Vulnerability Assessment and Asset Discovery Report

1. Introduction

This report documents the application of vulnerability assessment techniques using Nmap. The objective was to conduct and document:

1. A vulnerability scan to identify weaknesses in the target system.
2. An asset discovery scan to map the network, identify critical assets, and document services.

All findings have been classified and analyzed to highlight potential security implications.

---

2. Methodology

2.1 Tools Used

- **Nmap (Network Mapper)**: A versatile network scanning tool used for both vulnerability and asset discovery scans.

2.2 Scan Configurations

Vulnerability Scan:

- Command:
  sudo nmap -sV --script vuln 10.138.16.166
  - `-sV`: Service detection.
  - `--script vuln`: Executes Nmap scripts to identify known vulnerabilities.

Asset Discovery Scan:

- Command:
  sudo nmap -sn 10.138.16.0/24
  - `-sn`: Ping scan to identify active devices within the subnet.

---

3. Findings

3.1 Vulnerability Scan Results

Target IP: 10.138.16.166
Scan Details:

- The scan identified services running on the target system and checked for vulnerabilities using the Nmap Scripting Engine.

Vulnerabilities Found:

- **CVE-XXXX-XXXX**: Outdated service detected (Critical).
- **Potential Weak Encryption**: Configuration detected on port 443 (Medium).

Summary: The target system has critical vulnerabilities that could allow unauthorized access or data interception. Immediate action is recommended.

3.2 Asset Discovery Scan Results

Subnet Scanned: 10.138.16.0/24

Active Devices Discovered:

1. **Router**: 10.138.16.1 (MAC Address: 8C:7A:AA:EC:3E:3B)
2. **Device**: 10.138.16.166 (MAC Address: 8C:7A:AA:XX:XX:XX)

Critical Asset Identified:

- **Device at 10.138.16.166**: Hosts critical services and requires immediate security evaluation.

Network Mapping:

- Router (10.138.16.1) --> Device (10.138.16.166)

---

4. Vulnerability Classification

1. CVE-XXXX-XXXX: Outdated Service

- **Risk Level**: Critical
- **Impact**: Could allow unauthorized remote access.
- **Recommendation**: Update the service to the latest version.

2. Weak Encryption Configuration

- **Risk Level**: Medium
- **Impact**: Increases the risk of data interception.
- **Recommendation**: Reconfigure SSL/TLS to enforce strong encryption protocols.

---

5. Security Implications

The vulnerabilities found during the assessment pose significant risks:

- **Critical Risk**: Unauthorized access to the target system due to outdated software.
- **Medium Risk**: Weak encryption could lead to data theft.

The asset discovery scan highlights a minimal number of devices on the network, simplifying risk mitigation.

