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.

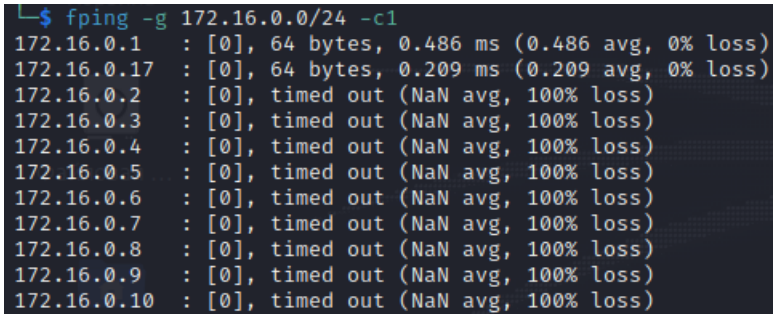
2022

Лабораторная работа №2

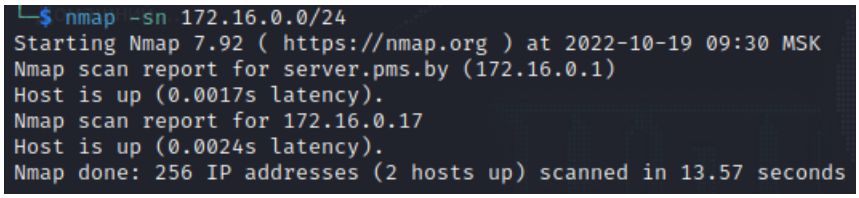
Цель работы: обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

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

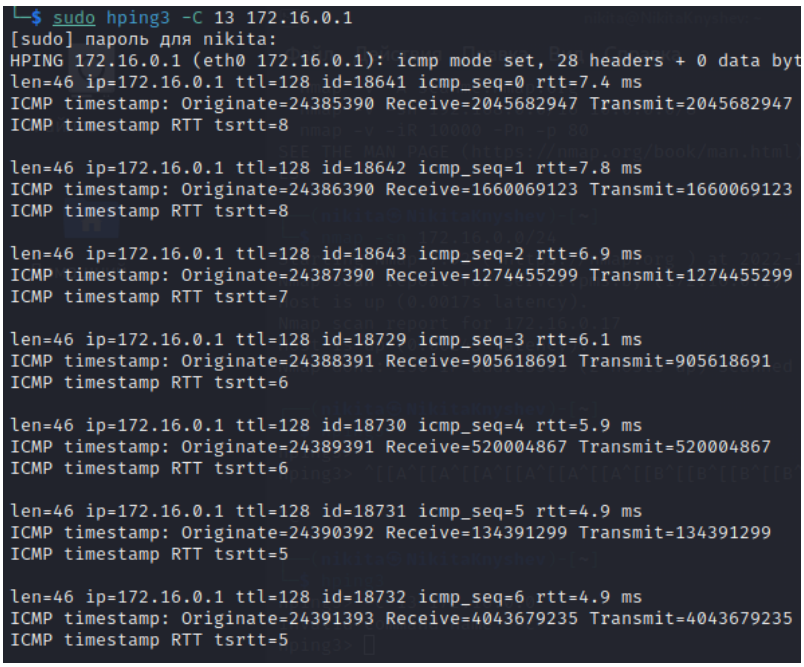
Шаг 1. Выполнить идентификацию узлов с помощью средства fping для сети 172.16.0.0/24. Просмотреть трассировку сканирования:



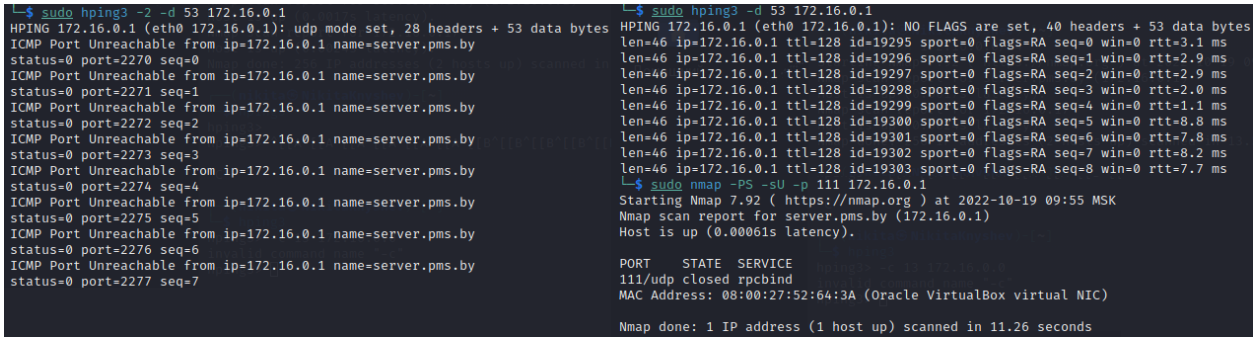
Шаг 2. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования:



