Deployment of Nessus Vulnerability Scanner

By Michael Emil Santos

Introduction

This project demonstrates the use of Nessus, a powerful vulnerability scanning tool, to assess and strengthen network security. By deploying Nessus on a Windows Server 2016 VM and conduct a comprehensive vulnerability scan to identify security gaps and mitigate risks.

Project Objectives and Steps

Nessus is a remote security scanning tool, scans a computer in the network and send an alert if it discovers any vulnerabilities that malicious hackers could use to gain access. In this lab the practice of how to use and benefits of such a tool is applied.it is the most trusted vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, use wizards to create policies, schedule scans and send results via email easily and quickly. Nessus supports more technologies than any other vendor, including operating systems, network devices, hypervisors, databases, tablets/phones, web servers and critical infrastructure.

1. **Installation and Setup**

   - **Objective**: Deploy Nessus on a virtual environment for a baseline vulnerability assessment.
   - **Steps**: Install Nessus on Windows Server 2016, activated a trial license, and configured a user account to initiate scans.

2. **Running a Baseline Scan**

   - **Objective**: Identify and categorize vulnerabilities in the server's configuration.
   - **Steps**: Created and ran a scan targeting the server, using Nessus's default scan settings. The scan detected various vulnerabilities, providing insights into potential security risks.

3. **Analyzing the Report**

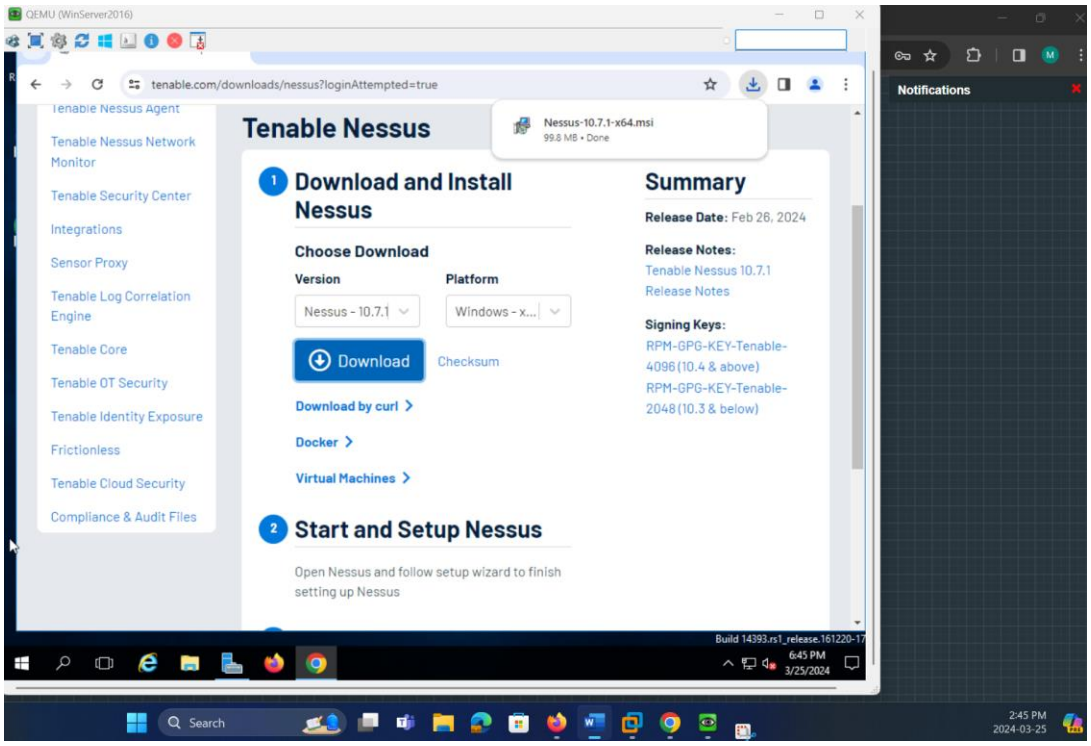
   - **Objective**: Examine and prioritize identified vulnerabilities for remediation.
   - **Steps**: Reviewed the report, which highlighted vulnerabilities like outdated protocols (SSL/TLS) and other security gaps. The report included severity levels (low, medium, high) for each vulnerability, helping to prioritize actions.

4. **Remediation Recommendations**

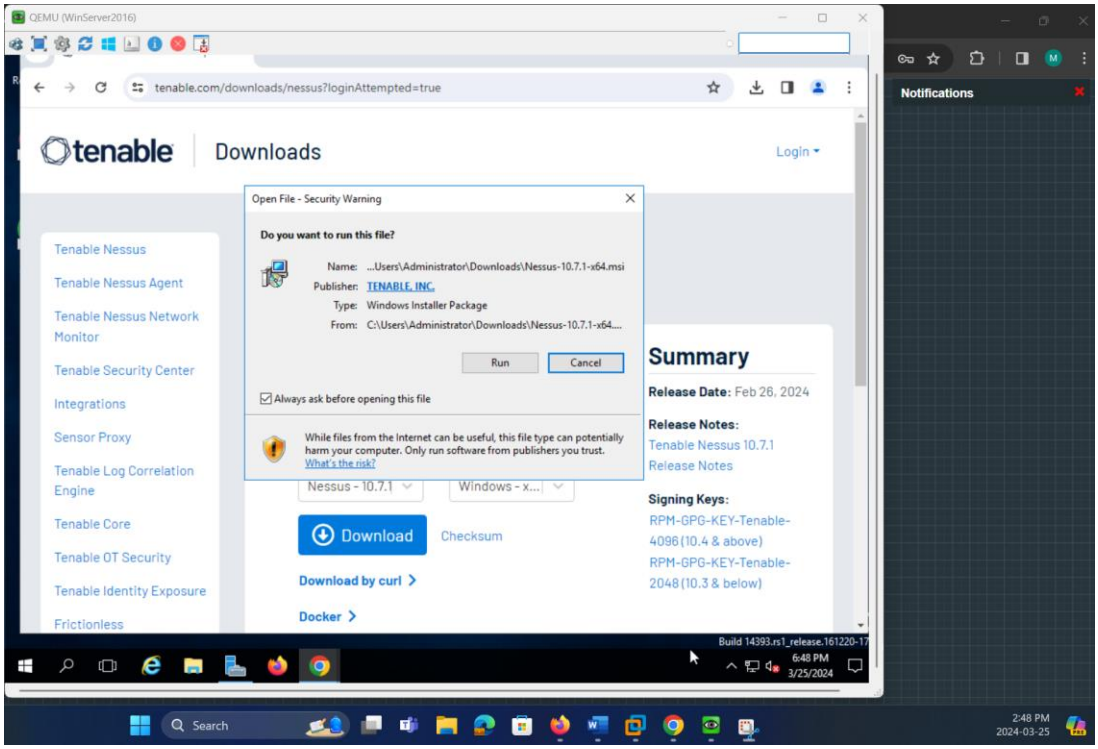
   - **Objective**: Develop a security improvement plan based on Nessus's findings.
   - **Steps**: Created a prioritized action plan, addressing critical vulnerabilities first through patching, configuration adjustments, and system hardening recommendations.

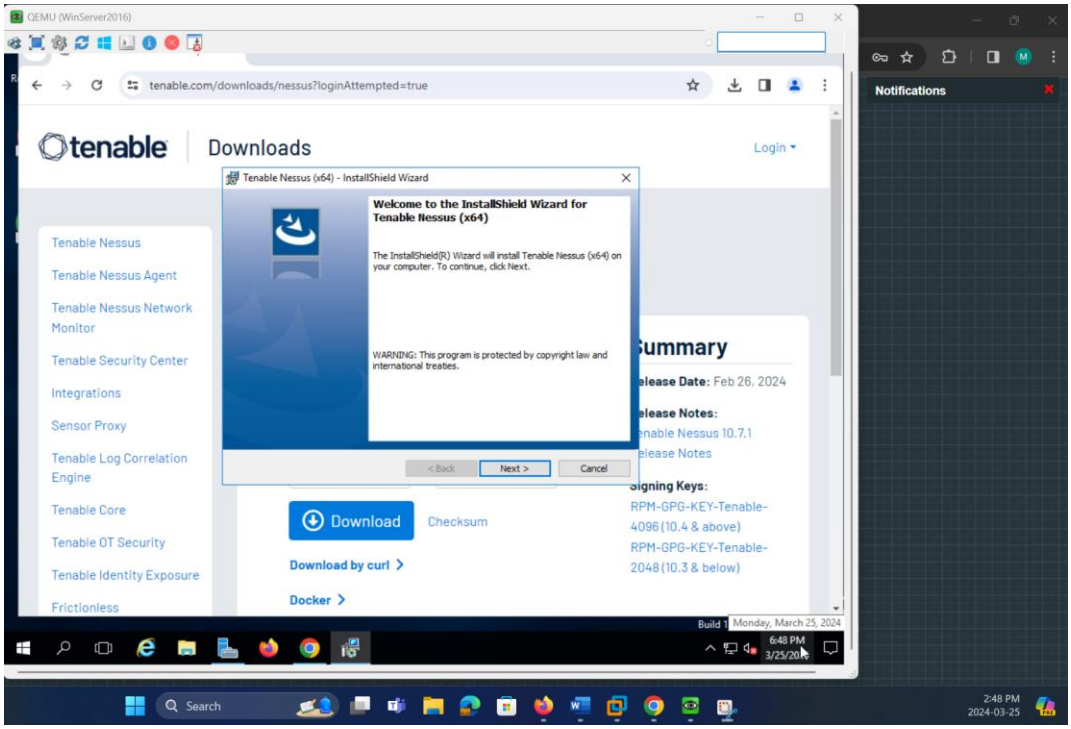
Lab Requirements:

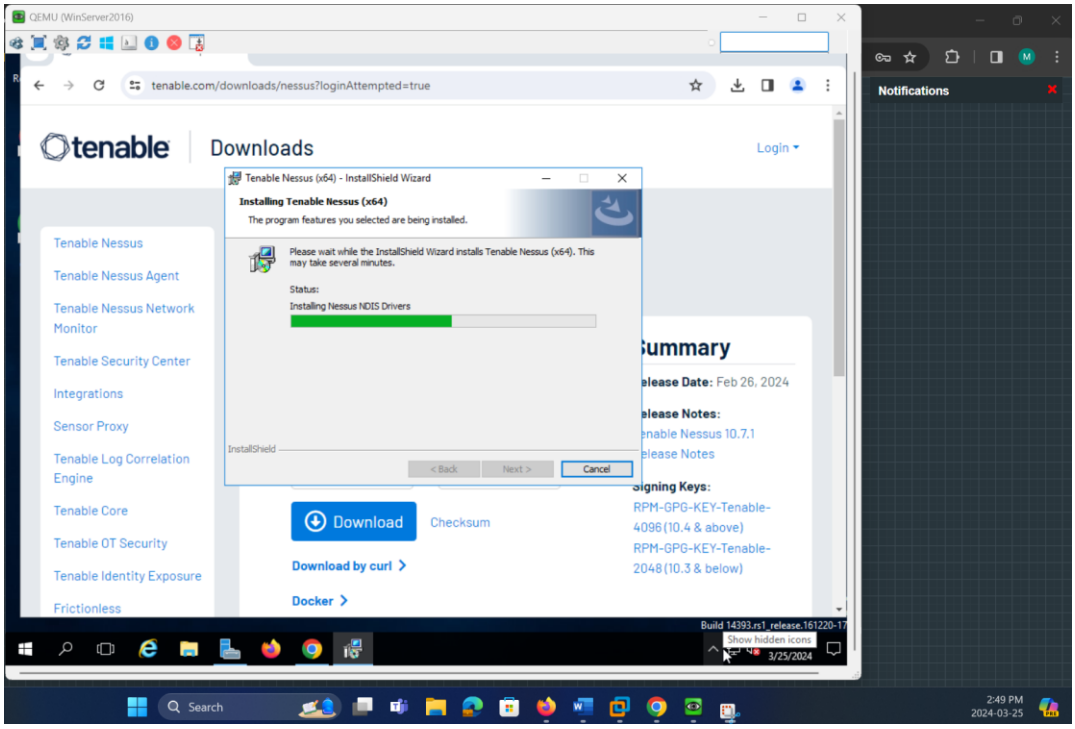
1. Downloading Nessus inside Windows 2016 Server VM