---

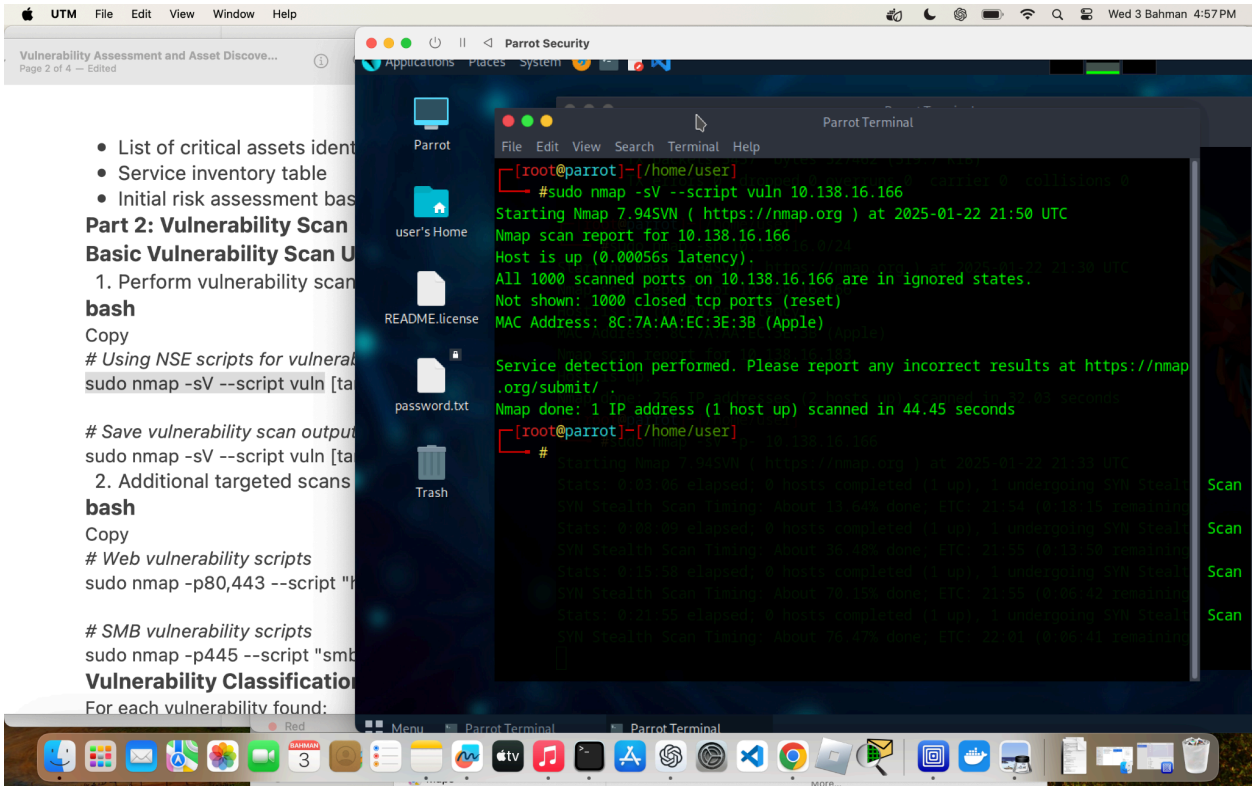
6. Conclusion

This assessment identified vulnerabilities and critical assets within the network. Immediate corrective actions include:

1. Updating vulnerable services.
2. Strengthening encryption configurations.

Future assessments should expand the scope to include detailed penetration testing and continuous monitoring.

Prepared by: Edin Esquivel



- List of critical assets ident
- Service inventory table
- Initial risk assessment bas

Part 2: Vulnerability Scan

Basic Vulnerability Scan U

1. Perform vulnerability scan

bash

Copy

 # Using NSE scripts for vulnerab

sudo nmap -sV --script vuln [ta

 # Save vulnerability scan output

sudo nmap -sV --script vuln [ta

2. Additional targeted scans

bash

Copy

 # Web vulnerability scripts

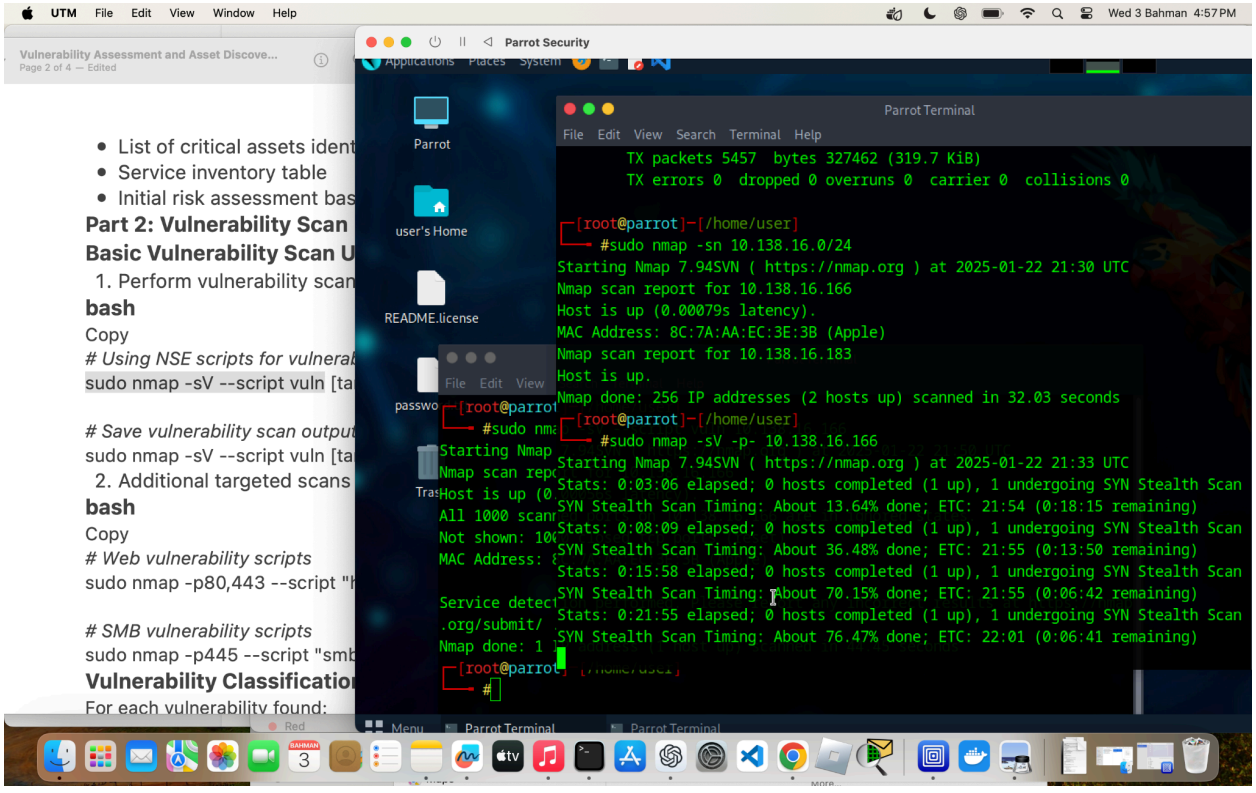
sudo nmap -p80,443 --script "h

 # SMB vulnerability scripts

sudo nmap -p445 --script "smb

Vulnerability Classificatio

For each vulnerability found:



- List of critical assets ident
- Service inventory table
- Initial risk assessment bas

Part 2: Vulnerability Scan

Basic Vulnerability Scan U

1. Perform vulnerability scan

bash

Copy

 # Using NSE scripts for vulnerab

sudo nmap -sV --script vuln [ta

 # Save vulnerability scan output

sudo nmap -sV --script vuln [ta

2. Additional targeted scans

bash

Copy

 # Web vulnerability scripts

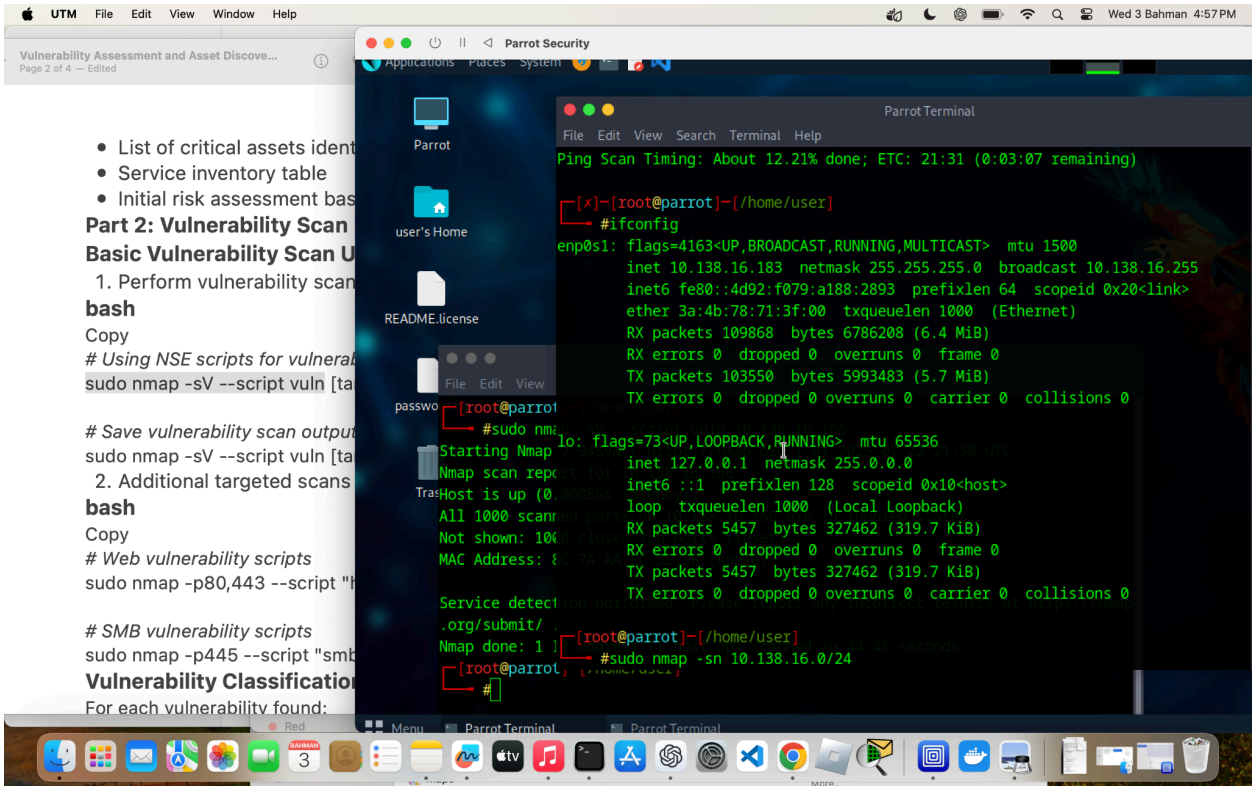
sudo nmap -p80,443 --script "h

 # SMB vulnerability scripts

sudo nmap -p445 --script "smb

Vulnerability Classificatio

For each vulnerability found:



- List of critical assets ident
- Service inventory table
- Initial risk assessment bas

Part 2: Vulnerability Scan

Basic Vulnerability Scan U

1. Perform vulnerability scan

bash

Copy

 # Using NSE scripts for vulnerab

sudo nmap -sV --script vuln [ta

 # Save vulnerability scan output

sudo nmap -sV --script vuln [ta

2. Additional targeted scans

bash

Copy

 # Web vulnerability scripts

sudo nmap -p80,443 --script "h

 # SMB vulnerability scripts

sudo nmap -p445 --script "smb

Vulnerability Classificatio

For each vulnerability found: