Vulnerability Assessment Report

Objective:

The objective of this assessment is to demonstrate vulnerability assessment capabilities by conducting and documenting the results of network scans. This includes a vulnerability scan to identify potential weaknesses and an asset discovery scan to map network devices and services.

Tools Used:

Nmap 7.94SVN

Vulnerability Scan

Target:

192.168.1.252

Methodology:

1. **Port Scan:** A basic port scan was performed to identify open ports on the target system. The command used was:
   ```
   sudo nmap -p- 192.168.1.252
   ```
2.
3.

   This command scans all 65535 TCP ports.
4. **Vulnerability Scan:** A vulnerability scan was conducted using Nmap's scripting engine. The command used was:
   ```
   sudo nmap -sV --script=vuln 192.168.1.252
   ```
5.
6.

    - `-sV`: Enables service version detection, which helps in identifying the specific software running on open ports.
    - `--script=vuln`: Runs Nmap's vulnerability scripts, which check for known vulnerabilities.

Findings:

- **Port Scan:** The initial port scan revealed two open TCP ports:
    - 51692/tcp: The service running on this port is unknown.
    - 64660/tcp: The service running on this port is unknown.
- **Vulnerability Scan:**
    - The vulnerability scan identified a potential vulnerability related to "broadcast-avahi-dos". Specifically, it detected the presence of the "After NULL UDP avahi packet DoS (CVE-2011-1002)" vulnerability. The scan output indicates that the scanned hosts were not vulnerable.
    - All 1000 scanned ports on 192.168.1.252 are in ignored states.

Vulnerability Classification:

- **CVE-2011-1002:** This vulnerability is classified as a Denial of Service (DoS) vulnerability. A successful exploit could cause the Avahi service to become unresponsive, potentially disrupting network services that rely on it. The report, however, states that the hosts are not vulnerable.

Potential Security Implications:

- **Open Ports with Unknown Services:** The open ports 51692/tcp and 64660/tcp with unknown services are a concern. Unknown services could potentially be vulnerable to exploits, or they could be backdoors. Further investigation is needed to determine the services running on these ports and assess their security.

- **Broadcast AVahi DOS:** Although the target host was reported as not vulnerable, the presence of this vulnerability in the network should be noted. If other devices on the network are vulnerable, it could lead to a denial-of-service condition.

Asset Discovery Scan

Target:

192.168.1.0/24 (This CIDR notation represents the entire 192.168.1.x network)

Methodology:

1. **Ping Sweep:** A ping sweep was performed to identify active hosts on the network. The command used was:
   ```
   sudo nmap -sn 192.168.1.0/24
   ```
2.
3.

    - `-sn`: Disables port scanning and performs a ping sweep. This option is used for host discovery.

Findings:

The asset discovery scan identified the following active hosts on the 192.168.1.0/24 network:

- 192.168.1.1: Docsis-Gateway (Ubee Interactive, Limited)
- 192.168.1.11: Apple device
- 192.168.1.14: Apple device
- 192.168.1.15: HP device (HP05282B)

- 192.168.1.53: Apple device (parrot)
- 192.168.1.54: Apple device
- 192.168.1.62: Unknown device
- 192.168.1.74: Device named DAEDMAC18

Critical Asset Identification:

Based on the scan results, the following assets can be considered critical:

- **192.168.1.1 (Docsis-Gateway):** This is likely the network's gateway, providing internet connectivity. Its compromise would have a significant impact on the entire network.
- **192.168.1.53 (parrot):** This is the system from which the scan was run, and is likely a system used for security testing.
- Other Apple devices (192.168.1.11, 192.168.1.14, 192.168.1.54): These may be user workstations or servers, and their criticality depends on the data they store and their function within the organization.
- 192.168.1.15 (HP device): This is a Hewlett Packard device.

Basic Network Mapping:

The asset discovery scan provides a basic map of the 192.168.1.0/24 network. The network consists of a gateway, several Apple devices, an HP device, and a few devices with unknown names. The scan reveals the IP addresses and MAC addresses of these devices.

Documentation:

All findings, methodologies, and potential security implications have been documented in this report. The Nmap commands used have been included to provide a clear record of the assessment process.