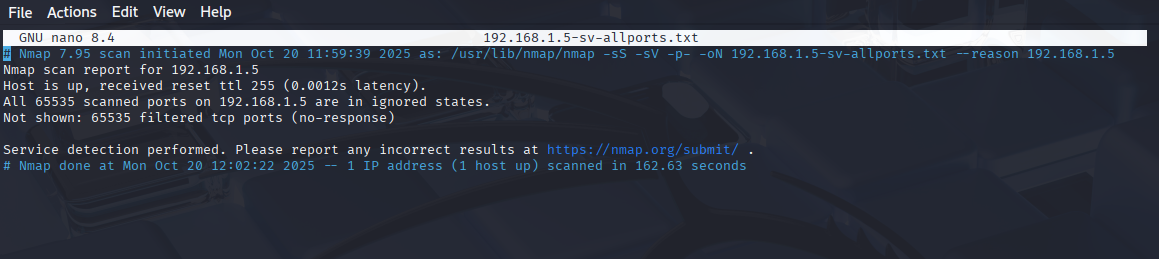
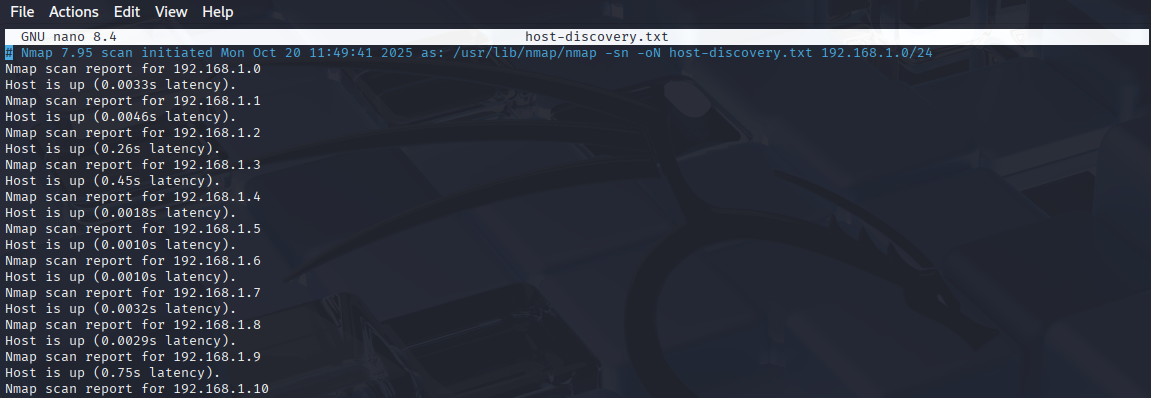
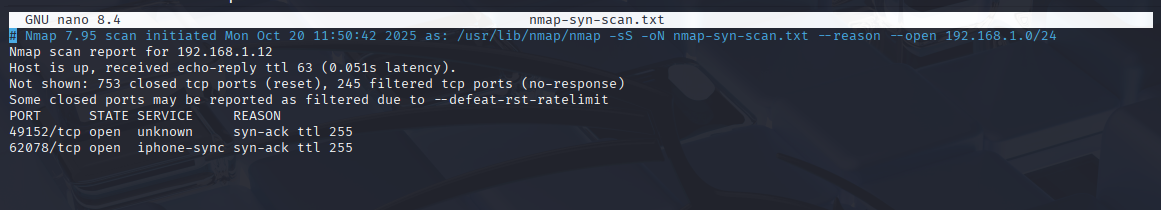
Joan Sara Joe

Task 1: (20|10|2025)







**Common Services Running on Ports**

| **Port Number** | **Service** | **Description** |
| --- | --- | --- |
| 20, 21 | FTP (File Transfer Protocol) | Used for file transfer between systems. |
| 22 | SSH (Secure Shell) | Used for secure remote login and command execution. |
| 23 | Telnet | Provides remote access without encryption. |
| 25 | SMTP (Simple Mail Transfer Protocol) | Used for sending emails. |
| 53 | DNS (Domain Name System) | Resolves domain names to IP addresses. |
| 80 | HTTP (HyperText Transfer Protocol) | Web traffic (insecure). |
| 110 | POP3 (Post Office Protocol v3) | Email retrieval from servers. |
| 143 | IMAP (Internet Message Access Protocol) | Email access protocol. |
| 443 | HTTPS (HTTP Secure) | Secure web traffic. |
| 3306 | MySQL | Database service. |
| 3389 | RDP (Remote Desktop Protocol) | Remote desktop access. |

**Potential Security Risks from Open Ports**

* **Unauthorized Access:** Attackers can exploit open ports (like Telnet, SSH, or RDP) to gain control of systems.
* **Data Interception:** Services like FTP or HTTP transmit data in plain text, allowing packet sniffing and credential theft.
* **Denial of Service (DoS):** Open ports can be targeted by DoS attacks to overload a service.
* **Malware Infection:** Open and unmonitored ports can be exploited to install malicious software or backdoors.
* **Information Disclosure:** Port scans can reveal which services are running, giving attackers clues for targeted attacks.
* **Weak Authentication:** Services like MySQL or SMTP may be misconfigured with weak passwords, leading to breaches.
* **Privilege Escalation:** Once inside, attackers can exploit vulnerabilities in those services to gain higher-level access.

