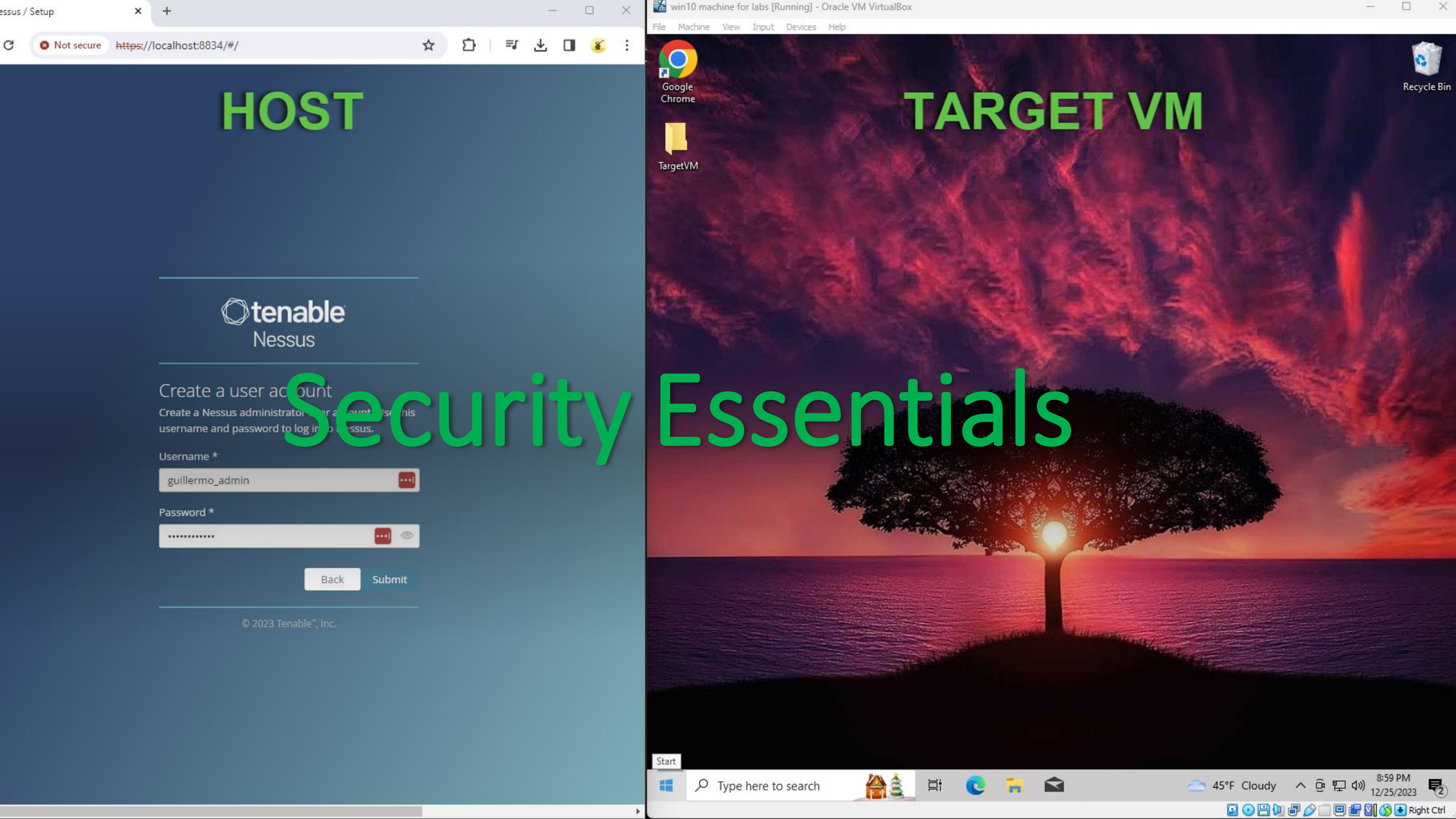
# Security Essentials



Create a user account

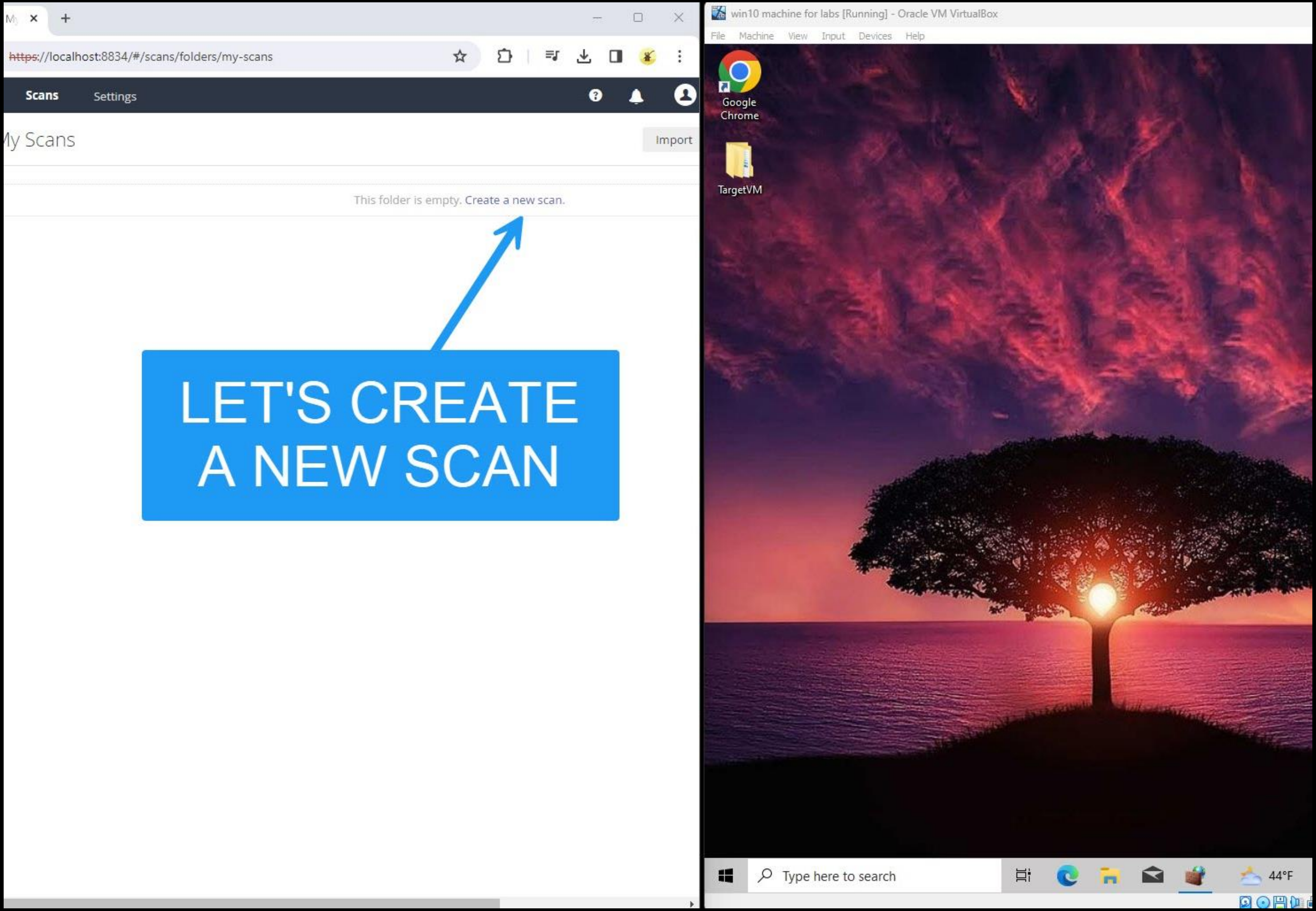
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username * guillermo_admin

Password * ••••••••••••

© 2023 Tenable™, Inc.

