CSF-II

Lab 1: NMAP: Network Mapping and Port Scanning

Objective:

To understand how to use NMAP for TCP port scanning and perform network monitoring tasks.

Tools Required:

- NMAP

Theory:

NMAP is a powerful open-source network scanning tool used to discover hosts, services, and open ports on a network. It supports a wide range of scanning options like SYN scan, version detection, OS detection, and more.

Procedure:

1. Basic Host Discovery:

   nmap -sn 192.168.1.0/24

2. TCP Port Scan:

   nmap -sT 192.168.1.1

3. SYN Scan (Stealth Scan):

   nmap -sS 192.168.1.1

4. OS Detection:

   nmap -O 192.168.1.1

5. Service Version Detection:

   nmap -sV 192.168.1.1

6. Scan Multiple IPs:

   nmap 192.168.1.1 192.168.1.2

7. Scan IP Range:

   nmap 192.168.1.1-20

8. Aggressive Scan:

   nmap -A 192.168.1.1

9. Detect Firewalls:

   nmap -PN 192.168.1.1

10. Output Scan to File:

   nmap -oN result.txt 192.168.1.1

Expected Output:

- List of active hosts, open ports, OS details, and running services.

Observations:

- Note different scan outputs and time for each.

Lab 2: Wireshark: Packet Capture and Analysis

Objective:

To use Wireshark for packet filtering and analyzing source and destination IP addresses.

Tools Required:

- Wireshark

Theory:

Wireshark is a network protocol analyzer used to capture and interactively browse network traffic. It supports hundreds of protocols and filtering mechanisms.

Procedure:

1. Launch Wireshark and select active network interface.
2. Start capture and filter traffic using:
   - ip.src == 192.168.1.2
   - ip.dst == 192.168.1.5
   - http, tcp.port == 80, udp
3. Analyze protocols using Statistics > Protocol Hierarchy.
4. Detect source and destination IPs via packet details.
5. Use color rules for better visibility.
6. Save capture file for later analysis.

Expected Output:

- Real-time display of packet traffic.
- Filters showing relevant data.

Observations:

- Record the number of packets captured.

- Note anomalies and frequent IPs.

Lab 3: DVWA: Attacks on Web Application

Objective:

To understand the working of DVWA and perform attacks such as XSS and SQL Injection.

Tools Required:

- DVWA (Damn Vulnerable Web Application)
- Web browser

Theory:

DVWA is a PHP/MySQL web application vulnerable to many web attacks. It is used for testing common vulnerabilities.

Procedure:

1. Start DVWA from localhost (XAMPP or Docker).
2. Set security level to low from setup.
3. Go to XSS (Reflected) module and input:

   <script>alert('XSS')</script>

4. Observe if an alert popup appears.
5. Go to SQL Injection module and input:

   ' OR 1=1 --

6. Observe if it retrieves all user data from the database.

Expected Output:

- XSS alert popup and user data from SQL Injection.

CSF-II

Observations:

- Behavior of DVWA on low, medium, high security.

- Payload effects and potential defenses.