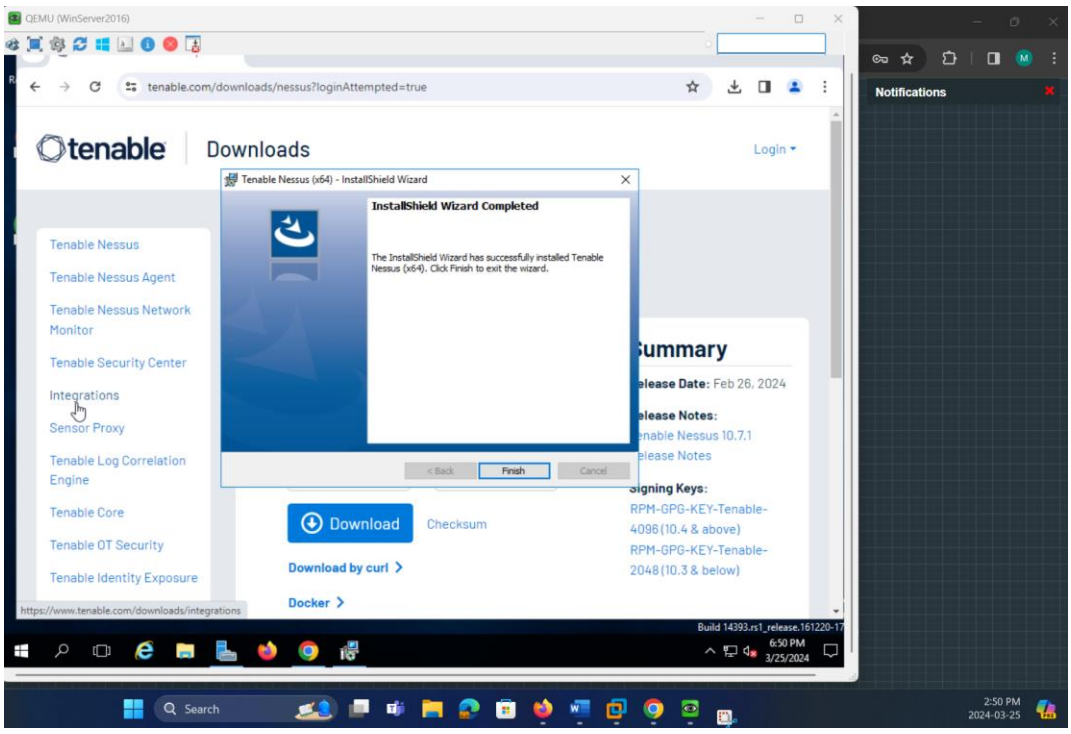


2. Installing Nessus inside Windows 2016 Server VM

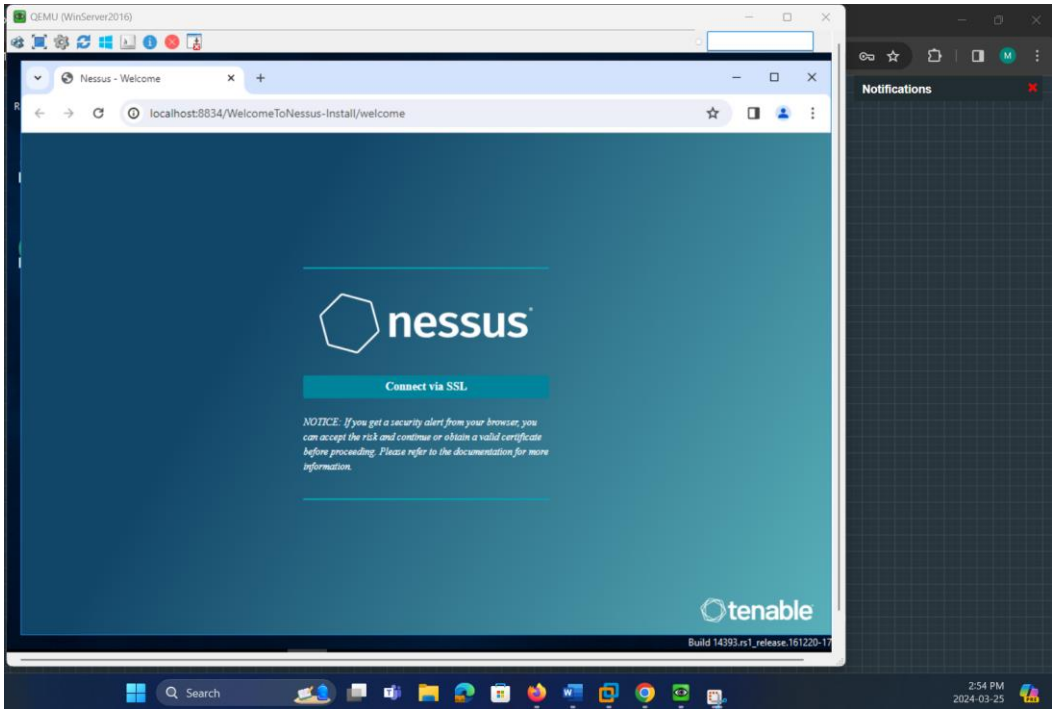


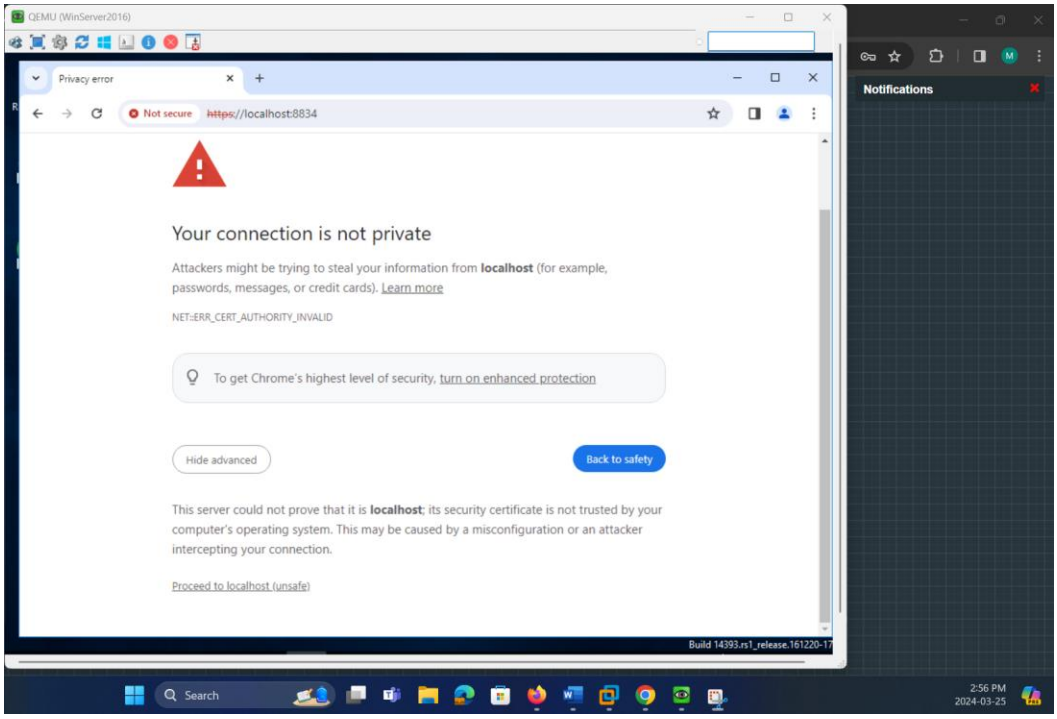

QEMU (WinServer2016)
tenable.com/downloads/nessus?loginAttempted=true
Notifications
tenable
Downloads
Login
Tenable Nessus (x64) - InstallShield Wizard
Welcome to the InstallShield Wizard for Tenable Nessus (x64)
The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel
Tenable Nessus
Tenable Nessus Agent
Tenable Nessus Network Monitor
Tenable Security Center
Integrations
Sensor Proxy
Tenable Log Correlation Engine
Tenable Core
Tenable OT Security
Tenable Identity Exposure
Frictionless
Summary
Release Date: Feb 26, 2024
Release Notes:
Tenable Nessus 10.7.1
Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)
Download
Checksum
Download by curl
Docker
Monday, March 25, 2024
6:48 PM
3/25/2024
Search
2:48 PM
2024-03-25

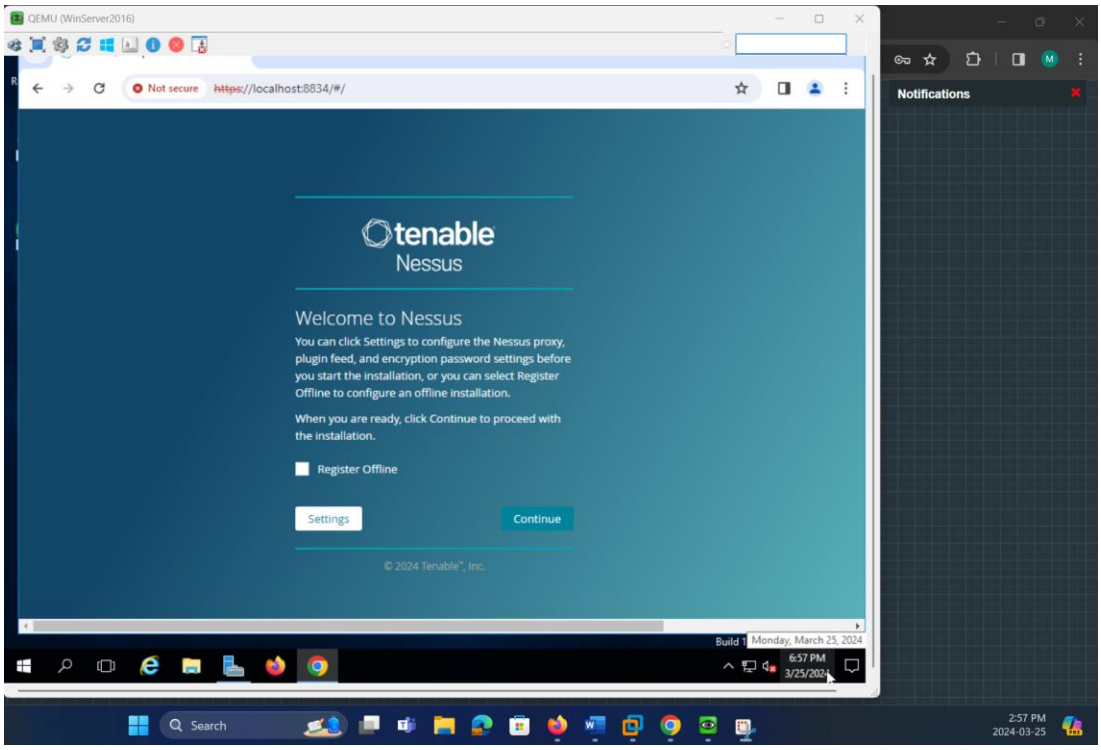

QEMU (WinServer2016)
tenable.com/downloads/nessus?loginAttempted=true
Notifications
tenable
Downloads
Login
Tenable Nessus (x64) - InstallShield Wizard
Installing Tenable Nessus (x64)
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.
Status:
Installing Nessus NDIS Drivers
InstallShield
< Back
Next >
Cancel
Tenable Nessus
Tenable Nessus Agent
Tenable Nessus Network Monitor
Tenable Security Center
Integrations
Sensor Proxy
Tenable Log Correlation Engine
Tenable Core
Tenable OT Security
Tenable Identity Exposure
Frictionless
Summary
Release Date: Feb 26, 2024
Release Notes:
Tenable Nessus 10.7.1
Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)
Download
Checksum
Download by curl
Docker
Build 14393.rs1_release.161220-17
Show hidden icons
3/25/2024
Search
2:49 PM
2024-03-25

