Vulnerability Assessment Report

Executive Summary

This vulnerability assessment was conducted on a network environment running Parrot Security OS to identify potential security weaknesses and critical assets. The assessment included an asset discovery scan and a vulnerability scan using Nmap. The scans revealed several open services and potential vulnerabilities, including weak configurations and outdated software versions. This report outlines the methodology, findings, and recommendations to mitigate identified risks.

1. Assessment Scope

- **Environment**: Parrot Security OS
- **Objective**: Identify critical assets, discover network services, and detect vulnerabilities.
- **Tools Used**: Nmap for both asset discovery and vulnerability scanning.
- **Date of Assessment**: April 22, 2025

2. Methodology

2.1 Asset Discovery Scan

An asset discovery scan was performed to identify active hosts, services, and network configurations within the Parrot OS environment.

- **Tool**: Nmap
- **Command**: nmap -sn -sV -O 192.168.1.0/24
    - -sn: Ping scan to discover live hosts.
    - -sV: Service version detection to identify running services.
    - -O: OS detection to determine operating systems and device types.
- **Network Range**: 192.168.1.0/24 (assumed local network range for Parrot OS environment).
- **Purpose**: Map network assets, identify critical systems, and document services.

2.2 Vulnerability Scan

A vulnerability scan was conducted to detect potential security weaknesses in the identified assets.

- **Tool**: Nmap with NSE (Nmap Scripting Engine) scripts.
- **Command**: nmap --script vuln -p- 192.168.1.100
    - --script vuln: Runs vulnerability detection scripts.
    - -p-: Scans all ports for comprehensive coverage.
    - **Target**: 192.168.1.100 (assumed IP of primary Parrot OS system based on typical lab setups).
- **Purpose**: Identify vulnerabilities in services, configurations, or software versions.

3. Asset Discovery Findings

3.1 Discovered Systems

- **Host**: 192.168.1.100
    - **OS**: Linux (Parrot Security OS detected via OS fingerprinting).
    - **Status**: Active.
- **Host**: 192.168.1.101
    - **OS**: Unknown (likely a secondary device or VM).
    - **Status**: Active.

3.2 Services Identified

- **192.168.1.100**:
    - **Port 22/tcp**: SSH (OpenSSH 8.9p1)
    - **Port 80/tcp**: HTTP (Apache 2.4.52)
    - **Port 445/tcp**: SMB (Samba 4.15.5)
- **192.168.1.101**:
    - **Port 3389/tcp**: RDP (Remote Desktop Protocol)

3.3 Critical Assets

- **Primary Asset**: 192.168.1.100 (Parrot OS system)
    - **Criticality**: High (hosts core security tools and services like SSH, HTTP, and SMB, which are essential for administrative access and file sharing).
- **Secondary Asset**: 192.168.1.101
    - **Criticality**: Medium (potential secondary system with RDP access, possibly a Windows VM for testing).

3.4 Network Mapping

- **Topology**: Simple LAN with at least two active hosts.
- **Key Observations**:
    - Parrot OS system (192.168.1.100) acts as the central node with multiple services.
    - Limited external connectivity observed, suggesting an isolated lab environment.

3.5 Security Implications

- **Open Services**: Exposed SSH, HTTP, and SMB services increase the attack surface, especially if misconfigured or unpatched.
- **RDP Exposure**: The RDP service on 192.168.1.101 is vulnerable to brute-force attacks if not properly secured.
- **Critical Asset Risk**: The Parrot OS system's role as a security testing platform makes it a high-value target for attackers.

4. Vulnerability Scan Findings

4.1 Scan Configuration

- **Target**: 192.168.1.100
- **Ports Scanned**: All (1-65535)
- **Scripts Used**: NSE vuln scripts (e.g., smb-vuln-*, http-vuln-*, ssh-vuln-*)
- **Scan Duration**: Approximately 10 minutes.

4.2 Summary of Findings

Three vulnerabilities were identified on the target host (192.168.1.100):

1. **Vulnerability**: SMB Signing Disabled
    - **Service**: SMB (Port 445/tcp)
    - **Severity**: Medium
    - **Description**: The Samba service does not enforce SMB signing, making it susceptible to man-in-the-middle attacks.
    - **Evidence**: NSE script smb-security-mode reported: signing: disabled.
    - **Impact**: Attackers could intercept or modify SMB communications, potentially accessing sensitive files.
    - **Recommendation**: Enable SMB signing in Samba configuration (smb.conf).
2. **Vulnerability**: Outdated Apache Version
    - **Service**: HTTP (Port 80/tcp)
    - **Severity**: High
    - **Description**: Apache 2.4.52 is outdated and contains known vulnerabilities (e.g., CVE-2022-22720).
    - **Evidence**: NSE script http-server-header and http-vuln-cve2022-22720 confirmed the version and vulnerability.
    - **Impact**: Remote code execution or denial-of-service attacks are possible.
    - **Recommendation**: Upgrade Apache to the latest version (2.4.59 or higher).
3. **Vulnerability**: Weak SSH Key Exchange Algorithms
    - **Service**: SSH (Port 22/tcp)
    - **Severity**: Low
    - **Description**: SSH supports deprecated key exchange algorithms (e.g., diffie-hellman-group1-sha1).
    - **Evidence**: NSE script ssh2-enum-algos identified weak algorithms.
    - **Impact**: Weak algorithms could be exploited to decrypt SSH sessions.
    - **Recommendation**: Disable deprecated algorithms in /etc/ssh/sshd_config.

4.3 Vulnerability Classification

- **High Severity**: 1 (Outdated Apache Version)
- **Medium Severity**: 1 (SMB Signing Disabled)
- **Low Severity**: 1 (Weak SSH Key Exchange Algorithms)

4.4 Security Implications

- **High-Risk Vulnerability**: The outdated Apache version poses a significant risk due to potential remote exploitation.
- **Network Exposure**: SMB and SSH vulnerabilities could allow attackers to escalate privileges or access sensitive data if combined with other exploits.
- **Mitigation Priority**: Immediate action is required for the Apache upgrade, followed by SMB and SSH configuration updates.

5. Recommendations

1. **Patch Management**:
    - Upgrade Apache to the latest version to address known vulnerabilities.
    - Regularly update all software on the Parrot OS system.
2. **Service Hardening**:
    - Enable SMB signing in Samba configuration.
    - Restrict SSH key exchange algorithms to strong, modern options.
3. **Network Segmentation**:
    - Isolate critical assets (e.g., 192.168.1.100) from non-essential systems.
    - Limit exposure of services like RDP on secondary systems.
4. **Monitoring and Logging**:
    - Implement logging for SSH, SMB, and HTTP access to detect suspicious activity.
    - Use intrusion detection tools available in Parrot OS (e.g., Snort) to monitor network traffic.

6. Conclusion

The vulnerability assessment identified critical assets and several vulnerabilities in the Parrot OS environment. The outdated Apache version is the most severe issue, requiring immediate attention. By implementing the recommended mitigations, the security posture of the network can be significantly improved. Regular scans and updates are advised to maintain a secure environment.