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.

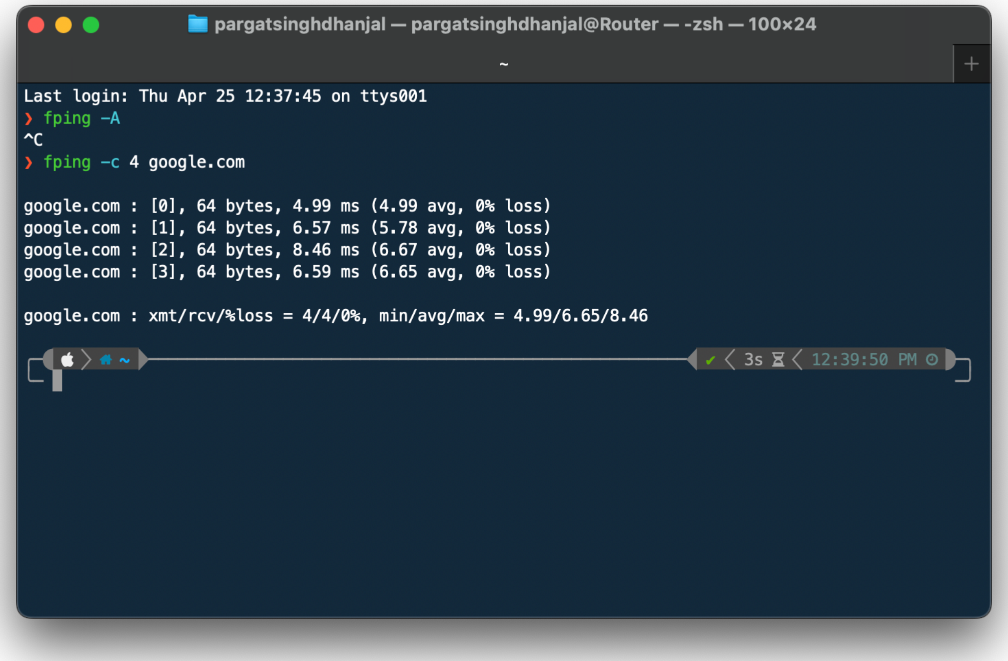
Organizations can employ various strategies to prevent reconnaissance:

- **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:

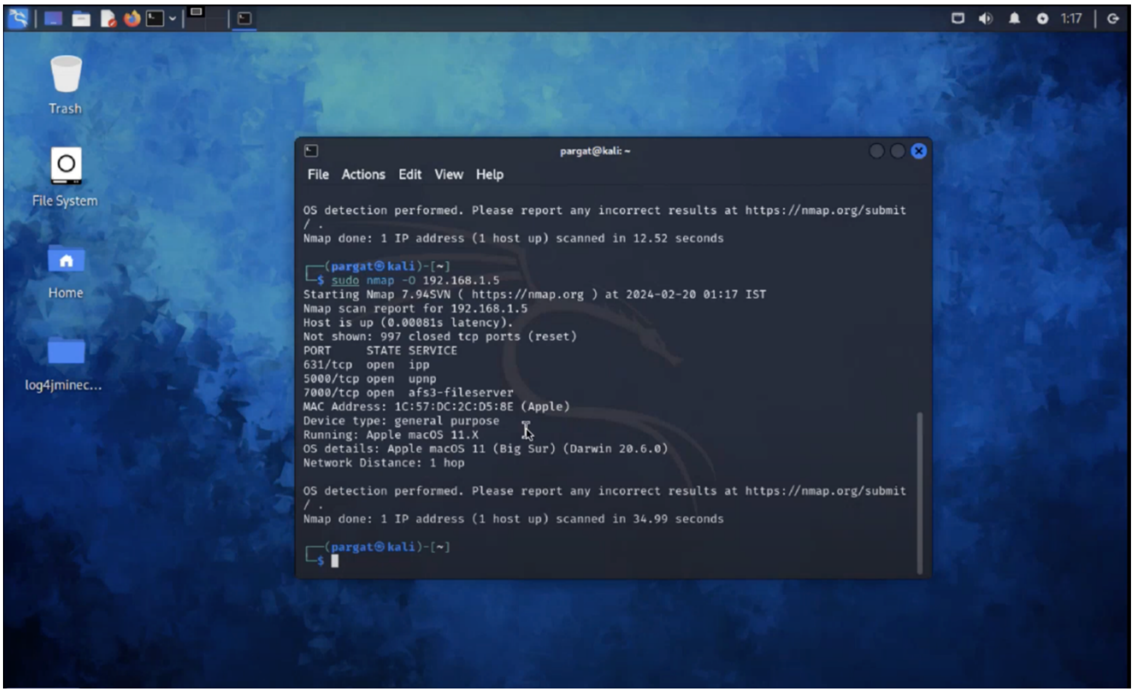
1. **Ping Sweep (ICMP)**:
   - Use a tool like **ping** or **fping** to perform a ping sweep across a range of IP addresses to identify which hosts are online.



