Vulnerability Assessment Report

1. Executive Summary

Purpose of the Assessment

The purpose of this vulnerability assessment was to identify potential security weaknesses in the network infrastructure, specifically targeting the host at IP address 192.168.1.251. The assessment aimed to discover active hosts, identify running services, and detect vulnerabilities that could be exploited by malicious actors.

Scope of the Engagement

The assessment focused on a single host, 192.168.1.251, within the local network. The scan included port enumeration, service version detection, and vulnerability scanning using Nmap's vulnerability scripts. The engagement was conducted on April 22, 2025, using Parrot OS.

High-Level Findings Summary

- **Host Discovered**: One host (192.168.1.251, named DAEDMAC05) was found active with a latency of 0.020 seconds.
- **Ports Status**: All 1000 scanned TCP ports were closed (reset state), indicating no open services were detected.
- **Vulnerability Check**: The broadcast-avahi-dos script tested for CVE-2011-1002 (Avahi DoS vulnerability) and confirmed the host was not vulnerable.
- **MAC Address**: The host was identified as an Apple device (MAC: 70:AE:D5:58:46:7D).
- **Key Observation**: The absence of open ports suggests a highly restricted or firewalled system, but further investigation is needed to confirm the presence of other services or misconfigurations.

General Recommendations

- Conduct additional scans with different protocols (e.g., UDP) or broader port ranges to identify any hidden services.
- Verify firewall configurations to ensure only necessary services are exposed.
- Implement regular vulnerability scanning to monitor for new vulnerabilities.
- Consider network segmentation to isolate critical assets.

2. Methodology

Tools and Techniques Used

- **Tool**: Nmap 7.94SVN
- **Techniques**:
    - Service version detection (-sV)
    - Vulnerability scanning using Nmap's vuln script category (--脚本=vuln)
    - Host discovery and port scanning

Description of Assessment Phases

1. **Asset Discovery**: Identified active hosts and their associated MAC addresses using Nmap's host discovery capabilities.
2. **Vulnerability Scanning**: Executed Nmap with the vuln script to check for known vulnerabilities, focusing on the Avahi DoS vulnerability (CVE-2011-1002).
3. **Service Enumeration**: Attempted to identify running services and their versions on the target host.

Scan Configurations

- **Command**: sudo nmap -sV --script=vuln 192.168.1.251
- **Target**: 192.168.1.251
- **Port Range**: Default 1000 TCP ports
- **Timing**: Default timing template
- **Credentials**: None used (non-authenticated scan)
- **Environment**: Parrot OS, executed on April 22, 2025, at 16:17 UTC

3. Asset Discovery

Overview of the Scan

The asset discovery phase utilized Nmap to identify active hosts and gather basic information about the target system. The scan targeted a single IP address and included MAC address detection to identify the device manufacturer.

Tool Used

- Nmap 7.94SVN

Target(s) Scanned

- IP Address: 192.168.1.251
- Hostname: DAEDMAC05

Scan Settings/Configuration

- Host discovery enabled (default ping scan)
- MAC address detection for device identification
- No specific port range specified (default 1000 TCP ports)

Discovered Systems and Services

IP Address	Hostname	MAC Address	Manufacturer	Ports Status	Services
192.168.1.251	DAEDMAC05	70:AE:D5:58:46:7D	Apple	1000 TCP ports closed	None

- **Note**: No services were detected due to all scanned ports being in a closed state.

Network Mapping

The scan identified a single host within the 192.168.1.0/24 network. No additional network structure details were provided by the scan output. The host appears to be a standalone device, likely an Apple workstation or server, based on the MAC address.

Critical Asset Identification

- **Asset**: DAEDMAC05 (192.168.1.251)
- **Criticality**: Potentially critical due to its presence on the network and identification as an Apple device, which may indicate a workstation or server. However, the lack of open ports limits further assessment of its role (e.g., domain controller, file server).

- **Reason**: The device's manufacturer and network presence suggest it could be a key system, but additional scans are needed to confirm its function.

4. Vulnerability Scan and Analysis

Overview of Scan

The vulnerability scan was performed using Nmap's vuln script category, which includes scripts to detect known vulnerabilities. The broadcast-avahi-dos script specifically checked for CVE-2011-1002, a denial-of-service vulnerability in the Avahi service.

