**Exercise 7:**

**7. External Penetration Testing**

**a. Evaluating external Infrastructure**

**b. Creating topological map & identifying IP address of target**

**a. Evaluating external Infrastructure**

**Aim:**

To perform external infrastructure evaluation by identifying live hosts, open ports, services, and potential vulnerabilities using real-world penetration testing techniques on a controlled lab environment.

### **Lab Requirements**

* Kali Linux
* Target VM or external test server (e.g., Metasploitable)
* Internet connection (if using online labs)
* Tools:
  + nmap
  + whois
  + netcat
  + curl
  + Optional: OpenVAS, Burp Suite, Shodan, Recon-ng

### ****Procedure:****

### Step 1: Information Gathering (Passive Reconnaicence)

### Use whois to gather domain ownership and contact details

### Step 2: Scanning (Active Recon)

1. Use nmap to scan the target network/IP range for live hosts:

nmap -sn <target-range>

1. Perform a detailed scan to identify open ports and services:

nmap -sV -sC -Pn <target-IP>

Step 3: Service Enumeration

1. Identify software versions and banner information.
2. For web servers, use:
   * WhatWeb
   * curl -I <URL> (to inspect HTTP headers)

Step 4: Vulnerability Detection

1. Match software versions with known vulnerabilities (CVE search).
2. Optionally, use:
   * Searchsploit
   * OpenVAS (if configured)

**b. Creating topological map & identifying IP address of target**

**Aim:**

To discover, analyze, and visually map a target's external infrastructure by identifying IP addresses, active hosts, and services using reconnaissance and scanning tools.

Create a basic **network topology map** of discovered systems.

Required softwares:

* **Operating System:** Kali Linux or Parrot OS
* **Scanning Tools:**
  + nmap, Zenmap (GUI version of Nmap)
  + Netdiscover (for LANs, if applicable)
  + traceroute, whois, nslookup, dig
  + theHarvester (for DNS and email footprinting)
* **Mapping Tools:**
  + **oDraw.io / Lucidchart**
  + Zenmap (built-in topology feature),
  + Maltego (for advanced visualizations)

Procedure

Use tools to identify the domain’s IP address and related information:

1. nslookup scanme.nmap.org
2. Zenmap (built-in topology feature),