pargatsinghdhanjal — pargatsinghdhanjal@Router — -zsh — 100×24
~

```
Last login: Thu Apr 25 12:37:45 on ttys001
❯ fping -A
^C
❯ fping -c 4 google.com

google.com : [0], 64 bytes, 4.99 ms (4.99 avg, 0% loss)
google.com : [1], 64 bytes, 6.57 ms (5.78 avg, 0% loss)
google.com : [2], 64 bytes, 8.46 ms (6.67 avg, 0% loss)
google.com : [3], 64 bytes, 6.59 ms (6.65 avg, 0% loss)

google.com : xmt/rcv/%loss = 4/4/0%, min/avg/max = 4.99/6.65/8.46

 ~                                                          ✓ 3s ⌛ 12:39:50 PM
```

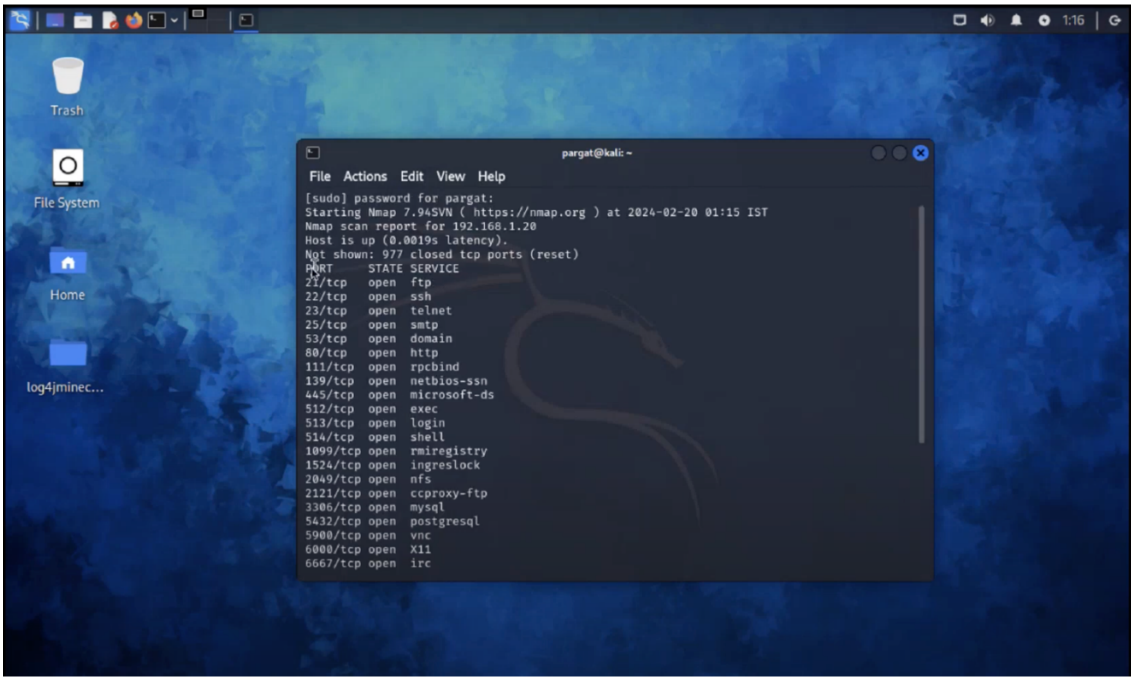
2. **Port Scanning**:
   - Utilize a port scanning tool like **Nmap** to scan the target network for open ports and the services running on those ports.
   - Example command: **nmap -O <target>** (Scan OS)
   - Example command: **nmap -sV <target>** (Service version detection)



```
OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 12.52 seconds

┌──(pargat㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 01:17 IST
Nmap scan report for 192.168.1.5
Host is up (0.00081s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
631/tcp  open  ipp
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 1C:57:DC:2C:D5:8E (Apple)
Device type: general purpose
Running: Apple macOS 11.X
OS details: Apple macOS 11 (Big Sur) (Darwin 20.6.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 34.99 seconds

┌──(pargat㉿kali)-[~]
└─$ 
```