Tool Used

- Nmap 7.94SVN with vuln scripts

Scan Type and Configuration

- **Type**: Non-intrusive vulnerability scan
- **Scripts**: broadcast-avahi-dos (part of vuln category)
- **Target**: 192.168.1.251
- **Output**: Detailed script results and port status

Summary of Findings

- **Total Vulnerabilities**: 0
- **Systems Affected**: None
- **Key Finding**: The host was tested for CVE-2011-1002 (Avahi DoS) and found not vulnerable.
- **Port Status**: All 1000 TCP ports were closed, preventing service-specific vulnerability detection.

Vulnerability Classification

- **Severity**: N/A (no vulnerabilities detected)
- **Categories**: N/A (no vulnerabilities detected)

Sample Vulnerability Details

- **Vulnerability**: Avahi DoS (CVE-2011-1002)
- **Description**: A denial-of-service vulnerability in Avahi that could be triggered by a NULL UDP packet.
- **Affected Asset**: 192.168.1.251 (DAEDMAC05)
- **CVE ID**: CVE-2011-1002
- **Risk Level**: Low (not vulnerable)
- **Potential Impact**: None (host is not vulnerable)
- **Status**: The broadcast-avahi-dos script confirmed the host is not susceptible to this vulnerability.

5. Security Implications

Analysis of Potential Impact

- **Current Impact**: The absence of detected vulnerabilities and open ports suggests a low immediate risk to the target host. The system appears to be well-secured or firewalled, reducing the attack surface.
- **Limitations**: The scan only covered 1000 TCP ports and a single vulnerability script. Other vulnerabilities (e.g., UDP-based, application-specific) may exist but were not tested.

Risk Posed to the Organization/Network

- **Low Risk**: The host's closed ports and non-vulnerable status for CVE-2011-1002 indicate minimal risk from external threats.
- **Potential Risks**:
    - Unscanned ports or protocols may host vulnerable services.
    - Internal threats or misconfigurations (e.g., weak credentials) were not assessed.
    - The device's role (e.g., workstation, server) is unclear, so its compromise could have varying impacts.

Real-World Exploitation Scenarios

- **Scenario**: If additional scans reveal open ports or services, attackers could exploit unpatched software or misconfigurations.

- **Likelihood**: Low, given the current scan results, but further investigation is needed.

6. Recommendations

Short-Term Fixes

- **Expand Scan Scope**: Perform UDP scans and full port range scans (e.g., -p-) to identify any hidden services.
- **Verify Firewall Rules**: Ensure the host's firewall is intentionally blocking all ports or confirm if services are running on non-standard ports.
- **Check for Avahi Service**: Although not vulnerable to CVE-2011-1002, verify if Avahi is installed and disable it if unnecessary.

Long-Term Improvements

- **Regular Scanning**: Implement a schedule for vulnerability scans using tools like Nmap, OpenVAS, or Nessus to detect new vulnerabilities.
- **Network Segmentation**: Isolate critical assets (e.g., DAEDMAC05) on a separate VLAN to limit exposure.
- **Patch Management**: Ensure the host's operating system and software are up to date, even if no services are currently exposed.
- **Monitoring**: Deploy intrusion detection systems (IDS) to monitor for suspicious activity on the network.

Tools or Frameworks to Improve Security Posture

- **CIS Controls**: Implement CIS Control 1 (Inventory and Control of Hardware Assets) and Control 3 (Continuous Vulnerability Management).
- **NIST SP 800-53**: Adopt security controls for vulnerability scanning (RA-5) and system monitoring (SI-4).
- **OpenVAS**: Use for comprehensive vulnerability scanning beyond Nmap's capabilities.

