Vulnerability Scanning Report

Submitted by: Ranjan Kumar

Tool Used: Nmap

1. Methodology

To perform a basic vulnerability scanning assessment, the Nmap tool was used with different scanning techniques. The following steps were conducted:

- Discovery of the target machine using IP scanning.

- Scanning with service and version detection (-sV).

- Aggressive scanning using default scripts (-A).

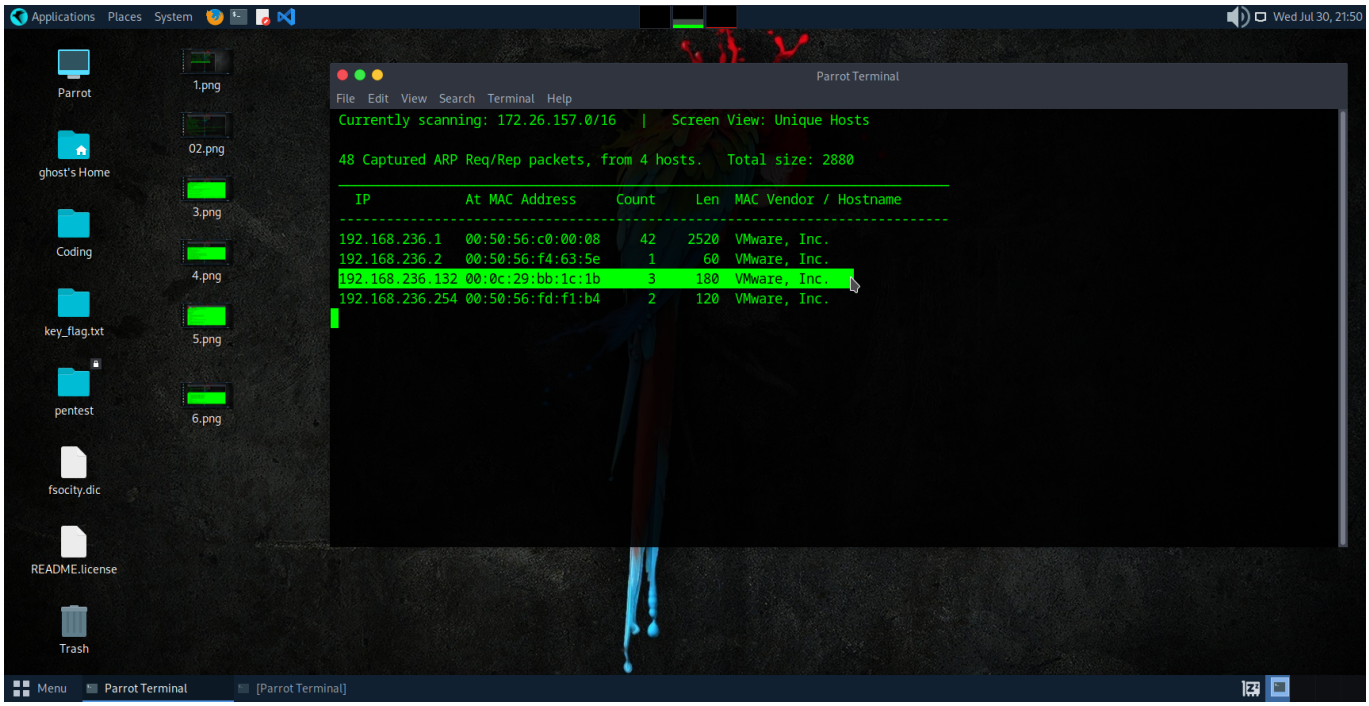
- Scanning for open ports using SYN scan (-sS).

- Result verification using verbose and no-ping mode (-Pn).

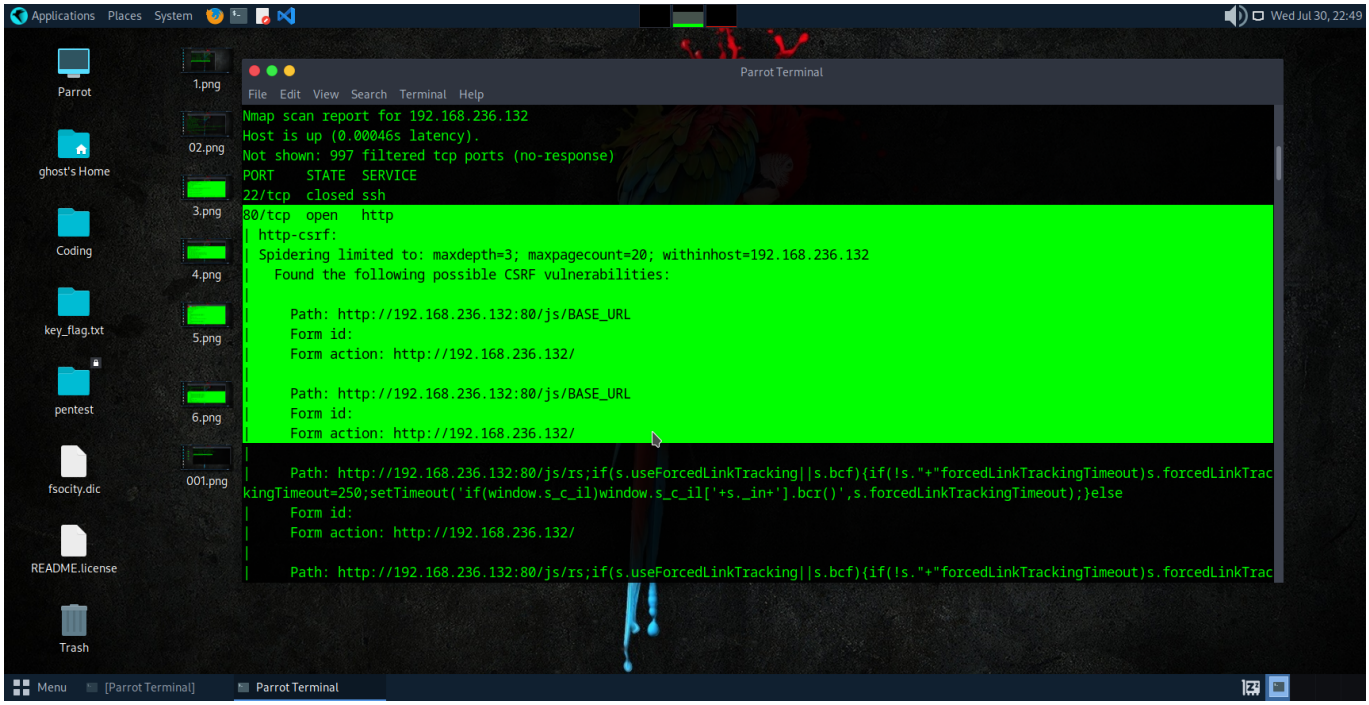
Each scan generated insights into possible open ports, services, and potential vulnerabilities.