**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.**



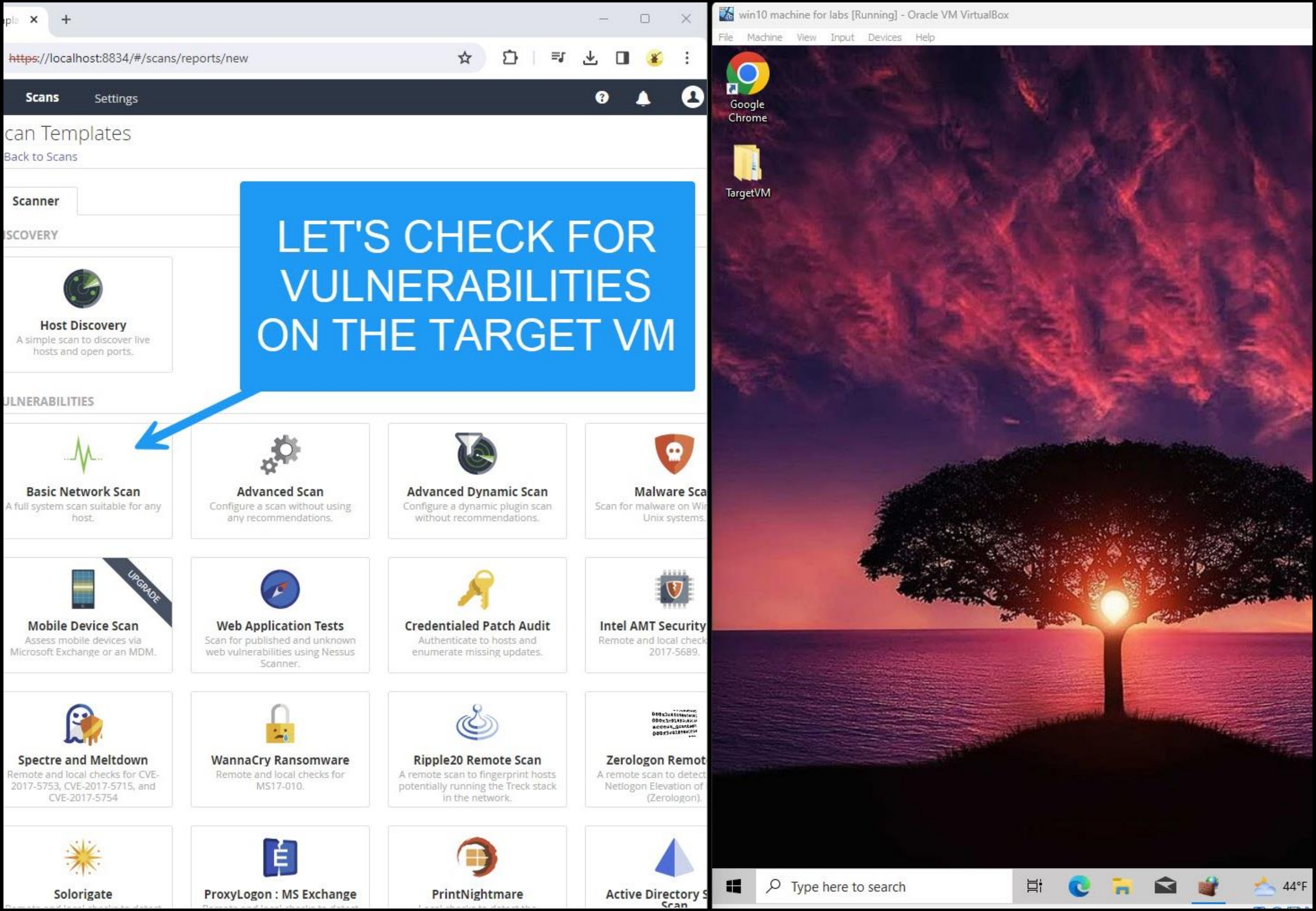
https://localhost:8834/#/scans/folders/my-scans

My Scans

This folder is empty. Create a new scan.

LET'S CREATE A NEW SCAN

win10 machine for labs [Running] - Oracle VM VirtualBox



LET'S CHECK FOR VULNERABILITIES ON THE TARGET VM

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

can Templates

Back to Scans

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

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 Sca — Scan for malware on Wi Unix 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 check 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.

