Task 3: Perform a Basic Vulnerability Scan on Your PC

Name : Rahul Malatesh Sannapujar

Date : 26-09-2025

Objective

The objective was to use a free vulnerability scanning tool, specifically

Nessus Essentials, to identify common vulnerabilities on a local machine (PC) and document the findings.

Tools Used

- [**Nessus Essentials** (Vulnerability Scanner)
- Local PC/Machine (Scan Target)

Implementation and Process

1. Tool Setup and Initialization

I installed and configured **Nessus Essentials**. Upon initial launch, the application began the process of downloading and initializing its plugins, a crucial step before a scan can be performed.

2. Scan Configuration

I configured a new scan, naming it 'patch_finder' and setting the scan target as the local machine's IP address (e.g., 172.16.xx.xxx). I selected the **Basic Network Scan** policy for a general vulnerability assessment.

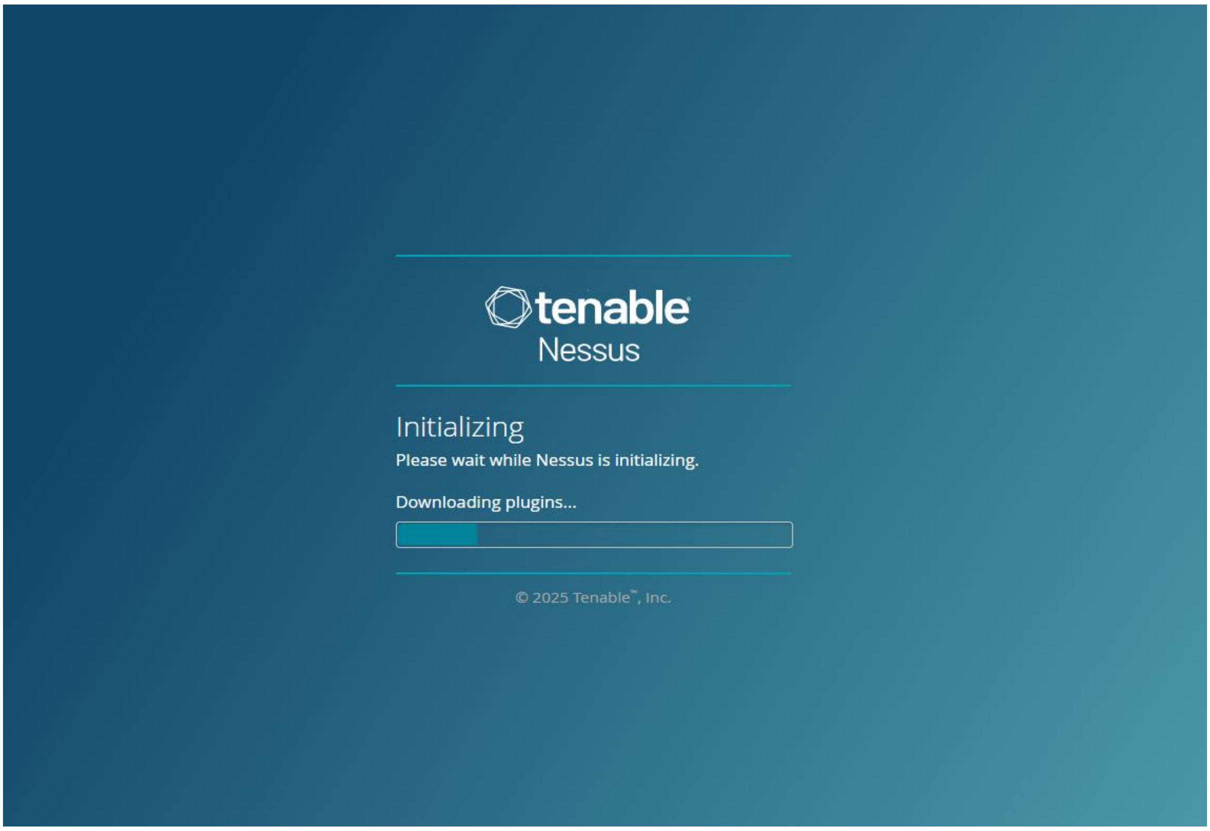
3. Scan Execution

The scan was initiated at **7:25 PM** and ran for **17 minutes**, completing at **7:42 PM**.