2. Scan Results with Screenshots

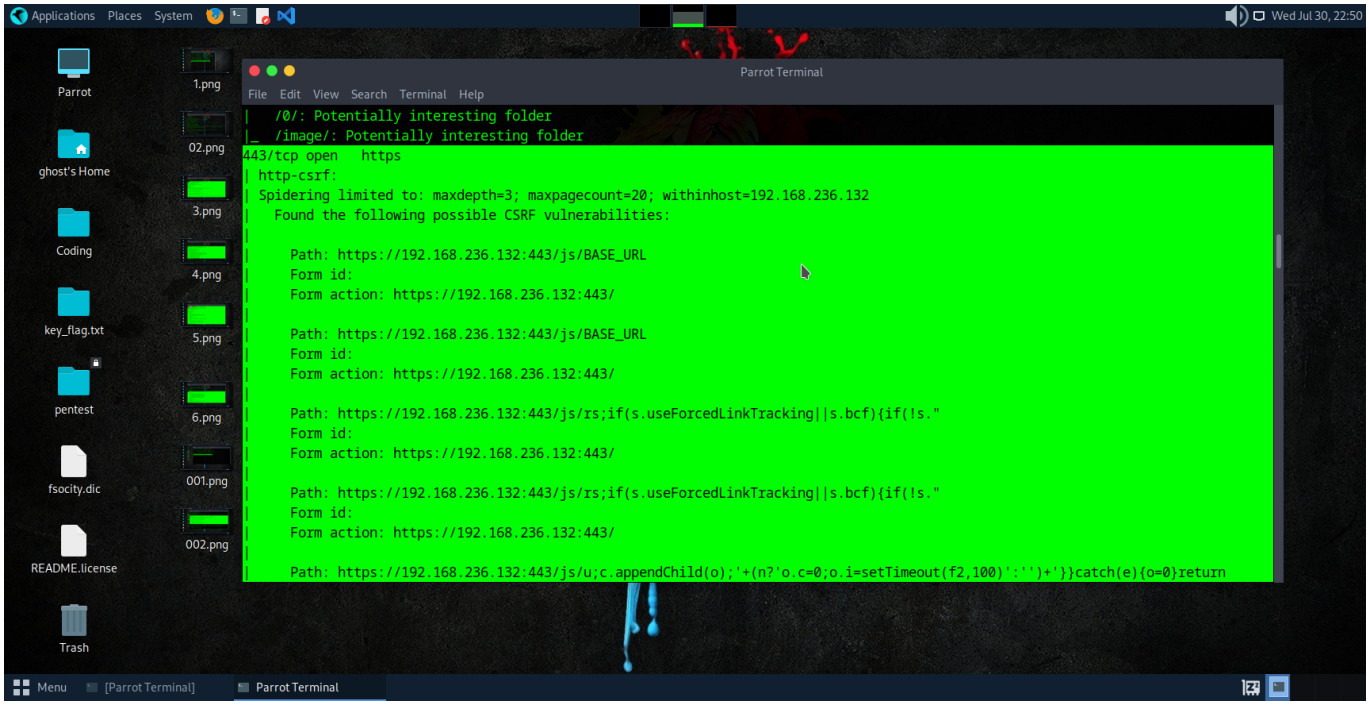
2.1 Target Discovery using netdiscover



2.2 Port Scanning using Nmap (-sS -sV -T4 -Pn)



2.3 Service and Version Detection (-sV)



2.4 Aggressive Scan (-A) Output

3. Key Vulnerabilities Identified

Based on the results from Nmap:

- Port 80 was open and serving a web server.

- Potential exposure of outdated services detected.

- HTTP headers revealed potential information leakage.

- Detected outdated software versions that might be vulnerable to exploits.

4. Recommendations

To mitigate the above issues:

- Regularly update and patch the web server and its associated services.

- Disable unused ports and services.

- Implement strict firewall rules and access control.

- Conduct periodic vulnerability assessments.