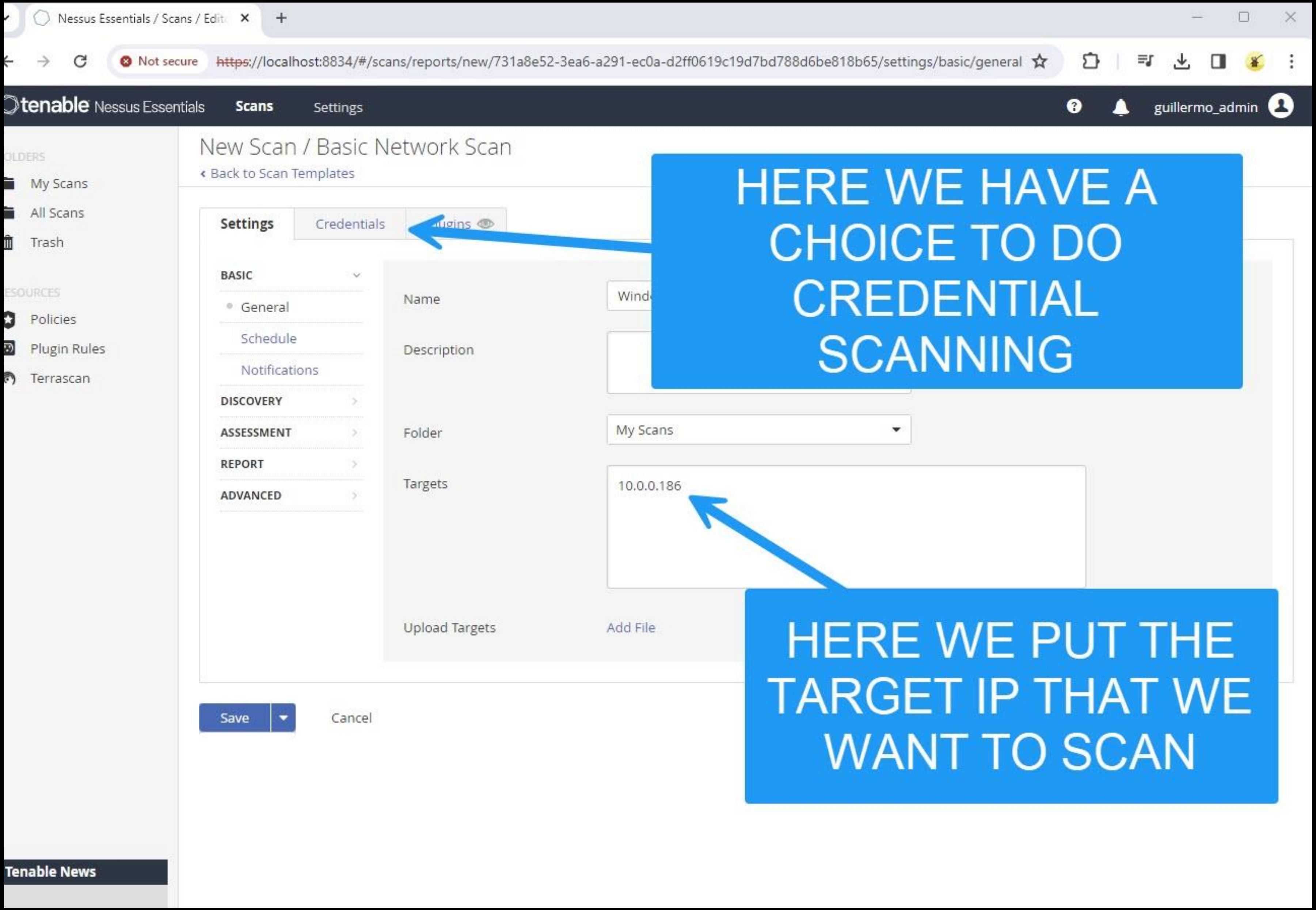
Ripple20 Remote Scan — A remote scan to fingerprint hosts potentially running the Treck stack in the network.

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