7. Appendices

Full Scan Output

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-22
16:17 UTC
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts are all up (not vulnerable).
Nmap scan report for DAEDMAC05 (192.168.1.251)
Host is up (0.020s latency).
All 1000 scanned ports on DAEDMAC05 (192.168.1.251) are in
ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 70:AE:D5:58:46:7D (Apple)
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.43
seconds
```

Scan Configuration

- **Command**: sudo nmap -sV --script=vuln 192.168.1.251
- **Target**: 192.168.1.251
- **Date/Time**: April 22, 2025, 16:17 UTC
- **Environment**: Parrot OS, Parrot Terminal

Network Diagram

- **Description**: A single host (DAEDMAC05, 192.168.1.251) was identified in the 192.168.1.0/24 network. No additional network topology details were available from the scan.

Definitions and Abbreviations

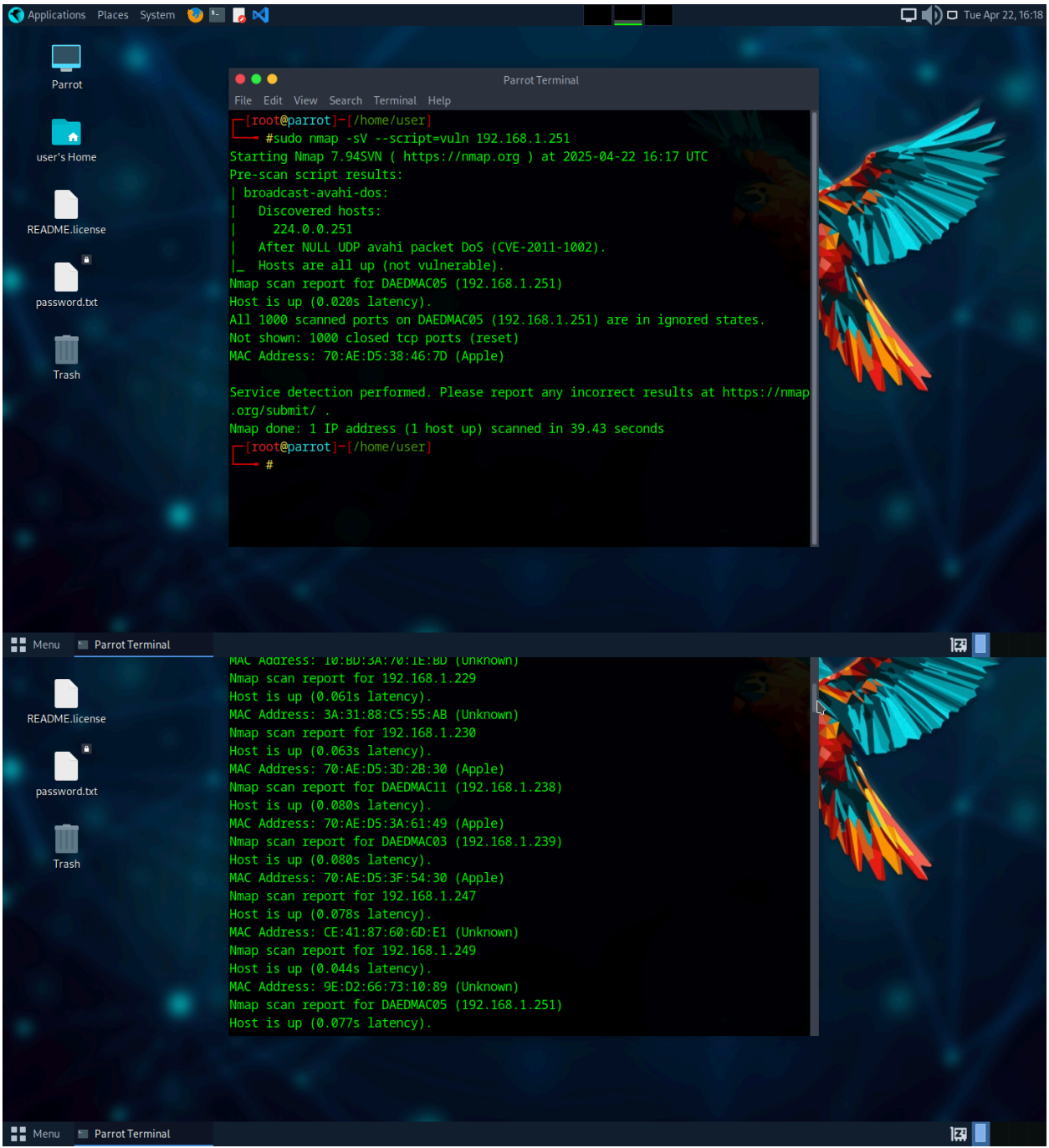
- **Nmap**: Network exploration tool and security/port scanner.
- **CVE**: Common Vulnerabilities and Exposures.
