

# **Vulnerability Assessment On a Windows Machine.**

**-Using Tenable Nessus**

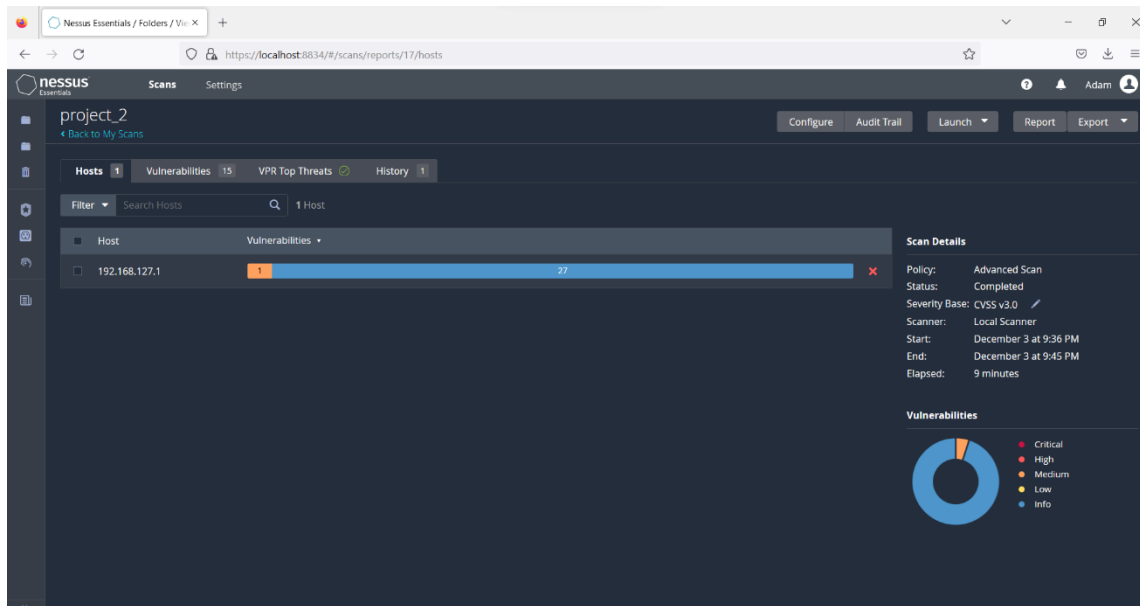
**-CVSS**

**-Authentication Protocol**

**-DCE Services Enumeration**

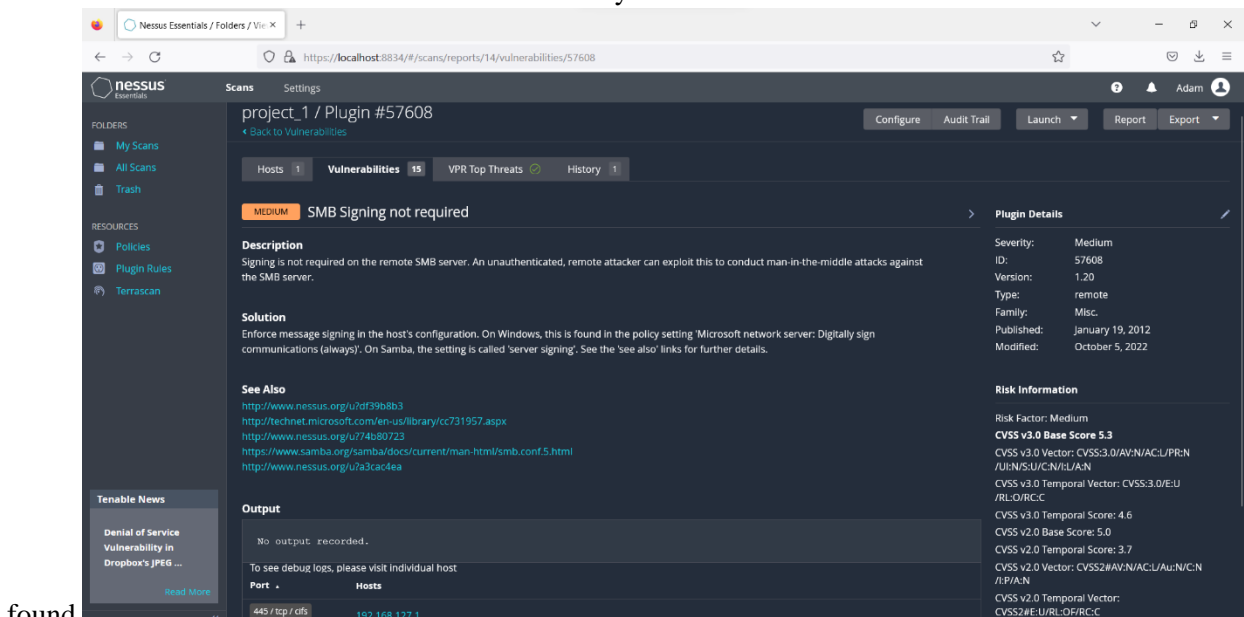
**-OS Security Patch  
Assessment**

# Vulnerability Assessment



About:

In this screen as we can see 1 Medium Vulnerability is



found.