Detail	Value
Policy	Basic Network Scan
Start Time	Today at 7:25 PM
End Time	Today at 7:42 PM
Elapsed	17 minutes
Status	Completed

Task 3: Perform a Basic Vulnerability Scan on Your PC

Title: Tenable Nessus: Plugin Initialization Screen



Initializing

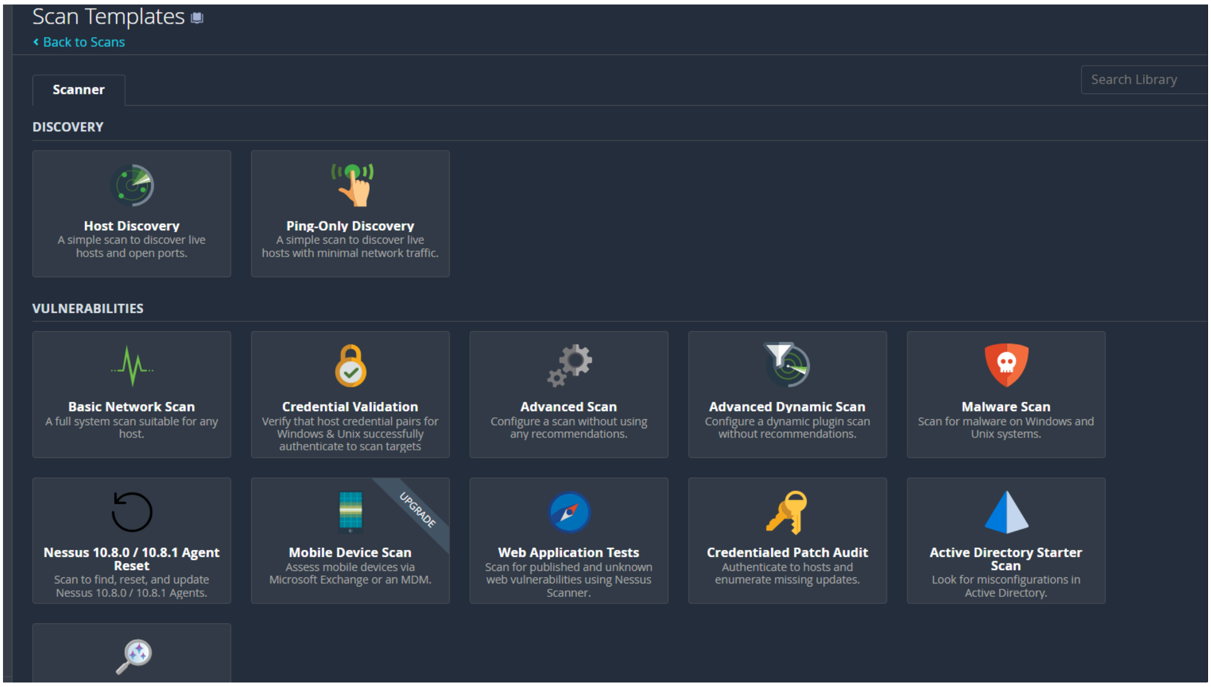
Please wait while Nessus is initializing.

Downloading plugins...

© 2025 Tenable™, Inc.

Description: This image displays the initial setup screen for **Tenable Nessus** as it prepares for use. The application is currently "Initializing" and showing a progress bar for "Downloading plugins...". This step is mandatory before performing any scans.