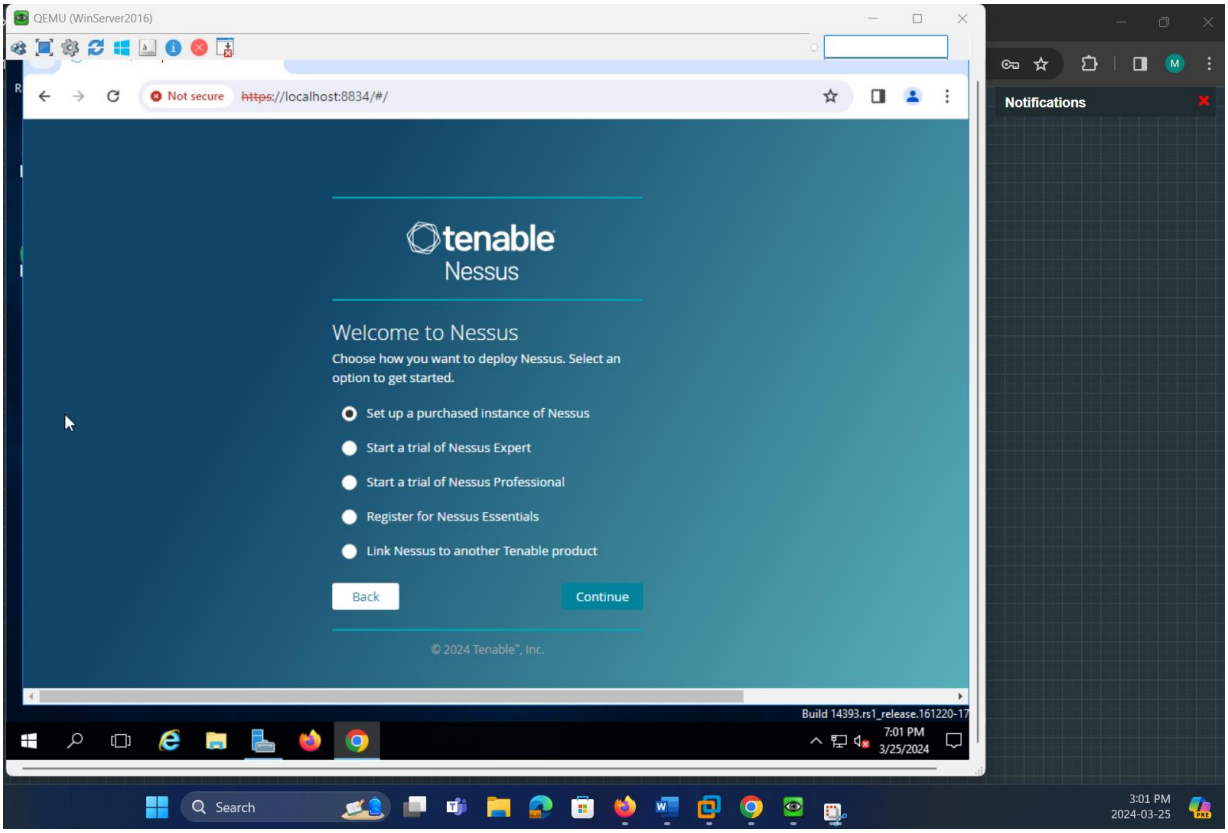


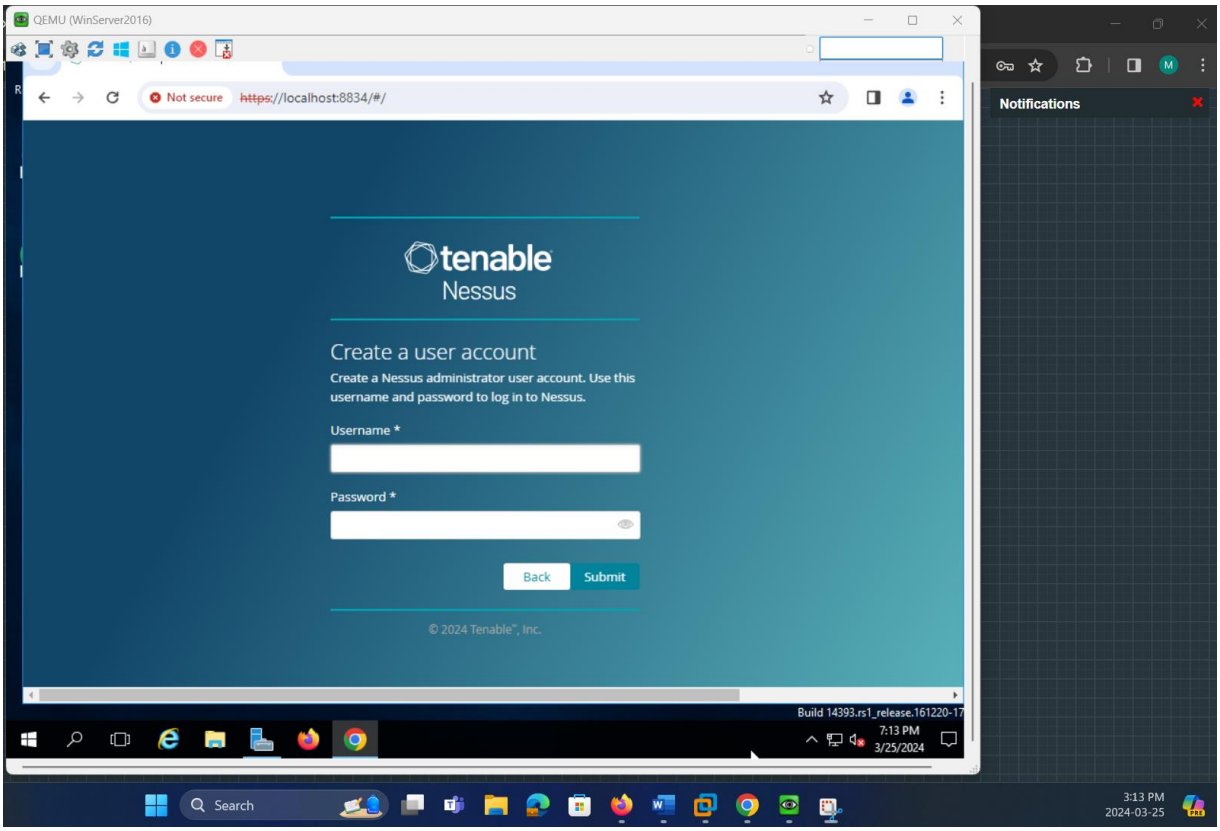
3. Registering and Configuring Nessus Account inside Windows 2016 Server VM

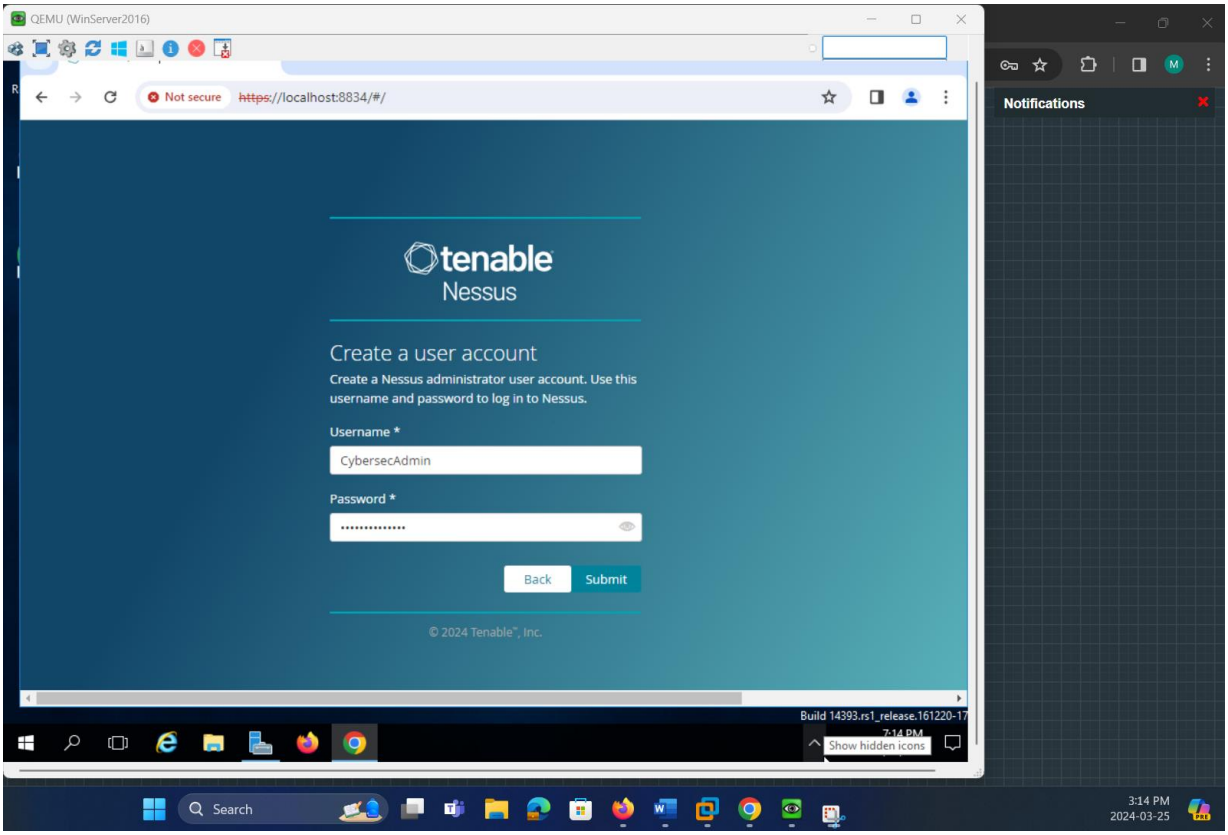


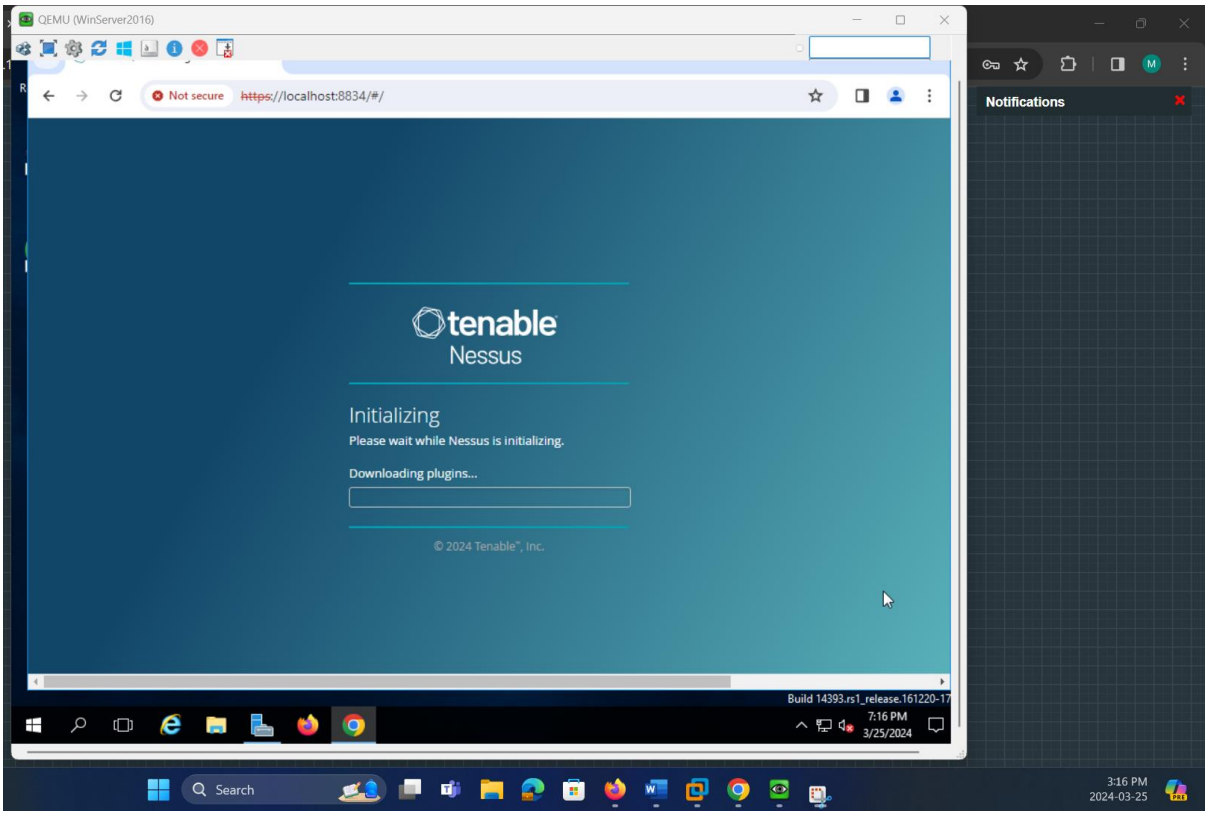

QEMU (WinServer2016)
Privacy error
Not secure
https://localhost:8834
Your connection is not private
Attackers might be trying to steal your information from localhost (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
To get Chrome's highest level of security, turn on enhanced protection
Hide advanced
Back to safety
This server could not prove that it is localhost; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to localhost (unsafe)
Notifications
Search
2:56 PM
2024-03-25

