Task 1: Scan Your Local Network for Open Ports.

Network Reconnaissance :-

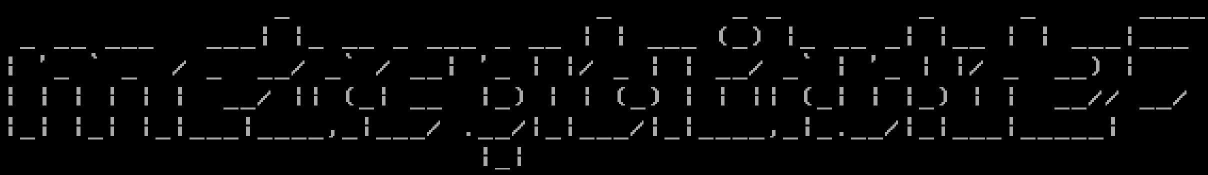
1. I am using my local system and scanned my local system to find any vulnerabilities.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.[redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:41 IST
Nmap scan report for 192.168.[redacted] (192.168.[redacted])
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.[redacted] (192.168.[redacted]) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

┌──(kali㉿kali)-[~]
└─$
```

2. Since, I didn't come across any vulnerabilities on my local system. So, now I am using some vulnerable system or machine. Using Metasploit Machine which is already vulnerable.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

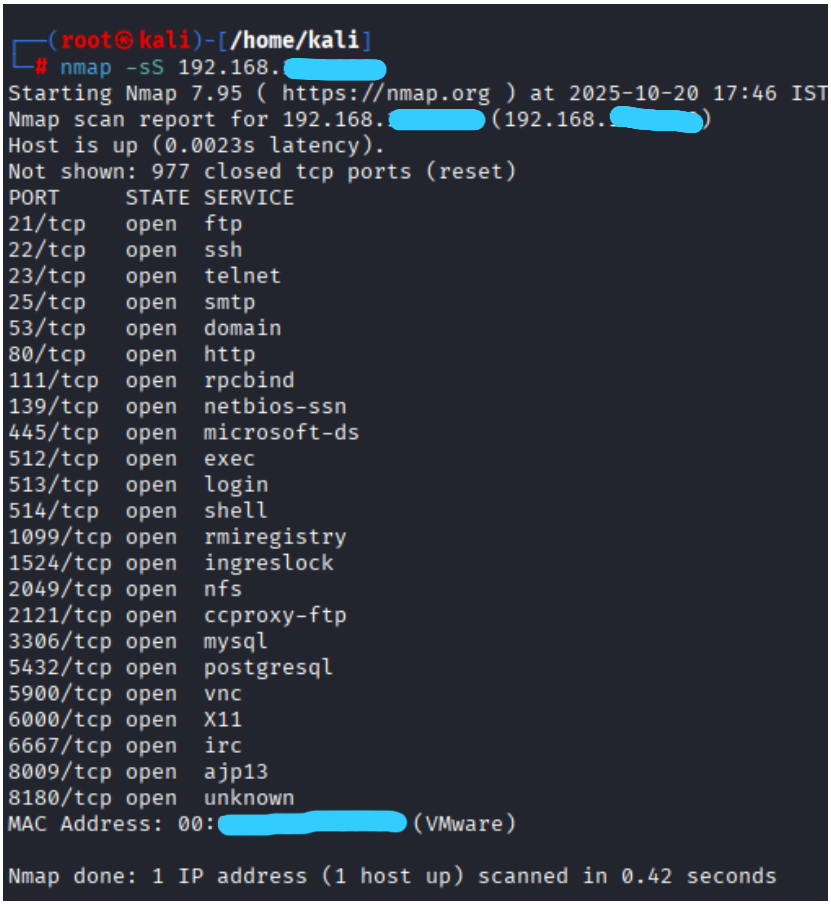
3. Getting the ip address for this machine.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:[redacted]
          inet addr:192.168.117.130  Bcast:192.168.[redacted]  Mask:255.255.255.0
          inet6 addr: [redacted] Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4678 (4.5 KB)  TX bytes:7112 (6.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)

msfadmin@metasploitable:~$
```

4. Scanned the machine or the particular machine's IP address.



5. Some information of the found vulnerabilities :-

- **Port 21 — FTP (File Transfer Protocol)**
  Risk: Credentials are transmitted in cleartext. Anonymous uploads and older vsftpd versions may allow exploits.
  Check: Use ftp or curl to gather banners; test anonymous login. Example: nmap -sV -p21 target.
  Mitigation: Turn off anonymous access, enable SFTP or FTPS, restrict via firewall, and keep the software up to date.
- **Port 22 — SSH (Secure Shell)**
  Risk: Weak credentials or outdated OpenSSH builds can allow user enumeration or exploitation through known CVEs.
  Check: Run ssh -v host or nmap -sV --version-intensity 9 -p22.
  Mitigation: Use key-based authentication, disable password login, limit connection attempts, apply fail2ban, and update OpenSSH regularly.
- **Port 23 — Telnet**
  Risk: Transmits all data, including passwords, in plain text—allowing attackers full access if intercepted.
  Check: Perform a simple banner grab or attempt a manual connection.
  Mitigation: Remove or disable Telnet, replace with SSH, and restrict via firewall.
- **Port 25 — SMTP (Mail Transmission)**
  Risk: Open-relay configurations, spoofing risks, and exposed vulnerabilities in mail servers.
  Check: Test with telnet host 25 followed by EHLO; use smtp-user-enum for user discovery.
  Mitigation: Prevent open-relay, require authentication, patch software, and restrict external access.

