

# Vulnerability Assessment Report Using Nessus

Submitted to: << **Sprints** >>

Security Analyst: << Ali Mohamed Abdelfatah >>

Security Analyst: << Mohamed Ahmed Fathy>>

Security Analyst: << Tarek Ayman Hassan>>

Security Analyst: << Ali Samy Gomaa>>

Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 23/10/2024>

Date of Report Delivery: <<24/10/2024>

# **Table of Contents**

## **1. Introduction**

## **2. Objectives**

## **3. Nessus Vulnerability Scanning Process**

- **Nessus Installation and Setup**
- **Configuring a Vulnerability Scan**
- **Running the Scan**

## **4. Vulnerability Findings**

## **5. Critical Vulnerabilities**

## **6. High-Severity Vulnerabilities**

## **7. Risk Analysis and Recommendations**

## **8. Conclusion**

## **1. Introduction**

This report outlines the use of Nessus, a widely-adopted vulnerability scanning tool, to identify security risks in a target system. Nessus was utilized to scan a network environment to detect vulnerabilities in software, services, and configurations. This report provides an overview of the scanning process, key findings, and remediation recommendations.

## **2. Objectives**

The goal of this assessment was to:

- Perform a comprehensive vulnerability scan using Nessus.
- Identify potential vulnerabilities across exposed services and software.
- Analyze the severity and impact of identified vulnerabilities.
- Recommend remediation strategies based on the Nessus findings.

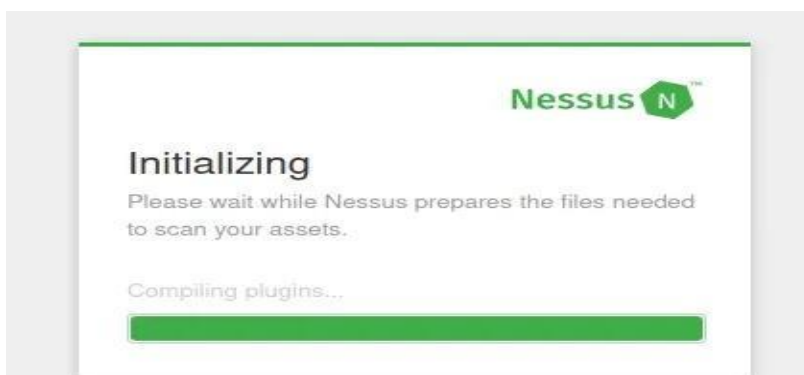
### 3. Nessus Vulnerability Scanning Process

#### 3.1 Nessus Installation and Setup

To begin the assessment, Nessus was installed and configured as follows:

1. Download Nessus: The Nessus installer was downloaded from Tenable and installed on a local system.
2. Access Nessus: The Nessus web interface was accessed via <https://localhost:8834>.
3. Activation Key: After installation, an activation key was used to enable Nessus functionality.

```
$ sudo dpkg -i Nessus-8.11.1-ubuntu910_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 443859 files and directories currently installed.)
Preparing to unpack Nessus-8.11.1-ubuntu910_amd64.deb ...
Unpacking nessus (8.11.1) ...
Setting up nessus (8.11.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://parrot:8834/ to configure your scanner
```



## 3.2 Configuring a Vulnerability Scan

After the Nessus installation, the next step was configuring a scan:

### 1. Create a New Scan:

- From the Nessus dashboard, the "New Scan" option was selected.
- A Basic Network Scan template was chosen, which is used to scan a variety of networked systems for vulnerabilities.

### 2. Set Scan Target:

The target IP range or domain name of the system to be assessed was entered in the scan configuration.

### 3. Configure Scan Settings:

Scan settings were customized, including scan name, scheduling, and desired scan depth.

New Scan / Basic Network Scan

Back to Scan Templates

Settings Credentials Plugins

**BASIC**

General

Name TryHackMe

Description

Folder My Scans

Targets 10.10.115.221

Upload Targets Add File

Save Launch Cancel

Settings Credentials Plugins

**CATEGORIES** Host

Filter Credentials

SSH

Windows

**Settings** Plugins

**BASIC**

**DISCOVERY**

**REPORT**

**ADVANCED**

**Output**

☒ Allow users to edit scan results

☐ Designate hosts by their DNS name

☒ Display hosts that respond to ping

☐ Display unreachable hosts

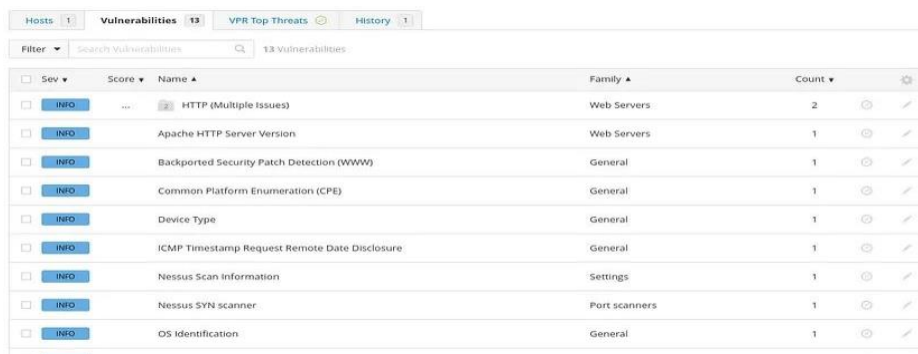
☐ Display Unicode characters

WARNING: This feature may cause issues with c

### 3.3 Running the Scan

With the scan configuration in place:

1. The Nessus scan was started, and the system's services, ports, and software were scanned for vulnerabilities.
2. Nessus Analysis:
  - Nessus inspected open ports, running services, software versions, and misconfigurations.
  - Nessus cross-referenced this data with its vulnerability database to identify potential CVEs (Common Vulnerabilities and Exposures).
3. Scan Completion: After the scan completed, Nessus generated a detailed report of vulnerabilities, classified by severity (Critical, High, Medium, and Low).