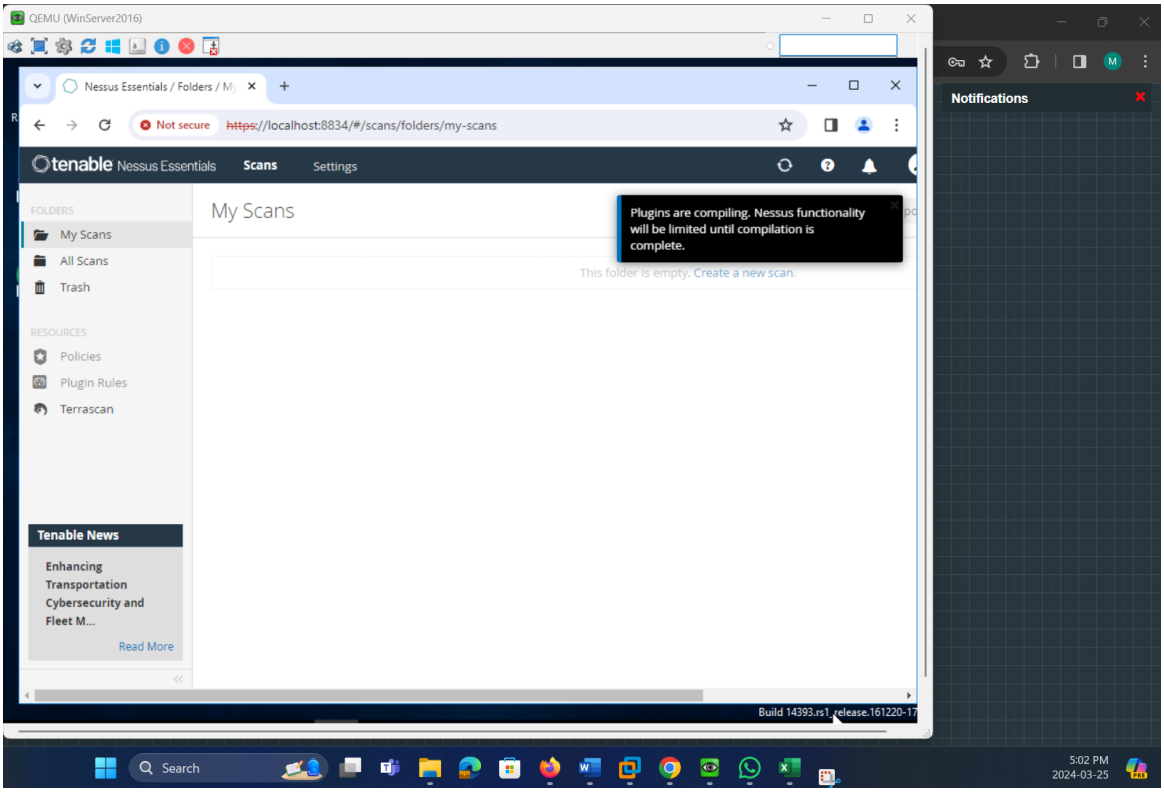

QEMU (WinServer2016)
Not secure
https://localhost:8834/#/
tenable
Nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue
© 2024 Tenable™, Inc.
Notifications
Monday, March 25, 2024
6:57 PM
3/25/2024
Search
2:57 PM
2024-03-25

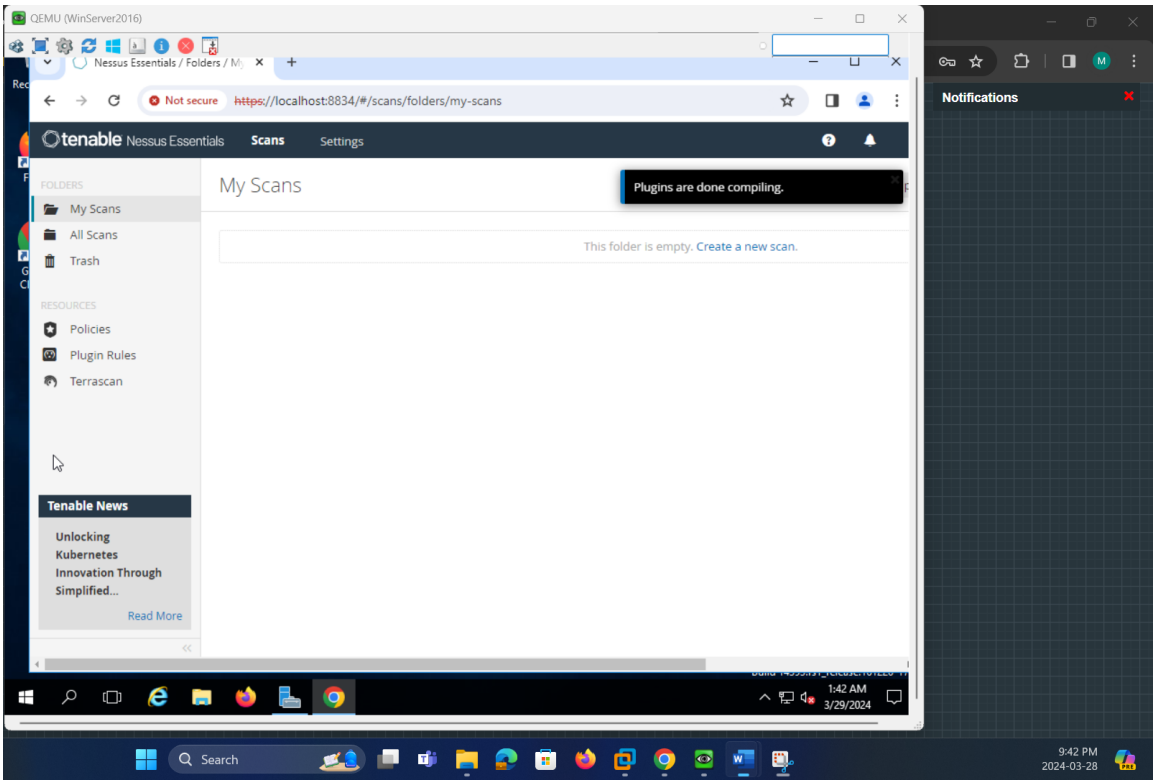

QEMU (WinServer2016)
Not secure
https://localhost:8834/#/
tenable
Nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
Link Nessus to another Tenable product
Back
Continue
© 2024 Tenable™, Inc.
Build 14393.rs1_release.161220-17
7:01 PM
3/25/2024
Notifications
Search
3:01 PM
2024-03-25


QEMU (WinServer2016)
Not secure
https://localhost:8834/#/
tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
Password *
Back
Submit
© 2024 Tenable™, Inc.
Build 14393.rs1_release.161220-17
7:13 PM
3/25/2024
Notifications
Search
3:13 PM
2024-03-25

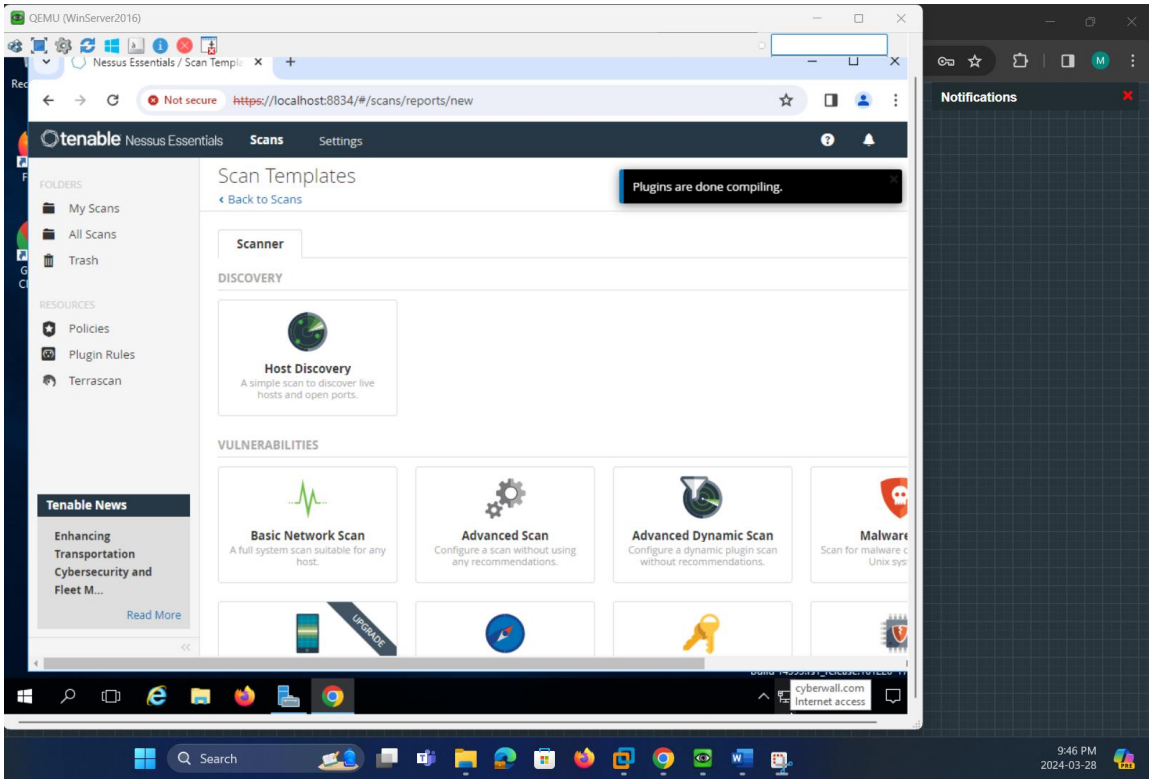

QEMU (WinServer2016)
Not secure https://localhost:8834/#/
Notifications
tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
CybersecAdmin
Password *
Back
Submit
© 2024 Tenable™, Inc.
Build 14393.rs1_release.161220-17
Show hidden icons
Search
3:14 PM
2024-03-25