win10 machine for labs [Running] - Oracle VM VirtualBox

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.**



New Scan / Basic Network Scan

Name: Wind

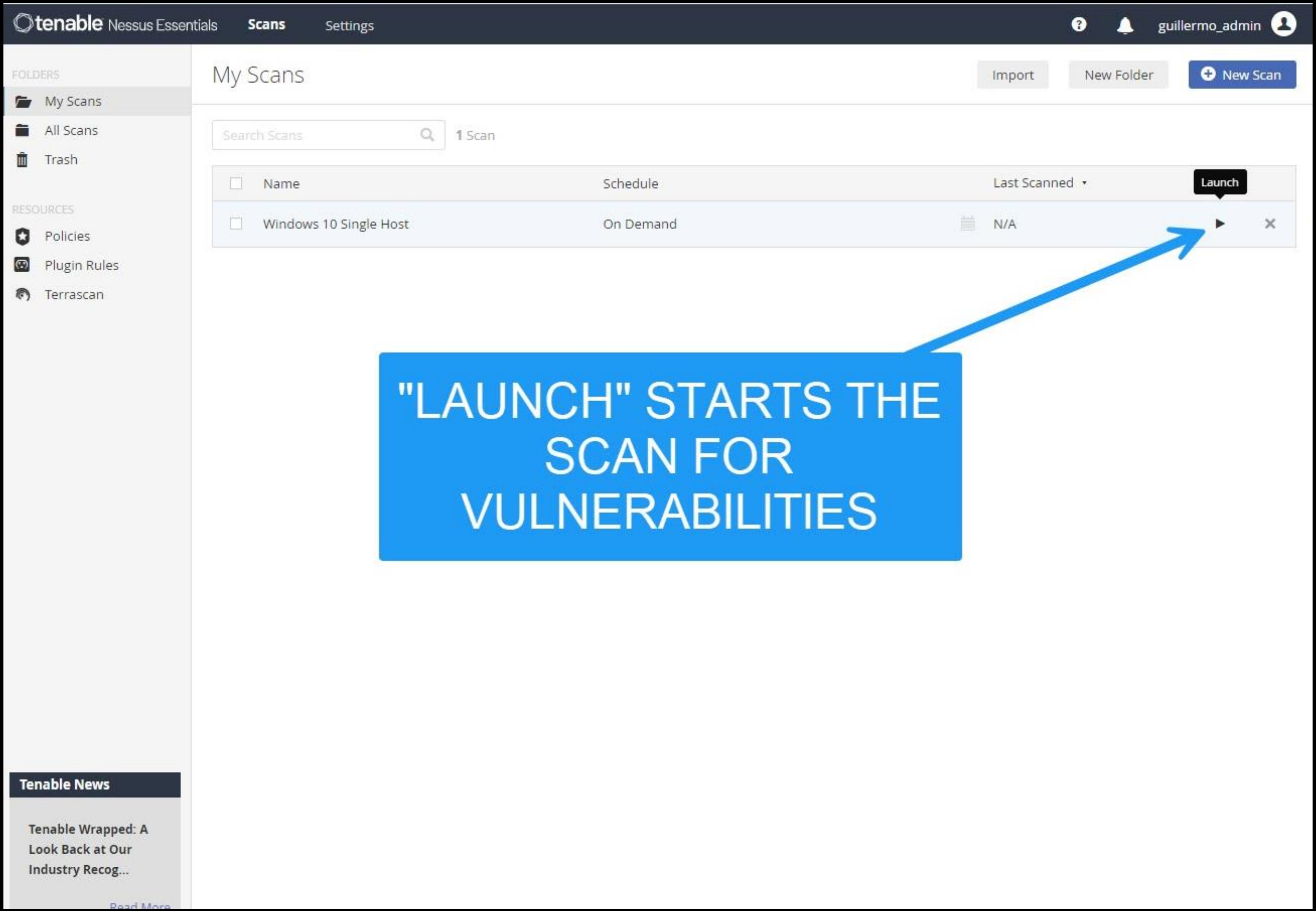
Description:

Folder: My Scans

Targets: 10.0.0.186

HERE WE HAVE A CHOICE TO DO CREDENTIAL SCANNING

HERE WE PUT THE TARGET IP THAT WE WANT TO SCAN



My Scans

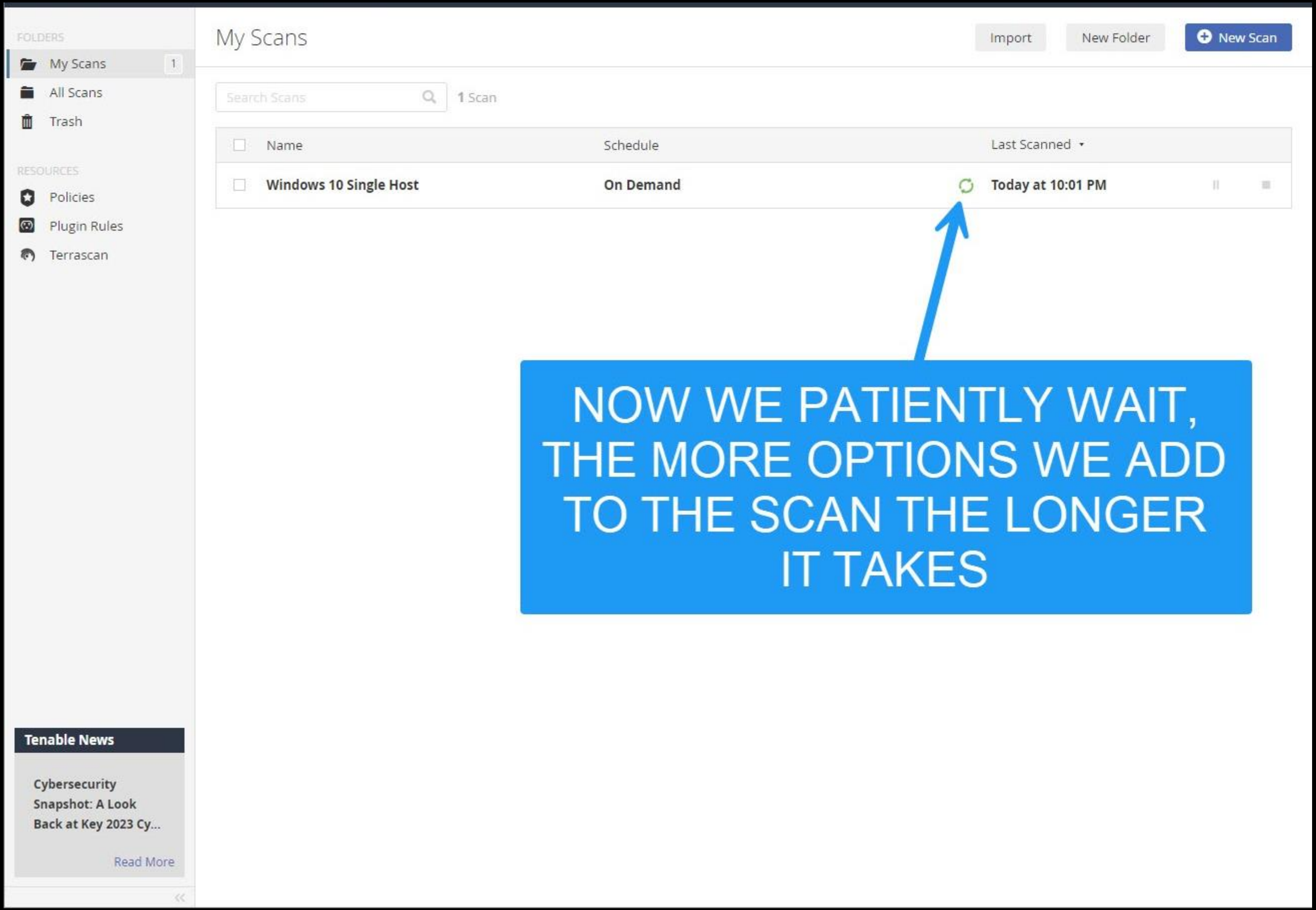
| □ | Name | Schedule | Last Scanned | |
|---|---|---|---|---|
| □ | Windows 10 Single Host | On Demand | N/A | ▶ ✕ |

