Nmap Network Scanning Project

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

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.

Content

1) Introduction

2) Tools and Techniques

3) Practical 1: Basic Host Discovery

4) Practical 2: Port Scan Basics (TCP)

5) Practical 3: Service/Version Detection & OS Fingerprinting

6) Practical 5: Evasion Techniques

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.

1) Introduction

1.1 General Introduction

A penetration test, or pen test, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The Nmap project is a core component of the initial reconnaissance phase. By scanning targets, a security professional can identify potential attack vectors, such as open ports, outdated services, and misconfigured systems. This information is critical for understanding the target's "attack surface."

1.2 Problem Definition

In any network, unknown or unmanaged devices and services represent a significant security risk. Administrators cannot fully ensure the safety of a system without first knowing what is running on their network. Automated tools are essential, but manual analysis is required to interpret the results.

This project aims to manually use Nmap to discover live hosts, identify open services that could be vulnerable, and fingerprint those services to find potential weaknesses, simulating the first step an attacker would take.

1.3 Methodology

The methodology for this project follows the steps outlined in the nmap projects (1).txt file, progressing from broad discovery to specific analysis:

- **Phase 1 - Reconnaissance (Host Discovery):** Identify all live hosts on the local network.
- **Phase 2 - Scanning (Port Scan):** Scan the public target for open TCP and UDP ports.
- **Phase 3 - Gaining Access (Service/OS Detection):** Enumerate service versions and operating systems to find potential vulnerabilities.
- **Phase 4 - Evasion:** Attempt to use scanning techniques that might bypass simple firewalls or Intrusion Detection Systems (IDS).
- **Phase 5 - IPv6 Analysis:** Confirm and note the target's IPv6 address.

2) Tools and Techniques

2.1 Nmap

For this project, the primary tool used was **Nmap (Network Mapper)**. Nmap is a free and open-source utility for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and dozens of other characteristics.

2.2 Nmap Features

The following Nmap features were used in this project:

- **Host Discovery:** (-sn) A "ping scan" that determines which hosts are online.
- **Port Scanning:** (-sT, -f) Identifies open, closed, and filtered ports on a target.
- **Version Detection:** (-sV) Interrogates open ports to determine the application and version number of the running service.
- **OS Detection:** (-O) Attempts to determine the operating system of the target.
- **Evasion:** (--data-string, --ttl) Techniques to modify scan packets to avoid detection.

