Metasploit - 1

Project report documenting the network discovery and vulnerability scanning of target systems as a part of practical coursework.

In Cyber Security

By Bhuriyaseth Mariya

To Easy Skill Career Academy

Candidate’s Declaration

I hereby declare that the work presented in this report titled “Nmap Network Scanning Project” is for the purpose of hands-on experience and to gain knowledge of network scanning and reconnaissance as part of this cybersecurity course.

The work performed on the scanme.nmap.org target and the local easyskill Wi-Fi network was carried out to deepen my practical understanding of host discovery, port scanning, and service fingerprinting. All activities were conducted in a controlled, authorized lab environment. The findings, analyses, and conclusions presented in this report are my own original work, completed to the best of my knowledge and ability.

Student signature

Bhuriyaseth Mariya

This is clarify that above statement made by candidate is true and best of my knowledge.

Supervisor signature

Siddharth Sharma

Acknowledgement

I wish to express my deep appreciation to the instructors at Easy Skill Career Academy for providing their guidance, invaluable support, and encouragement throughout the project work. I would also like to thank my colleagues who have given their moral support and advice throughout the completion of this work.

Abstract

Penetration Testing is a specialized security audit, and its first phase is almost always reconnaissance. This project utilizes the Nmap (Network Mapper) tool to perform active reconnaissance on both a public, authorized target (scanme.nmap.org) and a private, local network (easyskill Wi-Fi). The goal is to identify live hosts, discover open ports, fingerprint services and operating systems, and test basic evasion techniques. This report documents the steps taken, the commands used, and the analysis of the data gathered. The findings are rated according to their potential risk, and recommendations are provided to mitigate those risks.