- **Avahi**: A service discovery protocol used primarily in Linux/Unix environments.
- **DoS**: Denial of Service.

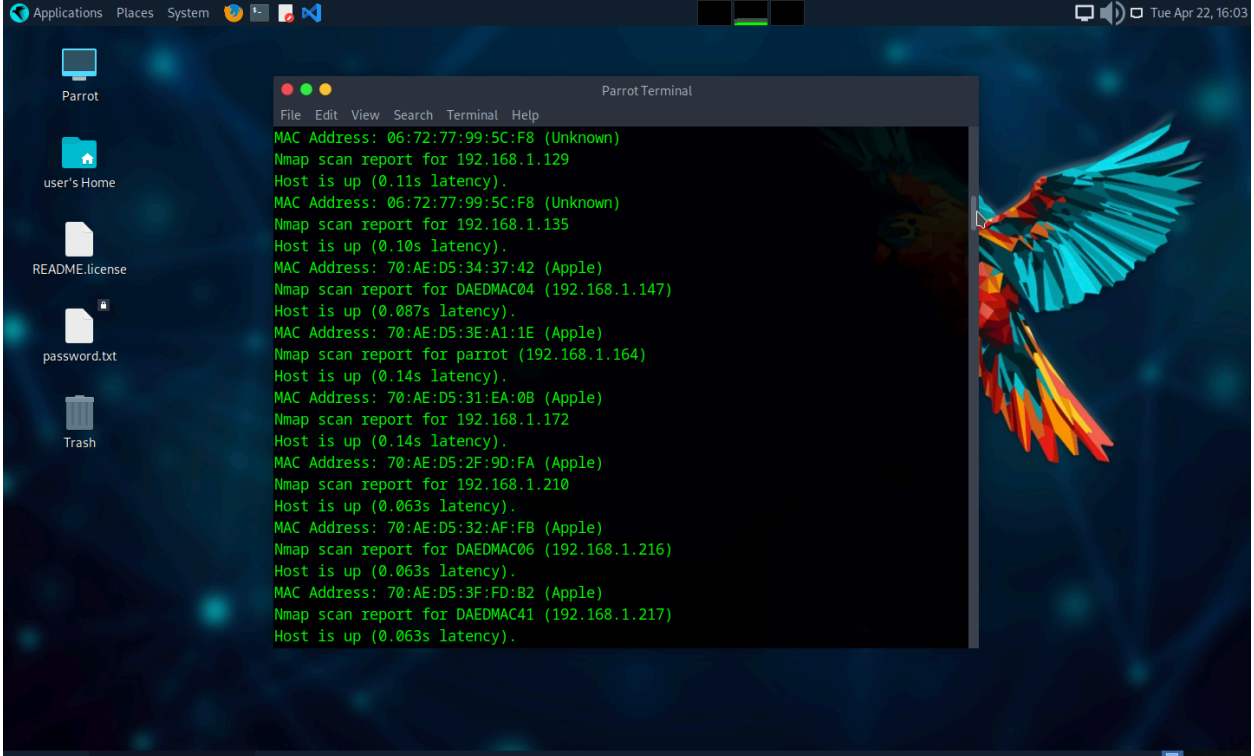
Timeline of Activities

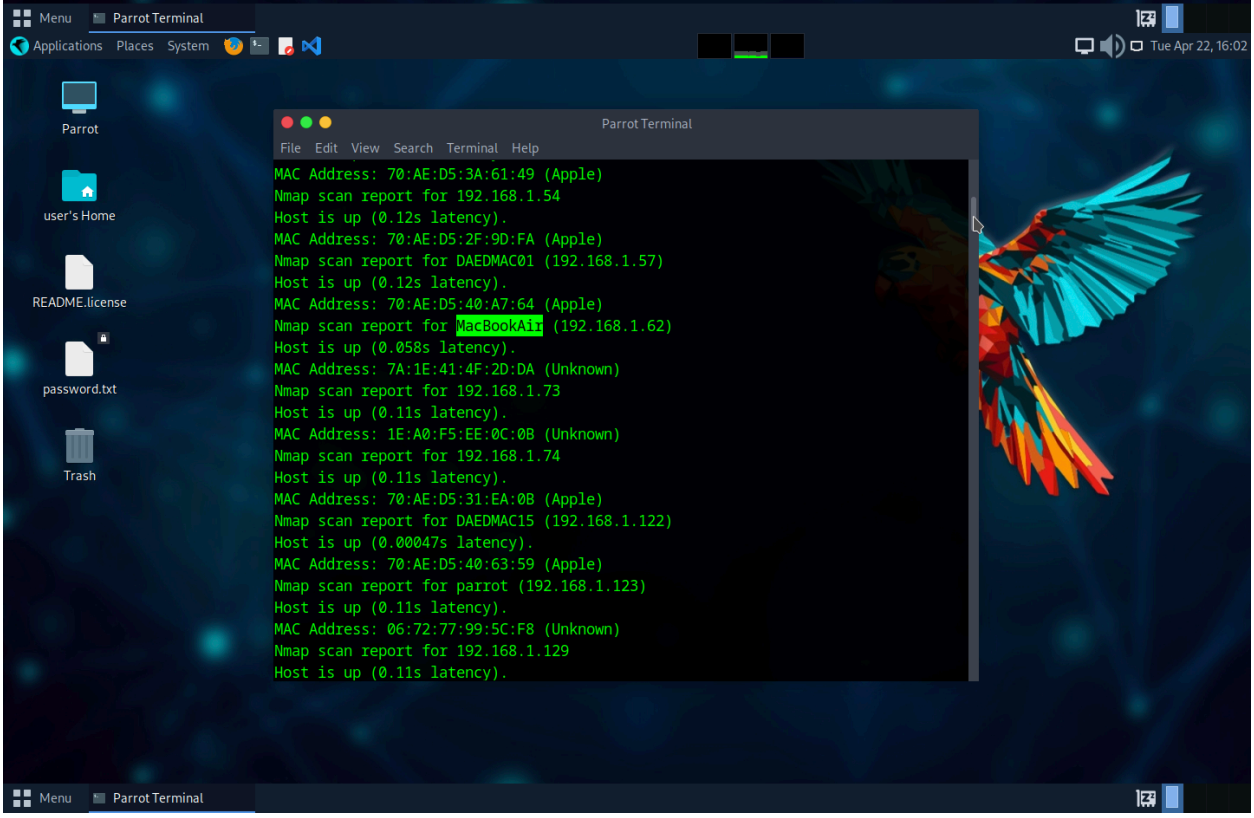
- **April 22, 2025, 15:18 UTC**: Initiated Parrot Terminal session.
- **April 22, 2025, 16:17 UTC**: Executed Nmap scan.
- **April 22, 2025, 16:17 UTC**: Scan completed (duration: 39.43 seconds).

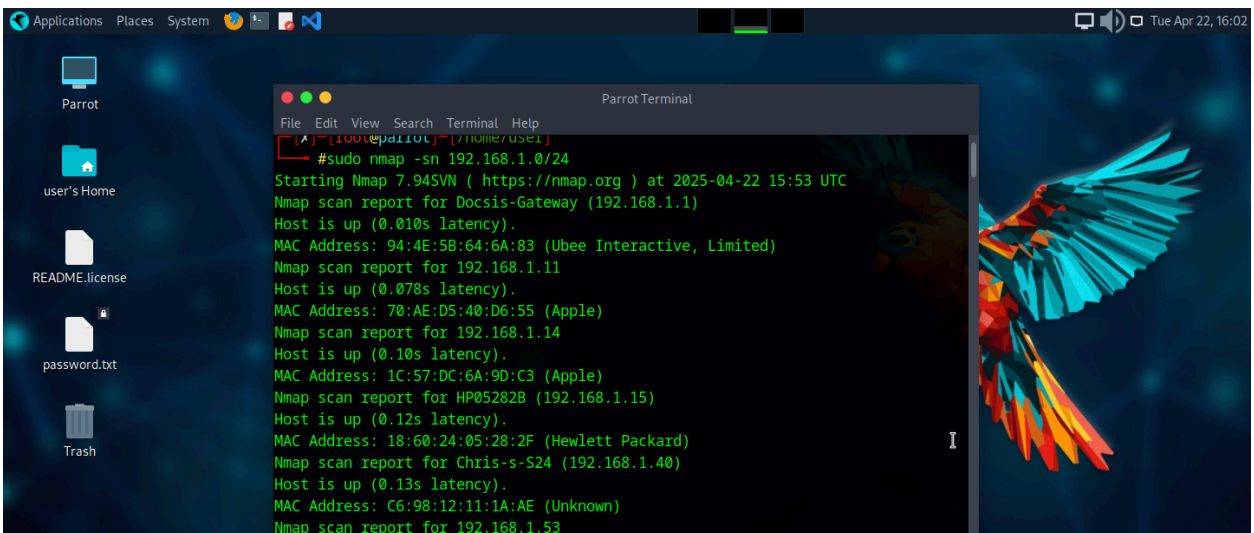
References to Security Frameworks

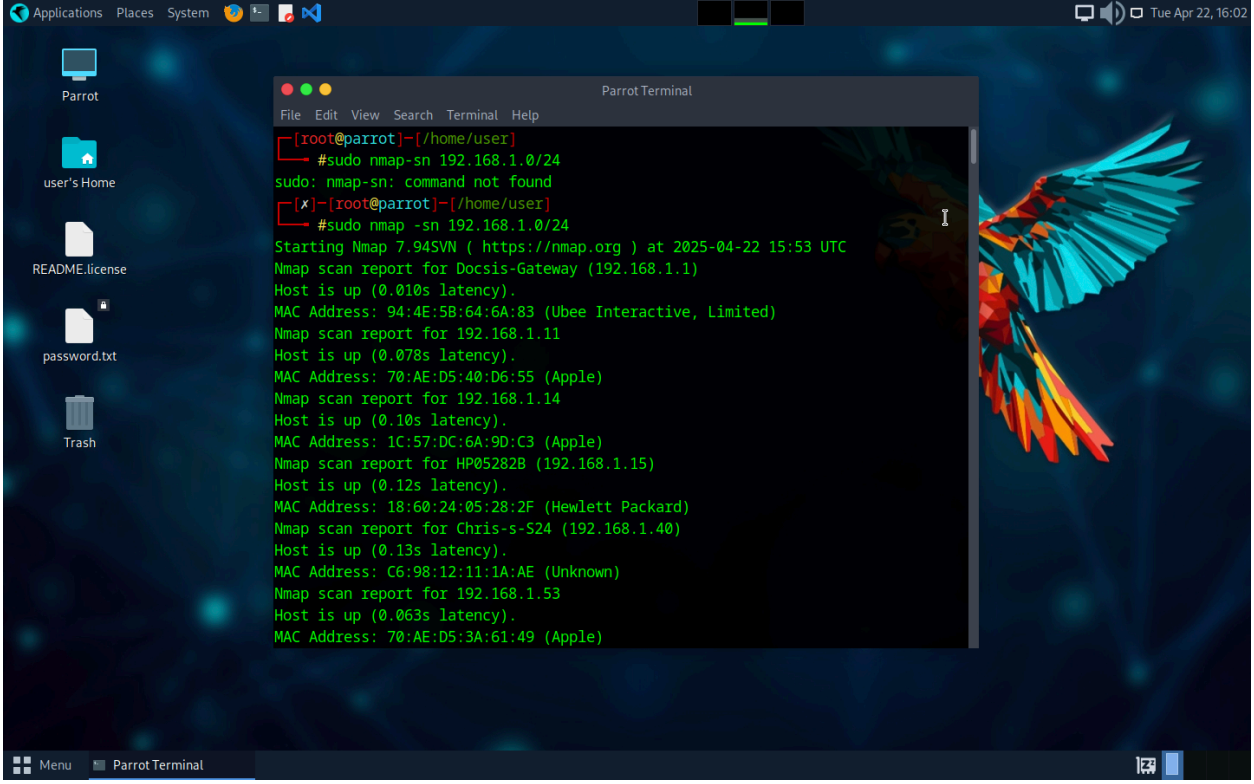
- **CIS Controls v8**: https://www.cisecurity.org/controls/
- **NIST SP 800-53**: https://nvd.nist.gov/800-53




Applications Places System
Tue Apr 22, 16:03
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
MAC Address: 06:72:77:99:5C:F8 (Unknown)
Nmap scan report for 192.168.1.129
Host is up (0.11s latency).
MAC Address: 06:72:77:99:5C:F8 (Unknown)
Nmap scan report for 192.168.1.135
Host is up (0.10s latency).
MAC Address: 70:AE:D5:34:37:42 (Apple)
Nmap scan report for DAEDMAC04 (192.168.1.147)
Host is up (0.087s latency).
MAC Address: 70:AE:D5:3E:A1:1E (Apple)