3) Practical 1: Basic Host Discovery

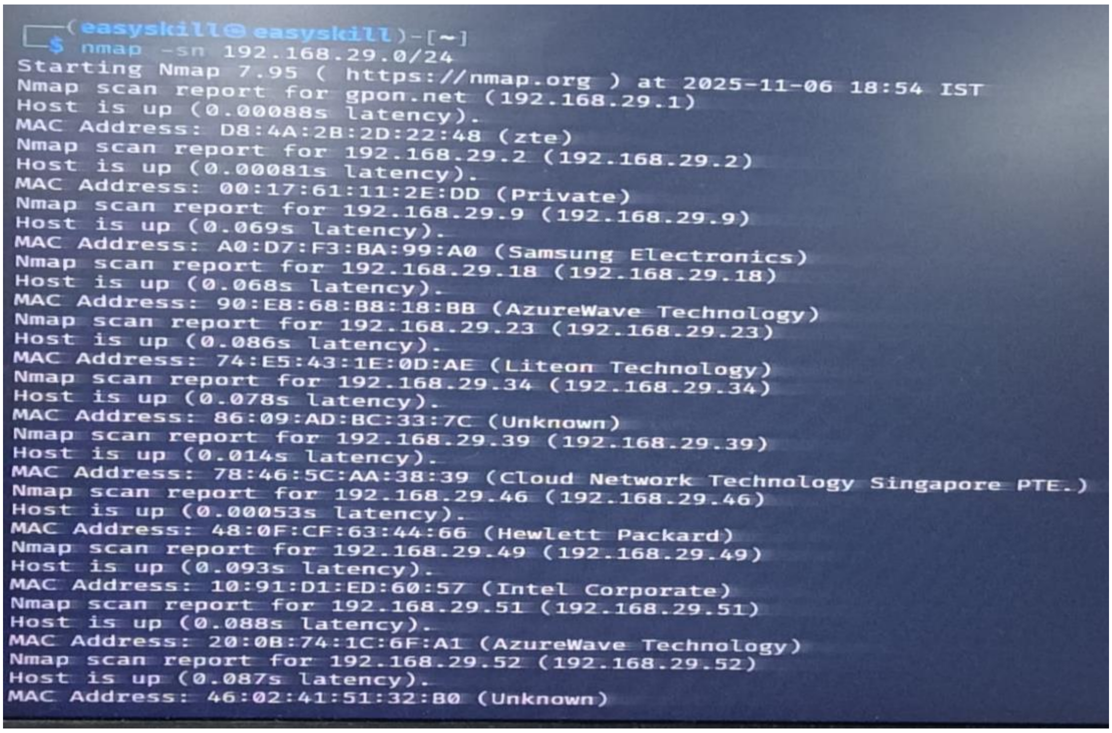
3.1 Scan and Findings

The first step was to map the local "easyskill" Wi-Fi network to find all live devices.

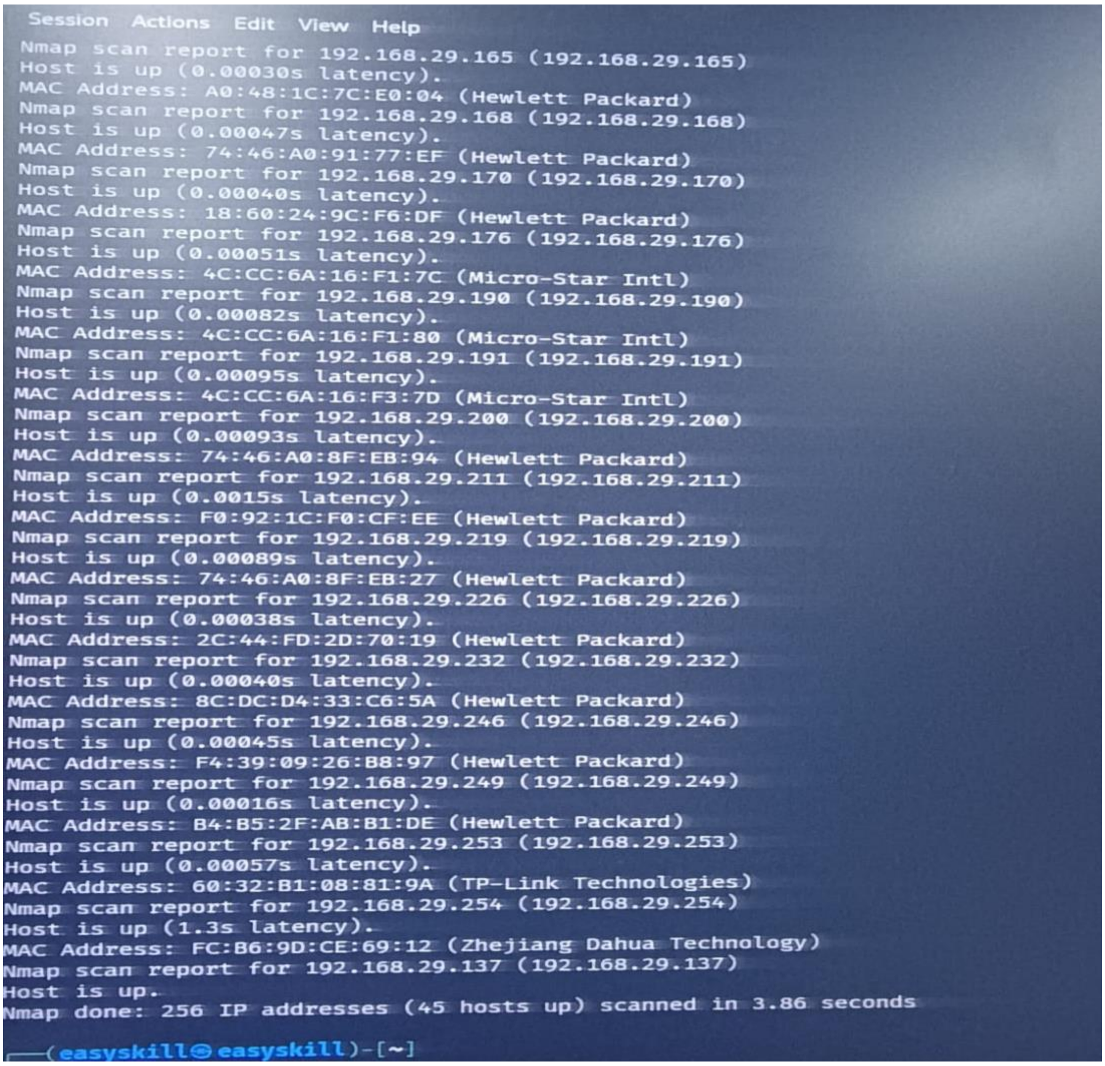
Command: nmap -sn 192.168.29.0/24 and nmap -sn 192.168.1.0/24

