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

Рыбалкин Д.С.

Проверил: Грищенко В.В.

2022

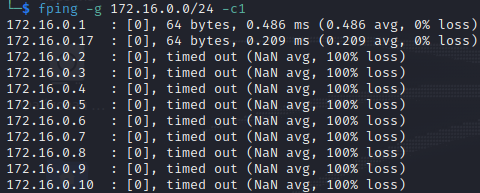
Лабораторная работа №2

***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.

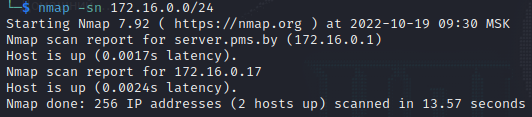
Шаг 1. Выполнить идентификацию узлов с помощью средства fping для

сети 172.16.0.0/24. Просмотреть трассировку сканирования:



Шаг 2. С помощью сетевого сканера nmap выполнить идентификацию

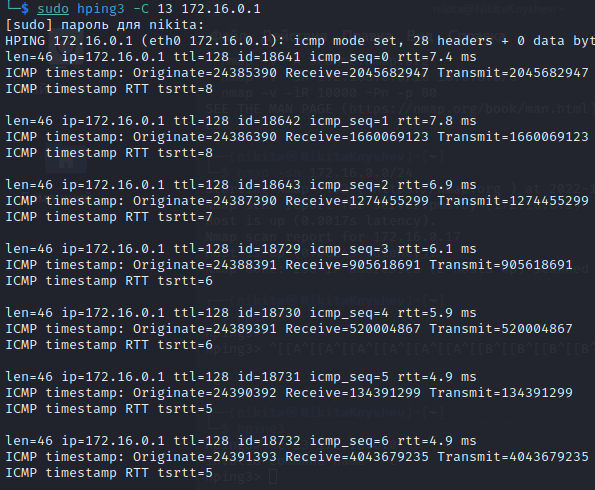
узлов методом ARP Scan. Просмотреть трассировку сканирования:



Шаг 3. С помощью средства hping2 выполнить идентификацию узлов

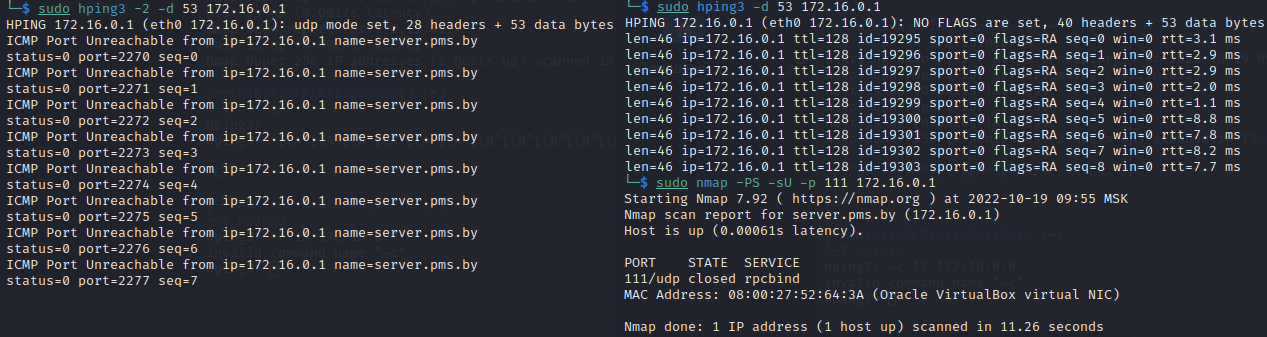
сети, используя ICMP-сообщения Information Request, Time Stamp Request,

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.



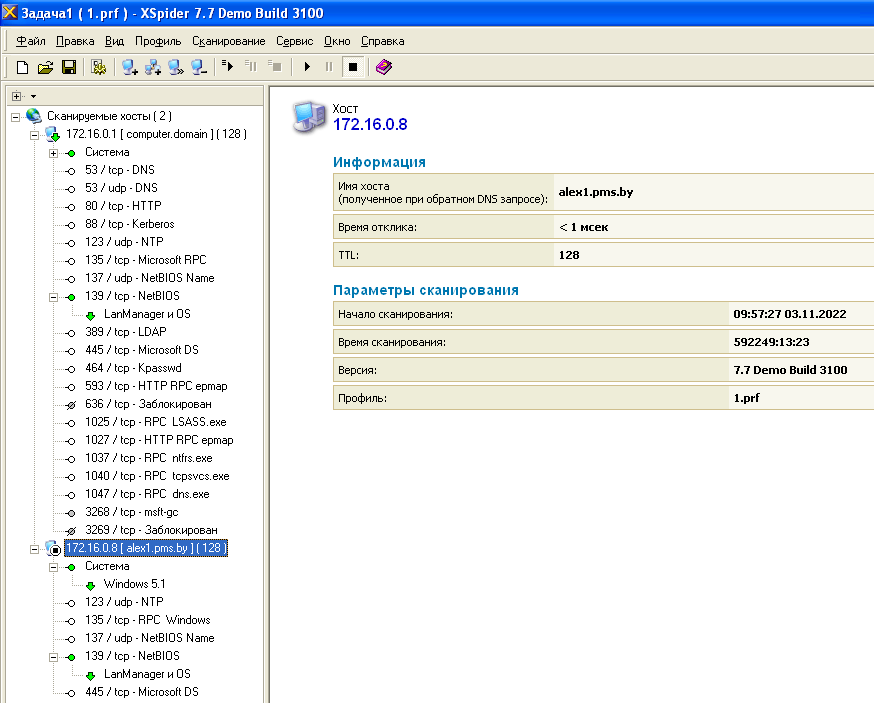
Шаг 5. На узле TWS2 запустить сканер безопасности XSpider. Создать

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

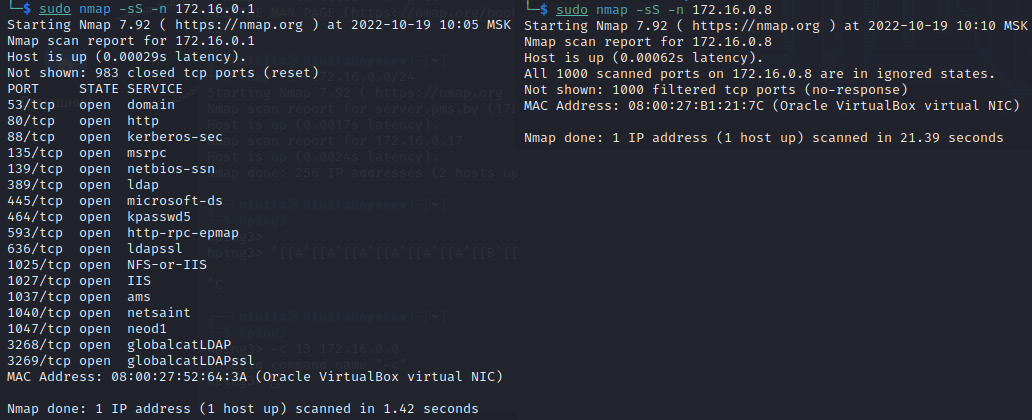
диапазон IP-адресов. Выполнить сканирование сети.



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.



**Вывод:** в ходе лабораторнойработыбыли 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.