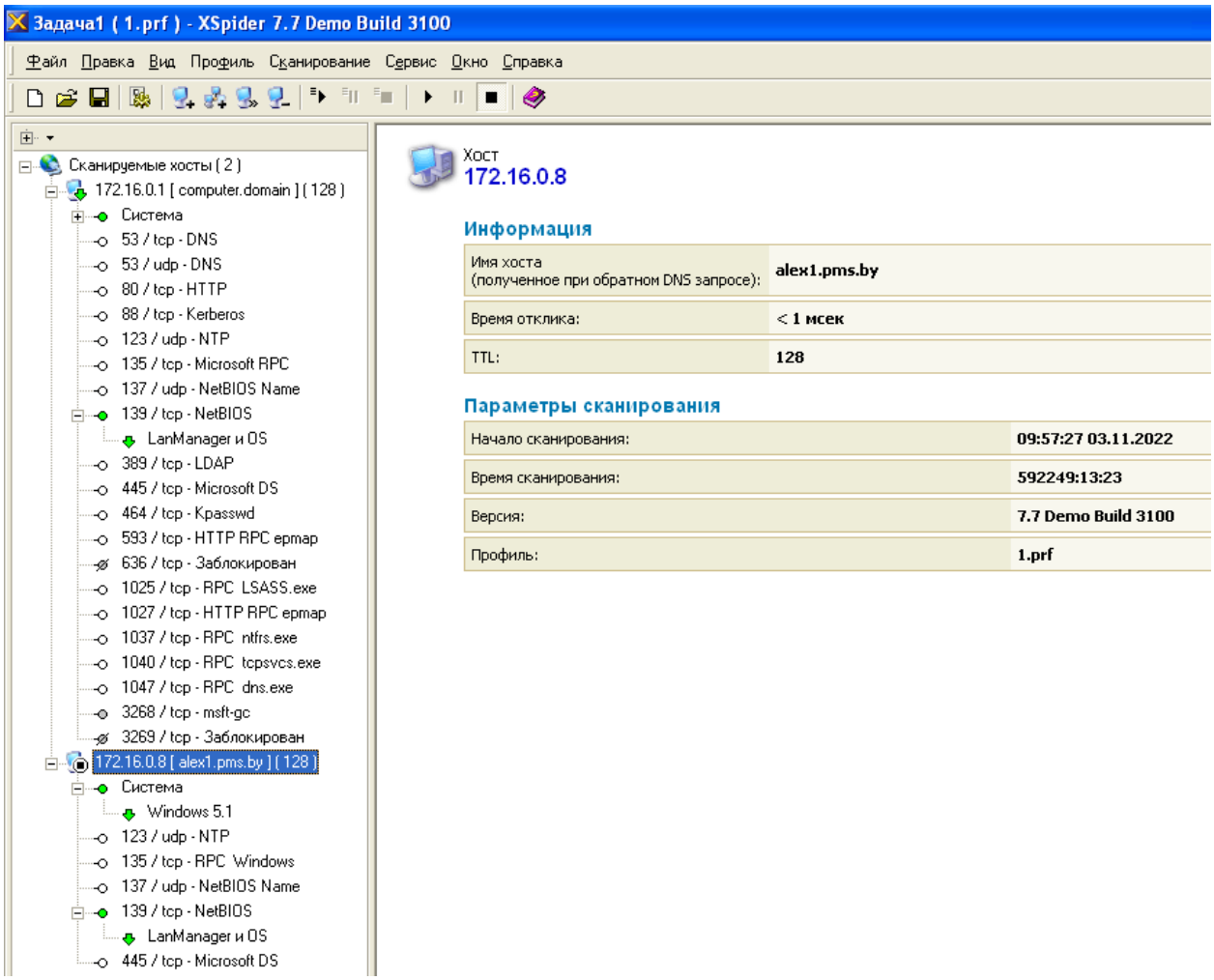
Шаг 3. С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request, просмотреть трассировку сканирования:



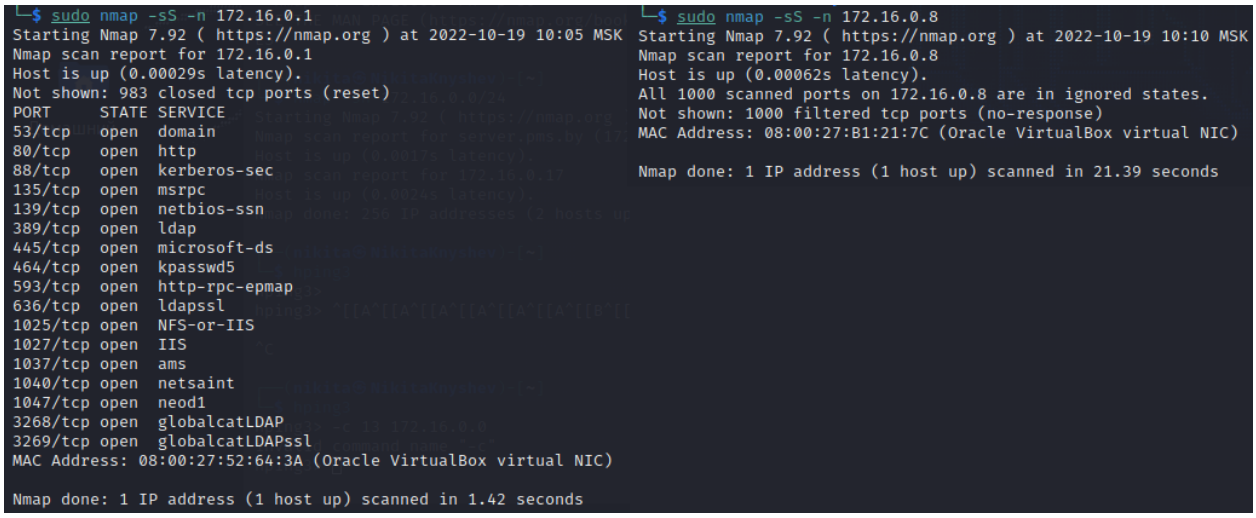
Шаг 4. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.



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.