Findings: The scans successfully identified numerous active devices, returning their IP, MAC address, and hardware manufacturer (e.g., "Hewlett Packard," "Samsung Electronics," "Intel Corporate").

Evidence:



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sn 192.168.29.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 18:54 IST
Nmap scan report for gpon.net (192.168.29.1)
Host is up (0.00088s latency).
MAC Address: D8:4A:2B:2D:22:48 (zte)
Nmap scan report for 192.168.29.2 (192.168.29.2)
Host is up (0.00081s latency).
MAC Address: 00:17:61:11:2E:DD (Private)
Nmap scan report for 192.168.29.9 (192.168.29.9)
Host is up (0.069s latency).
MAC Address: A0:D7:F3:BA:99:A0 (Samsung Electronics)
Nmap scan report for 192.168.29.18 (192.168.29.18)
Host is up (0.068s latency).
MAC Address: 90:E8:68:B8:18:BB (AzureWave Technology)
Nmap scan report for 192.168.29.23 (192.168.29.23)
Host is up (0.086s latency).
MAC Address: 74:E5:43:1E:0D:AE (Liteon Technology)
Nmap scan report for 192.168.29.34 (192.168.29.34)
Host is up (0.078s latency).
MAC Address: 86:09:AD:BC:33:7C (Unknown)
Nmap scan report for 192.168.29.39 (192.168.29.39)
Host is up (0.014s latency).
MAC Address: 78:46:5C:AA:38:39 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.29.46 (192.168.29.46)
Host is up (0.00053s latency).
MAC Address: 48:0F:CF:63:44:66 (Hewlett Packard)
Nmap scan report for 192.168.29.49 (192.168.29.49)
Host is up (0.093s latency).
MAC Address: 10:91:D1:ED:60:57 (Intel Corporate)
Nmap scan report for 192.168.29.51 (192.168.29.51)
Host is up (0.088s latency).
MAC Address: 20:0B:74:1C:6F:A1 (AzureWave Technology)
Nmap scan report for 192.168.29.52 (192.168.29.52)
Host is up (0.087s latency).
MAC Address: 46:02:41:51:32:B0 (Unknown)
```



