**Network Mapping and Intrusion Detection Report on Kali Linux**

**Objective:**

In this assignment, you will perform a network scan on a compromised server, **scanme.nmap.org**, using Nmap, and use Wireshark to detect and analyze the network traffic generated by the scan. This assignment will help you understand how network vulnerabilities can be exploited and how network traffic analysis tools can be used to detect such intrusions.

**Tasks:**

**Task 1: Scan the Compromised System, scanme.nmap.org, Using Nmap**

1. From your Kali Linux system (or VM), use Nmap to perform a detailed network scan of the compromised server. You should run both aggressive and version detection scans to map out the system's open ports and services.

2. Commands:

Perform an aggressive Nmap scan of the compromised system:

*sudo nmap -A -T4 -p- <server\_IP>*

Perform a version detection scan on a specific port, for example, FTP:

*sudo nmap -sV -p 21 --script ftp-anon <server\_IP>*

Record your observations on the services and versions running on the server.

**Task 2: Monitor Network Traffic with Wireshark**

1. While the Nmap scan is running, use Wireshark on Kali Linux to monitor the network traffic between your system and the compromised server.
   1. Capture the packets to detect any suspicious or intrusive activity related to the Nmap scan.

**Commands:**

Open Wireshark and start monitoring the correct network interface:

*sudo wireshark*

Select the interface (e.g., eth0 or wlan0) to begin capturing traffic.

Use display filters in Wireshark to focus on traffic coming from or going to the compromised system:

*ip.addr == <server\_IP>*

Look for signs of a network scan, such as numerous SYN packets, ICMP echo requests, or unusual TCP resets.

Capture at least 5 minutes of network traffic and save the results.

**Task 4: Analyze the Results**

1. Review the output from Nmap and note the open ports, services, and potential vulnerabilities discovered.
2. Examine the Wireshark packet capture to identify the scan signatures and document any unusual network activity that was observed.  
   - Look for SYN scans, OS fingerprinting packets, or service probes.
3. Submit a report that includes:  
   - A summary of the Nmap scan results (open ports, services, versions, potential vulnerabilities).  
   - A screenshot of the Wireshark capture highlighting suspicious activity.  
   - An explanation of how Wireshark detected the Nmap scan.  
   - Conclusions on the security weaknesses of the compromised system.

**Index of Commands**

|  |  |  |
| --- | --- | --- |
| Tool | Function | Command |
| Nmap | Perform an aggressive scan | sudo nmap -A -T4 -p- <server\_IP> |
| Nmap | Scan for service versions | sudo nmap -sV -p 21 --script ftp-anon <server\_IP> |
| Wireshark | Start Wireshark and monitor traffic | sudo wireshark |
| Wireshark | Apply display filter for specific IP address | ip.addr == <server\_IP> |
| Wireshark | Capture packets and save results | Use the 'Capture' menu and click 'Save As' |