Network Scanning with Nmap

KAIRIZ CYBER TECHNOLOGIES

HAFIZ NAVEED UDDIN

THIS IS COMPLETE REPORT OF TASK 3

YOGA

CYBERSECURITY

Task Overview

This report presents the results of a series of network scans performed on the target IP address `192.168.133.1` using Nmap. The scans were conducted to identify live hosts, open ports, service versions, operating systems, potential vulnerabilities, and to uncover any hidden or filtered ports. The findings from each step are documented in detail below.

Basic Scanning

1. Live Hosts Identify

Command:

```
bash
Copy code
nmap -sn 192.168.133.1/24
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00068s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.133.2
Host is up (0.00036s latency).
MAC Address: 00:50:56:FA:F6:1E (VMware)
Nmap scan report for 192.168.133.254
Host is up (0.00053s latency).
MAC Address: 00:50:56:FB:8C:8F (VMware)
Nmap scan report for 192.168.133.130
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.14 seconds
```

Findings: Four hosts are up within the network range `192.168.133.1/24`.

---

2. Open Ports Identify

Command:

```
bash
Copy code
nmap -sS 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00065s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
```

Findings: The following open ports were identified:

- Port 902/tcp: Service `iss-realsecure`
- Port 912/tcp: Service `apex-mesh`
- Port 5357/tcp: Service `wsdapi`

---

3. Services Versions Identify

Command:

```
bash
Copy code
nmap -sV 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00056s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC,
SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC,
SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Findings:

- Port 902/tcp: `VMware Authentication Daemon 1.10` (Uses VNC, SOAP)
- Port 912/tcp: `VMware Authentication Daemon 1.0` (Uses VNC, SOAP)
- Port 5357/tcp: `Microsoft HTTPAPI httpd 2.0` (SSDP/UPnP)
- Operating System: Windows

---

4. Operating System Detect

Command:

```
bash
Copy code
nmap -O 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00093s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X
(88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE
(88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Findings: The operating system is likely one of the following:

- Microsoft Windows 11 21H2
- FreeBSD 6.2-RELEASE
- Microsoft Windows 10
- Microsoft Windows Server 2022

Detailed Scanning

1. Detailed Scan with Multiple Options

Command:

```
bash
Copy code
nmap -A 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00055s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC,
SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC,
SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X
(88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE
(88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 192.168.133.1
```

Findings:

- Detailed scan confirms earlier findings about the open ports and services.
- HTTP title: Service Unavailable
- HTTP server header: Microsoft-HTTPAPI/2.0

---

2. Vulnerabilities Detect

Command:

```
bash
Copy code
nmap --script vuln 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00088s latency).
Not shown: 997 filtered tcp ports (no-response)
```

```
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
```

Findings: The script did not return specific vulnerabilities for the open ports identified.

---

3. Scan Results

Command:

```
bash
Copy code
nmap -oA scan_results 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00100s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
```

Findings: The results are saved in three formats: Nmap, XML, and Grepable.

Advanced Techniques for Hidden or Filtered Ports

1. ACK Scan

Command:

```
bash
Copy code
nmap -sA 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00038s latency).
```

```
All 1000 scanned ports on 192.168.133.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
```

Findings: All 1000 scanned ports are filtered (no-response).

---

2. Decoy Scanning Command:

```
bash
Copy code
nmap -D RND:10 192.168.133.1
```

Output:

```
plaintext
Copy code
Nmap scan report for 192.168.133.1
Host is up (0.00091s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
```

Findings: The decoy scan confirmed the same open ports as previous scans.

Conclusion

The scans conducted on `192.168.133.1` revealed the following:

- **Live Hosts:** Four hosts are up within the network range.
- **Open Ports:** Ports 902/tcp, 912/tcp, and 5357/tcp are open.
- **Service Versions:** Detailed versions of services running on the open ports were identified.
- **Operating System:** Likely running Microsoft Windows 11/10/2022 or FreeBSD 6.X.
- **Vulnerabilities:** No specific vulnerabilities were detected for the identified open ports.
- **Advanced Scanning:** ACK and decoy scans confirmed the filtered state of other ports and the consistency of open port results.

In Task 3, I used Nmap to:

- Identify live hosts using a basic ping scan.
- Detect open ports and their associated services versions using SYN scans.
- Attempted to determine the operating system running on the target.

- Conducted a detailed scan combining various options, including using NSE scripts to detect specific vulnerabilities.
- Saved scan results in multiple formats for analysis.
- Employed advanced techniques like ACK scans and decoy scans to uncover hidden or filtered ports.
- Compiled all findings into a comprehensive report detailing open ports, services, versions, potential vulnerabilities, and OS details.