```
Nmap scan report for 192.168.29.165 (192.168.29.165)
Host is up (0.00030s latency).
MAC Address: A0:48:1C:7C:E0:04 (Hewlett Packard)
Nmap scan report for 192.168.29.168 (192.168.29.168)
Host is up (0.00047s latency).
MAC Address: 74:46:A0:91:77:EF (Hewlett Packard)
Nmap scan report for 192.168.29.170 (192.168.29.170)
Host is up (0.00040s latency).
MAC Address: 18:60:24:9C:F6:DF (Hewlett Packard)
Nmap scan report for 192.168.29.176 (192.168.29.176)
Host is up (0.00051s latency).
MAC Address: 4C:CC:6A:16:F1:7C (Micro-Star Intl)
Nmap scan report for 192.168.29.190 (192.168.29.190)
Host is up (0.00082s latency).
MAC Address: 4C:CC:6A:16:F1:80 (Micro-Star Intl)
Nmap scan report for 192.168.29.191 (192.168.29.191)
Host is up (0.00095s latency).
MAC Address: 4C:CC:6A:16:F3:7D (Micro-Star Intl)
Nmap scan report for 192.168.29.200 (192.168.29.200)
Host is up (0.00093s latency).
MAC Address: 74:46:A0:8F:EB:94 (Hewlett Packard)
Nmap scan report for 192.168.29.211 (192.168.29.211)
Host is up (0.0015s latency).
MAC Address: F0:92:1C:F0:CF:EE (Hewlett Packard)
Nmap scan report for 192.168.29.219 (192.168.29.219)
Host is up (0.00089s latency).
MAC Address: 74:46:A0:8F:EB:27 (Hewlett Packard)
Nmap scan report for 192.168.29.226 (192.168.29.226)
Host is up (0.00038s latency).
MAC Address: 2C:44:FD:2D:70:19 (Hewlett Packard)
Nmap scan report for 192.168.29.232 (192.168.29.232)
Host is up (0.00040s latency).
MAC Address: 8C:DC:D4:33:C6:5A (Hewlett Packard)
Nmap scan report for 192.168.29.246 (192.168.29.246)
Host is up (0.00045s latency).
MAC Address: F4:39:09:26:B8:97 (Hewlett Packard)
Nmap scan report for 192.168.29.249 (192.168.29.249)
Host is up (0.00016s latency).
MAC Address: B4:B5:2F:AB:B1:DE (Hewlett Packard)
Nmap scan report for 192.168.29.253 (192.168.29.253)
Host is up (0.00057s latency).
MAC Address: 60:32:B1:08:81:9A (TP-Link Technologies)
Nmap scan report for 192.168.29.254 (192.168.29.254)
Host is up (1.3s latency).
MAC Address: FC:B6:9D:CE:69:12 (Zhejiang Dahua Technology)
Nmap scan report for 192.168.29.137 (192.168.29.137)
Host is up.
Nmap done: 256 IP addresses (45 hosts up) scanned in 3.86 seconds

