PRACTICAL NO. 3

A. Perform Enumeration using the following tools

Aim

To perform **enumeration** on a target system using various tools in order to extract detailed information such as open ports, services, shared resources, users, and network details.

Tools / Software Used

- Kali Linux
- Nmap
- NetBIOS Enumeration Tool
- SuperScan
- Hyena
- SoftPerfect Network Scanner
- OpUtils
- SolarWinds Engineer’s Toolset
- Wireshark

Theory

Enumeration is the process of actively connecting to a target system to gather detailed information.
It is performed **after footprinting and scanning** and helps in identifying:

- User accounts
- Network shares
- Open ports and services
- System names and configurations

◆ (i) Nmap

Aim

To enumerate open ports and services using Nmap.

Steps / Procedure

1. Start **Kali Linux**.
2. Open **Terminal**.
3. Type the command:
4. `nmap 192.168.1.1`
5. Press Enter.
6. To detect services, use:
7. `nmap -sV 192.168.1.1`

Result

Nmap displays open ports and running services.

◆ (ii) NetBIOS Enumeration Tool

Aim

To enumerate NetBIOS information such as shared resources and machine names.

Steps

1. Open **NetBIOS Enumeration Tool**.
2. Enter target IP address.
3. Click **Scan**.
4. Observe shared folders and NetBIOS names.

Result

NetBIOS details of the target system are obtained.

◆ (iii) SuperScan

Aim

To enumerate IP addresses and open ports.

Steps

1. Open **SuperScan**.
2. Enter target IP range.
3. Select scan type (TCP/UDP).
4. Click **Start Scan**.
5. View open ports and services.

Result

SuperScan lists open ports and active hosts.

◆ (iv) Hyena

Aim

To enumerate users, groups, and network resources.

Steps

1. Open **Hyena** tool.
2. Connect to the target system.
3. Browse users and groups.
4. View shared folders and permissions.

Result

User and group information is displayed.

◆ (v) SoftPerfect Network Scanner

Aim

To scan and enumerate network devices.

Steps

1. Open **SoftPerfect Network Scanner**.
2. Enter IP address range.
3. Click **Start Scanning**.

4. View device name, MAC address, and shared folders.

Result

Network devices are successfully enumerated.

◆ (vi) OpUtils

Aim

To enumerate IP and switch port details.

Steps

1. Open **OpUtils**.
2. Select IP Scanner.
3. Enter IP range.
4. Start scanning.
5. Analyze IP and port information.

Result

IP address and port usage details are obtained.

◆ (vii) SolarWinds Engineer’s Toolset

Aim

To enumerate network performance and devices.

Steps

1. Open **SolarWinds Engineer’s Toolset**.
2. Select network discovery tools.
3. Enter target IP range.
4. Run scan.
5. View detailed network information.

Result

Network infrastructure details are displayed.

◆ (viii) Wireshark

Aim

To enumerate network traffic and protocols.

Steps

1. Open **Wireshark**.
2. Select active network interface.
3. Click **Start Capture**.
4. Observe packets and protocols.
5. Stop capture after analysis.

Result

Network traffic and protocol details are captured.