Vulnerability:

## **SMB signing not required**

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

SMB signing is a security mechanism in the SMB protocol. It means that every SMB 3.1.1 message contains a signature that is generated by using the session key and the Advanced Encryption Standard (AES) algorithm. The session key is derived from a negotiated key and the server's secret key.

## **How to solve?**

- If you are a system admin, Login to the Windows Server with admin rights and on run Prompt, type gpedit.msc to open Local Group Policy.
- Browse to this Path: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
- Click on 'Microsoft network server: Digitally sign communications (always). By default, this setting is usually disabled. Double click on it and change it to enabled.
- If you are not a system admin than you need to share these details with your system administrator in order to create a domain level policy for all the affected Servers.

In screenshots we can see "CVSS"

What is CVSS?

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Nessus Essentials / Folders / Vie X

+

← → ↺

🔒 https://localhost:8834/#/scans/reports/17/vulnerabilities/group/11011/11011

☆ 🛡️ ⬇️ ☰

nessus

Essentials

Scans

Settings

🔔

🔔

Adam

FOLDERS

My Scans

All Scans

Trash

RESOURCES

🔗 Policies

🔗 Plugin Rules

🔗 Terrascan

Tenable News

Cybersecurity

Snapshot: insights on

Hive Ransomwar...

Read More

project\_2 / Plugin #11011

⬅️ [Back to Vulnerability Group](#)

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 15

VPR Top Threats 🟢

History 1

INFO

Microsoft Windows SMB Service Detection

>

Plugin Details

✎

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Output

An SMB server is running on this port.

To see debug logs, please visit individual host

Port

Hosts

139 / tcp / smb

192.168.127.1

A CIFS server is running on this port.

To see debug logs, please visit individual host

Port

Hosts

445 / tcp / cifs

192.168.127.1

Severity: Info

ID: 11011

Version: 1.43

Type: remote

Family: Windows

Published: June 5, 2002

Modified: February 11, 2021

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

70°F

Mostly cloudy

🔍 Search

📁 📧 📅 📌 📎 📏 📐 📑 📔 📕 📖 📗 📙 📚 📛 📜 📝 📞 📟 📠 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿

ENG IN 📶 🔊 🔇 🔈 🔉 🔊 🔋 🔌 🔍 🔎 🔏 🔐 🔑 🔒 🔓 🔔 🔕 🔖 🔗 🔘 🔙 🔚 🔛 🔜 🔝 🔞 🔟 🔠 🔡 🔢 🔣 🔤 🔥 🔦 🔧 🔨 🔩 🔪 🔫 🔬 🔭 🔮 🔯 🔰 🔱 🔲 🔳 🔴 🔵 🔶 🔷 🔸 🔹 🔺 🔻 🔼 🔽 🔾 🔿 🔸 🔹 🔺 🔻 🔼 🔽 🔾 🔿

9:53 PM 12/3/2022 🔔

Nessus Essentials / Folders / Vie X

+

← → ↺

🔒 https://localhost:8834/#/scans/reports/17/vulnerabilities/group/11011/10150

☆ 🛡️ ⬇️ ☰

nessus

Essentials

Scans

Settings

🔔

🔔

Adam

FOLDERS

My Scans

All Scans

Trash

RESOURCES

🔗 Policies

🔗 Plugin Rules

🔗 Terrascan

Tenable News

NETGEAR Nighthawk

WiFi6 Router

Network

Misconfigur...

Read More

project\_2 / Plugin #10150

⬅️ [Back to Vulnerability Group](#)

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 15

VPR Top Threats 🟢

History 1

INFO

Windows NetBIOS / SMB Remote Host Information Disclosure

<

Plugin Details

✎

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbstscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Output

The following 2 NetBIOS names have been gathered :