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

"LAUNCH" STARTS THE SCAN FOR VULNERABILITIES

**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.**



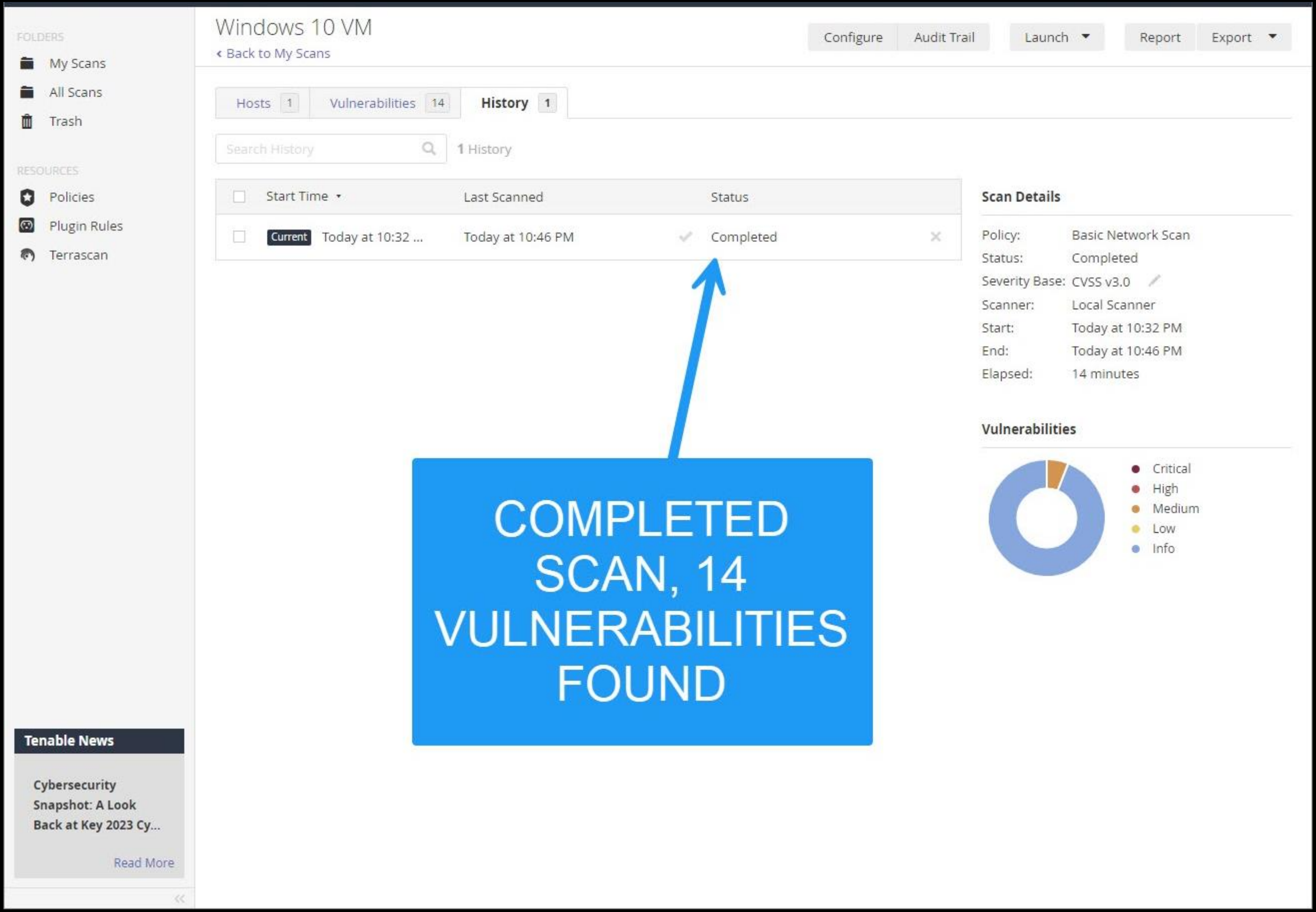
## My Scans

1 Scan

| Name | Schedule | Last Scanned |
|---|---|---|
| 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