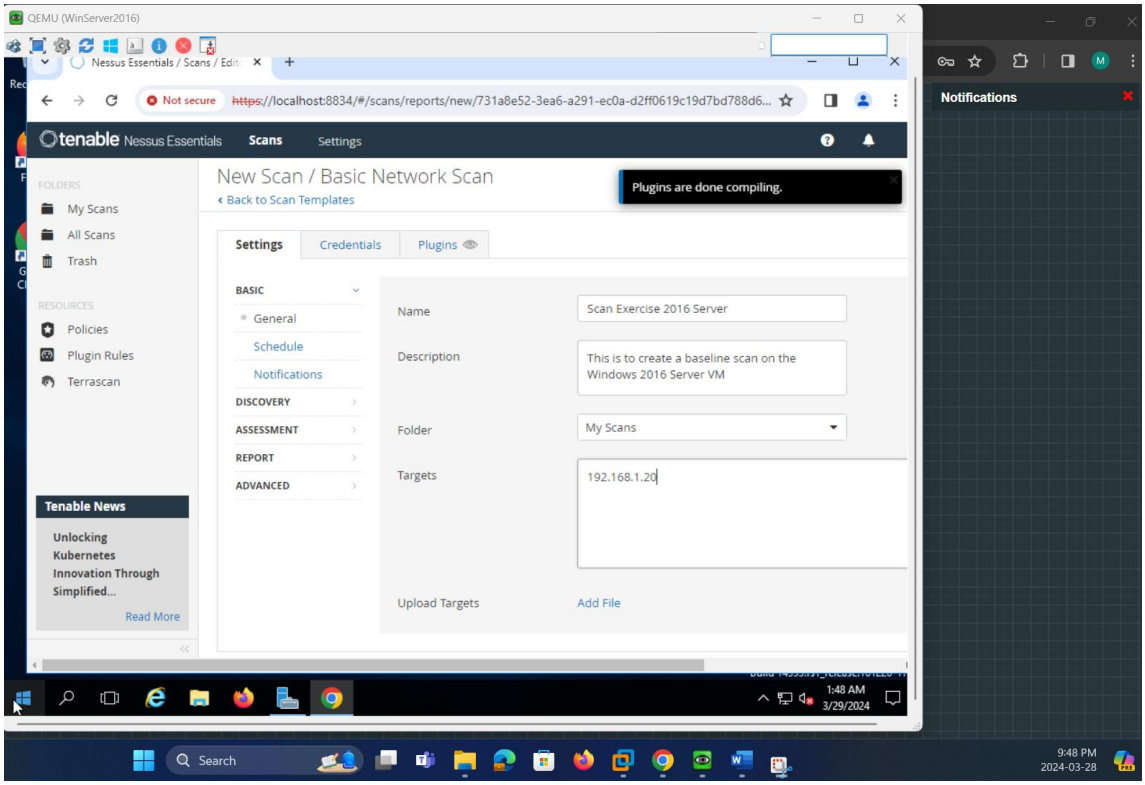

QEMU (WinServer2016)
Not secure https://localhost:8834/#/
Notifications
tenable
Nessus
Initializing
Please wait while Nessus is initializing.
Downloading plugins...
© 2024 Tenable™, Inc.
Build 14393.rs1_release.161220-17
7:16 PM
3/25/2024
Search
3:16 PM
2024-03-25



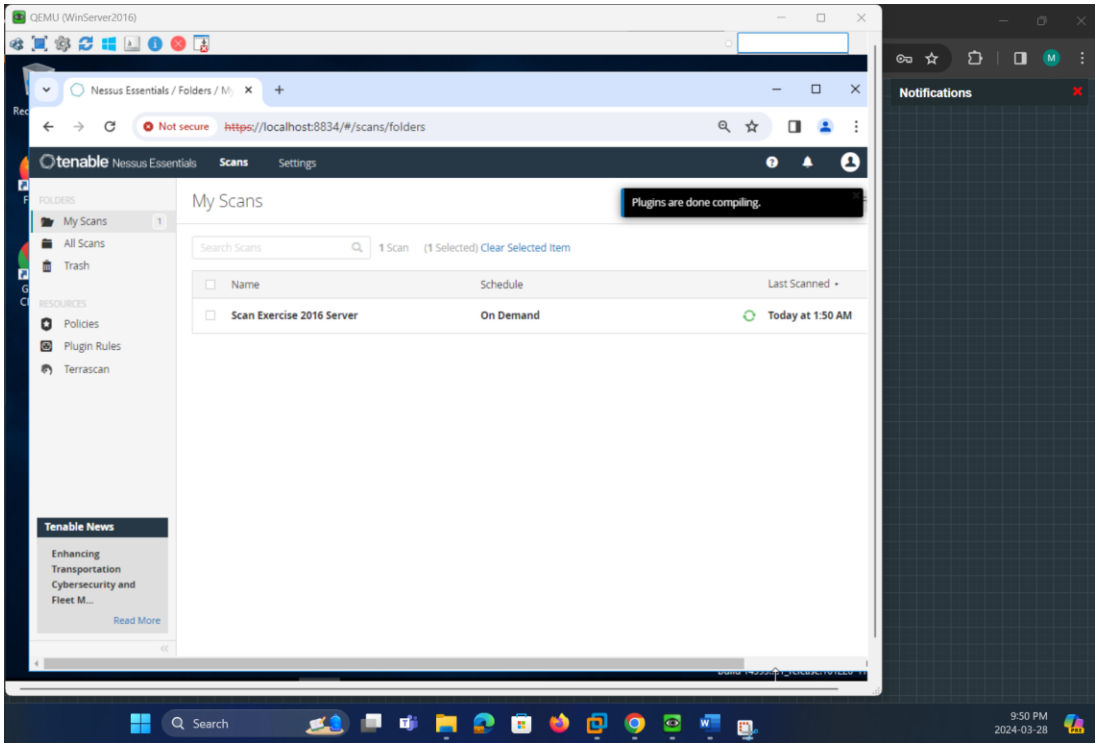


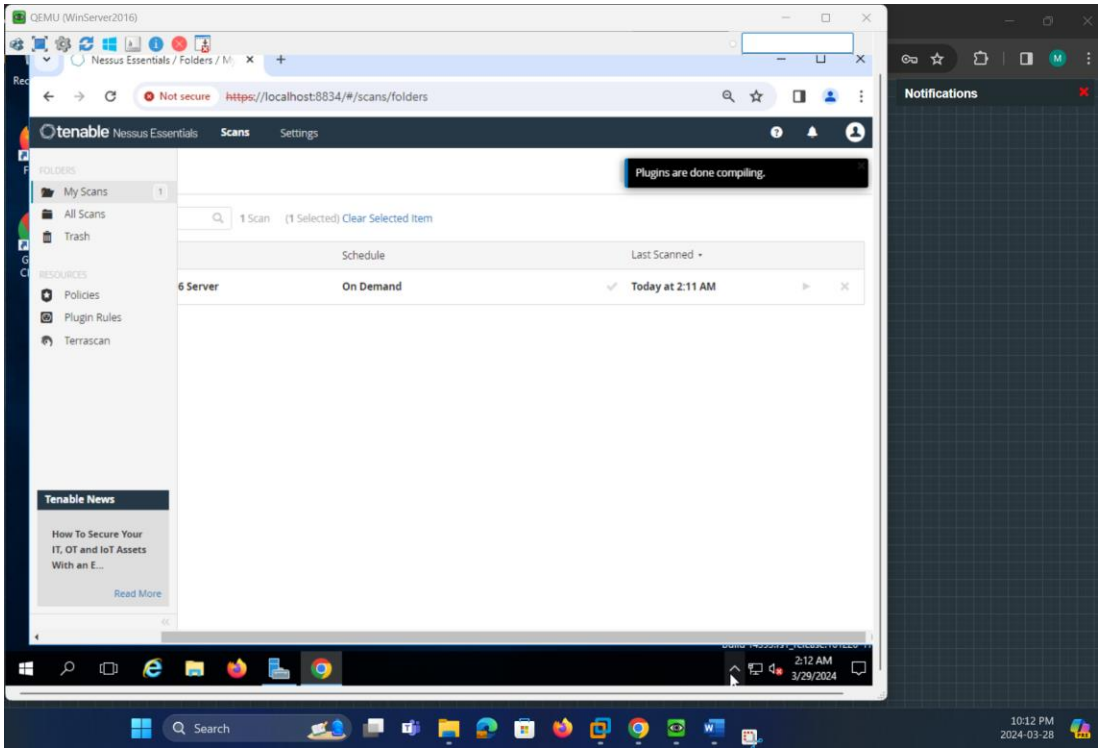
4. Creating a New Scan for the Windows 2016 Server VM



