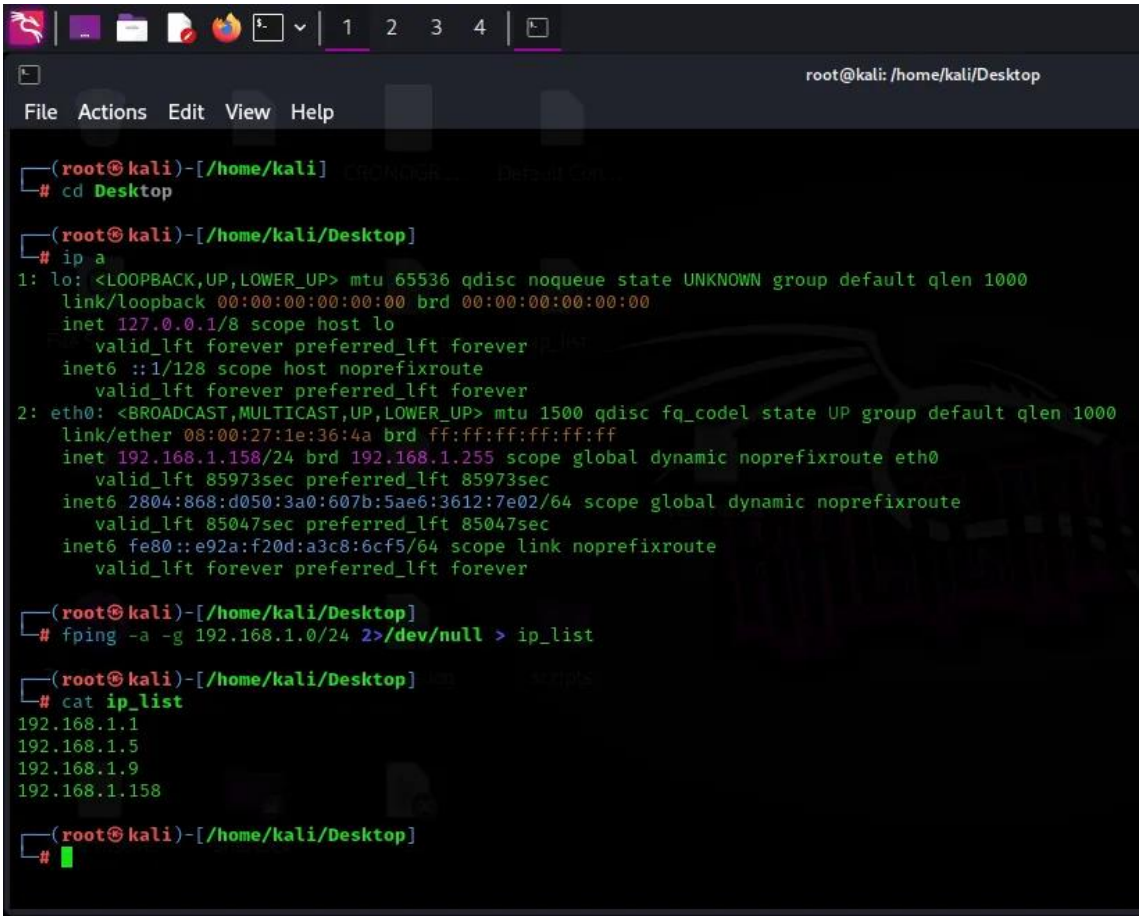
Name: Ruan Saure 23/06/2025

Summer Intership – Task 1



First of all, I entered in the Desktop directory to organize better the results of the scan, then, I executed the "***ip a***" command to Discover my ip, and the first ip of my network.

As my ipv4 is ***".158***" and my network is "***/24***", the network ip is "***.0***", so, I executed the "***fping -a -g ... 2>/dev/null > ip_list***" command to Discover all the online hosts in my network, that command will ignore all offline ips and will save the results in "ip_list", to let my scan with nmap easier.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS -iL ip_list > port_scan

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat port_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 12:17 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
MAC Address: C4:27:28:DE:92:AD (zte)

Nmap scan report for 192.168.1.5
Host is up (0.0045s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
1033/tcp  open  netinfo
1187/tcp  open  alias
2010/tcp  open  search
3000/tcp  open  ppp
3001/tcp  open  nessus
7000/tcp  open  afs3-fileserver
9080/tcp  open  glrpc
```

Here, I took the “ip_list” and have did a portscan with nmap in each host in that archive, and all of the open ports and it’s weakness will be reported below:

192.168.1.1:

Open Ports: 23, 53, 80 and 443

23 → Telnet: Telnet is a way to connect to a computer or other network device through a terminal.

Risk: Telnet transmits all data in plain text, making it vulnerable to packet sniffing and man-in-the-middle attacks.

53 → DNS: DNS converts website's URL to IP number

Risks:

- If this is a DNS resolver exposed to public access, it can be exploited in DNS amplification attacks.
- It may leak internal DNS queries, exposing infrastructure information.

80 → HTTP: HTTP is a text transfer protocol for websites

Risks:

- Traffic is unencrypted, allowing attackers to sniff sensitive data (credentials, cookies, etc.).
- Vulnerable to man-in-the-middle attacks, especially on public or shared networks.

443 → HTTPS: HTTPS is a secure text transfer protocol for websites

Risks:

- If misconfigured (weak SSL/TLS ciphers, expired certs), it can be exploited.
- The application served may still have vulnerabilities (e.g., outdated CMS, file upload flaws, XSS).

192.168.1.5

1033 → NetInfo: NetInfo was an old network information service used by macOS for managing system configuration. It has been deprecated.

Risks:

- This is a deprecated macOS configuration service. If active, it may indicate outdated systems and expose legacy vulnerabilities.
- Deprecated services are often **unpatched** and risky to leave exposed.

1187 → Alias: Alias is not a well-documented standard service. It may refer to a custom or internal service running on this port.

Risk: It might be a **custom or proprietary service**, which increases uncertainty.

2010 → Search: Search is a generic label. This port could be used by internal or proprietary search-related services, not a standard one.

Risk: Generic services may be **unintentionally exposed** to the network

3000 → PPP / Web App: Often used by web applications (like Node.js dev servers). Though historically linked to PPP, it's now commonly used in development environments.

Risk: If exposed, could leak **debug info**, config files, or have **insecure default settings**.

3001 → Nessus: Nessus is a vulnerability scanner used for security auditing. If open, this port likely belongs to a system running Nessus services.

Risk: If accessible, it could **leak sensitive data**

7000 → AFS3-FileServer: AFS (Andrew File System) is a distributed network file system. This port is used by its file server service.

Risk: Exposing it could allow **unauthorized access to files**.

9080 → GLRPC / Web Service: Commonly used by alternative web services or Java-based applications. Sometimes used as a non-standard HTTP port.

Risk: If hosting a web app, it may be subject to **typical web app vulnerabilities**

49152 → Unknown (Ephemeral Port): This is the first port in the dynamic (ephemeral) range. It's typically used for temporary connections by client applications but can also be misused by malware or misconfigured services.

Risk: If something is **listening** on it persistently, it may be **misconfigured** or **malicious**.

192.168.1.9

Open Port: 7

7 → Echo: Echo is a diagnostic service that sends back any data it receives.

Risk: Can be abused in **reflection/amplification DDoS attacks**