┌──(easyskill㉿easyskill)-[~]
```

3.2 Risk Rating: Low

The act of discovering hosts is low risk, but the *information* gathered is the first step for an attacker. It provides a complete map of all devices on the network.

3.3 Recommendation

1. **Network Segmentation:** Implement VLANs (Virtual LANs) to separate sensitive devices (like servers) from guest devices or general workstations.
2. **MAC Filtering:** As a basic deterrent, use MAC address filtering on the Wi-Fi router to only allow known, authorized devices.

4) Practical 2: Port Scan Basics (TCP)

4.1 - Scan and Findings

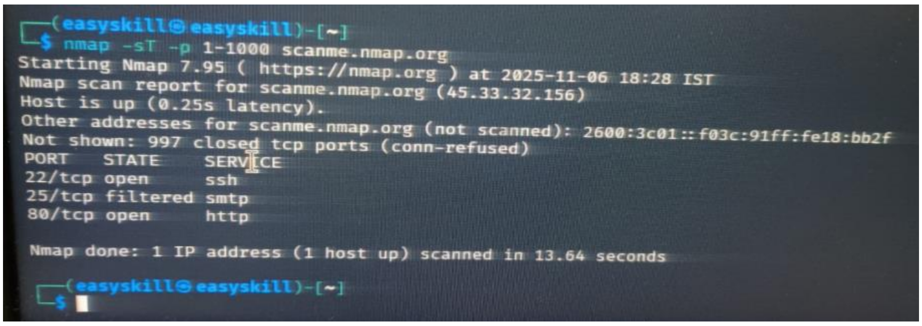
This practical involved scanning the public target scanme.nmap.org for open TCP ports.

Commands: nmap -sT -p 1-1000 scanme.nmap.org and nmap -f scanme.nmap.org

Findings:

- A TCP Connect Scan (-sT) revealed ports 22/tcp (ssh) and 80/tcp (http) were **OPEN**, while 25/tcp (smtp) was **FILTERED**.
- A Fast Scan (-f) confirmed these and also found 5060/tcp (sip), 9929/tcp (nping-echo), and 31337/tcp (Elite) to be open.

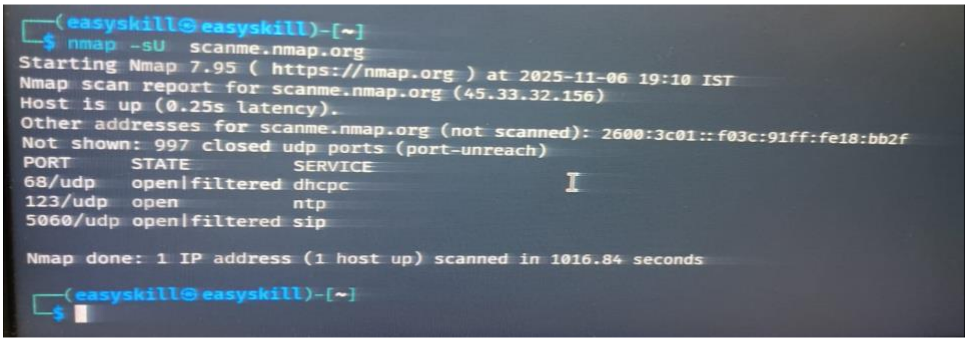
Evidence:



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sT -p 1-1000 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 18:28 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   filtered smtp
80/tcp   open     http

Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sU  scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:10 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 closed udp ports (port-unreach)
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
123/udp  open          ntp
5060/udp open|filtered sip

Nmap done: 1 IP address (1 host up) scanned in 1016.84 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```

