Internship Report: Network Scanning and Packet Analysis Using Nmap and Wireshark

1. Introduction

As part of my internship assignment, I conducted a network reconnaissance and packet analysis activity using Nmap and Wireshark. The goal of this task was to understand the structure of a local network, identify open ports, active services, and evaluate potential vulnerabilities that could pose security threats.

2. Tools and Environment Setup

2.1 Operating Environment

The scanning and packet analysis were performed on a system running Windows 10, using the command-line interface PowerShell. Network connectivity was established through a Wi-Fi interface.

2.2 Tools Used

- Nmap 7.97: A powerful open-source network scanner
- Wireshark: A packet analyzer for network troubleshooting and protocol development
- PowerShell: Windows shell used for executing scanning commands
- Target Network: 192.168.1.0/24

3. Network Scanning Procedure

3.1 Nmap Installation Verification

To verify Nmap installation, the following command was executed:

```
nmap -v
```

The output confirmed that Nmap version 7.97 was installed, and data files were correctly loaded from the path: C:\Program Files (x86)\Nmap.

3.2 Determining Local IP and Network Range

Using the command 'ipconfig', the following network configuration was found:
- IPv4 Address: 192.168.1.184
- Subnet Mask: 255.255.255.0

- Default Gateway: 192.168.1.254
This implies the local IP range is 192.168.1.0/24.

3.3 Performing TCP SYN Scan

The following scan command was executed:

nmap -sS 192.168.1.0/24

Open ports found on host 192.168.1.184 are as follows:

Port	State	Service
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3306/tcp	open	mysql
6646/tcp	open	unknown/custom

4. Packet Capture Analysis with Wireshark

4.1 Capturing Packets

Wireshark was used to capture live network traffic on the Wi-Fi interface. The interface displayed thousands of network packets, revealing how the system interacts within the local network and beyond.

4.2 Key Observations

- Frequent ARP broadcasts identified 192.168.1.184 as actively announcing its MAC address.
- Duplicate use of IP 192.168.0.1 was detected across multiple devices, suggesting network misconfiguration.
- ICMPv6 neighbor solicitation and advertisement packets were noted.
- DNS and mDNS queries such as '_tcp.local' indicated the presence of IoT or LAN-based devices.
- External IPs observed included 57.144.169.33, 204.79.197.222, and 20.190.145.141.
- Communication was seen on ports such as 5222 and high ephemeral client ports.

5. Security Risk Assessment and Recommendations

Port	Risk Description	Recommendation
135	May expose DCOM, allowing remote code execution	Restrict/block externally, patch system
139	Legacy NetBIOS could be exploited for SMB relay attacks	Disable NetBIOS if unused

445	Vulnerable to known SMB attacks like EternalBlue	Apply latest patches and use firewall rules
3306	Potential MySQL exposure to unauthorized access	Bind MySQL to localhost or secure with firewall
6646	Unknown service could indicate custom or rogue application	Investigate service and disable if unnecessary

6. Saving and Exporting Nmap Scan Results

To retain scan results for future reference, the following commands were used:

```
nmap -sS 192.168.1.0/24 -oN scan_output.txt
```

For HTML export:

```
nmap -sS 192.168.1.0/24 -oX scan_output.xml
xsltproc scan_output.xml -o scan_output.html
```

7. Conclusion

The Nmap and Wireshark-based analysis successfully identified active services, open ports, and potential security risks on the local network. The task strengthened practical skills in vulnerability detection, network traffic monitoring, and risk analysis. Future exercises could explore deeper packet inspection, automated vulnerability scoring, and segment-wise network mapping.