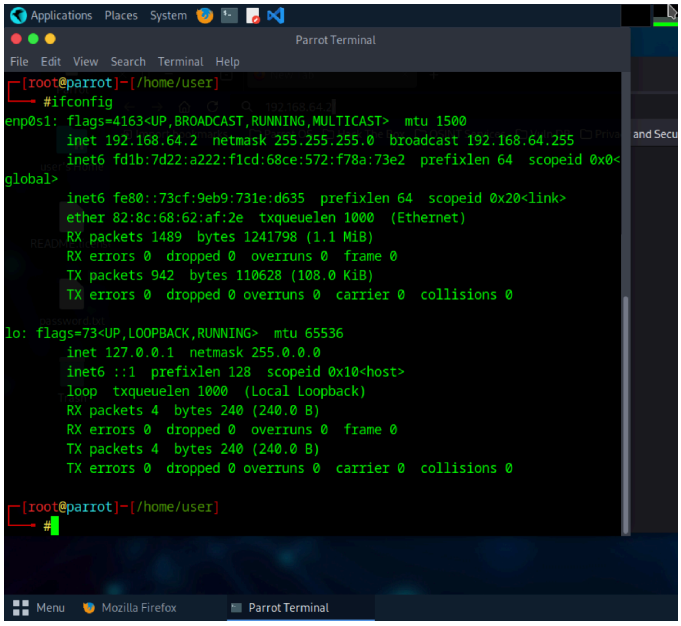
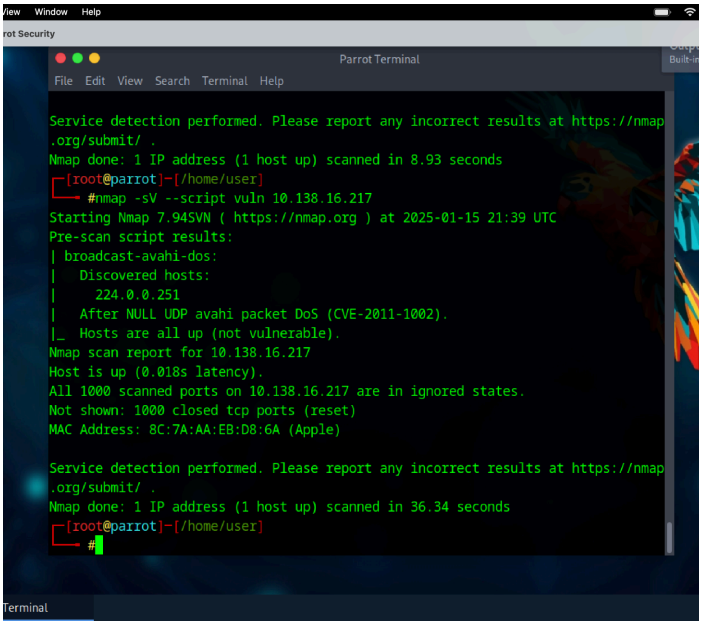
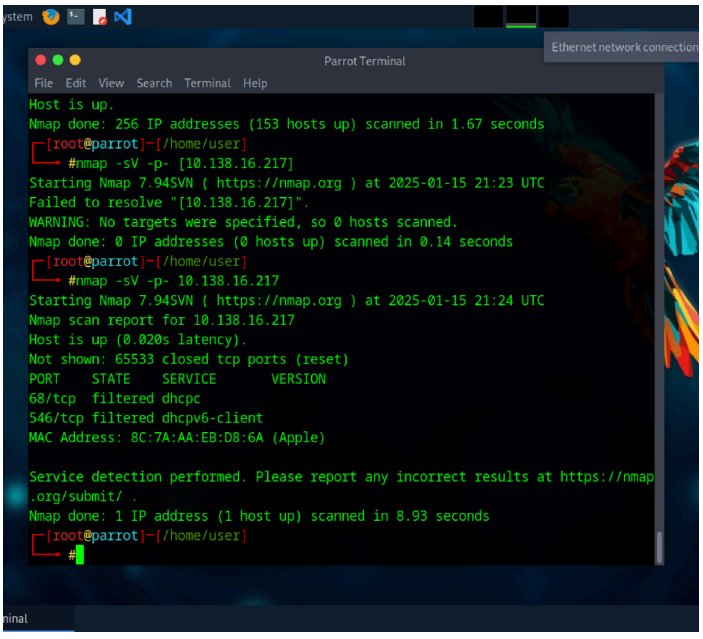
- **Apply Vulnerability Assessment Techniques**







- Asset Discovery Scan
  - Methodology:
    - The ifconfig command was initially used to identify the host's network interface details, including the IP address (192.168.64.2). Nmap was then utilized to conduct a network scan of the subnet, identifying live hosts and their basic details. The scan used the command nmap -sP

192.168.64.0/24, which performs a ping scan to discover systems within the network range.
    - Findings:
        - The asset discovery identified multiple active hosts on the subnet, confirming the presence of 153 hosts out of 256 scanned IP addresses. This information provides a basic network mapping and an overview of potentially critical assets within the environment.
    - Security Implications:
        - The discovered systems and their active states are critical for understanding the attack surface of the network. Ensuring these devices are secured and patched is necessary to reduce the likelihood of unauthorized access or exploitation.
- Vulnerability Scan
    - Methodology:
        - A targeted vulnerability scan was conducted on an identified host with IP 10.138.16.217. The following Nmap scans were performed:
    1. Service and Version Detection:
        - nmap -sV -p- 10.138.16.217 to identify open ports and running services.
    2. Vulnerability Script Execution:
        - nmap -sV --script vuln 10.138.16.217 to assess the target for known vulnerabilities using Nmap's vulnerability detection scripts.
- Findings:
    - Ports and Services:
        - The host showed no open TCP ports in the initial scan, with all detected ports either filtered or closed. This indicates strong firewall or network security configurations, limiting exposed services.
    - Vulnerability Assessment:
        - A pre-scan script result identified that the target was not vulnerable to the Avahi NULL UDP Packet DoS vulnerability (CVE-2011-1002). All other ports and services remained in ignored or filtered states, further confirming minimal exposure.
- Security Implications:
    - While the results show minimal vulnerabilities, the lack of open ports and identified services could either indicate a highly secure system or the presence of a host actively employing cloaking techniques. Continuous monitoring and deeper assessments may be required to validate these findings further.
- Conclusion and Documentation
    - The project effectively applied vulnerability assessment techniques through:
        - Asset Discovery: Identification and mapping of network systems and services.
        - Vulnerability Scanning: Detection of potential vulnerabilities and confirmation of secured configurations.