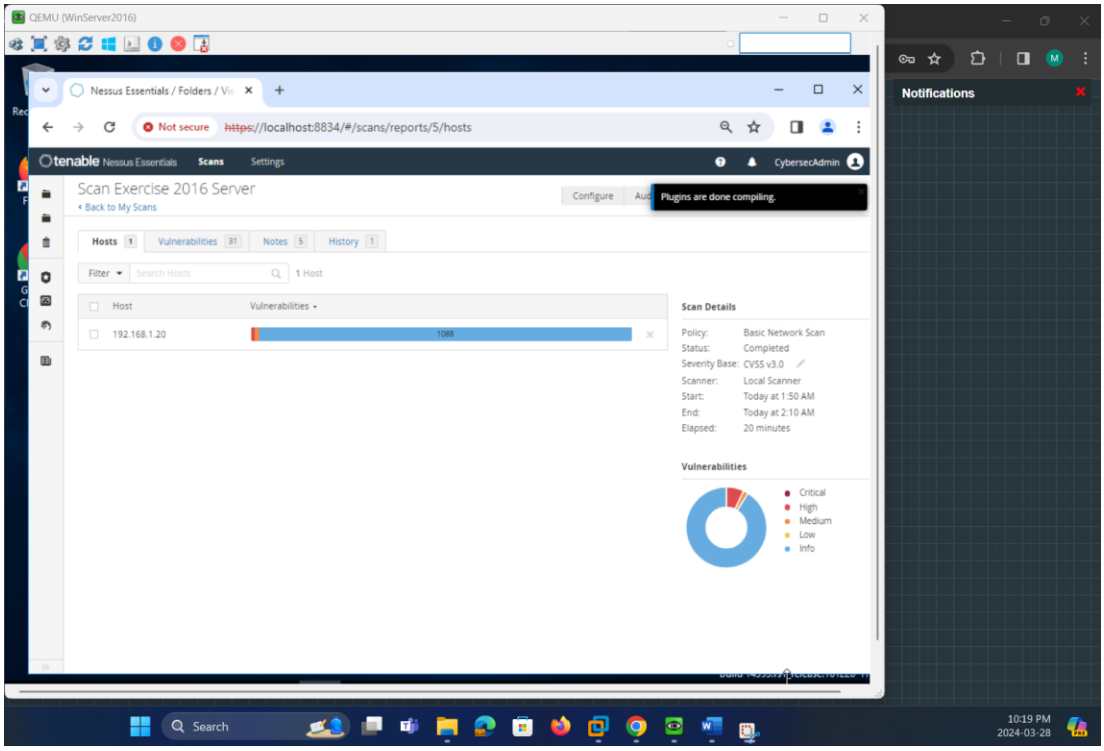


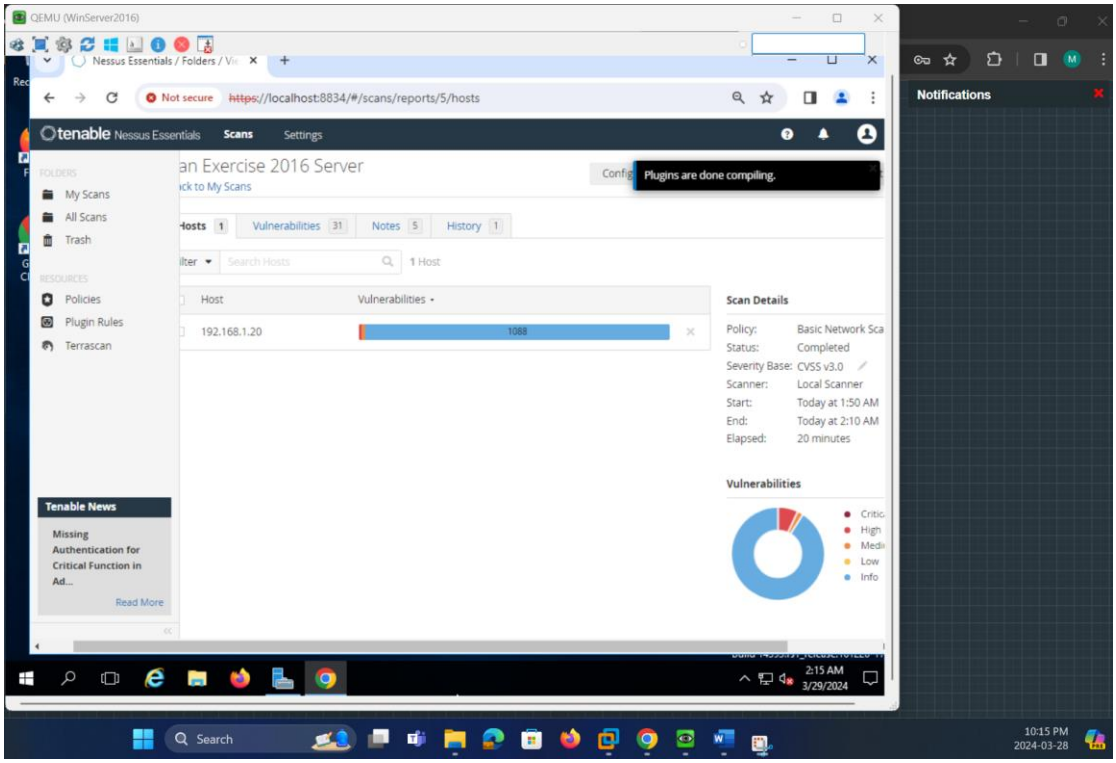
5. Conducting Scan of Windows 2016 Server VM

