Vulnerability Assessment Report

Objective:

Demonstrate vulnerability assessment capabilities by conducting and documenting results.

Tools Used:

- Nmap 7.94SVN

Part 1: Vulnerability Scan

1. Scan Configuration:

* Target IP: 192.168.1.253

* Command Used: sudo nmap -SV --script vuln 192.168.1.253

* Options:

* -SV: Performs service version detection to identify what services are running on open ports, along with their version numbers.

* --script vuln: Runs the Nmap Scripting Engine (NSE) with the 'vuln' category of scripts. This category contains scripts designed to find known vulnerabilities in the services detected.

* The scan was initiated with sudo privileges to ensure all ports are scanned and scripts have the necessary permissions.

2. Summary of Findings:

* The initial scan reported that the host seemed down. Nmap was unable to get a response.

* The Pre-scan script, broadcast-avahi-dos, discovered hosts and indicated they were not vulnerable to the Avahi DoS vulnerability (CVE-2011-1002).

* A subsequent scan using sudo nmap -p1-1000-T4 192.168.1.253 also reported the host as down.

* A port scan was run against 192.168.1.93 using sudo nmap -p 192.168.1.93. This scan found one open port: 6783/tcp, labeled as "unknown".

3. Vulnerability Classification:

* CVE-2011-1002 (Avahi DoS): The pre-scan script broadcast-avahi-dos checked for this vulnerability. This is a Denial-of-Service vulnerability in the Avahi service. A successful exploit could cause the Avahi service to crash, potentially disrupting network services that rely on it. The report indicates the scanned hosts were not vulnerable.

* Open Port 6783/tcp: The open port on 192.168.1.93 is classified as "unknown." Open ports are potential areas of vulnerability. Without knowing the service running on this port, it's impossible to determine the exact vulnerability. However, any open port can be a target for attackers attempting to find a way into the system. Further investigation is needed to determine the service and potential vulnerabilities.

4. Methodology and Potential Security Implications

* Methodology: Nmap was used to perform host discovery and vulnerability scanning. The -SV option was used for service and version detection, and the --script vuln option was used to run vulnerability scripts.

* Potential Security Implications:

* Denial of Service: Although the scanned hosts were not vulnerable to the Avahi DoS, DoS attacks can disrupt critical services, causing downtime and loss of productivity.

* Open Ports: Open ports represent potential entry points for attackers. If a vulnerable service is running on an open port, an attacker could exploit that vulnerability to gain unauthorized

access to the system. The "unknown" service on port 6783/tcp is particularly concerning because its purpose and potential vulnerabilities are unknown. This port should be investigated immediately.
* Host Down: The report shows that the host 192.168.1.253 was not responding to the Nmap scans. This could indicate a network issue, that the host is down, or that the host is actively blocking Nmap. If the host is blocking Nmap, it could be a security measure, but it could also hide vulnerabilities.

Part 2: Asset Discovery Scan

1. Asset Discovery Scan:
* Command Used: sudo nmap -sn 192.168.1.0/24
* Option:
* -sn: Performs a ping scan. This type of scan sends ICMP echo requests to each IP address in the specified range to determine which hosts are up and responsive. It avoids port scanning, making it quicker for host discovery.
* Target Network: 192.168.1.0/24 (This CIDR notation specifies a range of IP addresses from 192.168.1.0 to 192.168.1.255)
2. Documented Systems and Services:
* The scan discovered the following systems:
* Docsis-Gateway (192.168.1.1)
* 192.168.1.15 (Hewlett Packard)
* 192.168.1.59 (Apple)
* DAEDMAC08 (192.168.1.93) (Apple)
* DAEDMAC43 (192.168.1.125) (Unknown)
* 192.168.1.131 (Unknown)
* 192.168.1.146 (Apple)
* parrot (192.168.1.153)
* DAEDMAC02 (192.168.1.211) (Apple)
* DAEDMAC06 (192.168.1.217) (Apple)
* 192.168.1.253 (Apple)
* The scan identifies the MAC address and, in some cases, the vendor (e.g., Apple, Hewlett Packard, Ubee Interactive) for each discovered device, providing clues about the device type. However, specific services running on each host were not determined by this particular scan. A separate service discovery scan (e.g., using the -SV option) would be needed for that.
3. Critical Asset Identification:
* Based on the scan results, the following could be considered critical assets:
* Docsis-Gateway (192.168.1.1): This is likely the network's gateway, providing internet access. Its compromise could disrupt the entire network.
* parrot (192.168.1.153): Given the hostname "parrot", this is likely the system from which the scans were being run and could contain sensitive tools or data.
* 192.168.1.15 (Hewlett Packard): Without more information, it's hard to classify, but it could be a server or workstation.
* Apple Devices (192.168.1.59, DAEDMAC08, 192.168.1.146, DAEDMAC02, DAEDMAC06, 192.168.1.253): These could be workstations or servers. Their criticality depends on their role

within the network.
* Unknown Devices (DAEDMAC43, 192.168.1.131): Any unknown device should be considered potentially critical until its function is identified.
4. Basic Network Mapping:
* The -sn scan provides a basic network map by identifying the active hosts on the 192.168.1.0/24 network. The network appears to be a small local network. The gateway is at 192.168.1.1, and several other devices, including computers (some Apple devices) and an HP device, are present. A more detailed network map would require additional tools and techniques, such as traceroute, or a dedicated network mapping tool.
5. Methodology and Potential Security Implications
* Methodology: The -sn option in Nmap was used to perform a ping sweep of the 192.168.1.0/24 network. This method is quick and efficient for identifying active hosts.
* Potential Security Implications:
* Network Mapping: Attackers often start with network mapping to understand the network layout, identify potential targets, and discover vulnerabilities. This scan provides a basic map that could be used for malicious purposes.
* Asset Valuation: Identifying critical assets is crucial for prioritizing security efforts. The report highlights several devices that should be given higher security priority. If these assets are not adequately protected, the organization is at increased risk.
* Rogue Devices: The presence of unknown devices (DAEDMAC43, 192.168.1.131) on the network is a security concern. These devices could be unauthorized and potentially malicious. They should be investigated to determine their purpose and ensure they are not posing a threat.