4.2 Risk Rating: Medium

Open ports are necessary for services to function, but they are also direct entry points for attackers.

- **Port 22 (SSH):** High risk if weak credentials are used.
- **Port 80 (HTTP):** Medium risk; indicates an unencrypted web server.
- **Port 31337 (Elite):** High risk; this is a non-standard port, often associated with backdoors (historically, "Back Orifice").

4.3 Recommendation

1. **Firewall Rules:** Block all ports that are not absolutely necessary for business function.
2. **SSH Hardening:** For port 22, disable password authentication and use key-based authentication only. Restrict access to trusted IP addresses.
3. **Use HTTPS:** For port 80, implement an SSL/TLS certificate and redirect all HTTP traffic to HTTPS (port 443).
4. **Investigate Non-Standard Ports:** Any non-standard port like 31337 should be investigated to ensure it is a legitimate service and not a backdoor.

5) Practical 3: Service/Version Detection & OS Fingerprinting

5.1 Scan and Findings

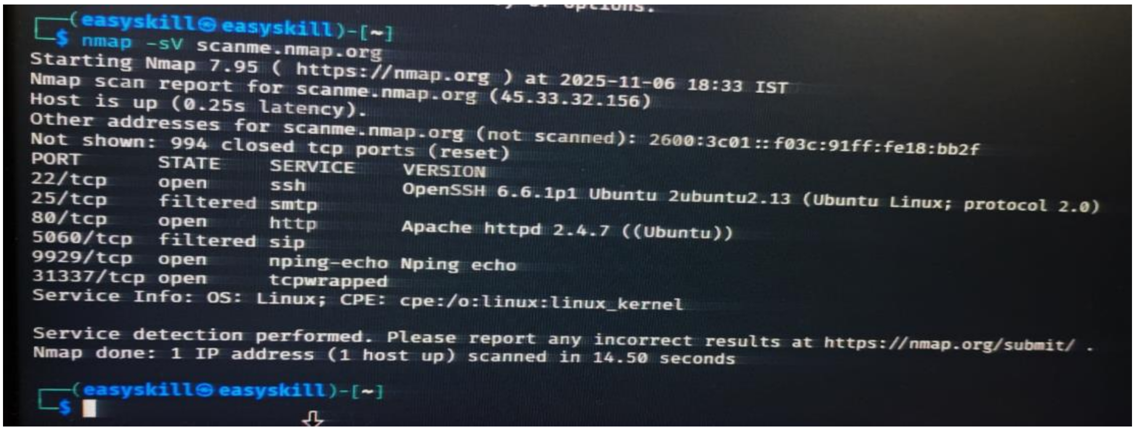
This practical aimed to identify the *specific* software and operating system on scanme.nmap.org.

Commands: nmap -sV scanme.nmap.org and nmap -sV scanme.nmap.org -O

Findings:

- **Port 22/tcp:** OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
- **Port 80/tcp:** Apache httpd 2.4.7 ((Ubuntu))
- **OS:** Linux 5.x or Microtek RouterOS 7.X

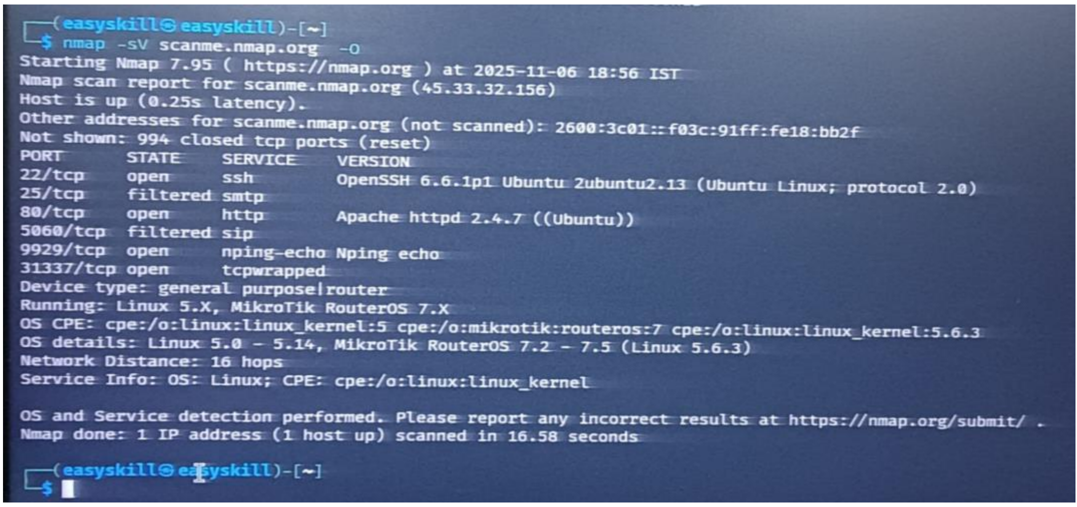
Evidence:



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sV scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 18:33 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
5060/tcp  filtered sip