Title: Tenable Nessus: Library of Scan Templates



DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Task 3: Perform a Basic Vulnerability Scan on Your PC

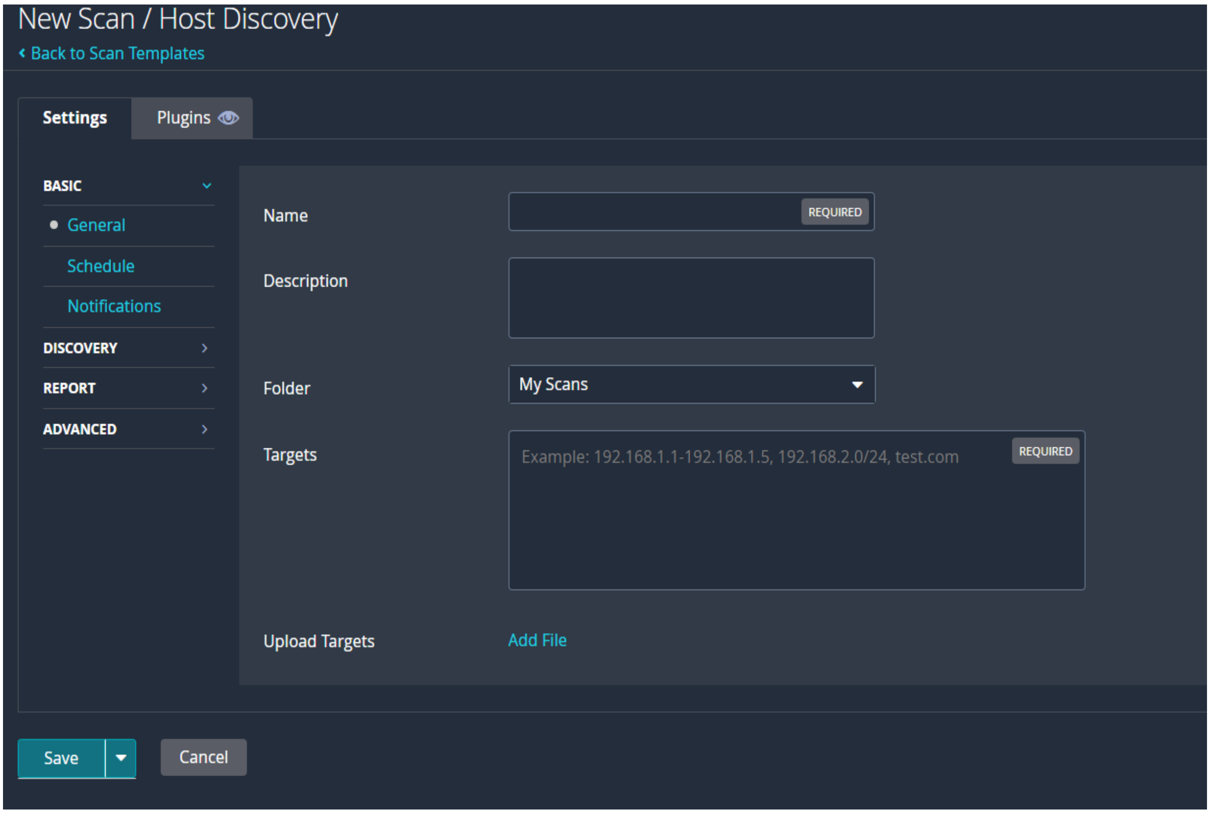
Description:

This screenshot displays the full library of **Scan Templates** available within the Tenable Nessus interface. These templates are organized into categories like **Discovery** and **Vulnerabilities**.

Key templates visible include:

- **Host Discovery** and **Ping-Only Discovery**.
- **Basic Network Scan**: A full system scan for any host.
- **Advanced Scan**: Allows for customized configuration without recommendations.
- **Credential Validation**: Used to verify host credentials.
- Specialized scans like **Malware Scan**, **Web Application Tests**, and **Active Directory Starter Scan** are also present.