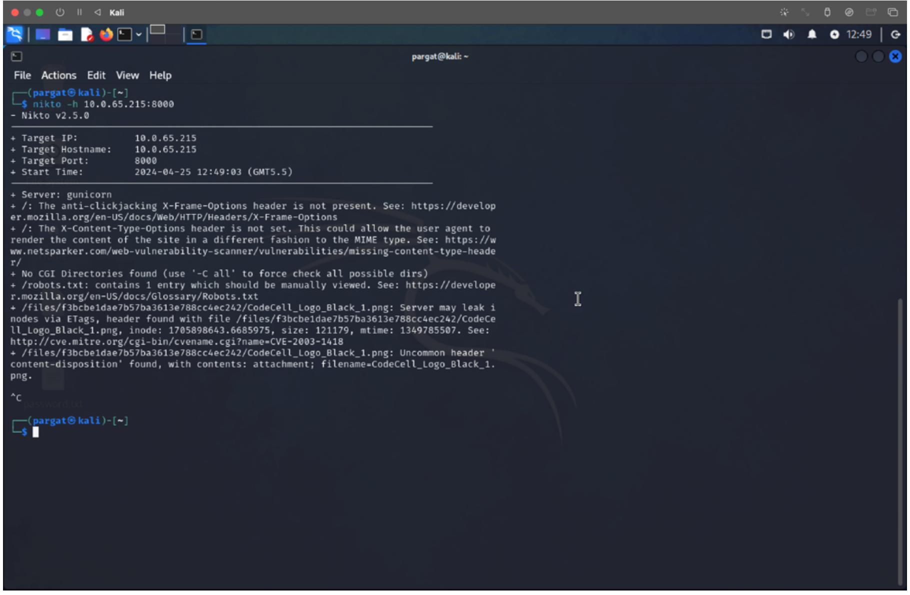
3. **Service Enumeration**:

- 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)



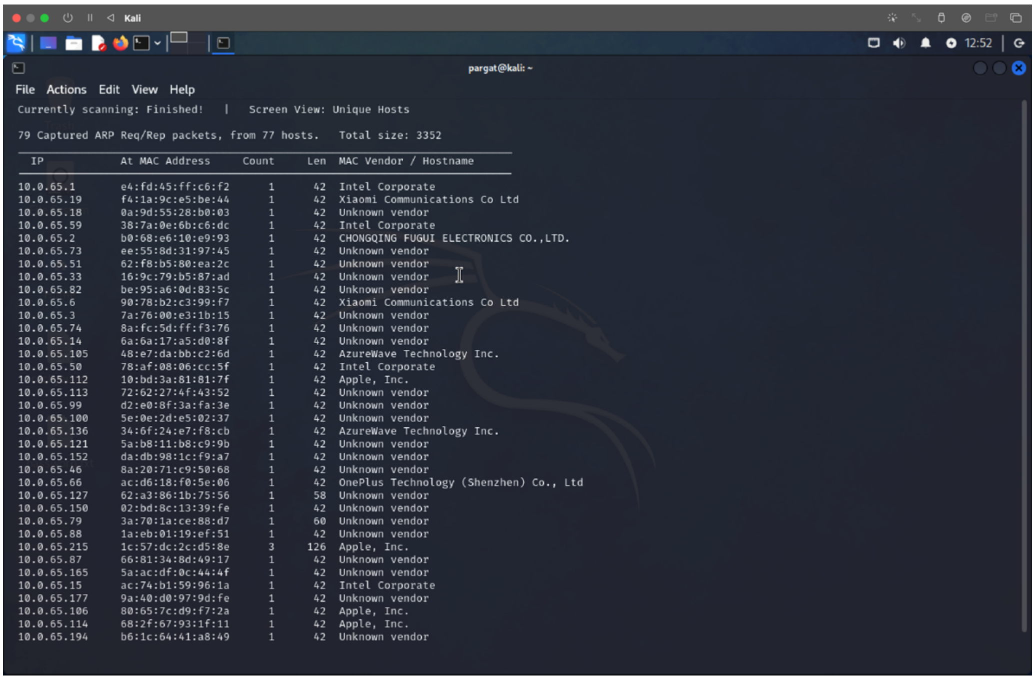
```
[sudo] password for pargat:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 01:15 IST
Nmap scan report for 192.168.1.20
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
```

