


nessus / Setup

Not secure https://localhost:8834/#/

HOST



Create a user account

Create a Nessus administrator account. Use this username and password to log into Nessus.

Username *


Password *

Back Submit


© 2023 Tenable™, Inc.

win10 machine for labs [Running] - Oracle VM VirtualBox


File Machine View Input Devices Help



Google Chrome



TargetVM



Recycle Bin

TARGET VM

Security Essentials

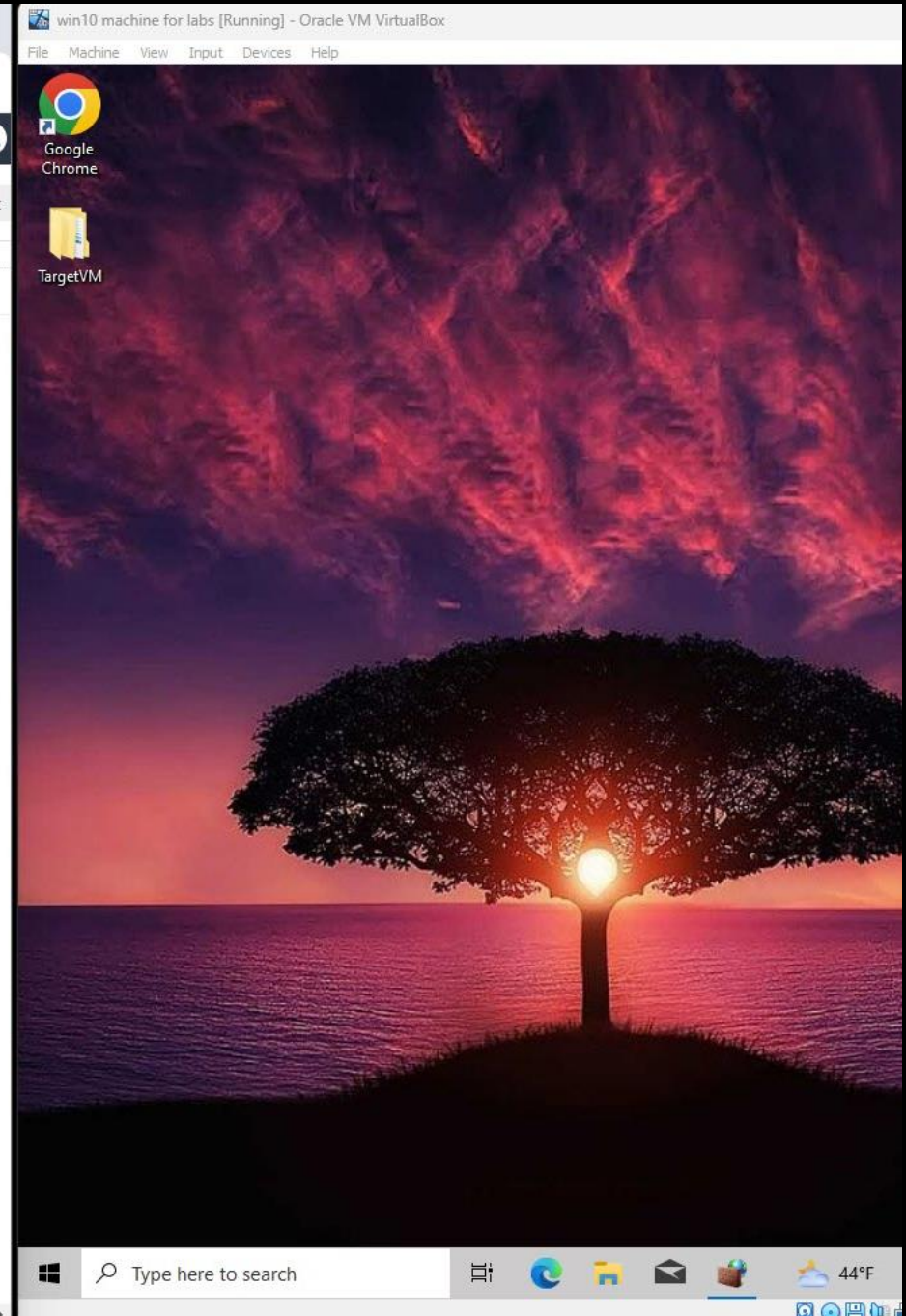
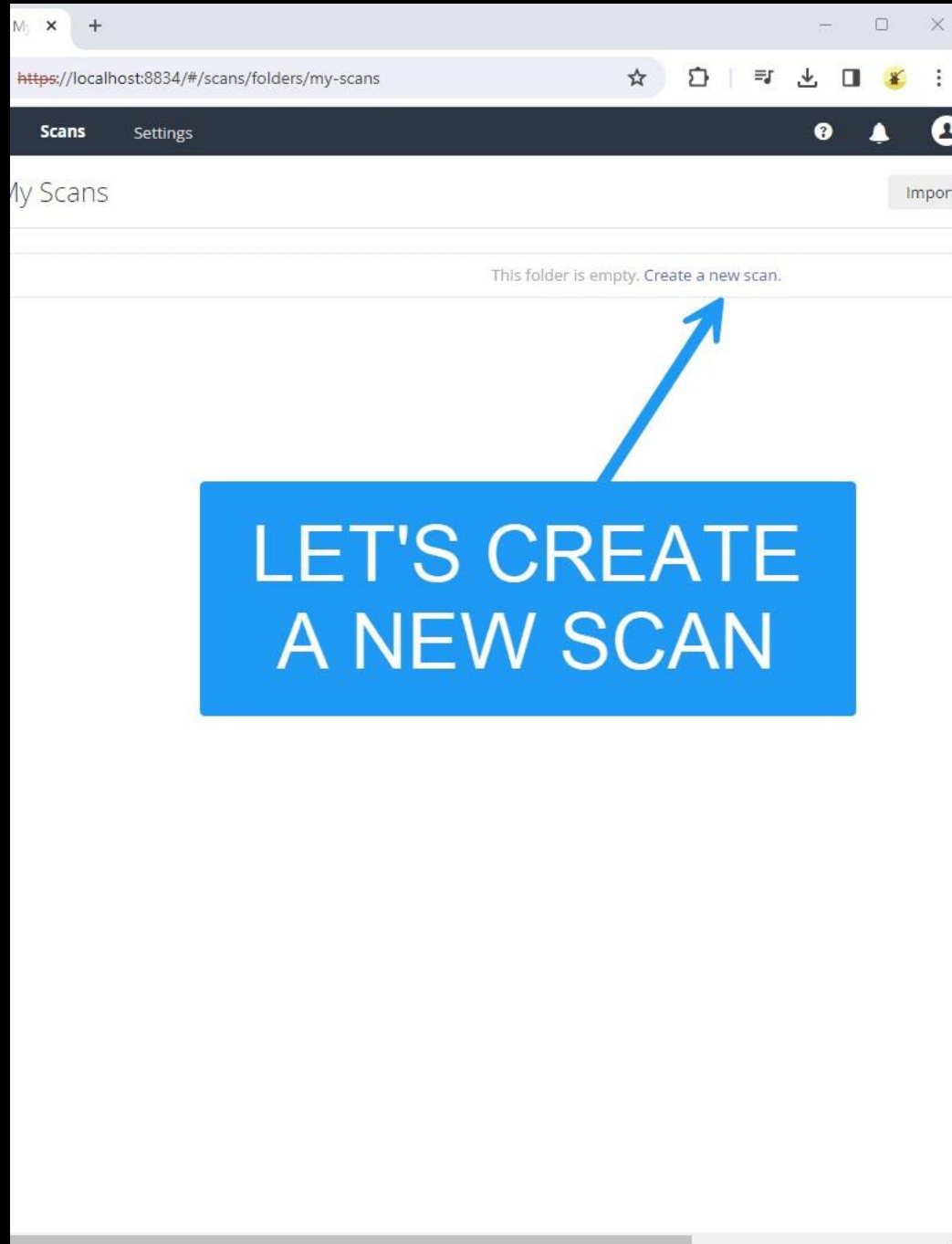
Start