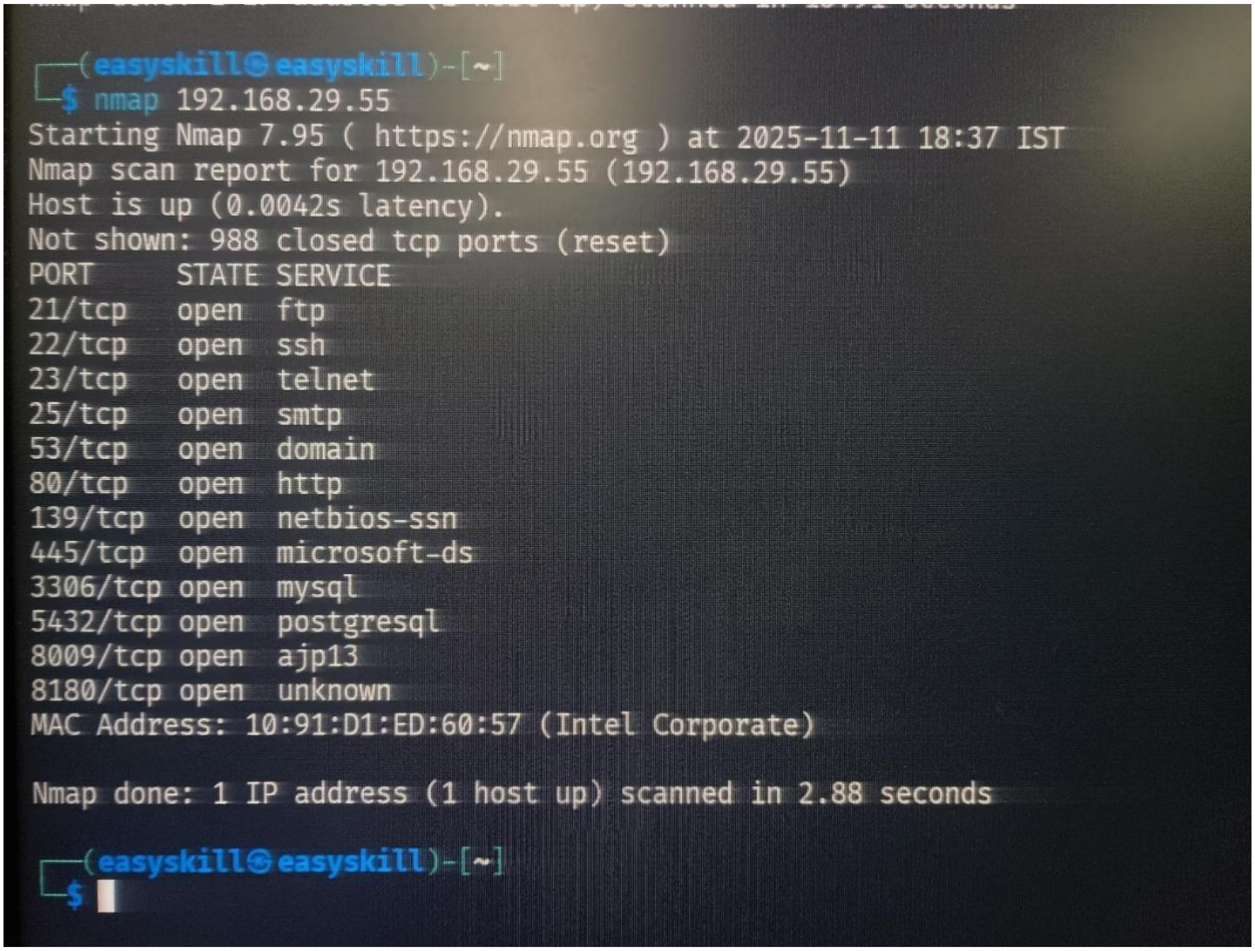
Targeted IP: 192.168.29.55

Command Scan: nmap -sV -Pn 192.168.29.55

Open Ports: 12

Closed Ports:988

Evidence:

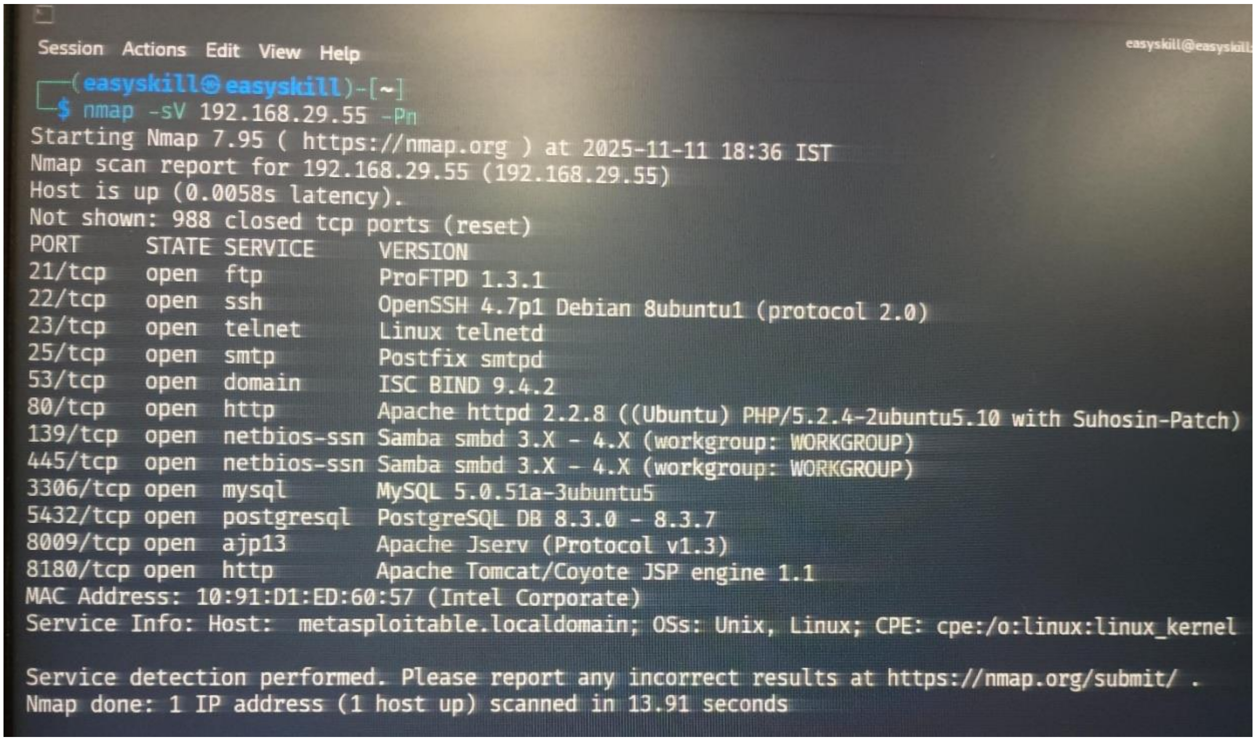


```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap 192.168.29.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 18:37 IST
Nmap scan report for 192.168.29.55 (192.168.29.55)
Host is up (0.0042s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 10:91:D1:ED:60:57 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```

Findings:

All Ports : TCP Ports

MAC Address: 10:91:D1:ED:60:57



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sV 192.168.29.55 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 18:36 IST
Nmap scan report for 192.168.29.55 (192.168.29.55)
Host is up (0.0058s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 10:91:D1:ED:60:57 (Intel Corporate)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.91 seconds
```

Command used : nmap -sV 192.168.29.55 -Pn

Found vulnerability:

After searching all the version in Searchsploit it came to the conclusion that all the version didn't have any exploits but may be in future