Vulnerability Assessment Report

1. Introduction

In today's ever-evolving digital threat landscape, the importance of identifying and mitigating vulnerabilities cannot be overstated. Cybersecurity professionals and enthusiasts alike must develop a strong foundation in vulnerability assessment methodologies and tools. This report presents a basic yet essential demonstration of using Nmap one of the most widely used open-source tools in the cybersecurity industry to identify potential vulnerabilities on a system within a private network. The primary objective of this exercise was to perform a practical reconnaissance of a specific host (192.168.x.x) and interpret the scan results through a security-focused lens. By simulating the initial phases of penetration testing, this activity enhances hands-on experience and nurtures critical analysis of system exposure.

2. Tools & Methodology

1. Tool Used: Nmap v7.94SVN
2. Operating Environment: Ubuntu (via WSL on Windows 11)
3. Scan Type: TCP SYN (Stealth) Scan, Service Version Detection, and OS Detection

Commands Executed:
1. nmap -A -Pn 192.168.x.x - performs an advanced scan with OS detection, version detection, and script scanning on a host that's treated as online even if it blocks ping requests.

Initially, the host appeared down, likely due to firewall rules blocking ICMP echo requests (pings). Using the '-Pn' flag allowed bypassing the ping check & conducting a scan, regardless of the host's ping response. This is especially useful when scanning hardened devices that silently drop ICMP traffic.

3. Scan Findings

Upon scanning the IP address 192.168.x.x, the following results were observed:
- Host Status: Online (with -Pn override)
- Ports Scanned: 1000 common TCP ports
- Result: All 1000 ports filtered

The status 'filtered' indicates that no response was received for the scanned ports. This typically means that a firewall or packet filtering device is in place, dropping the probes silently. Filtered ports are harder for attackers to fingerprint because the system does not return useful error messages. From a security standpoint, this demonstrates good network hygiene i.e. the device is not advertising unnecessary services and is following the principle of least privilege.

4. Interpretation & Relevance

Although no open ports were discovered, the scan results are still valuable. A filtered state on all scanned ports implies a secure default-deny approach to incoming traffic. Such a configuration is a strong foundational measure in defense-in-depth strategies. It ensures that only explicitly allowed connections can reach the system.

In real-world scenarios, systems often expose services unintentionally due to misconfigurations. By regularly scanning for exposed services, organizations can catch and remediate issues before they're exploited. Tools like Nmap are commonly used during the reconnaissance phase of penetration testing or red-teaming exercises, making familiarity with its output critical for cybersecurity professionals.

Vulnerability scanning is a proactive step in identifying weak points before they can be exploited by attackers. Regular scanning not only helps in recognizing configuration flaws and exposed services, but also supports compliance with security standards such as ISO 27001 and GDPR. By performing scans on internal and external assets, organizations can maintain visibility over their digital footprint and respond swiftly to potential issues. Even in home networks, such assessments add a valuable layer of defense, especially when Internet of Things (IoT) devices are present.

5. Recommendations

Based on the current findings, the following recommendations are made:

1. Broader Network Scanning: Conduct subnet-wide scanning (e.g., 192.168.225.0/24) to identify any potentially exposed devices on the network.
2. Include UDP Scans: Some services operate over UDP and are invisible to TCP scans. Use 'nmap -sU 192.168.x.x' to detect these.
3. Employ Vulnerability Scanners: Use tools such as OpenVAS, Nessus, or Nikto for deeper inspection of any discovered open ports.
4. Network Segmentation: Ensure proper segmentation between public, private, and admin-facing devices.
5. Harden Devices: Apply the principle of least privilege, disable unused services, and enforce strict firewall rules.
6. Monitor Traffic: Use tools like Wireshark or Zeek to passively monitor the network and detect anomalies.

