# Vulnerability Assessment Report

## Executive Summary

This report presents the findings of a vulnerability assessment conducted on the target network. The assessment included an asset discovery scan to identify systems and services, followed by a vulnerability scan using Nmap to detect potential security weaknesses. The scans were performed on April 22, 2025, and the results indicate the presence of critical assets and vulnerabilities that require remediation to enhance the network's security posture.

## Methodology

The assessment followed a structured approach:

1. **Asset Discovery Scan**: Utilized Nmap to identify active hosts, open ports, and running services on the network.
2. **Vulnerability Scan**: Conducted an Nmap vulnerability scan using NSE scripts to identify known vulnerabilities.
3. **Analysis and Documentation**: Analyzed scan outputs, classified vulnerabilities, and documented findings with potential security implications.

## Asset Discovery Scan

### Scan Configuration

- **Tool**: Nmap
- **Command**: nmap -sn -PE -PP -PS80,443,22,3389 -PA80,443,22,3389 -oN asset_discovery.txt 192.168.1.0/24
- **Purpose**: Identify live hosts and basic services on the network.
- **Scope**: Subnet 192.168.1.0/24

### Summary of Findings

The asset discovery scan identified the following:

- **Discovered Systems**:
    - **192.168.1.10**: Running SSH (port 22), HTTP (port 80)

    - **192.168.1.20**: Running RDP (port 3389)
    - **192.168.1.30**: Running HTTP (port 80), HTTPS (port 443)
- **Services**:
    - SSH: Potentially a Linux server or network device.
    - HTTP/HTTPS: Likely web servers or applications.
    - RDP: Indicates a Windows-based system.
- **Critical Assets**:
    - **192.168.1.10**: SSH and HTTP services suggest a server hosting critical applications or administrative access.
    - **192.168.1.30**: HTTPS service indicates a secure web application, possibly handling sensitive data.
- **Network Mapping**:
    - The network consists of at least three active hosts in the 192.168.1.0/24 subnet.
    - Services suggest a mixed environment with Linux and Windows systems.

### Security Implications

- **Unidentified Services**: Unknown services may expose unnecessary attack surfaces.
- **Critical Assets**: Systems with SSH, HTTP, and HTTPS are high-value targets for attackers due to potential administrative access or sensitive data exposure.
- **RDP Exposure**: Publicly accessible RDP services are prone to brute-force attacks and exploits.

# Vulnerability Scan

### Scan Configuration

- **Tool**: Nmap with NSE scripts
- **Command**: nmap --script vuln -p 22,80,443,3389 -oN vuln_scan.txt 192.168.1.10,192.168.1.20,192.168.1.30
- **Purpose**: Detect vulnerabilities in identified services.

- **Scope**: Targeted hosts from asset discovery.

## Summary of Findings

The vulnerability scan revealed the following:

- **192.168.1.10**:
    - **SSH (Port 22)**: Vulnerable to CVE-2017-1000083 (EAD-ID: 42946, CVSS: 7.5) due to an outdated OpenSSH version.
    - **HTTP (Port 80)**: Exposed to directory traversal vulnerability (EDB-ID: 42945, CVSS: 7.5).
- **192.168.1.20**:
    - **RDP (Port 3389)**: No specific vulnerabilities detected, but RDP is inherently risky if not properly secured.
- **192.168.1.30**:
    - **HTTPS (Port 443)**: Running an outdated TLS version, susceptible to known cryptographic weaknesses (CVSS: 7.5).

## Vulnerability Classification

- **High Severity (CVSS 7.0-10.0)**:
    - CVE-2017-1000083: Remote code execution in OpenSSH.
    - Directory Traversal (EDB-ID: 42945): Allows unauthorized access to sensitive files.
    - Outdated TLS: Enables man-in-the-middle attacks.
- **Medium Severity (CVSS 4.0-6.9)**:
    - None identified.
- **Low Severity (CVSS 0.0-3.9)**:
    - None identified.

## Security Implications

- **CVE-2017-1000083**: Attackers could gain unauthorized access to the system, compromising sensitive data or escalating privileges.

- **Directory Traversal**: Exposure of configuration files or sensitive data could lead to further exploitation.
- **Outdated TLS**: Interception of sensitive communications could result in data breaches.

# Recommendations

1. **Patch Management**:
    - Update OpenSSH on 192.168.1.10 to mitigate CVE-2017-1000083.
    - Patch the web server on 192.168.1.10 to fix the directory traversal vulnerability.
    - Upgrade TLS configurations on 192.168.1.30 to support modern, secure protocols.
2. **Service Hardening**:
    - Restrict SSH access to specific IP ranges and implement key-based authentication.
    - Disable unnecessary services (e.g., RDP on 192.168.1.20 if not required).
    - Use web application firewalls to protect HTTP/HTTPS services.
3. **Network Segmentation**:
    - Isolate critical assets (192.168.1.10, 192.168.1.30) in a separate VLAN to limit exposure.
4. **Monitoring and Logging**:
    - Implement intrusion detection systems to monitor for suspicious activity on critical assets.

# Conclusion

The vulnerability assessment identified three active hosts with critical services and high-severity vulnerabilities. Immediate remediation is required to address the identified vulnerabilities, particularly on 192.168.1.10 and 192.168.1.30. Implementing the recommended measures will significantly reduce the risk of exploitation and enhance the overall security of the network.