**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.**



Windows 10 VM

1 History

| □ | Start Time | Last Scanned | Status |
|---|---|---|---|
| □ | Current Today at 10:32 ... | Today at 10:46 PM | ✓ Completed |

**Scan Details**

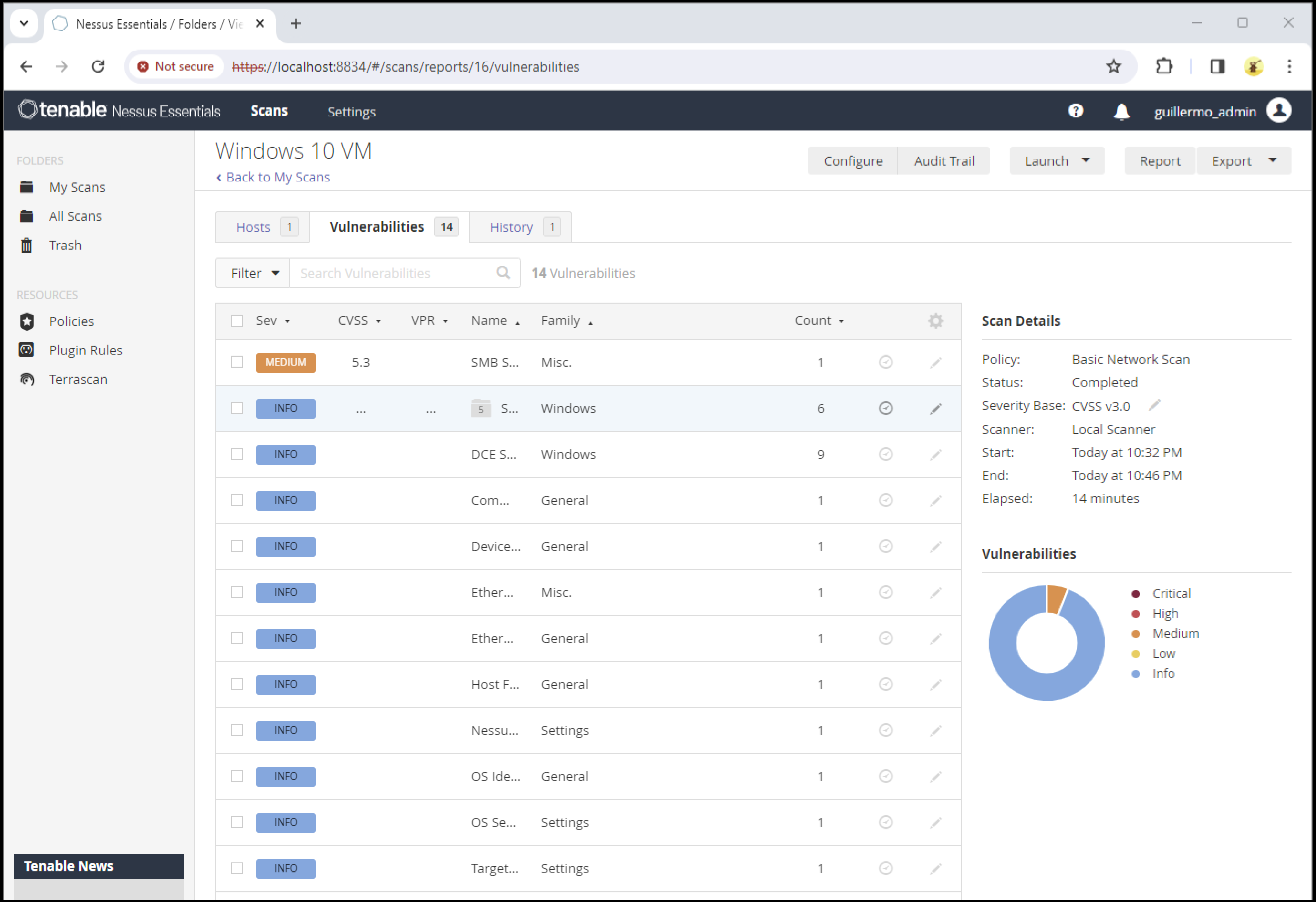
| | |
|---|---|
| Policy: | Basic Network Scan |
| Status: | Completed |
| Severity Base: | CVSS v3.0 |
| Scanner: | Local Scanner |
| Start: | Today at 10:32 PM |
| End: | Today at 10:46 PM |
| Elapsed: | 14 minutes |

**Vulnerabilities**

**Tenable News**

Cybersecurity Snapshot: A Look Back at Key 2023 Cy...

