МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Лабораторная работа №8

По дисциплине «Аппаратное и программное обеспечение сетей»

Тема: «Утилита для сканирования и исследования безопасности сети NMAP»

Выполнил:

студент 3 курса

группы ИИ-23

Макаревич Н.Р.

Проверил:

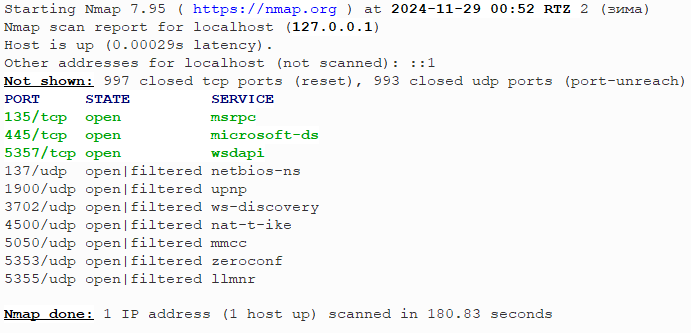
Степанчук В.И.

Брест 2024

Цель: Изучение и практическое применение утилиты для сканирования и исследования безопасности сети nmap.

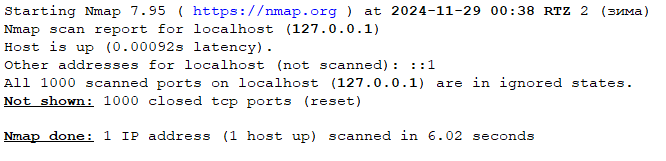
1. Получите список открытых портов (TCP и UDP) машины, за которой выполняется лабораторная работа (localhost). Воспользуйтесь несколькими методами сканирования. Сравните результаты.

**Список портов TCP SYN/UDP:**

nmap -sS -sU localhost 

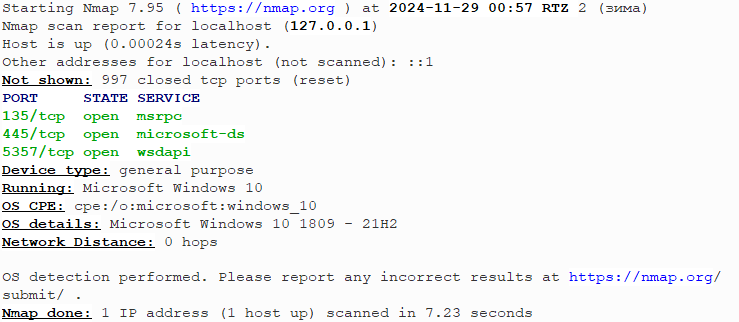
**Попытка NULL сканирования:**

nmap -sN localhost



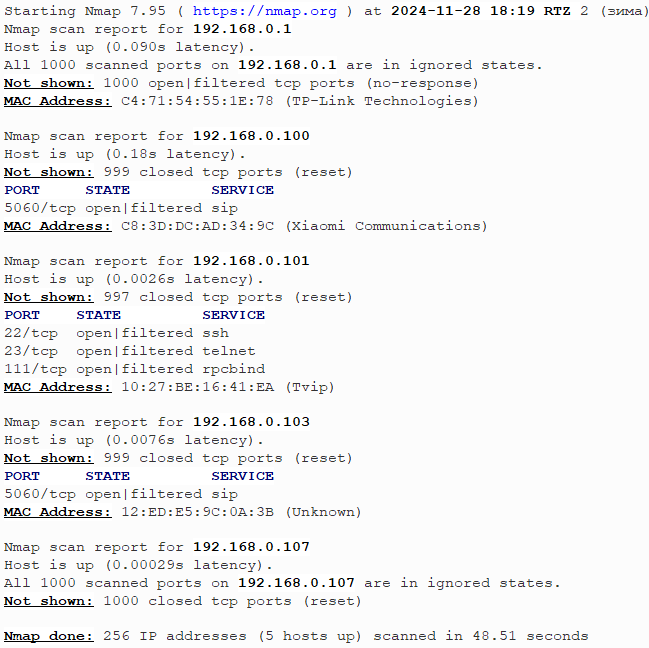
1. **Определите операционную систему этой же машины**

nmap -O localhost



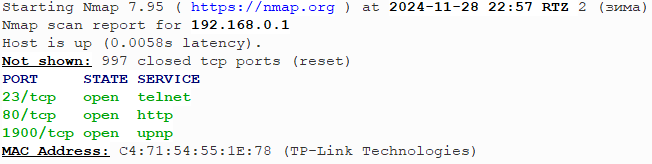
1. **Узнать адреса активных хостов в сети**

nmap -sN 192.168.0.0/24

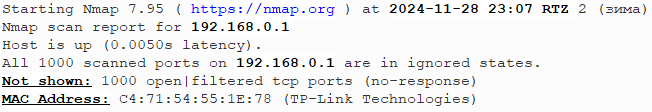


**4. Просканируйте хост №1, разными методами. Сравните результаты.**

nmap -sS 192.168.0.1



nmap -sF 192.168.0.1



1. **5. Для четырех хостов (№2-5), выполните следующие действия:**
   1. Определите, защищен ли хост межсетевым экраном.
   2. Определите поддерживаемые протоколы.
   3. Выберите оптимальный метод сканирования портов, чтобы избежать обнаружения. Определите открытые и фильтрованные порты и по возможности версии служб. При необходимости используйте RPC-сканирование.
   4. Определите операционную систему.

**Определение защиты хоста:**

Nmap scan report for 192.168.0.100

Host is up (0.18s latency).

Not shown: 999 closed tcp ports (reset)

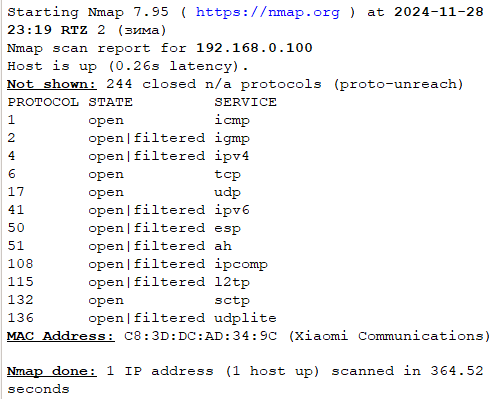
PORT STATE SERVICE

5060/tcp open|filtered sip

MAC Address: C8:3D:DC:AD:34:9C (Xiaomi Communications)

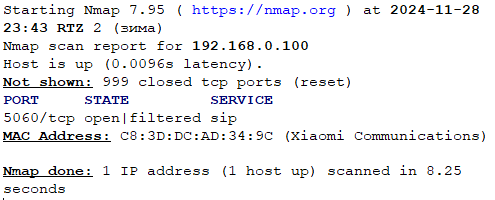
**Определение поддерживаемых протоколов**

nmap -sO 192.168.0.100

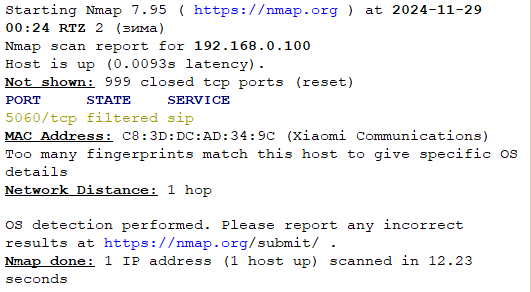


**Сканирование портов без обнаружения:**

nmap -sN 192.168.0.100



nmap -O 192.168.0.100



Вывод: изучил и практически применил утилиту nmap для сканирования и исследования безопасности сети nmap