Title: Nessus Scan Configuration: New Host Discovery



New Scan / Host Discovery

Name REQUIRED

Description

Folder My Scans

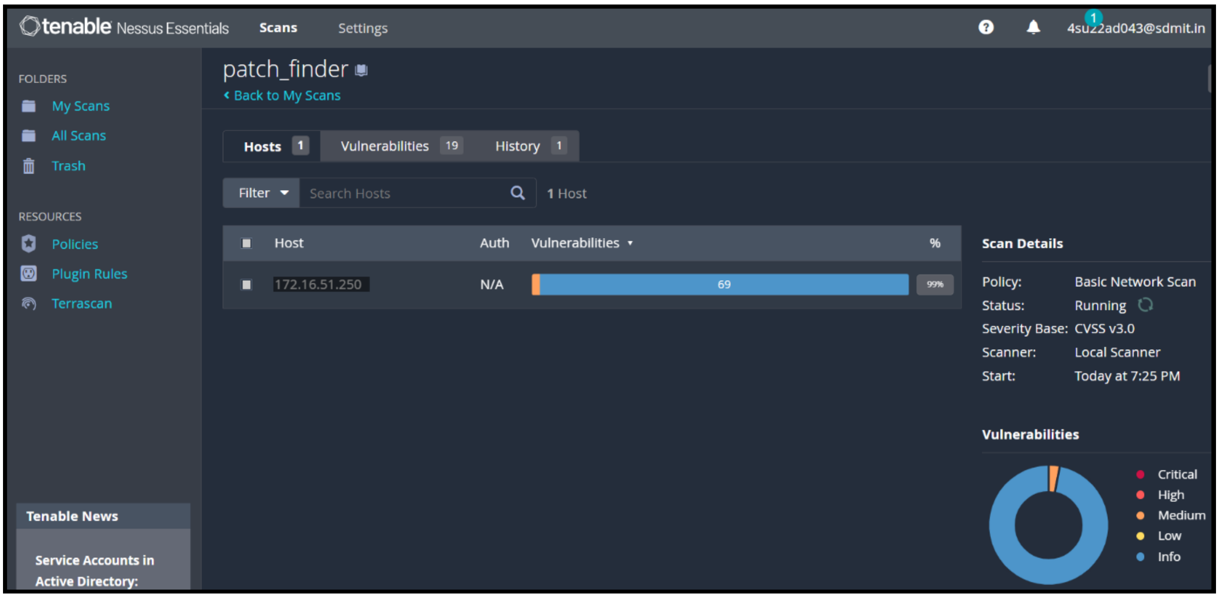
Targets Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets Add File

Description: A screenshot of the Nessus interface for creating a new scan or performing host discovery. It shows the required fields for configuring the scan, including **Name**, **Description**, **Folder** (set to "My Scans"), and the required field for **Targets** (IP addresses or ranges)

Task 3: Perform a Basic Vulnerability Scan on Your PC

Title: Nessus Scan Status: "patch_finder" Running



Host	Auth	Vulnerabilities	%
172.16.51.250	N/A	69	99%

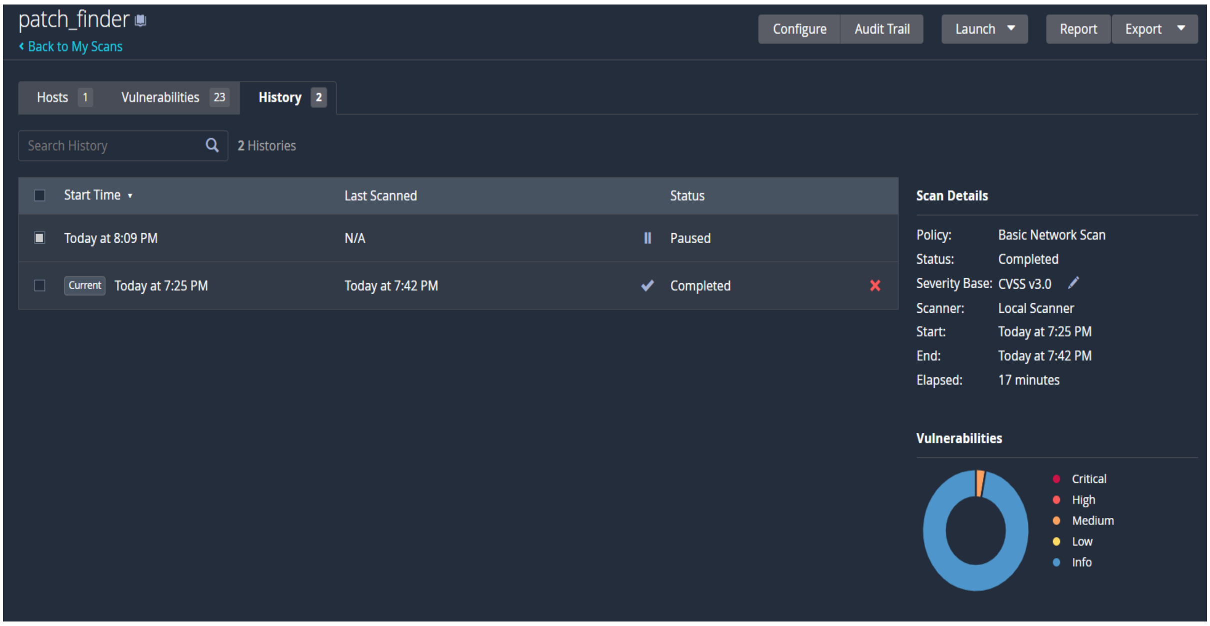
Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:25 PM

