Tools Used

- **Nmap**: Used for host discovery and service enumeration within the target subnet.
- **Metasploit Framework**: Exploitation framework used to scan and exploit MS17-010 (EternalBlue).
- **Hydra**: Performed brute-force attacks on login forms over HTTP.
- **Gobuster**: Conducted directory brute-forcing to discover hidden paths like `/reports/`.
- **cURL**: Used to craft and send HTTP POST requests to test Local File Inclusion (LFI).
- **SSH (OpenSSH)**: Accessed the CentOS server interactively after obtaining valid credentials.
- **smbclient**: Enumerated and tested SMB shares on both target machines.