- **Port 53 — DNS (Domain Name System)**
  Risk: Zone transfers (AXFR), cache poisoning, and abuse of recursive resolvers.
  Check: Use dig @host axfr domain or dig +short -t ANY domain.
  Mitigation: Restrict zone transfers, secure DNS daemons, and limit recursion to trusted clients.
- **Port 80 — HTTP**
  Risk: Web application flaws (XSS, SQL injection), outdated servers, or default setup pages.
  Check: Scan with nikto, gobuster, or nmap -sV -sC -p80.
  Mitigation: Patch servers, secure web apps, deploy a WAF, and remove demo or default content.
- **Port 111 — rpcbind**
  Risk: Unrestricted RPC enumeration or remote code execution from old bugs.
  Check: rpcinfo -p host.
  Mitigation: Turn off if not needed, restrict access, and patch regularly.
- **Ports 139 / 445 — NetBIOS / SMB**
  Risk: Weak SMB credentials, exposed shares, SMBv1 vulnerabilities (like EternalBlue), data leaks.
  Check: Use enum4linux, smbclient -L //host, or nmap --script smb*.
  Mitigation: Disable SMBv1, limit to internal use, enforce strong auth, and stay updated.
- **Ports 512 / 513 / 514 — rsh / rexec / rlogin**
  Risk: Insecure remote commands and no encrypted login; .rhosts entries allow unauthorized access.
  Check: Capture banners and inspect .rhosts if available.
  Mitigation: Disable these legacy protocols and switch to SSH.
- **Port 1099 — RMI Registry**
  Risk: Java RMI endpoints may permit remote class loading and RCE if unsecured.
  Check: nmap --script java-rmi-info -p1099.
  Mitigation: Limit access, enable authentication, patch Java services, and isolate behind a firewall.
- **Port 1524 — ingreslock**
  Risk: Known to be used in old backdoors; indicates outdated or compromised systems.
  Check: Examine the banner or running process.
  Mitigation: Investigate thoroughly, remove if unused, and update the OS.
- **Port 2049 — NFS (Network File System)**
  Risk: Data leakage through public exports, privilege escalation if root_squash misconfigured.
  Check: showmount -e host.
  Mitigation: Limit to trusted IPs, enforce root_squash, and restrict via firewall.
- **Port 2121 — ccproxy-ftp (Alternate FTP)**
  Risk: Weak configurations may allow unauthorized proxying or FTP access.
  Check: Capture banner or connect manually.
  Mitigation: Disable unused services, apply strong auth, and restrict access.
- **Port 3306 — MySQL Database**
  Risk: Weak/default credentials, SQL injection amplification, or RCE in outdated versions.
  Check: mysql -h host -u root -p; nmap -sV --script=mysql*.
  Mitigation: Bind to localhost, enforce strong passwords and TLS, and patch frequently.
- **Port 5432 — PostgreSQL Database**
  Risk: Default access, weak passwords, or exploits in old versions.
  Check: psql -h host -U postgres; observe banner info.

Mitigation: Run locally only, enforce TLS and strong credentials, keep updated, apply firewall limits.

- **Port 5900 — VNC**
  Risk: Weak or absent authentication gives attackers direct desktop control.
  Check: nmap --script vnc-info -p5900.
  Mitigation: Require strong passwords, tunnel over SSH, or disable entirely.
- **Port 6000 — X11 Display Server**
  Risk: Network-exposed X servers may allow screen snooping or command execution.
  Check: Attempt session connect or inspect X display settings.
  Mitigation: Restrict network access, use SSH X11 forwarding only.
- **Port 6667 — IRC (Internet Relay Chat)**
  Risk: Potential C2 communication or exploited public IRC services.
  Check: Review banner and monitor for suspicious channels.
  Mitigation: Limit to trusted use, patch software, and monitor activity.
- **Port 8009 — AJP13 (Tomcat AJP)**
  Risk: Ghostcat vulnerability (CVE-2020-1938) can expose files or lead to RCE.
  Check: nmap --script ajp-info -p8009.
  Mitigation: Disable AJP if unused, restrict to localhost, patch Tomcat.
- **Port 8180 — Alternate HTTP Service**
  Risk: Secondary web interface or admin panel with default or weak credentials.
  Check: Open in browser or scan with nikto.
  Mitigation: Secure with authentication, patch, and limit external exposure.