Vulnerabilities

Description: A live view of a Nessus Essentials scan named "**patch_finder**". The scan is currently **Running** and shows 99% progress on the target host 172.16.xx.xx. Details on the right confirm the scan policy is "Basic Network Scan" and the Severity Base is **CVSS v3.0**.

Title: Nessus Scan History and Completion Details



Start Time	Last Scanned	Status
Today at 8:09 PM	N/A	Paused
Current Today at 7:25 PM	Today at 7:42 PM	✓ Completed

Scan Details

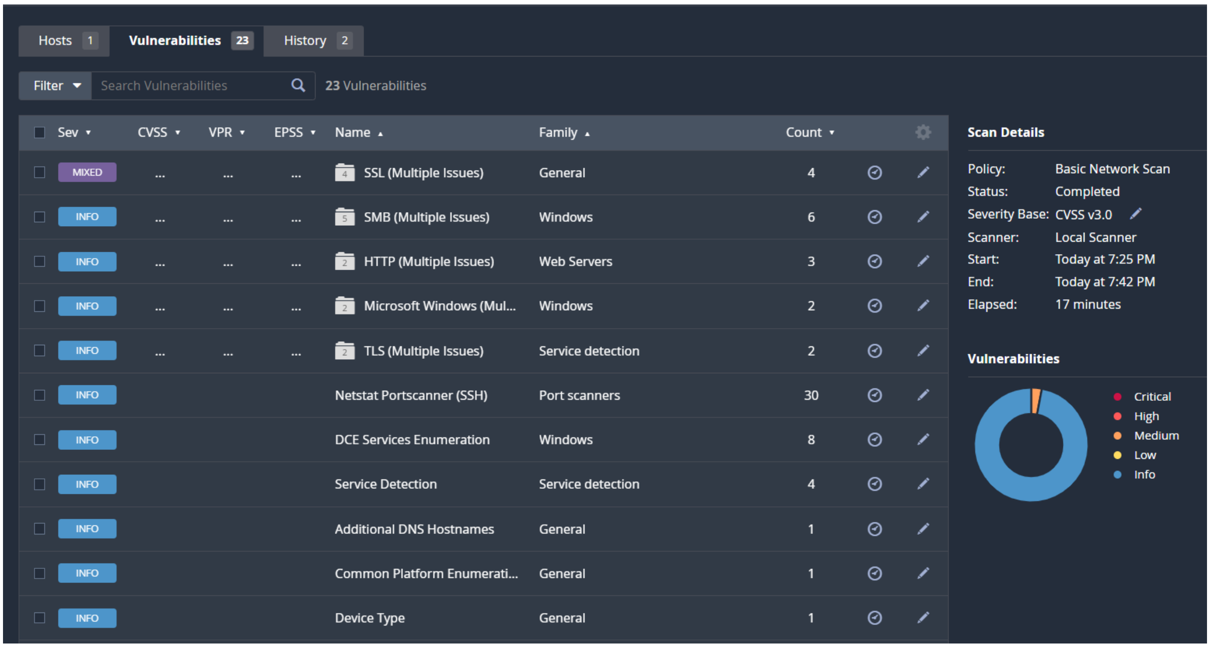
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:25 PM
End: Today at 7:42 PM
Elapsed: 17 minutes