Nmap scan report for parrot (192.168.1.164)
Host is up (0.14s latency).
MAC Address: 70:AE:D5:31:EA:0B (Apple)
Nmap scan report for 192.168.1.172
Host is up (0.14s latency).
MAC Address: 70:AE:D5:2F:9D:FA (Apple)
Nmap scan report for 192.168.1.210
Host is up (0.063s latency).
MAC Address: 70:AE:D5:32:AF:FB (Apple)
Nmap scan report for DAEDMAC06 (192.168.1.216)
Host is up (0.063s latency).
MAC Address: 70:AE:D5:3F:FD:B2 (Apple)
Nmap scan report for DAEDMAC41 (192.168.1.217)
Host is up (0.063s latency).
Menu
Parrot Terminal


Applications Places System
Tue Apr 22, 16:02
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
MAC Address: 70:AE:D5:3A:61:49 (Apple)
Nmap scan report for 192.168.1.54
Host is up (0.12s latency).
MAC Address: 70:AE:D5:2F:9D:FA (Apple)
Nmap scan report for DAEDMAC01 (192.168.1.57)
Host is up (0.12s latency).
MAC Address: 70:AE:D5:40:A7:64 (Apple)
Nmap scan report for MacBookAir (192.168.1.62)
Host is up (0.058s latency).
MAC Address: 7A:1E:41:4F:2D:DA (Unknown)
Nmap scan report for 192.168.1.73
Host is up (0.11s latency).