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: 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 14.50 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap -sV scanme.nmap.org  -O
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 18:56 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
5060/tcp  filtered sip
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```

5.2 –

5.2 Risk Rating: High

This information is extremely valuable to an attacker. They no longer have to guess; they can now search for specific exploits for OpenSSH 6.6.1p1 or Apache 2.4.7. A quick search reveals that OpenSSH 6.6.1p1 is vulnerable to several known exploits (e.g., username enumeration).

5.3 Recommendation

- **Patch Management:** This is the most critical defense. All services (OpenSSH, Apache) and the underlying operating system (Ubuntu, Linux) must be kept up to date with the latest security patches.
- **Minimize Banners:** Configure services (like Apache) to not display their version number in banners, making fingerprinting more difficult.

6) Practical 5: Evasion Techniques

6.1 Scan and Findings

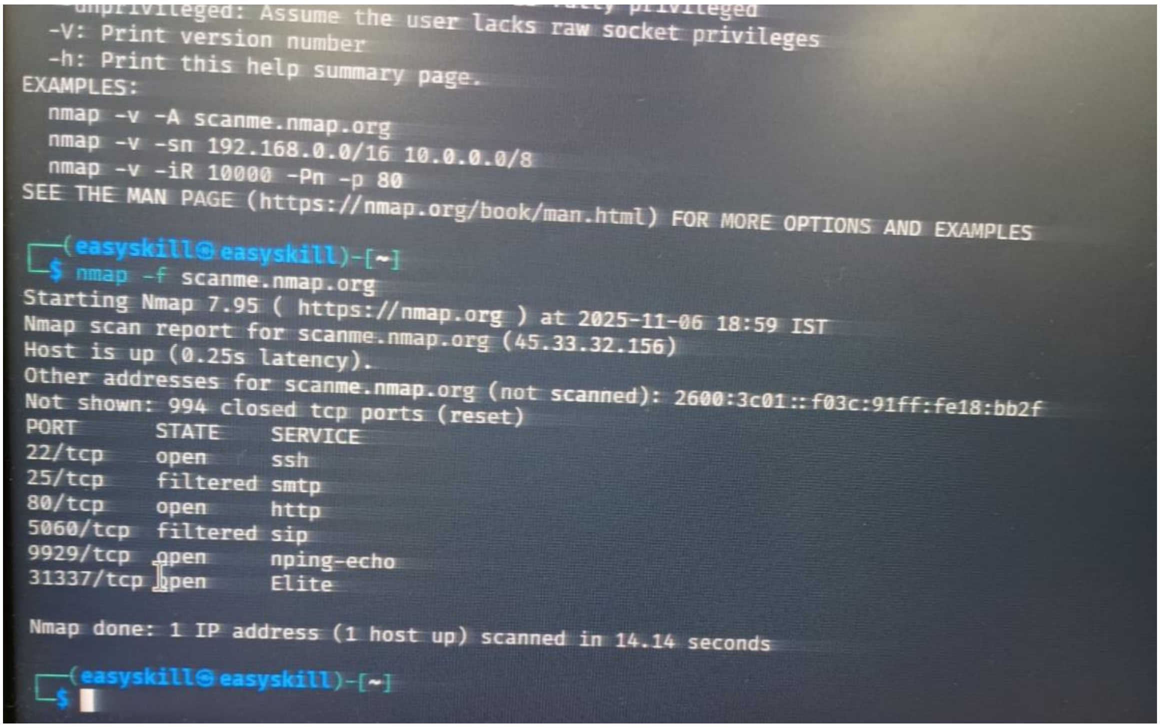
This practical tested Nmap's ability to alter its scans to potentially evade detection.

Commands: nmap --data-string -p 1-100 scanme.nmap.org and nmap --ttl -p 1-100 scanme.nmap.org

6.2 Findings:

- **--data-string:** This scan, which adds random data to packets, completed successfully. This could bypass very simple IDS systems that only look for standard Nmap probes.
- **--ttl:** This scan was attempted, but the syntax was incorrect, causing Nmap to fail. This demonstrates the importance of correct command syntax in penetration testing.

Evidence:

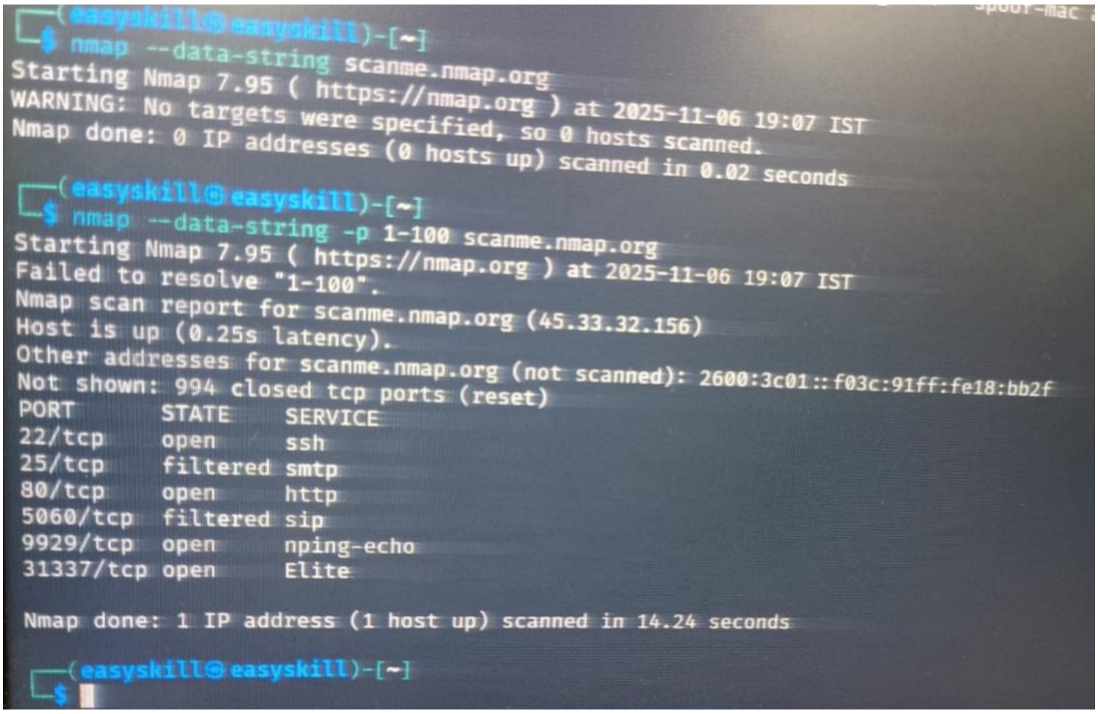


