PRACTICAL NO. 1

A. Use the following tools to perform Foot printing and Reconnaissance

---

Aim

To perform foot printing and reconnaissance using various tools in order to collect preliminary information about the target such as domain details, IP address, network paths, email information, and server details.

Tools / Software Used

- Kali Linux
- Recon-ng
- FOCA Tool
- Windows Command Prompt
- HTTrack Website Copier
- Metasploit Framework
- SmartWhois
- eMailTracker Pro
- Mobile Network Tools

Theory (Write Once)

Footprinting is the initial phase of ethical hacking where information about the target system is collected using passive and active methods. Reconnaissance helps attackers and security professionals understand the target's infrastructure without directly attacking it.

◆ (i) Recon-ng (Using Kali Linux)

Aim

To collect reconnaissance information about a target domain using Recon-ng.

Steps / Procedure

1. Start **Kali Linux**.
2. Open **Terminal**.
3. Type the command:
4. `recon-ng`

   and press Enter.

5. To search available modules, type:
6. `marketplace search`
7. To install a module, type:
8. `marketplace install hackertarget`
9. Load the installed module using:
10. `modules load hackertarget`
11. View available options:
12. `show options`
13. Set the target domain:
14. `options set SOURCE tesla.com`
15. Execute the scan:
16. `run`

Result

Recon-ng successfully collects domain and reconnaissance details.

◆ (ii) FOCA Tool

Aim

To extract metadata from publicly available documents.

Steps / Procedure

1. Open **FOCA Tool**.
2. Click on **Project → New Project**.
3. Enter the target website URL.
4. Click **Create**.
5. Select search engine and file extensions.
6. Click on **Search All**.
7. Download the discovered documents.
8. Analyze metadata such as usernames and software details.

Result

Metadata information from documents is successfully extracted.

◆ (iii) Windows Command Line Utilities

a) Ping

Aim: To check connectivity between systems.

Steps

1. Open **Command Prompt**.
2. Type:
3. `ping google.com`
4. Press Enter.

---

b) Tracert using Ping

Aim: To identify the path using ping options.

Steps

1. Open **Command Prompt**.
2. Type:
3. `ping certifiedhacker.com -n 1 -I 1`
4. Press Enter.

---

c) Tracert

Aim: To trace the route taken by packets.

Steps

1. Open **Command Prompt**.
2. Type:
3. `tracert www.reddit.com`
4. Press Enter.

---

d) NSLookup

Aim: To retrieve DNS records.

Steps

1. Open **Command Prompt**.
2. Type:
3. `nslookup google.com`
4. Press Enter.

◆ (iv) Website Copier Tool – HTTrack

Aim

To create an offline copy of a website.

Steps / Procedure

1. Open **HTTrack Website Copier**.
2. Click **Next** to create a new project.
3. Enter project name.
4. Click **Add URL** and enter website URL.
5. Click **Next → Finish**.
6. Wait for mirroring process to complete.
7. Browse the mirrored website.

Result

Website is successfully copied offline.

◆ (v) Metasploit (Information Gathering)

Aim

To gather information using Metasploit framework.

Steps / Procedure

1. Open **Kali Linux Terminal**.
2. Type:
3. `msfconsole`

4. Use auxiliary scanning modules.
5. Scan target to gather service and host details.

Result

Target system information is obtained.

◆ (vi) Whois Lookup Tools for Mobile

Aim

To perform WHOIS lookup using mobile tools.

Steps

1. Install **DNS Tools / Whois / Ultra Tools Mobile**.
2. Enter domain name.
3. View registration and IP details.

◆ (vii) SmartWhois

Aim

To obtain domain ownership information.

Steps

1. Open **SmartWhois**.
2. Enter IP address or domain name.
3. Click **Search**.
4. View WHOIS information.

◆ (viii) eMailTracker Pro

Aim

To trace email origin.

Steps

1. Open **eMailTracker Pro**.
2. Enter email address.
3. Click **Trace**.
4. View location and server details.
5. Click **View Report**.

◆ (ix) Mobile Network Tools

Aim

To scan network using mobile applications.

Steps

1. Install **Fing / Network Scanner / PortDroid**.
2. Connect to Wi-Fi network.
3. Start scan.
4. View connected devices and ports.