COMPLETED SCAN, 14 VULNERABILITIES FOUND



## Windows 10 VM

‹ Back to My Scans

14 Vulnerabilities

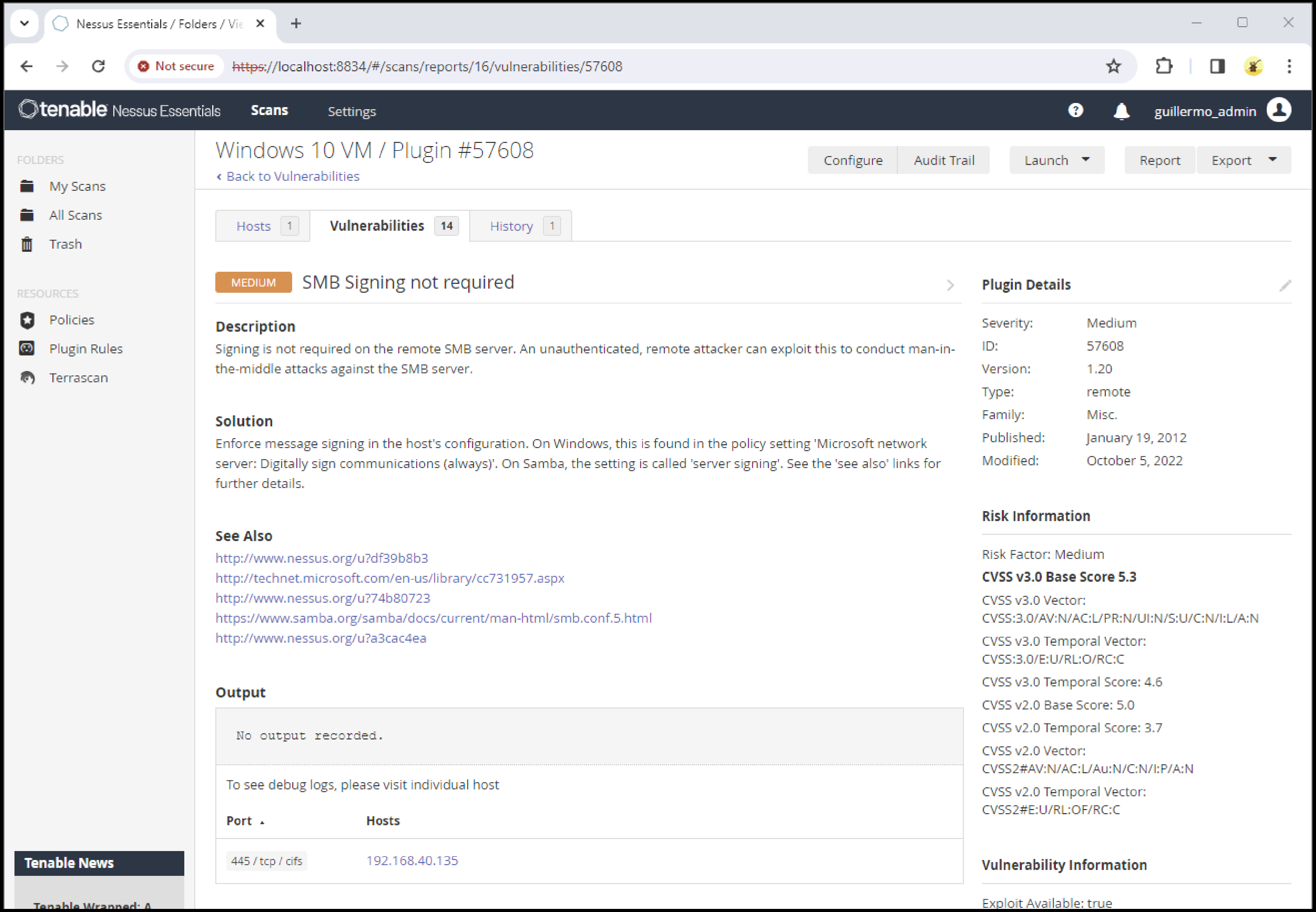
| Sev | CVSS | VPR | Name | Family | Count |
|---|---|---|---|---|---|
| MEDIUM | 5.3 | | SMB S... | Misc. | 1 |
| INFO | ... | ... | 5 S... | Windows | 6 |
| INFO | | | DCE S... | Windows | 9 |
| INFO | | | Com... | General | 1 |
| INFO | | | Device... | General | 1 |
| INFO | | | Ether... | Misc. | 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**

**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.**



## Windows 10 VM / Plugin #57608

‹ Back to Vulnerabilities

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.