**Batch: B1 Roll No.: 16010121045**

**Experiment No. 2**

|  |
| --- |
| **Title:**  Perform reconnaissance using network information gathering tool |

**Objective:**

Perform reconnaissance using network information gathering tool

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO1** | Understand penetration testing with scope of its ethical implications, documentation and reporting |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Books/ Journals/ Websites referred:**

* <https://www.blumira.com/glossary/reconnaissance/#:~:text=In%20the%20context%20of%20cybersecurity,ethical%20hacking%20or%20penetration%20testing>
* <https://www.firecompass.com/blog/top-10-tools-for-reconnaissance/>
* <https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/>

**Introduction:**

**Reconnaissance:** Reconnaissance, as utilized in cybersecurity, refers to the clandestine process of gathering data and insights into a system. Commonly employed in penetration testing or ethical hacking, this technique originates from military operations designed to gather intelligence from hostile territories. Reconnaissance typically involves seven sequential steps:

1. **Collect initial information**
2. **Determine the network range**
3. **Identify active machines**
4. **Find access points and open ports**
5. **Fingerprint the operating system**
6. **Discover services on ports**
7. **Map the network**

By following these steps, an attacker seeks to gather crucial information about a network, including file permissions, running network services, OS platform, trust relationships, and user account information. Port scanning, a common technique within reconnaissance, entails sending data to various TCP and UDP ports on a device to evaluate responses. Active and passive reconnaissance are the primary categories of reconnaissance techniques.

* **Active reconnaissance** involves direct interaction with the computer system, utilizing methods such as manual testing, automated scanning, and tools like ping and netcat. While active recon is faster and more precise, it's riskier due to increased system noise and visibility.
* **Passive reconnaissance** collects data without interacting with systems directly, using tools like Wireshark and Shodan, as well as techniques like OS fingerprinting.

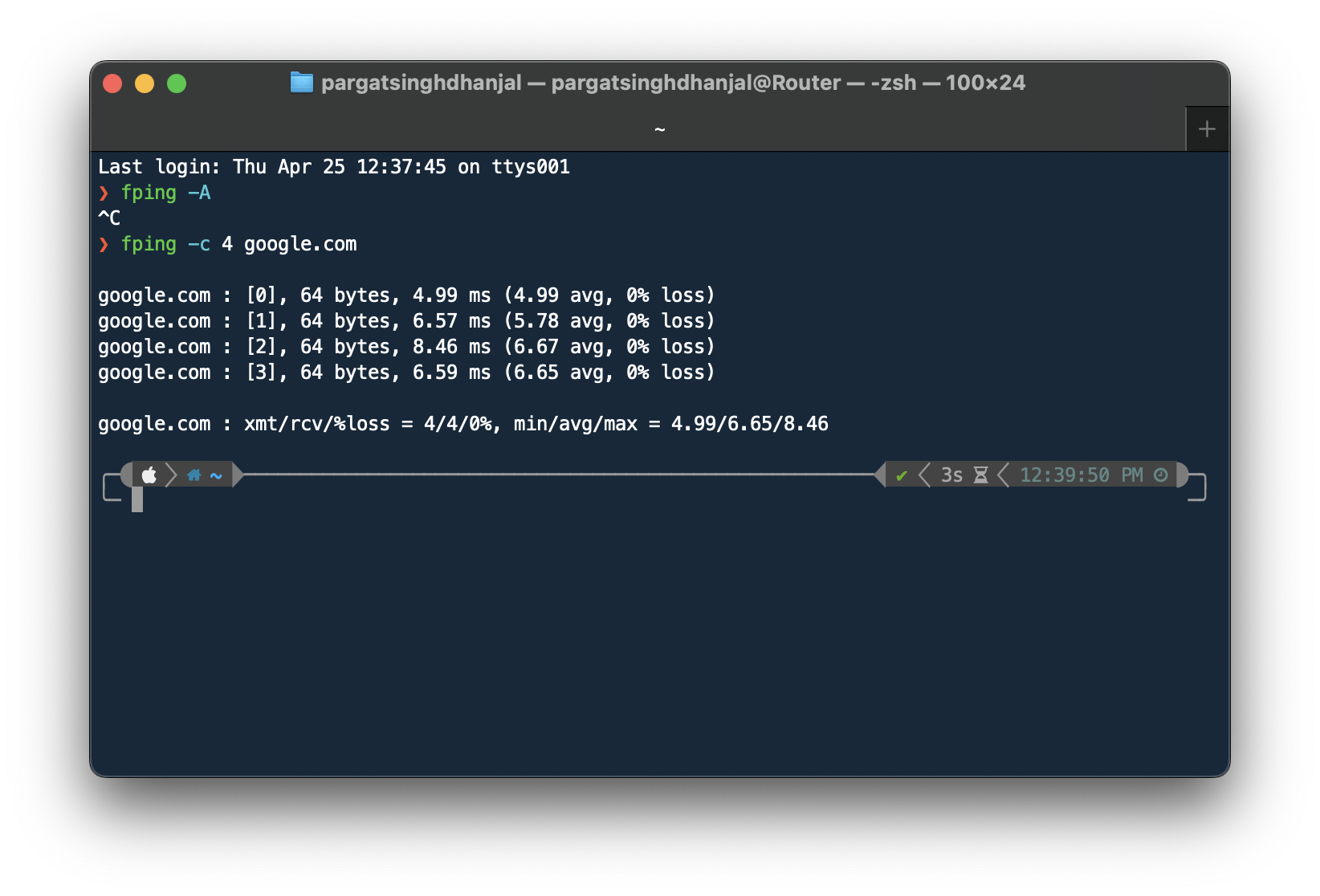
Organizations can employ various strategies to prevent reconnaissance:

* **Penetration testing** allows businesses to assess potential vulnerabilities through simulated attacks. Employing security testing experts for penetration testing, vulnerability assessments, and compliance testing can help organizations outsource this task.
* Utilizing **vulnerability scanners** and port scanning software during testing can identify active hosts and known vulnerabilities within the network.
* **SIEM solutions** can help detect source IPs running port scanners on the network.
* The **MITRE ATT&CK Framework** offers further insights into reconnaissance prevention methods.

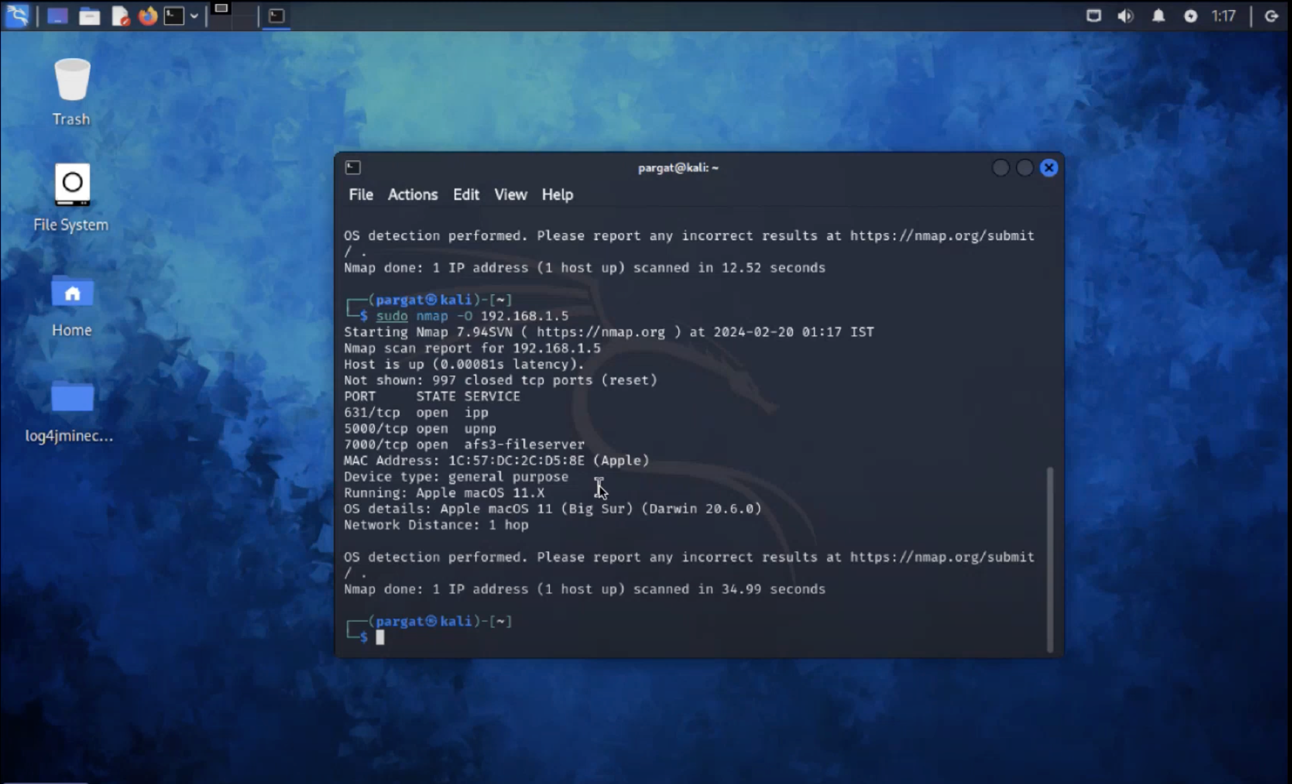
**Implementation details:**

Performing reconnaissance using network information gathering tools typically involves using a variety of tools to gather information about a target network, such as its IP addresses, open ports, services running on those ports, and potentially even vulnerabilities present. Here's a basic outline of how you might perform reconnaissance using some common tools:

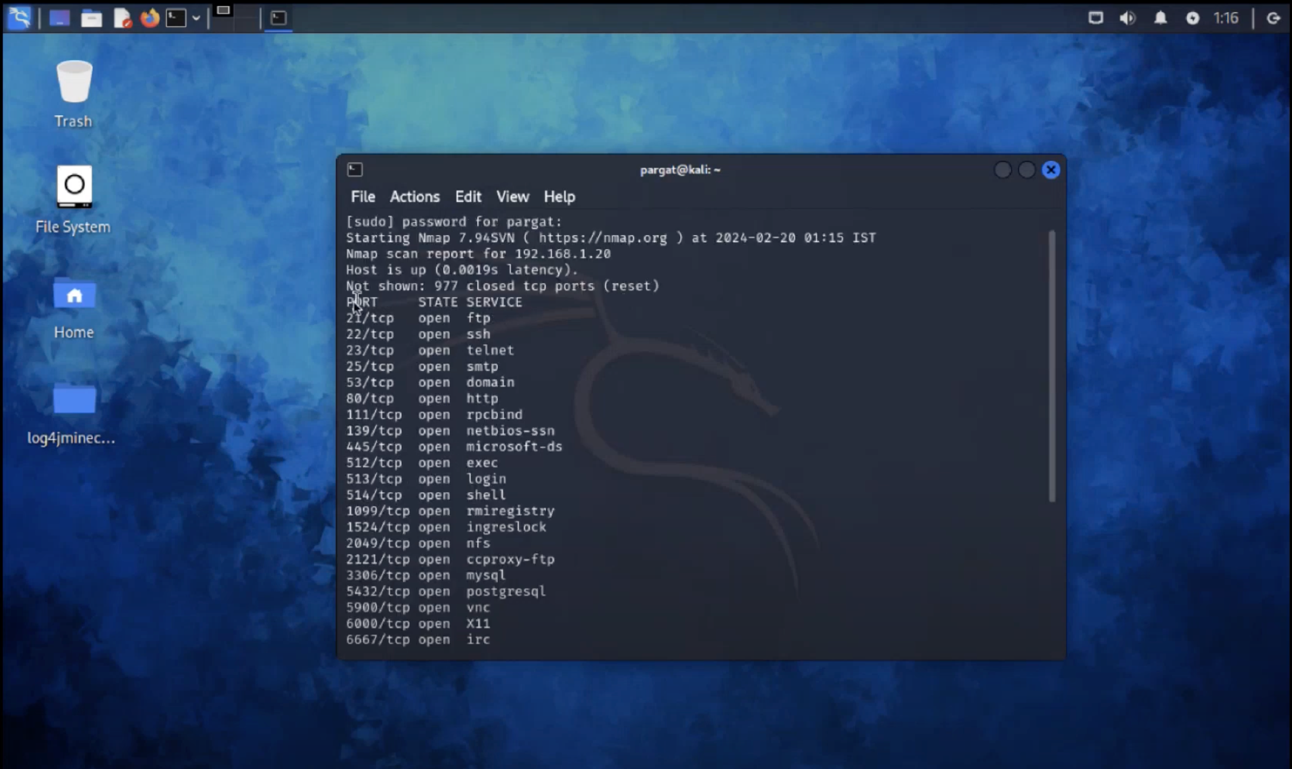
1. **Ping Sweep (ICMP)**:
   * Use a tool like **ping** or **fping** to perform a ping sweep across a range of IP addresses to identify which hosts are online.