Type here to search

45°F Cloudy 8:59 PM 12/25/2023

Right Ctrl

Here we have a split-screen view on my computer. To the left, the Tenable Nessus Essentials portal is ready for me to create a new network vulnerability scan. On the right, my Oracle VM VirtualBox is running a virtualized Windows 10 environment.



https://localhost:8834/#/scans/reports/new

Scans Settings

Scan Templates

Back to Scans

Scanner

DISCOVERY

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

VULNERABILITIES

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

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 Linux systems.

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.

Intel AMT Security
Remote and local checks for Intel AMT vulnerabilities (CVE-2017-5689).

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remot
A remote scan to detect Netlogon Elevation of Privilege (Zerologon).

Solorigate

ProxyLogon : MS Exchange

PrintNightmare

Active Directory Scan

LET'S CHECK FOR VULNERABILITIES ON THE TARGET VM

win10 machine for labs [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Google Chrome

TargetVM

Type here to search

44°F

Here we have a detailed view of my cybersecurity setup. On the left side, I'm using Tenable Nessus Essentials to check for vulnerabilities, with a selection of scan templates available, including options like Basic Network Scan and Advanced Dynamic Scan. I'm about to start a security scan to check for vulnerabilities on a target VM, which is visible on the right side of the screen in the Oracle VM VirtualBox window.

Here we have the configuration page for a Basic Network Scan within the Tenable Nessus Essentials interface. I have the option to perform credential scanning, and I've entered the target IP address that I want to scan. With this setup, I'm preparing to conduct a thorough assessment of the network security for the specified IP.

The screenshot displays the Tenable Nessus Essentials interface for configuring a new scan. The browser address bar shows the URL: `https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general`. The page title is "New Scan / Basic Network Scan".

On the left sidebar, there are sections for "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). The main content area has tabs for "Settings", "Credentials", and "Plugins". A blue callout box with white text points to the "Credentials" tab, stating: "HERE WE HAVE A CHOICE TO DO CREDENTIAL SCANNING".

The "Settings" tab is active, showing a left-hand menu with sections: "BASIC" (General, Schedule, Notifications), "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED". The main form fields include:

- Name: [Empty]
- Description: [Empty]
- Folder: My Scans
- Targets: 10.0.0.186

A second blue callout box with white text points to the "Targets" field, stating: "HERE WE PUT THE TARGET IP THAT WE WANT TO SCAN". At the bottom of the form, there are "Save" and "Cancel" buttons.

tenable Nessus Essentials Scans Settings guillermo_admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

My Scans

Import New Folder + New Scan

Search Scans 1 Scan

<input type="checkbox"/>	Name	Schedule	Last Scanned	Launch
<input type="checkbox"/>	Windows 10 Single Host	On Demand	N/A	