MAC Address: 1E:A0:F5:EE:0C:0B (Unknown)
Nmap scan report for 192.168.1.74
Host is up (0.11s latency).
MAC Address: 70:AE:D5:31:EA:0B (Apple)
Nmap scan report for DAEDMAC15 (192.168.1.122)
Host is up (0.00047s latency).
MAC Address: 70:AE:D5:40:63:59 (Apple)
Nmap scan report for parrot (192.168.1.123)
Host is up (0.11s latency).
MAC Address: 06:72:77:99:5C:F8 (Unknown)
Nmap scan report for 192.168.1.129
Host is up (0.11s latency).
Menu
Parrot Terminal


Applications Places System
Tue Apr 22, 16:02
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
#sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-22 15:53 UTC
Nmap scan report for Docsis-Gateway (192.168.1.1)
Host is up (0.010s latency).
MAC Address: 94:4E:5B:64:6A:83 (Ubee Interactive, Limited)
Nmap scan report for 192.168.1.11
Host is up (0.078s latency).
MAC Address: 70:AE:D5:40:D6:55 (Apple)
Nmap scan report for 192.168.1.14
Host is up (0.10s latency).
MAC Address: 1C:57:DC:6A:9D:C3 (Apple)
Nmap scan report for HP05282B (192.168.1.15)
Host is up (0.12s latency).
MAC Address: 18:60:24:05:28:2F (Hewlett Packard)