4. **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)



```
┌──(pargat㉿kali)-[~]
└─$ nikto -h 10.0.65.215:8000
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.65.215
+ Target Hostname:    10.0.65.215
+ Target Port:        8000
+ Start Time:         2024-04-25 12:49:03 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gunicorn
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type. See: https://w
ww.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-heade
r/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://develope
r.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /files/f3bcbe1dae7b57ba3613e788cc4ec242/CodeCell_Logo_Black_1.png: Server may leak i
nodes via ETags, header found with file /files/f3bcbe1dae7b57ba3613e788cc4ec242/CodeCe
ll_Logo_Black_1.png, inode: 1705898643.6685975, size: 121179, mtime: 1349785507. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /files/f3bcbe1dae7b57ba3613e788cc4ec242/CodeCell_Logo_Black_1.png: Uncommon header '
content-disposition' found, with contents: attachment; filename=CodeCell_Logo_Black_1.
png.

^C

┌──(pargat㉿kali)-[~]
└─$ 
```

5. **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.



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 79 Captured ARP Req/Rep packets, from 77 hosts.   Total size: 3352
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.65.1       e4:fd:45:ff:c6:f2      1      42  Intel Corporate
 10.0.65.19      f4:1a:9c:e5:be:44      1      42  Xiaomi Communications Co Ltd
 10.0.65.18      0a:9d:55:28:b0:03      1      42  Unknown vendor
 10.0.65.59      38:7a:0e:6b:c6:dc      1      42  Intel Corporate
 10.0.65.2       b0:68:e6:10:e9:93      1      42  CHONGQING FUGUI ELECTRONICS CO.,LTD.
 10.0.65.73      ee:55:8d:31:97:45      1      42  Unknown vendor
 10.0.65.51      62:f8:b5:80:ea:2c      1      42  Unknown vendor
 10.0.65.33      16:9c:79:b5:87:ad      1      42  Unknown vendor
 10.0.65.82      be:95:a6:0d:83:5c      1      42  Unknown vendor
 10.0.65.6       90:78:b2:c3:99:f7      1      42  Xiaomi Communications Co Ltd
 10.0.65.3       7a:76:00:e3:1b:15      1      42  Unknown vendor
 10.0.65.74      8a:fc:5d:ff:f3:76      1      42  Unknown vendor
 10.0.65.14      6a:6a:17:a5:d0:8f      1      42  Unknown vendor
 10.0.65.105     48:e7:da:bb:c2:6d      1      42  AzureWave Technology Inc.
 10.0.65.50      78:af:08:06:cc:5f      1      42  Intel Corporate
 10.0.65.112     10:bd:3a:81:81:7f      1      42  Apple, Inc.
 10.0.65.113     72:62:27:4f:43:52      1      42  Unknown vendor
 10.0.65.99      d2:e0:8f:3a:fa:3e      1      42  Unknown vendor
 10.0.65.100     5e:0e:2d:e5:02:37      1      42  Unknown vendor
 10.0.65.136     34:6f:24:e7:f8:cb      1      42  AzureWave Technology Inc.
 10.0.65.121     5a:b8:11:b8:c9:9b      1      42  Unknown vendor
 10.0.65.152     da:db:98:1c:f9:a7      1      42  Unknown vendor
 10.0.65.46      8a:20:71:c9:50:68      1      42  Unknown vendor
 10.0.65.66      ac:d6:18:f0:5e:06      1      42  OnePlus Technology (Shenzhen) Co., Ltd
 10.0.65.127     62:a3:86:1b:75:56      1      58  Unknown vendor
 10.0.65.150     02:bd:8c:13:39:fe      1      42  Unknown vendor
 10.0.65.79      3a:70:1a:ce:88:d7      1      60  Unknown vendor
 10.0.65.88      1a:eb:01:19:ef:51      1      42  Unknown vendor
 10.0.65.215     1c:57:dc:2c:d5:8e      3     126  Apple, Inc.
 10.0.65.87      66:81:34:8d:49:17      1      42  Unknown vendor
 10.0.65.165     5a:ac:df:0c:44:4f      1      42  Unknown vendor
 10.0.65.15      ac:74:b1:59:96:1a      1      42  Intel Corporate
 10.0.65.177     9a:40:d0:97:9d:fe      1      42  Unknown vendor
 10.0.65.106     80:65:7c:d9:f7:2a      1      42  Apple, Inc.
 10.0.65.114     68:2f:67:93:1f:11      1      42  Apple, Inc.
 10.0.65.194     b6:1c:64:41:a8:49      1      42  Unknown vendor
```

6. **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.

7. **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.