Vulnerabilities

Description: This view shows the **History** tab for the "patch_finder" scan, listing two entries. One scan is currently **Paused**, and the other is **Completed**. The completed scan ran from 7:25 PM to 7:42 PM, with an elapsed time of **17 minutes**.

Task 3: Perform a Basic Vulnerability Scan on Your PC

Title: Nessus Scan Results: Overall Vulnerability Summary



23 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	4 SSL (Multiple Issues)	General	4
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	3
INFO	...	...	...	2 Microsoft Windows (Mul...	Windows	2
INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	30
INFO				DCE Services Enumeration	Windows	8
INFO				Service Detection	Service detection	4
INFO				Additional DNS Hostnames	General	1
INFO				Common Platform Enumerati...	General	1
INFO				Device Type	General	1

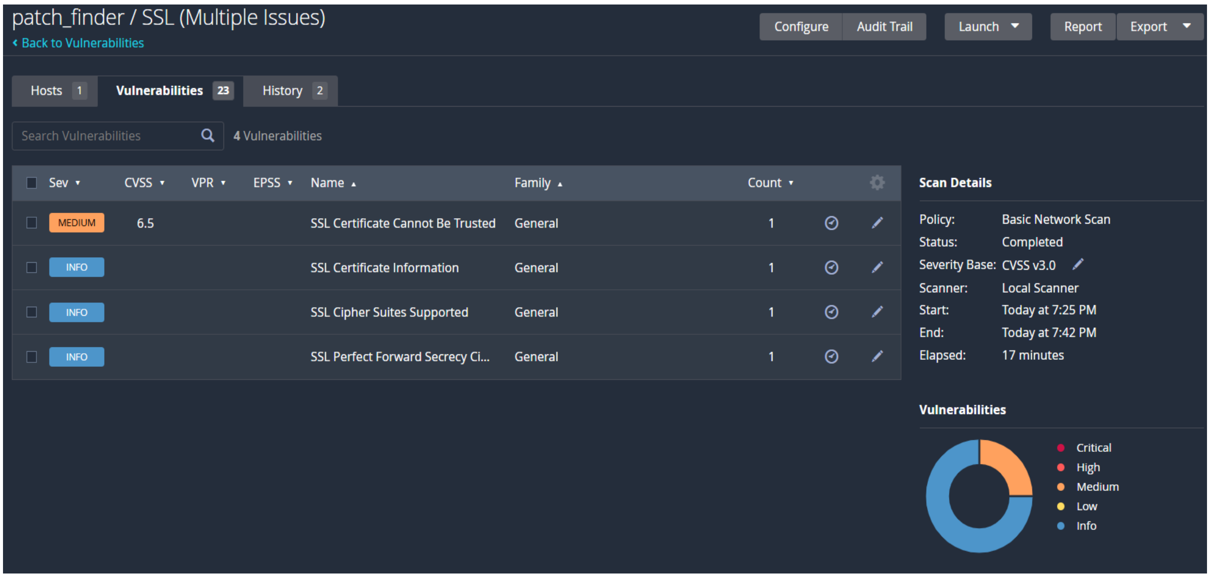
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:25 PM
End:	Today at 7:42 PM
Elapsed:	17 minutes

Vulnerabilities

Description: A screenshot of the overall vulnerability results showing **23 Vulnerabilities** found on the host. The chart and list indicate the findings are predominantly **Info** severity, with a single group showing a **Mixed** severity (which includes the medium finding). Key vulnerability groups listed include **SSL (Multiple Issues)**, **SMB (Multiple Issues)**, and **Netstat Portscanner (SSH)**.