"LAUNCH" STARTS THE SCAN FOR VULNERABILITIES

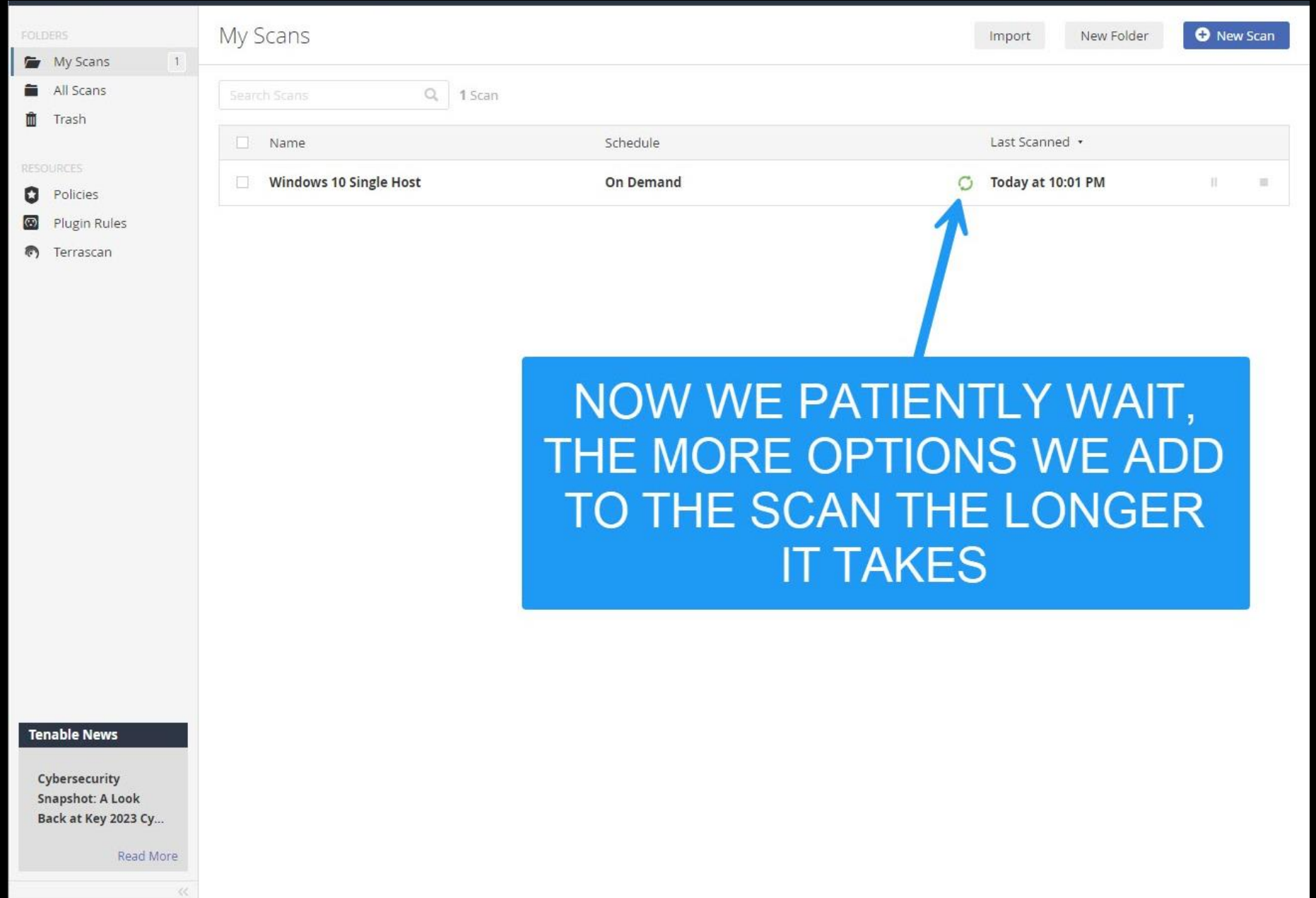
Tenable News

Tenable Wrapped: A Look Back at Our Industry Recog...

Read More

In this image, the scan is being initiated to detect vulnerabilities after all the configuration and setup have been completed within the Tenable Nessus Essentials interface. This action marks the beginning of the vulnerability assessment process.

It's important to note that credential scans typically take much longer compared to non-credential scans. The waiting period for the scan's completion depends on the details and filters we add towards the scan.



The screenshot displays the 'My Scans' interface in the Tenable console. On the left, there are navigation menus for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area shows a table of scans with columns for Name, Schedule, and Last Scanned. A single scan is listed: 'Windows 10 Single Host' with a schedule of 'On Demand' and a last scanned time of 'Today at 10:01 PM'. A blue arrow points to a green circular progress indicator next to the scan name. A blue text box with white text is overlaid on the right side of the image, pointing to the progress indicator.