DELLHOME = Computer name

DELLHOME = Workgroup / Domain name

To see debug logs, please visit individual host

Port

Hosts

445 / tcp / cifs

192.168.127.1

Severity: Info

ID: 10150

Version: 1.91

Type: remote

Family: Windows

Published: October 12, 1999

Modified: February 10, 2021

Risk Information

Risk Factor: None

70°F

Mostly cloudy

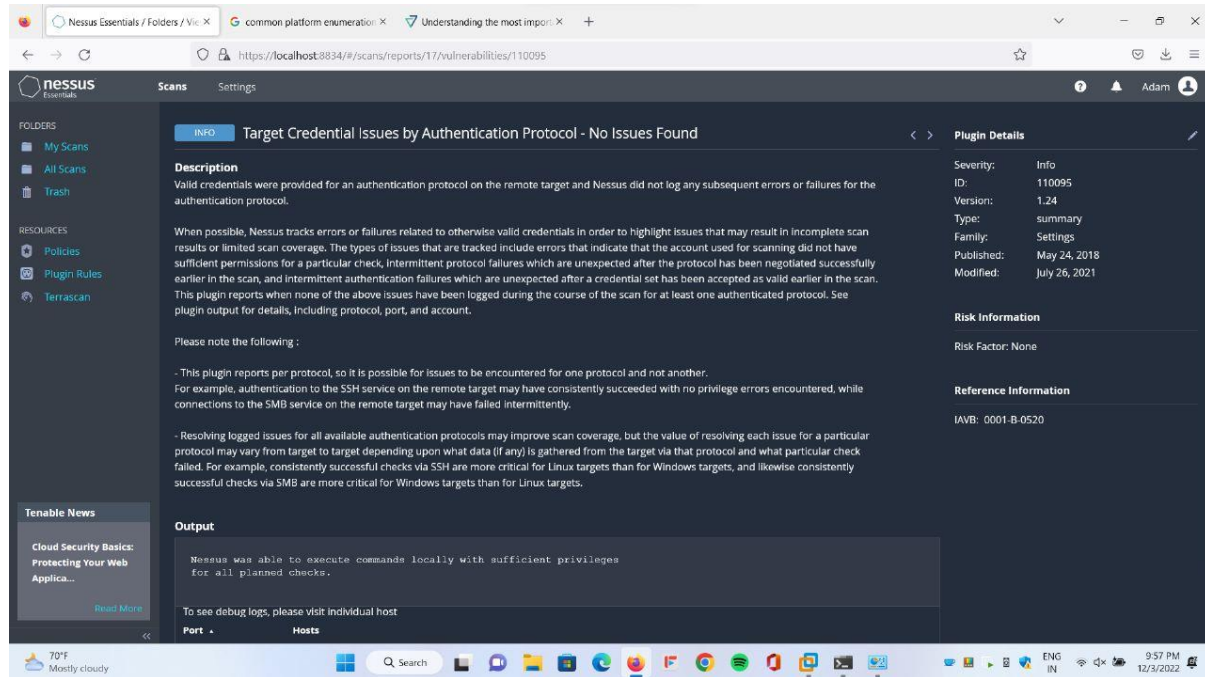
🔍 Search

📁 📧 📅 📌 📎 📏 📐 📑 📔 📕 📖 📗 📙 📚 📛 📜 📝 📞 📟 📠 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿

ENG IN 📶 🔊 🔇 🔈 🔉 🔊 🔋 🔌 🔍 🔎 🔏 🔐 🔑 🔒 🔓 🔔 🔕 🔖 🔗 🔘 🔙 🔚 🔛 🔜 🔝 🔞 🔟 🔠 🔡 🔢 🔣 🔤 🔥 🔦 🔧 🔨 🔩 🔪 🔫 🔬 🔭 🔮 🔯 🔰 🔱 🔲 🔳 🔴 🔵 🔶 🔷 🔸 🔹 🔺 🔻 🔼 🔽 🔾 🔿

9:53 PM 12/3/2022 🔔

# Target credential issues by Authentications Protocol – No issues found:



This an info Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

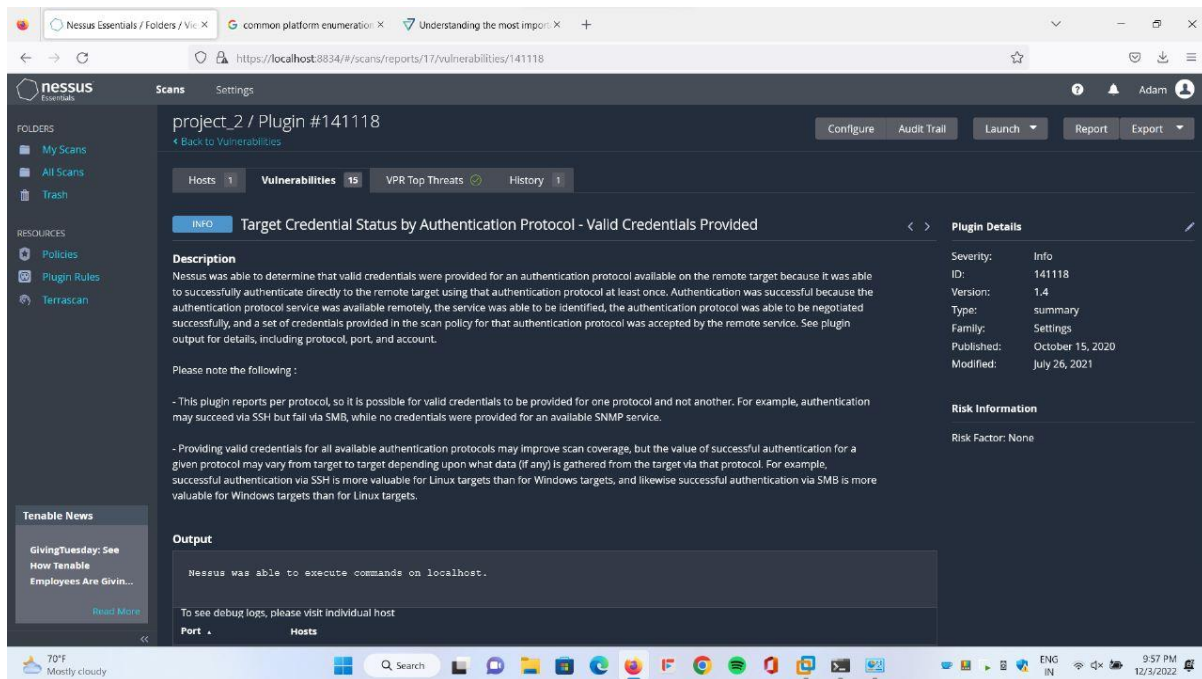
This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the

remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

## Target credential status by authentication protocol – valid credential provided:



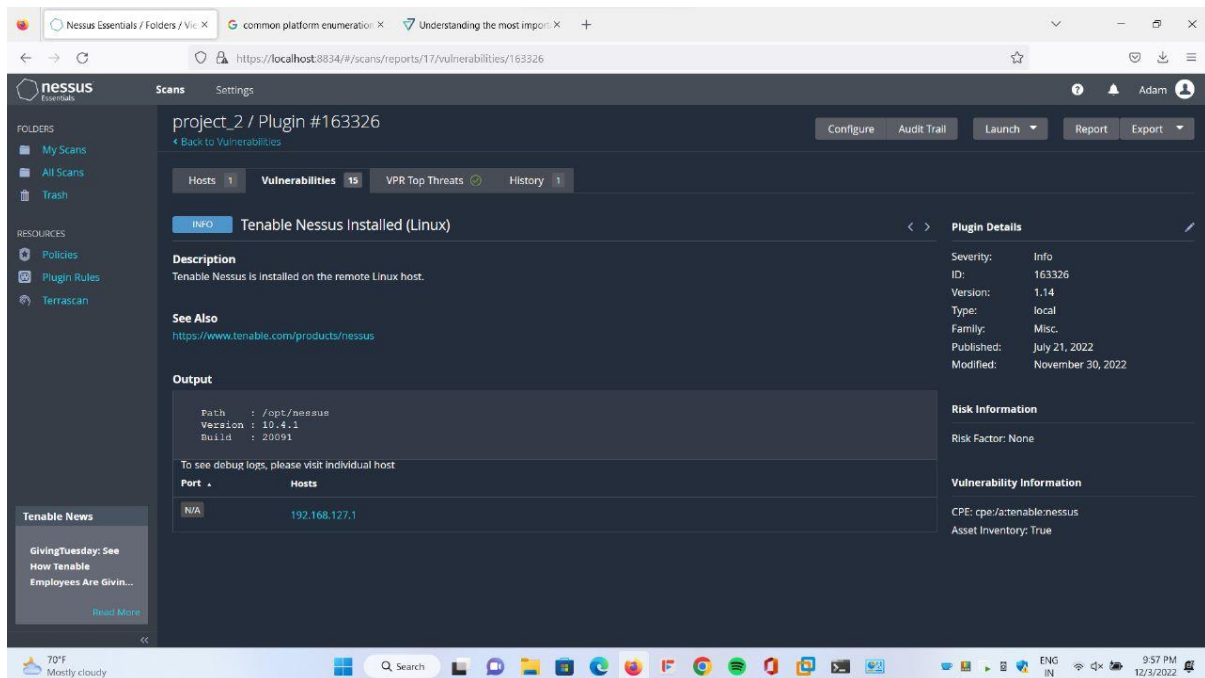
Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following:

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

## Tenable Nessus installed (Linux):



It is plugin checks whether tenable Nessus is installed on the remote Linux successfully or not.

Dependency:

Authenticated check: OS Name and installed package Enumeration:

This plugin gathers information about the remote host via an authenticated session.

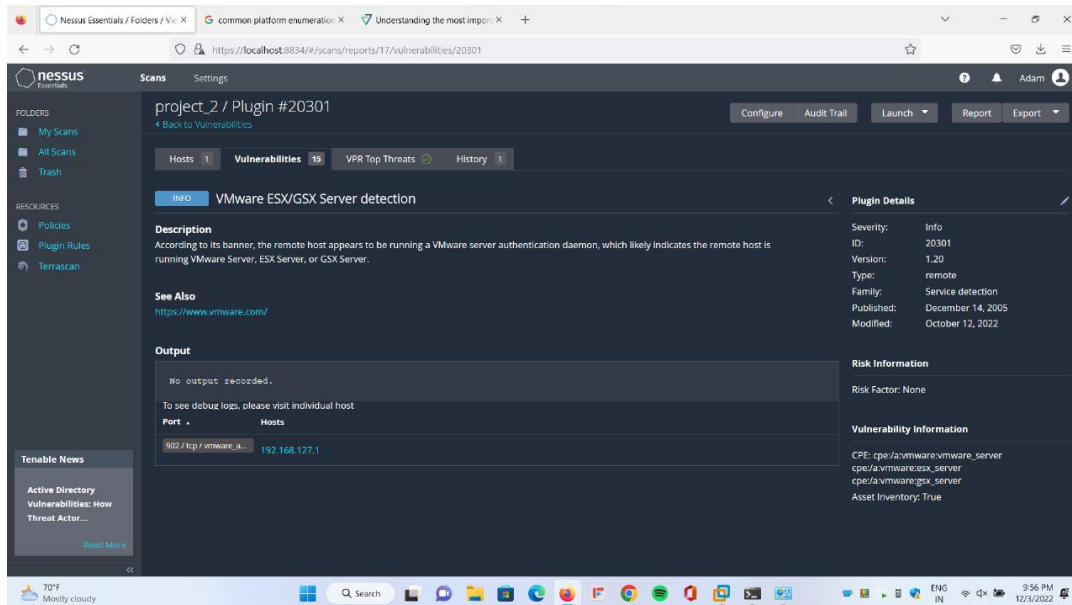
It logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