Nmap scan report for Chris-s-S24 (192.168.1.40)
Host is up (0.13s latency).
MAC Address: C6:98:12:11:1A:AE (Unknown)


Applications
Places
System
Tue Apr 22, 16:02
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/user]
#sudo nmap-sn 192.168.1.0/24
sudo: nmap-sn: command not found
[✗]-[root@parrot]-[/home/user]
#sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-22 15:53 UTC
Nmap scan report for Docsis-Gateway (192.168.1.1)
Host is up (0.010s latency).
MAC Address: 94:4E:5B:64:6A:83 (Ubee Interactive, Limited)
Nmap scan report for 192.168.1.11
Host is up (0.078s latency).
MAC Address: 70:AE:D5:40:D6:55 (Apple)
Nmap scan report for 192.168.1.14
Host is up (0.10s latency).
MAC Address: 1C:57:DC:6A:9D:C3 (Apple)
Nmap scan report for HP05282B (192.168.1.15)
Host is up (0.12s latency).
MAC Address: 18:60:24:05:28:2F (Hewlett Packard)
Nmap scan report for Chris-s-S24 (192.168.1.40)
Host is up (0.13s latency).
MAC Address: C6:98:12:11:1A:AE (Unknown)
Nmap scan report for 192.168.1.53
Host is up (0.063s latency).
MAC Address: 70:AE:D5:3A:61:49 (Apple)
Menu
Parrot Terminal