<input type="checkbox"/>	Name	Schedule	Last Scanned		
<input type="checkbox"/>	Windows 10 Single Host	On Demand	Today at 10:01 PM		■

NOW WE PATIENTLY WAIT, THE MORE OPTIONS WE ADD TO THE SCAN THE LONGER IT TAKES

Tenable News

Cybersecurity
Snapshot: A Look
Back at Key 2023 Cy...
[Read More](#)

As the initial vulnerability scan concludes, it has successfully identified a total of 14 vulnerabilities. To provide a visual overview of these findings, there's a pie chart on display. This pie chart effectively categorizes the vulnerabilities into various severity levels, including Critical, High, Medium, Low, and Informational.

The screenshot displays the Tenable Nessus interface for a scan titled "Windows 10 VM". The interface includes a left sidebar with navigation options like "My Scans", "All Scans", and "Trash". The main content area shows a table of scan history with columns for "Start Time", "Last Scanned", and "Status". A single scan entry is shown as "Completed" with a checkmark icon. A blue arrow points from a callout box to this entry. To the right, the "Scan Details" section provides metadata such as "Policy: Basic Network Scan", "Status: Completed", and "Elapsed: 14 minutes". Below this, the "Vulnerabilities" section features a donut chart and a legend for severity levels: Critical (dark red), High (red), Medium (orange), Low (yellow), and Info (blue).

Start Time	Last Scanned	Status
Current Today at 10:32 ...	Today at 10:46 PM	Completed

COMPLETED SCAN, 14 VULNERABILITIES FOUND

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:32 PM
- End: Today at 10:46 PM
- Elapsed: 14 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Tenable News

Cybersecurity Snapshot: A Look Back at Key 2023 Cy...
[Read More](#)

Nessus Essentials / Folders / Vie x +

Not secure https://localhost:8834/#/scans/reports/16/vulnerabilities

tenable Nessus Essentials Scans Settings guillermo_admin

Windows 10 VM

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 14 History 1

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
MEDIUM	5.3		SMB S...	Misc.	1		
INFO	S...	Windows	6		
INFO			DCE S...	Windows	9		
INFO			Com...	General	1		
INFO			Device...	General	1		
INFO			Ether...	Misc.	1		
INFO			Ether...	General	1		
INFO			Host F...	General	1		
INFO			Nessu...	Settings	1		
INFO			OS Ide...	General	1		
INFO			OS Se...	Settings	1		
INFO			Target...	Settings	1		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:32 PM
End: Today at 10:46 PM
Elapsed: 14 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

In this particular slide, we have a clear view of our Windows 10 virtual machine (VM) alongside the previously identified 14 vulnerabilities. Among these vulnerabilities, one specific issue stands out: a Medium-severity vulnerability with a CVSS (Common Vulnerability Scoring System) score of 5.3. This particular vulnerability is related to SMB (Server Message Block), highlighting a potential security concern that merits attention and further assessment.

Nessus Essentials / Folders / Vie x +

Not secure https://localhost:8834/#/scans/reports/16/vulnerabilities/57608

tenable Nessus Essentials Scans Settings guillermo_admin

Windows 10 VM / Plugin #57608

Configure Audit Trail Launch Report Export

Back to Vulnerabilities

Hosts 1 Vulnerabilities 14 History 1

MEDIUM SMB Signing not required

Description
 Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
 Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also
<http://www.nessus.org/u?df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?74b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.40.135

Plugin Details

Severity: Medium
 ID: 57608
 Version: 1.20
 Type: remote
 Family: Misc.
 Published: January 19, 2012
 Modified: October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 5.3
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
 CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
 CVSS v3.0 Temporal Score: 4.6
 CVSS v2.0 Base Score: 5.0
 CVSS v2.0 Temporal Score: 3.7
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
 CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

Exploit Available: true

This scan highlights the importance of routine vulnerability assessments. It underscores that even basic vulnerabilities, such as those lacking SMB signing, can be exploited using tools like Wireshark, Ettercap, and BetterCAP for man-in-the-middle attacks. The key takeaway is the necessity of regular checks to detect and address vulnerabilities before they become major security risks. In the ever-changing landscape of cybersecurity, our commitment to continuous learning and vigilance is crucial for staying resilient and adaptable to new challenges.