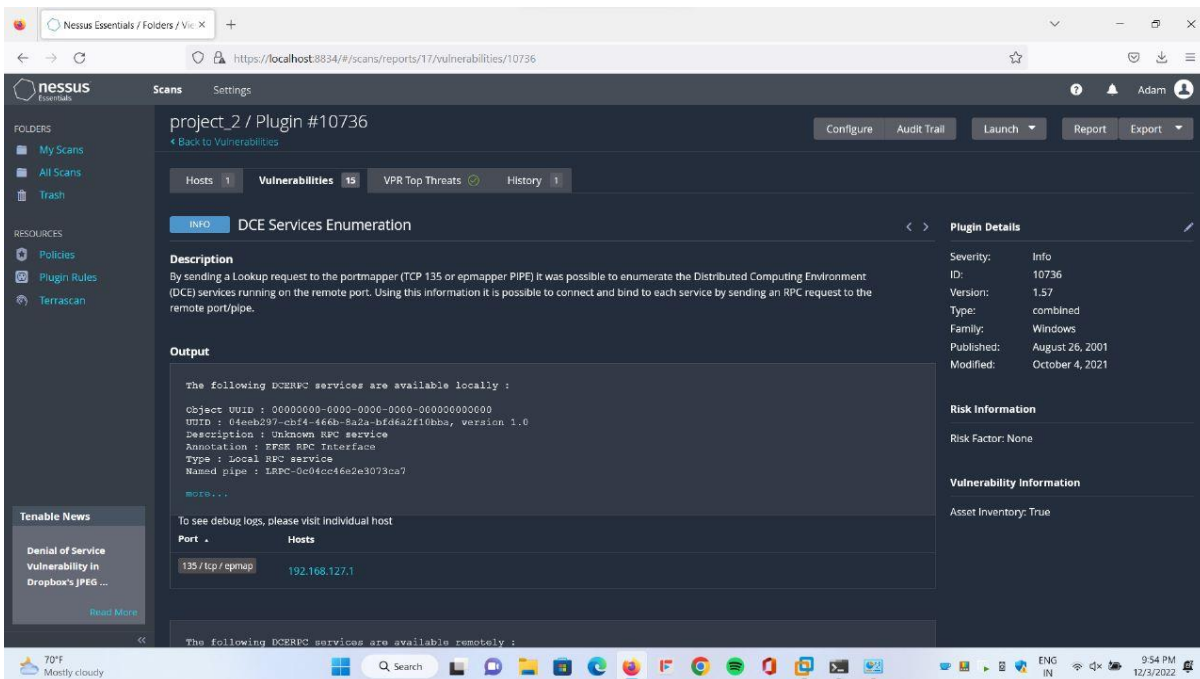


## VMware ESX/GSX server detection:

It is a plugin thoroughly checks the remote host appears to be running VMware server, ESX server or GSX Server.



## DCE Services Enumeration:





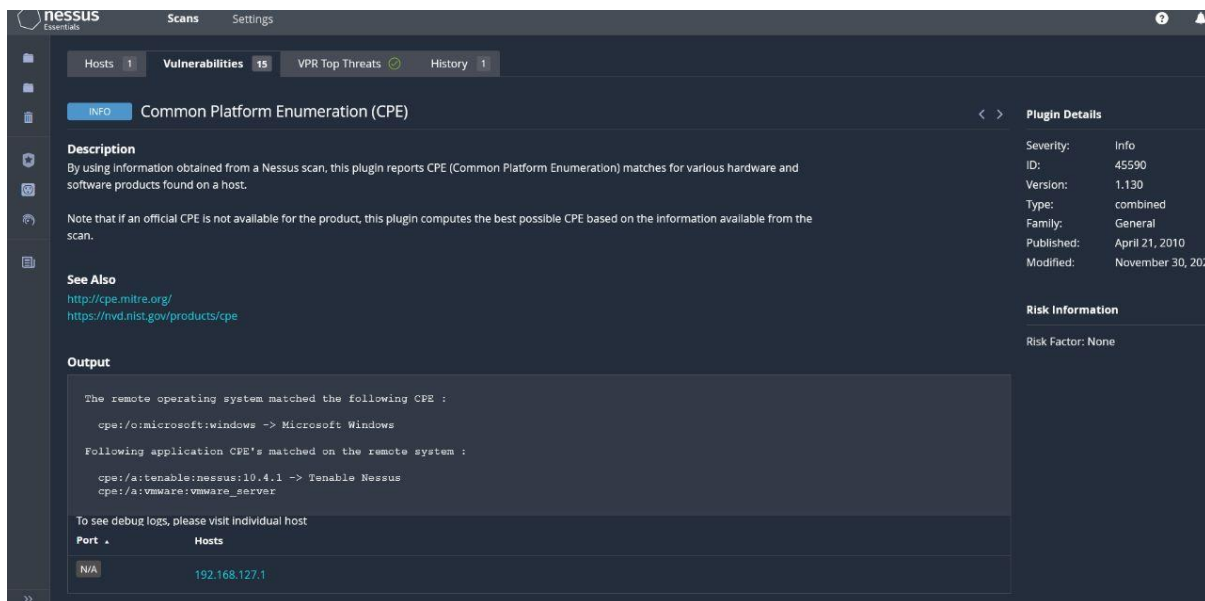
This is an information. By sending a lookup request to the portmapper (TCP 135), it is possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port.

The attacker might leverage the services that the DCE portmapper offers to exploit the computer if those services include any vulnerabilities.

Additionally, we should be cautious if any accounts with weak passwords have been set up on such platforms.

It is not a vulnerability in and of itself, however, in order to prevent any exploitation of our system, we should only open port 135 to trustworthy networks. It is not a good idea to leave this port open to the internet since doing so expands the attack surface and puts the system at risk for vulnerabilities that may be discovered in the future with this service or the services that it enables enumeration of.

## Common Platform Enumeration:



The screenshot displays the Nessus Essentials interface, specifically the 'Vulnerabilities' tab. The main content area shows the details for the 'Common Platform Enumeration (CPE)' plugin. The interface is divided into several sections:

- INFO**: Common Platform Enumeration (CPE)
- Description**: By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.
- See Also**: <http://cpe.mitre.org/>, <https://nvd.nist.gov/products/cpe>
- Output**:
  - The remote operating system matched the following CPE :  
cpe:/o:microsoft:windows -> Microsoft Windows
  - Following application CPE's matched on the remote system :  
cpe:/a:tenable:nessus:10.4.1 -> Tenable Nessus  
cpe:/a:vmware:vmware\_server
  - To see debug logs, please visit individual host
- Plugin Details**:
  - Severity: Info
  - ID: 45590
  - Version: 1.130
  - Type: combined
  - Family: General
  - Published: April 21, 2010
  - Modified: November 30, 2022
- Risk Information**:
  - Risk Factor: None

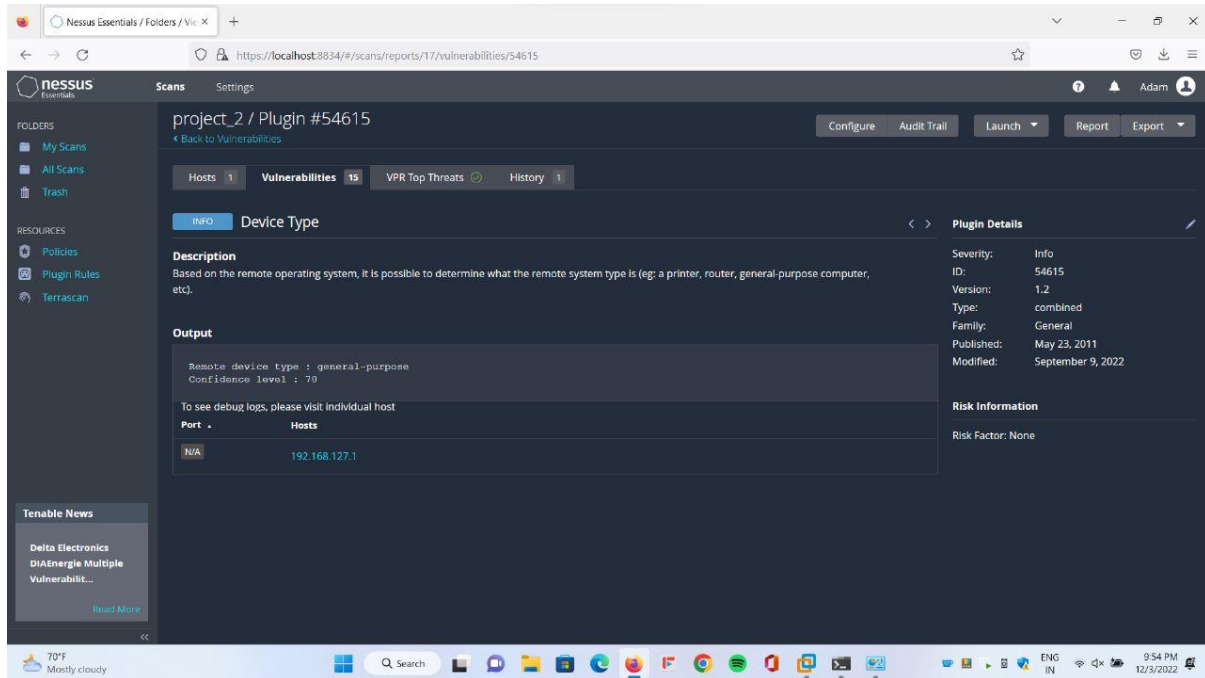
At the bottom, there is a table showing the results of the scan for the host 192.168.127.1:

Port	Hosts
N/A	192.168.127.1

It provides information about the matches for various hardware and software products found on the host based on the reports of the Nessus scan of the system.

