Cybersecurity Internship Task 1: Network Port Scanning Report

Objective

Conduct a scan of the local network to identify live hosts and open ports using Nmap. Analyze the network exposure, determine associated risks, and document the findings in a structured manner.

Tools Utilized

- **Nmap** – Used for discovering hosts and services on a network.
- **Wireshark (Optional)** – Used to monitor and analyze network packets during the scan.
- **GitHub** – Used to maintain version-controlled documentation and share findings.

Procedure

1. Installing Nmap

Nmap was downloaded from the official nmap.org site and installed on a Kali Linux virtual machine environment. The command-line interface was used to run all scans.

---

2. Determining Local IP Range

Using ifconfig, the primary interface (eth0) details were retrieved:

- **IPv4 Address**: 192.168.xxx.xxx
- **Subnet Mask**: 255.255.255.0
- **Broadcast**: 192.168.xxx.255
- **MAC Address**: 00:0c:xx:d4:xx:f8

From the above, the subnet range was calculated as:
CIDR Range: 192.168.xxx.0/24
Addressable Range: 192.168.xxx.1 to 192.168.xxx.254

---

3. Conducting the Scan

A stealth SYN scan was performed using the following command:

nmap -sS 192.168.xxx.0/24

Scan Results

IP Address	Status	Open Ports	MAC Address	Device Type
192.168.xxx.1	Up	All Filtered	00:50:56:C0:00:08	VMware NAT
192.168.xxx.2	Up	53/tcp	00:50:56:F5:CE:57	VMware Host
192.168.xxx.254	Up	All Filtered	00:50:56:EE:52:74	VMware NAT
192.168.xxx.xxx	Up	None	(This System)	Kali Linux

Observations:

- DNS service (port 53) was found open on 192.168.xxx.2.
- Other hosts returned filtered or closed results, indicating tight firewall controls or minimal exposure.
- All MAC addresses point to VMware virtual adapters.

---

4. Result Analysis

The network scan identified a limited number of open ports, which is consistent with a securely configured virtual environment.

Only **port 53 (DNS)** was found open, hosted by dnsmasq 2.51, a lightweight DNS forwarder and DHCP server often used in virtual or isolated test networks.

The rest of the devices showed no open ports, suggesting firewall filtering or services being disabled.

Common Ports in Broader Scans

Although the current environment had limited exposure, typical port scan results often include:

Port	Protocol	Service	Description
22	TCP	SSH	Secure shell access
23	TCP	Telnet	Obsolete remote login
25	TCP	SMTP	Mail service
53	TCP/UDP	DNS	Domain name resolution
80	TCP	HTTP	Unencrypted web traffic
110	TCP	POP3	Email retrieval
139	TCP	NetBIOS	Windows networking
443	TCP	HTTPS	Encrypted web service
445	TCP	SMB	Windows file sharing

Security Risk Assessment

While this scan revealed a low-visibility network setup, it's critical to understand potential vulnerabilities in other real-world contexts. The following ports and services are considered risky:

Port	Service	Risk Description
21	FTP	Sends credentials in cleartext
23	Telnet	No encryption; deprecated
25	SMTP	Can be abused for spam relays
110	POP3	Lacks modern encryption
139/445	SMB	Exploitable via known vulnerabilities (e.g., EternalBlue)

Even benign services like DNS (e.g., dnsmasq) should be monitored for known CVEs if they run outdated versions.

Optional: Wireshark Packet Inspection

Using Wireshark during the Nmap scan revealed:

- Outgoing TCP SYN packets targeting various ports/IPs.
- Only 192.168.xxx.2 responded with SYN-ACK (port 53), confirming it was open.
- No full TCP handshakes occurred, confirming stealth behavior from -sS scan.
- No anomalies or unauthorized data exchanges were captured.

This packet-level validation supports the minimal exposure results seen in Nmap

---

Saving Scan Results

Text Format

nmap -sS 192.168.xxx.0/24 -oN network_scan.txt

HTML Report

nmap -sS 192.168.xxx.0/24 -oX scan.xml xsltproc scan.xml -o scan_report.html

Alternative – Save in All Formats

nmap -sS 192.168.xxx.0/24 -oA complete_scan

This will generate:

- complete_scan.nmap
- complete_scan.xml
- complete_scan.gnmap

Conclusion

The scan confirmed that the local virtual environment operates in a tightly secured state, exposing minimal services. This controlled setup is ideal for security-focused experimentation and training. In real-world networks, regularly auditing open ports and their corresponding services is essential to prevent unauthorized access or exploitation.