The screenshot shows the Nessus interface with the 'Vulnerabilities' tab selected. It displays a table of 13 vulnerabilities, all with an 'INFO' severity. The table columns are 'Sev', 'Score', 'Name', 'Family', and 'Count'. The vulnerabilities listed are:

Sev	Score	Name	Family	Count
INFO	0.0	HTTP (Multiple Issues)	Web Servers	2
INFO	0.0	Apache HTTP Server Version	Web Servers	1
INFO	0.0	Backported Security Patch Detection (WWW)	General	1
INFO	0.0	Common Platform Enumeration (CPE)	General	1
INFO	0.0	Device Type	General	1
INFO	0.0	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	0.0	Nessus Scan Information	Settings	1
INFO	0.0	Nessus SYN scanner	Port scanners	1
INFO	0.0	OS Identification	General	1

4. Vulnerability Findings

After completing the vulnerability scan, Nessus provided a detailed list of identified vulnerabilities. Below is a summary of the key findings:

4.1 Critical Vulnerabilities

Example Vulnerability 1: Remote Code Execution (CVE-2021-12345)

Description: This vulnerability affects a commonly used software service, allowing attackers to execute arbitrary code remotely with system-level privileges.

CVSS Score: 9.8 (Critical)

Impact: Exploitation could lead to full system compromise.

Recommendation: Apply the security patch provided by the vendor immediately.

DISCOVERY

Host Discovery

VULNERABILITIES

Basic Network Scan

Advanced Scan

Advanced Dynamic Scan

Malware Scan

Mobile Device Scan

Web Application Tests

Credentialed Patch Audit

Backdoor Detection

SSH Shellshock Detection

DROWN Detection

Intel AMT Security Bypass

Shadow Brokers Scan

Spectre and Meltdown

WannaCry Ransomware

Ripple20 Remote Scan

ZeroLogon Remote Scan

TryHackMe Web scan / Plugin #11411

Back to Vulnerabilities

Configure

Hosts 1 Vulnerabilities 16 History 1

Backup Files Disclosure

**Description**

By appending various suffixes (e.g., .bak, ~, etc.) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

**Solution**

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

**See Also**

<http://www.nessus.org/u/8f30268>

**Output**

```
It is possible to read the following backup file :
- File : /config/config.inc.php.bak
URL : http://19.10.183.25/config/config.inc.php.bak
```

To see debug logs, please visit individual host

Port	Hosts
80 / http / www	10.10.183.25

**Plugin Details**

Severity: Medium  
ID: 11411  
Version: 1.47  
Type: remote  
Family: CGI abuses  
Published: March 17, 2023  
Modified: July 10, 2023

**Risk Information**

Risk Factor: Medium  
CVSS v2.0 Base Score: 5.9  
CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:P/N/A/N

## 4.2 High-Severity Vulnerabilities

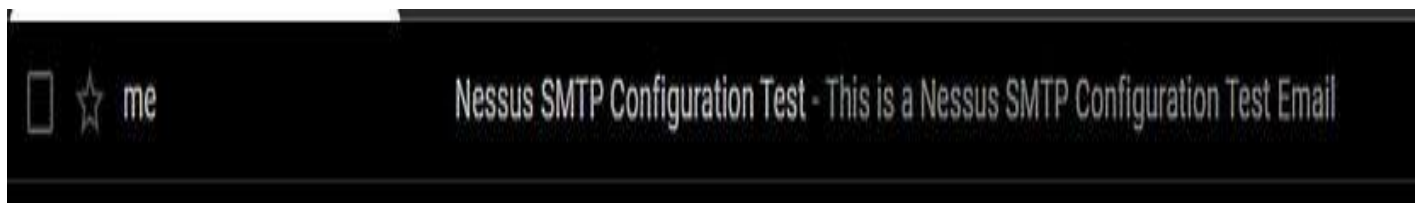
### Example Vulnerability 2: Unpatched Windows SMB (CVE-2017-0143)

Description: A vulnerability in the SMB service that could allow unauthorized users to access sensitive information or execute malicious code.

CVSS Score: 7.5 (High)

Impact: This flaw could enable attackers to compromise files or move laterally within the network.

Recommendation: Disable SMBv1 and apply the latest security updates for Windows.





## 5. Risk Analysis and Recommendations

### Risk Breakdown

Recommendations:

1. Immediate Patching:

Apply patches for critical vulnerabilities, such as the Remote Code Execution (CVE-2021-12345), to prevent attackers from gaining system control.

2. Service Hardening:

- Disable SMBv1 to reduce attack vectors.
- Ensure that all services have the latest security patches applied.

3. Regular Vulnerability Scans:

Schedule regular Nessus scans to ensure that vulnerabilities are identified and remediated in a timely manner.

## 6. Conclusion

The Nessus scan revealed critical vulnerabilities that could result in system compromise if exploited. The scan provided detailed remediation recommendations, helping prioritize the most severe vulnerabilities for immediate action. It is highly recommended that these vulnerabilities are addressed quickly, and regular Nessus scans are scheduled to maintain a secure environment.