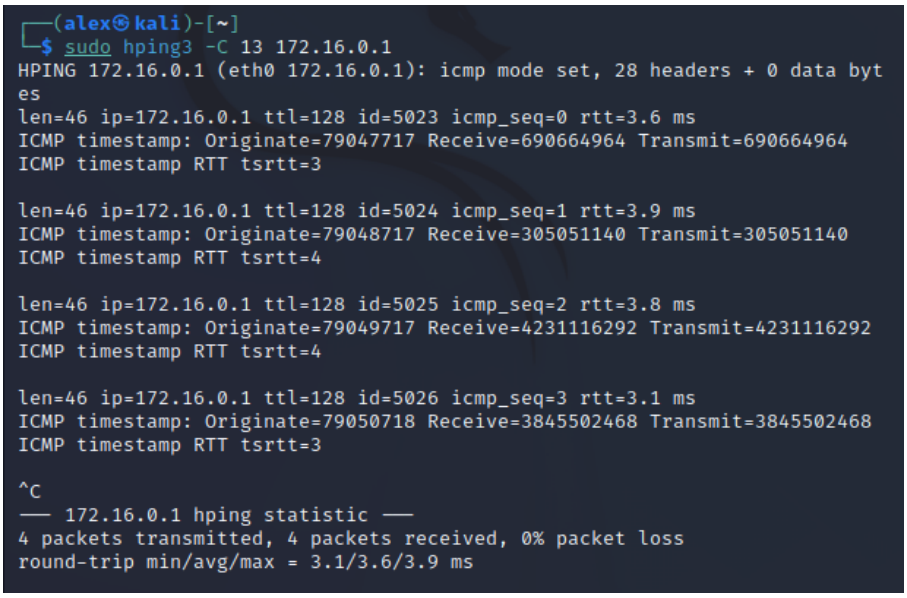


Шаг 2. С помощью сетевого сканера nmap выполним идентификацию узлов методом ARP Scan. Просмотрим трассировку сканирования:
nmap –sn 172.16.0.0/24



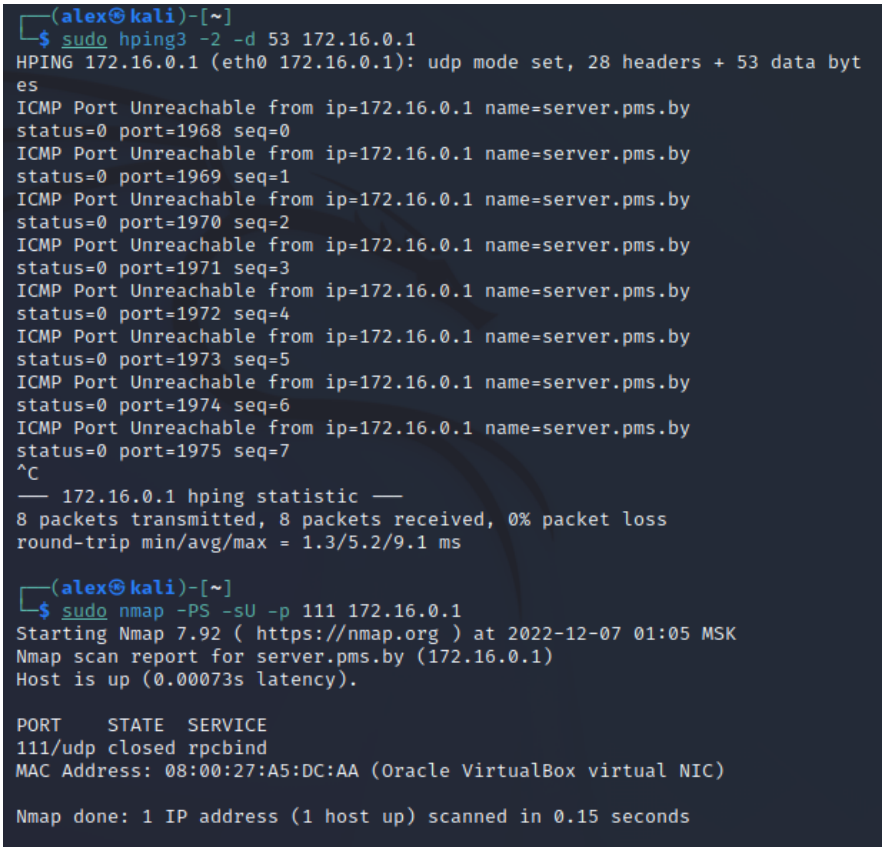
Шаг 3. С помощью средства hping2 выполним идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, AddressMask Request.

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

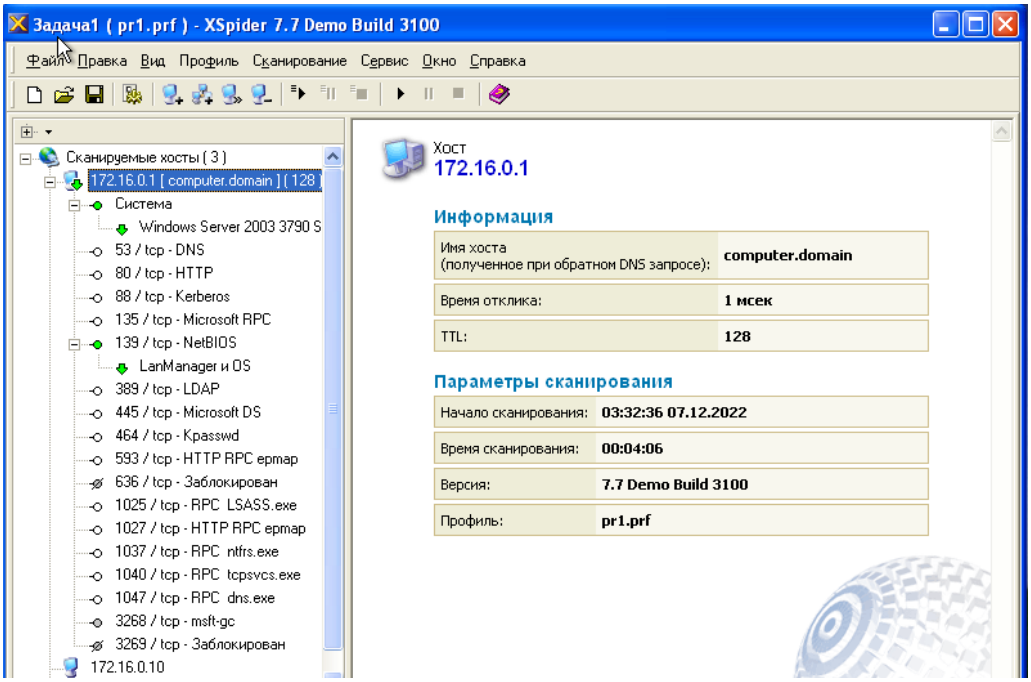


Шаг 4. С помощью средств hping2 и nmap выполним идентификацию узловсети, используя методы UDP Discovery и TCP Ping.

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



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 идентификациюоткрытых 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.