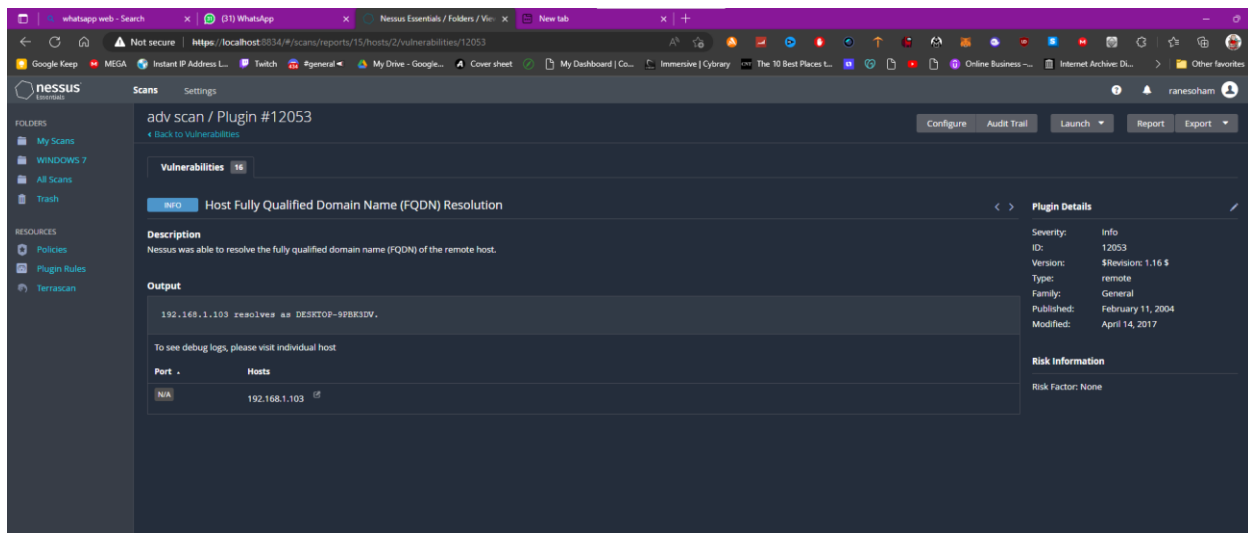
It is a systematic naming convention for software, systems, and packages used in information technology. CPE comprises a formal name format, a technique for comparing names to a system, and a description format for associating text and tests with a name. These components are based on the general syntax for Uniform Resource Identifiers (URI).

## Device Type:



It gives information about the what type of remote system is being scanned based on the remote operating system. For example- printer, router, computer/laptop etc.

## Host Fully Qualified Domain Name Resolution:



About:

In this screen as we can see info level severity vulnerability.

Description:

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Vulnerability:

### **Host Fully Qualified Domain Name (FQDN) Resolution -**

A fully-qualified domain name (FQDN) is a complete domain name that specifies the exact location of a computer or a host on the internet. It consists of the hostname and domain name. In addition, a FQDN can be found through terminal on MacOS and Linux or through the advanced system settings on Windows.

**OS IDENTIFICATION:**

**tenable** | Plugins Settings ▾

Plugins / Nessus / 11936 Language: English ▾

**OS Identification**  
Nessus Plugin ID 11936

**Synopsis**  
It is possible to guess the remote operating system.

**Description**  
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

**Plugin Details**

- Severity:** Info
- ID:** 11936
- File Name:** os\_fingerprint.nasl
- Version:** 2.61
- Type:** combined
- Agent:** windows, macosx, unix
- Family:** [General](#)
- Published:** 12/9/2003
- Updated:** 3/9/2022
- Asset Inventory:** true
- OS Identification:** true
- Supported Sensors:** Nessus Agent

It is possible to guess the remote operating system.

When scanning devices and systems I am always amazed at how many different services will hint at, or even flat out reveal, the operating system and version. Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

## NESSUS SCAN INFORMATION:

**tenable** | Plugins Settings ▾

Plugins / Nessus / 19506 Language: English ▾

**Nessus Scan Information**  
Nessus Plugin ID 19506

**Synopsis**  
This plugin displays information about the Nessus scan.

**Description**  
This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialiaed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

**Plugin Details**

- Severity:** Info
- ID:** 19506
- File Name:** scan\_info.nasl
- Version:** 1.116
- Type:** summary
- Agent:** windows, macosx, unix
- Family:** [Settings](#)
- Published:** 8/26/2005
- Updated:** 6/9/2022
- Configuration:** Enable thorough checks
- Supported Sensors:** Nessus Agent

This plugin displays information about the Nessus scan.