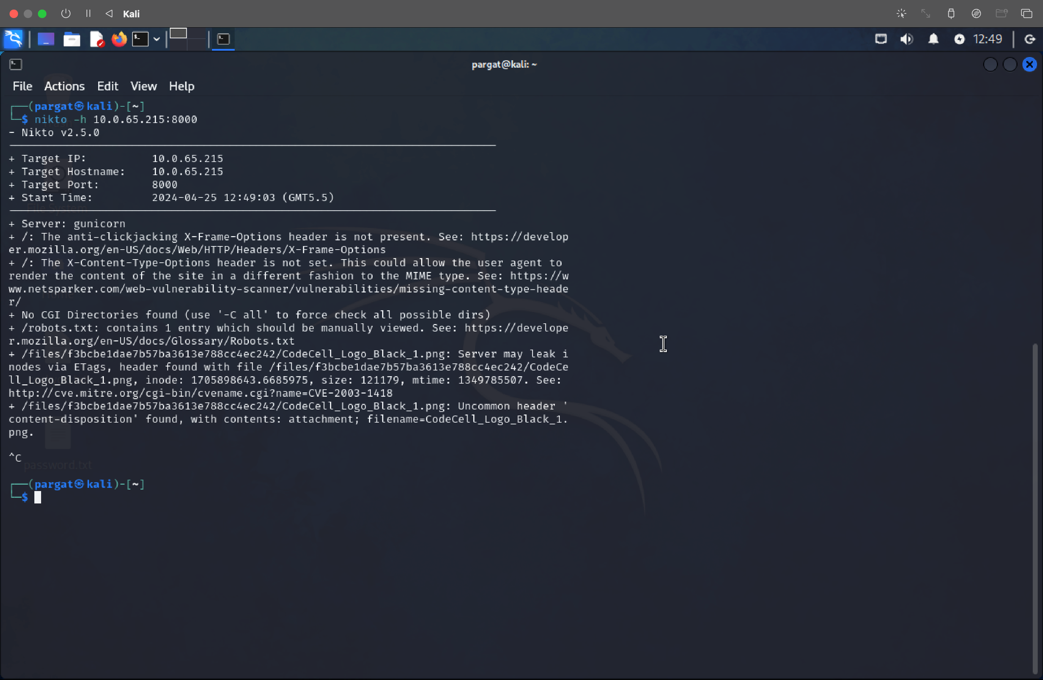
1. **Port Scanning**:
   * Utilize a port scanning tool like **Nmap** to scan the target network for open ports and the services running on those ports.
   * Example command: **nmap -O <target>** (Scan OS)
   * Example command: **nmap -sV <target>** (Service version detection)



1. **Service Enumeration**:
   * Once open ports are identified, use **Nmap** or other tools like **Netcat** or **Telnet** to connect to open ports and gather more information about the services running on them.
   * Example command: **nmap --script=default <target>** (Run default Nmap scripts for service enumeration)

****

1. **Web Application Analysis**:
   * If web services are discovered, use tools like **nikto**, **dirb**, or **gobuster** to identify directories, files, and potentially vulnerabilities on web servers.
   * Example command: **nikto -h <target>** (Web server vulnerability scanner)



1. **Network Mapping**:
   * Use tools like **Netdiscover** or **Arp-scan** to discover hosts on the local network or use **Traceroute** to map the network path between your system and the target.



1. **Exploitation**:
   * If vulnerabilities are discovered, you may attempt to exploit them using appropriate tools or manual techniques. However, ensure you have proper authorization before attempting any exploitation.
2. **Documentation**:
   * Throughout the reconnaissance process, document all findings, including IP addresses, open ports, services running, potential vulnerabilities, and any other relevant information.

**Conclusion:**

Hence we performed reconnaissance using network information gathering tool and listed some ways one may explore and attack on vulnerabilities.