1.B. Scan the network using the following tools

Aim

To identify active hosts, open ports, and network services.

◆ (i) Hping2 / Hping3

Steps

1. Open Kali Linux Terminal.
2. Type:
3. `hping3 -S 192.168.1.1 -p 80`
4. Observe packet response.

◆ (ii) Advanced IP Scanner

Steps

1. Open Advanced IP Scanner.
2. Enter IP range.
3. Click **Scan**.
4. View connected devices.

◆ (iii) Angry IP Scanner

Steps

1. Open Angry IP Scanner.
2. Enter IP range.
3. Click **Start**.
4. View open ports.

◆ (iv) Masscan

Steps

1. Open Kali Linux Terminal.
2. Type:
3. `masscan -p22,80,445 192.168.1.0/24`
4. Press Enter.

◆ (v) NEET

Steps

1. Open NEET tool.
2. Configure scan parameters.
3. Start scan.
4. Analyze vulnerabilities.

◆ (vi) CurrPorts

Steps

1. Open CurrPorts.
2. View active TCP/UDP connections.
3. Identify suspicious processes.

◆ (vii) Colasoft Packet Builder

Steps

1. Open Colasoft Packet Builder.
2. Create custom packet.
3. Send packet to target.
4. Analyze response.

◆ (viii) The Dude

Steps

1. Open The Dude.
2. Add network devices.
3. Monitor device status.
4. View network topology.

Result

Thus, footprinting, reconnaissance, and network scanning were successfully performed using various tools.

🎯 Viva Line

“Footprinting is a critical phase that helps in identifying system weaknesses before an attack.”