Title: Nessus Scan Detail: SSL (Multiple Issues) Findings


patch_finder / SSL (Multiple Issues)

4 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
INFO				SSL Certificate Information	General	1
INFO				SSL Cipher Suites Supported	General	1
INFO				SSL Perfect Forward Secrecy Ci...	General	1

Scan Details

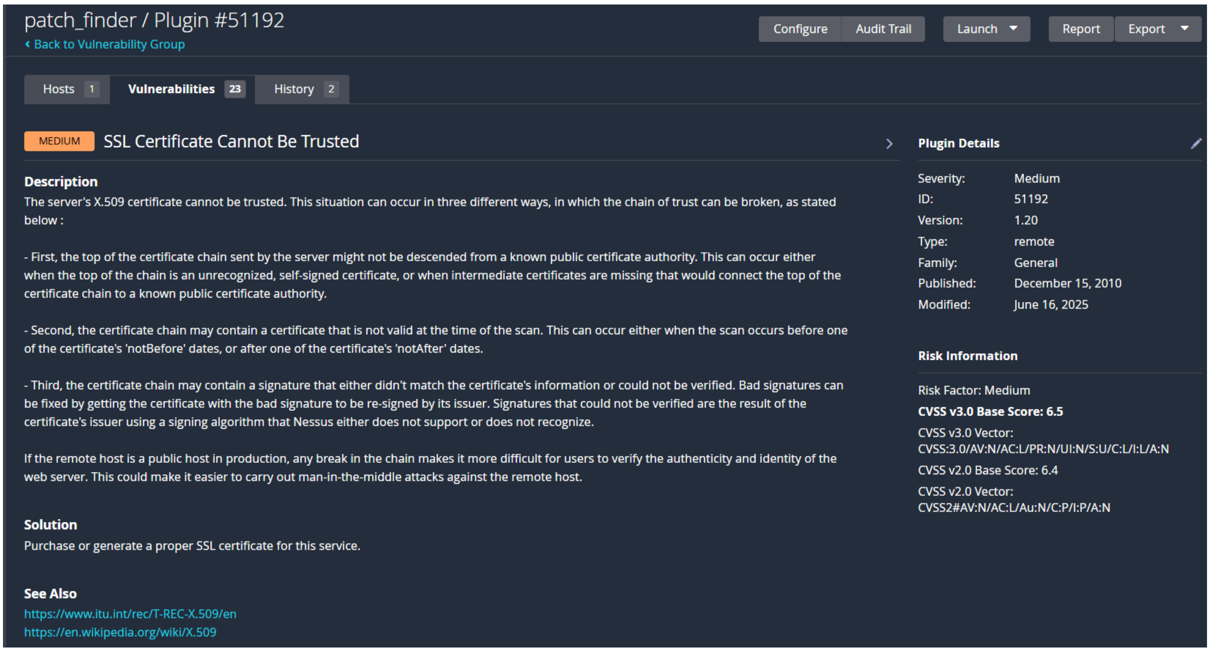
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:25 PM
End:	Today at 7:42 PM
Elapsed:	17 minutes

Vulnerabilities

Description: A drill-down view of the **SSL (Multiple Issues)** vulnerability group. It lists four individual findings, the most severe being a **MEDIUM**-rated issue titled "**SSL Certificate Cannot Be Trusted**," which has a **CVSS** score of 6.5.

Task 3: Perform a Basic Vulnerability Scan on Your PC

Title: Nessus Plugin Detail: Medium Severity SSL Issue



SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Plugin Details

Severity:	Medium
ID:	51192
Version:	1.20
Type:	remote
Family:	General
Published:	December 15, 2010
Modified:	June 16, 2025

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Base Score: 6.4

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Description: The full details pane for the **Medium** vulnerability, "**SSL Certificate Cannot Be Trusted**" (Plugin ID 51192). It provides the technical description of the root causes (e.g., untrusted certificate chain, invalid dates), the **Risk Factor** (Medium), the **CVSS v3.0 Base Score** (6.5), and the recommended **Solution**: "Purchase or generate a proper SSL certificate for this service".