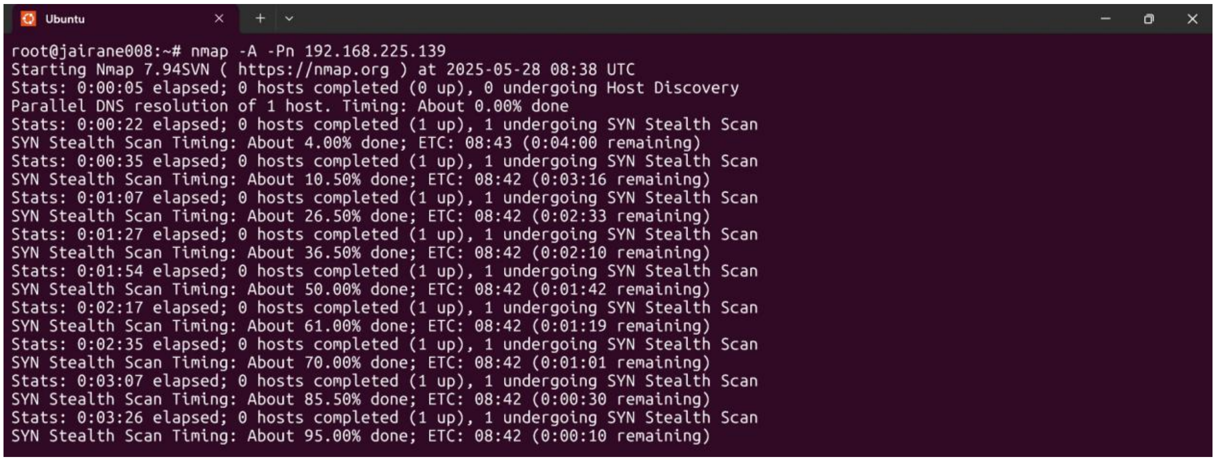
6. References

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment
- OWASP Testing Guide: https://owasp.org/www-project-web-security-testing-guide/stable/
- CIS Controls v8: https://www.cisecurity.org/controls
- Nmap Official Guide: https://nmap.org/book/

7. Visual Evidence

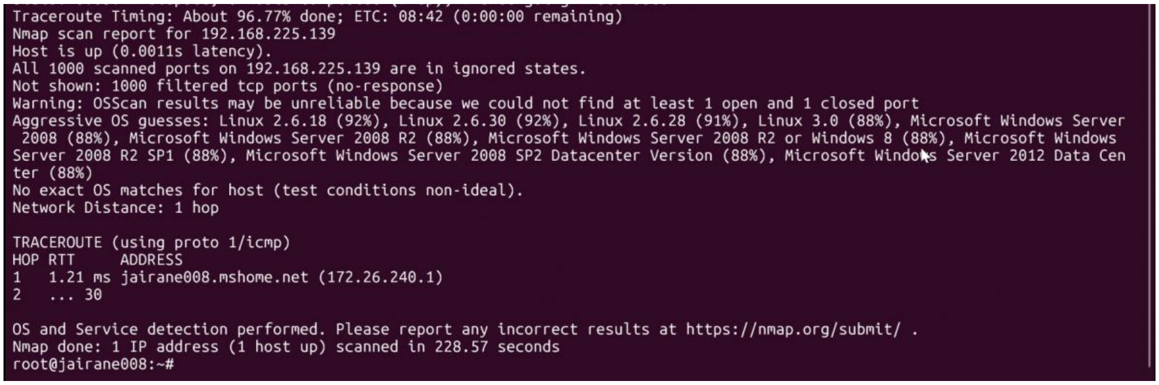
Below is a screenshot of the Nmap scan executed using the '-Pn' and '-sV' flags on the IP address 192.168.x.x. The results confirm that the host was up and protected by a firewall, as all ports were filtered.

Figure 1: Nmap Scan (in-process) on Network 192.168.x.x



```
root@jairane008:~# nmap -A -Pn 192.168.225.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 08:38 UTC
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.00% done; ETC: 08:43 (0:04:00 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.50% done; ETC: 08:42 (0:03:16 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.50% done; ETC: 08:42 (0:02:33 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.50% done; ETC: 08:42 (0:02:10 remaining)
Stats: 0:01:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.00% done; ETC: 08:42 (0:01:42 remaining)
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.00% done; ETC: 08:42 (0:01:19 remaining)
Stats: 0:02:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.00% done; ETC: 08:42 (0:01:01 remaining)
Stats: 0:03:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.50% done; ETC: 08:42 (0:00:30 remaining)
Stats: 0:03:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.00% done; ETC: 08:42 (0:00:10 remaining)
```

Figure 2: Output of scanning, Network 192.168.x.x



```
Traceroute Timing: About 96.77% done; ETC: 08:42 (0:00:00 remaining)
Nmap scan report for 192.168.225.139
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.225.139 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.18 (92%), Linux 2.6.30 (92%), Linux 2.6.28 (91%), Linux 3.0 (88%), Microsoft Windows Server
 2008 (88%), Microsoft Windows Server 2008 R2 (88%), Microsoft Windows Server 2008 R2 or Windows 8 (88%), Microsoft Windows
Server 2008 R2 SP1 (88%), Microsoft Windows Server 2008 SP2 Datacenter Version (88%), Microsoft Windows Server 2012 Data Cen
ter (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   1.21 ms jairane008.mshome.net (172.26.240.1)
2   ... 30

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 228.57 seconds
root@jairane008:~#
```

8. Author Details

Prepared by: Jai Rane
Date: May 29, 2025
Subject: Vulnerability Scanning – using Nmap
Role Applied: Cybersecurity Content Specialist Intern