```
  unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(easyskill㉿easyskill)-[~]
└─$ nmap -f scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 18:59 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 14.14 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```

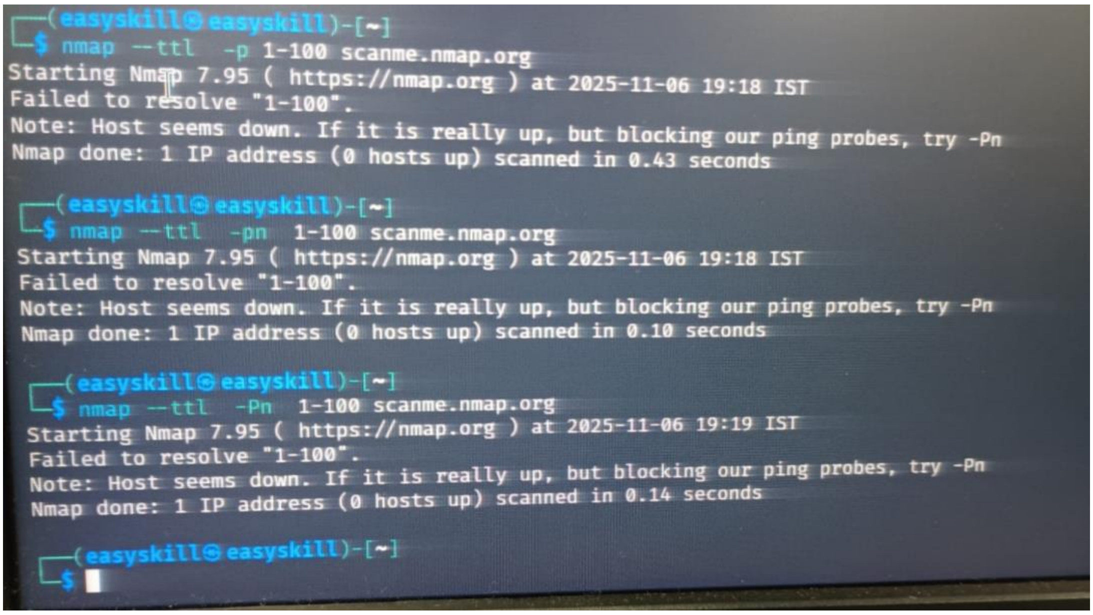


```
                                                              spoof-mac
┌──(easyskill㉿easyskill)-[~]
└─$ nmap --data-string scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:07 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ nmap --data-string -p 1-100 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:07 IST
Failed to resolve "1-100".
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```



```
┌──(easyskill㉿easyskill)-[~]
└─$ nmap --ttl  -p 1-100 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:18 IST
Failed to resolve "1-100".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.43 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ nmap --ttl  -pn  1-100 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:18 IST
Failed to resolve "1-100".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.10 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ nmap --ttl  -Pn  1-100 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 19:19 IST
Failed to resolve "1-100".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.14 seconds

┌──(easyskill㉿easyskill)-[~]
└─$ 
```

7) Conclusion

The Nmap project successfully demonstrated the core principles of active reconnaissance. The scans on the local "easyskill" network revealed a clear map of live devices, while the scans on scanme.nmap.org identified open ports, outdated services, and a precise OS fingerprint.

This project highlights that even basic scanning can reveal critical vulnerabilities. The findings—such as specific, exploitable versions of OpenSSH and Apache—underscore the importance of continuous patch management, proper firewall configuration, and service hardening. The failed --ttl scan also serves as a valuable lesson in the precision required for these tools. By addressing the recommendations in this report, an organization could significantly reduce its attack surface and improve its overall security posture.