This plugin displays, for each tested host, information about the scan itself:

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

#### VULNERABILITIES FOUND:

<input type="checkbox"/>	INFO	OS Identification and Installed Software Enumeration ov...	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	OS Security Patch Assessment Available	Settings	1	🔄	✎
<input type="checkbox"/>	INFO	Target Credential Issues by Authentication Protocol - No...	Settings	1	🔄	✎

#### VULNERABILITY ASSESMENT:

project\_2 / Plugin #110095

[← Back to Vulnerabilities](#)

Hosts 1

**Vulnerabilities 15**

VPR Top Threats 🟢

History 1

INFO Target Credential Issues by Authentication Protocol - No Issues Found

#### Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during

the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Output	
Nessus was able to execute commands locally with sufficient privileges for all planned checks.	
To see debug logs, please visit individual host	
Port	Hosts
N/A	192.168.127.1

## OS SECURITY PATCH ASSESSMENT AVAILABLE:

Newest

Updated

Search

Nessus Families

WAS Families

NNM Families

LCE Families

Tenable.ot Families

About Plugin Families

Nessus Release Notes

Tenable.ad Indicators

Plugins / Nessus / 117887

OS Security Patch Assessment Available

INFO Nessus Plugin ID 117887

InformationDependenciesDependentsChangelog

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Plugin Details

Severity: Info

ID: 117887

File Name: local\_checks\_enabled.nasl

Version: 1.5

Type: summary

Agent: windows, macosx, unix

Family: Settings

Published: 10/2/2018

Updated: 7/12/2021

Supported Sensors: Nessus Agent

Reference Information

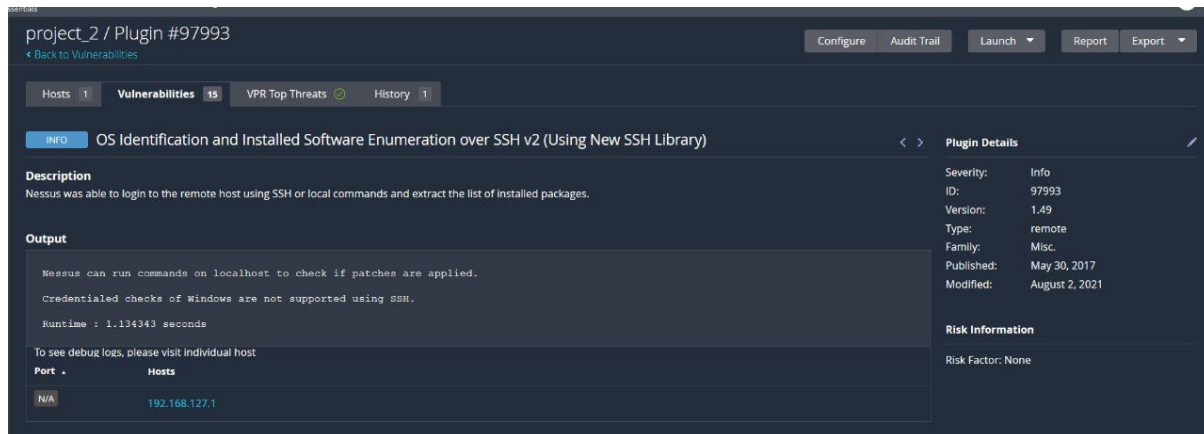
IAVB: 0001-B-0516

## DESCRIPTION:

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

## OS Identification and Installed Software Enumeration over SSHv2:



The screenshot displays the Nessus web interface for a specific plugin. At the top, the breadcrumb 'project\_2 / Plugin #97993' is visible, along with action buttons: 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this is a navigation bar with tabs for 'Hosts' (1), 'Vulnerabilities' (15), 'VPR Top Threats' (with a green checkmark), and 'History' (1). The main content area is titled 'OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)'. It is divided into three sections: 'Description', 'Output', and 'Plugin Details'. The 'Description' section states: 'Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.' The 'Output' section contains a text box with the following content: 'Nessus can run commands on localhost to check if patches are applied. Credentialed checks of Windows are not supported using SSH. Runtime : 1.134343 seconds. To see debug logs, please visit individual host'. Below the output is a table with two columns: 'Port' and 'Hosts'. The 'Port' column shows 'N/A' and the 'Hosts' column shows '192.168.127.1'. The 'Plugin Details' section on the right lists the following information: Severity: Info, ID: 97993, Version: 1.49, Type: remote, Family: Misc., Published: May 30, 2017, Modified: August 2, 2021. At the bottom of the plugin details, it shows 'Risk Information' with a 'Risk Factor: None'.

It provides the information that Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

SSHv2, also known as Secure Shell 2.0 or SSH 2, is a secure communications protocol that includes the architectural levels of connection, transport, and authentication. SSHv2 is used to transfer many different protocols, including SFTP, SCP, SSFS, GIT, SVN, and many more. One of the most popular uses for SSHv2 is as a stand-alone for basic terminal connection (TTY).

SSHv2 Server implementations may be tested for robustness using this test suite.

Using this, information about the remote host can be disclosed via an authenticated session.