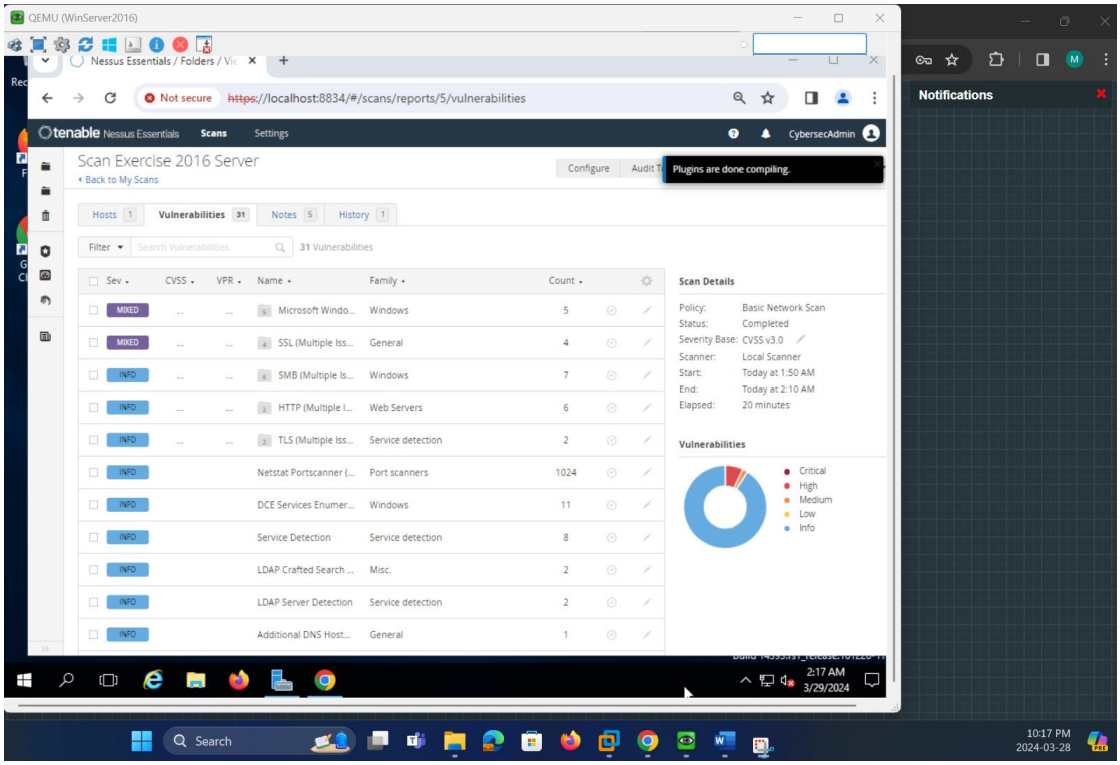


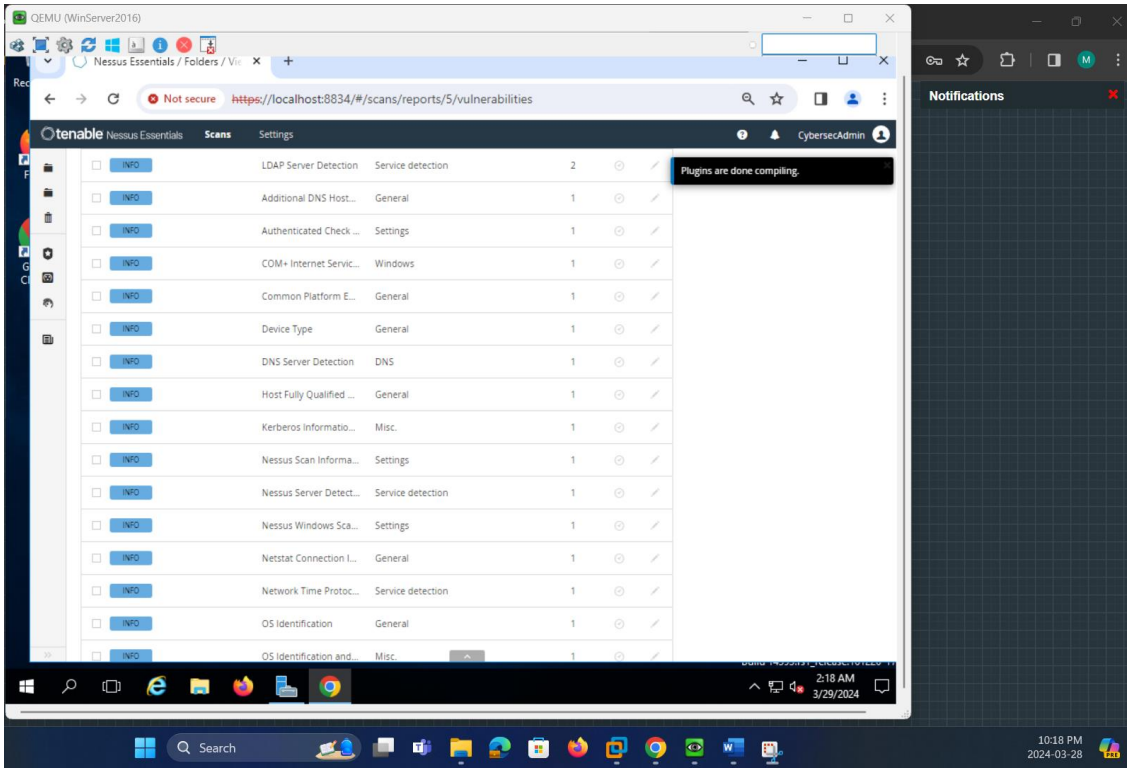


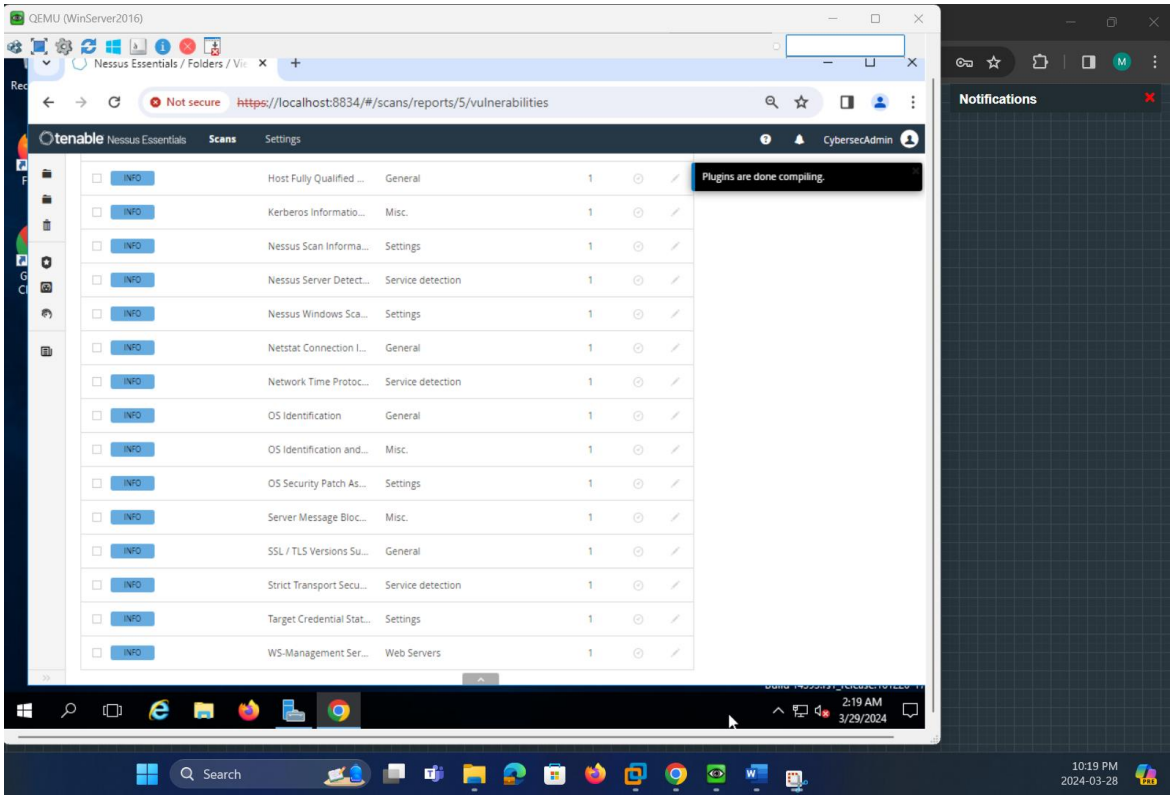
6. Scan Results of Windows 2016 Server

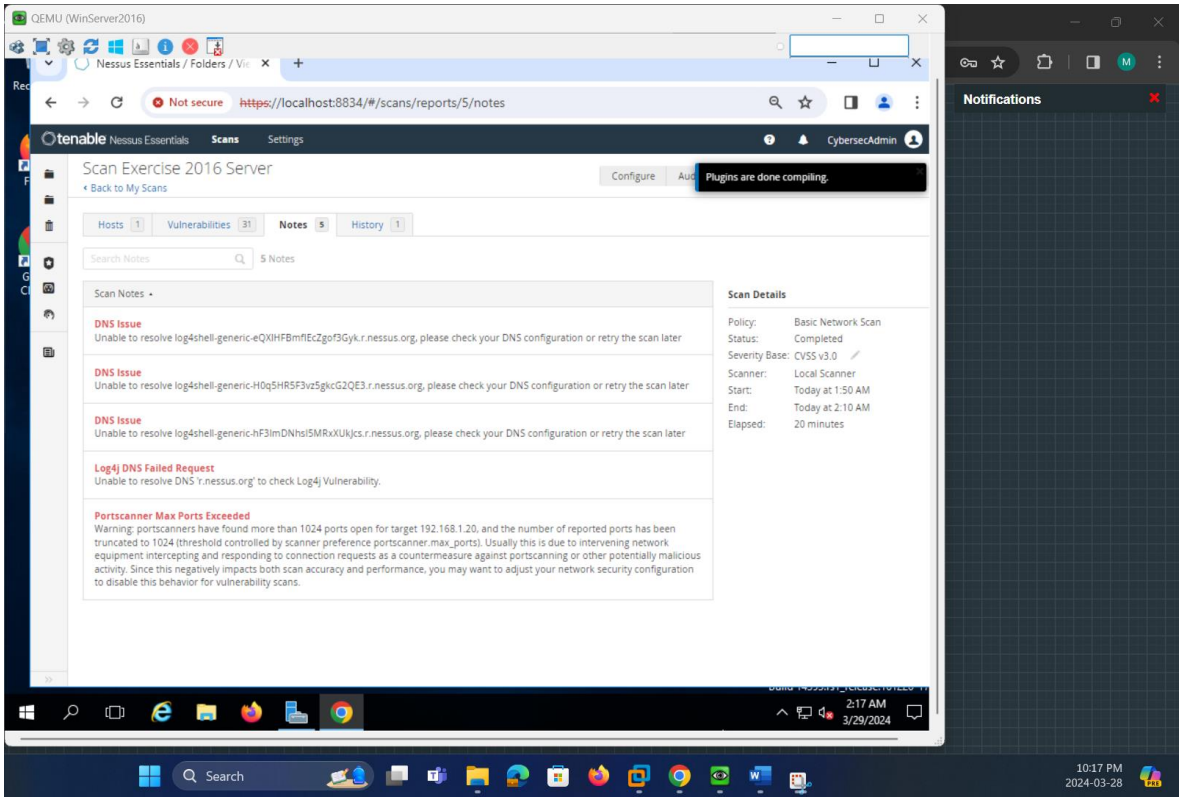

QEMU (WinServer2016)
Nessus Essentials / Folders / Vi
Not secure https://localhost:8834/#/scans/reports/5/hosts
tenable Nessus Essentials
Scans
Settings
CybersecAdmin
Scan Exercise 2016 Server
Back to My Scans
Configure
Plugins are done compiling.
Hosts 1
Vulnerabilities 31
Notes 5
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.1.20
1088
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:50 AM
End: Today at 2:10 AM
Elapsed: 20 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Notifications
Search
10:19 PM
2024-03-28

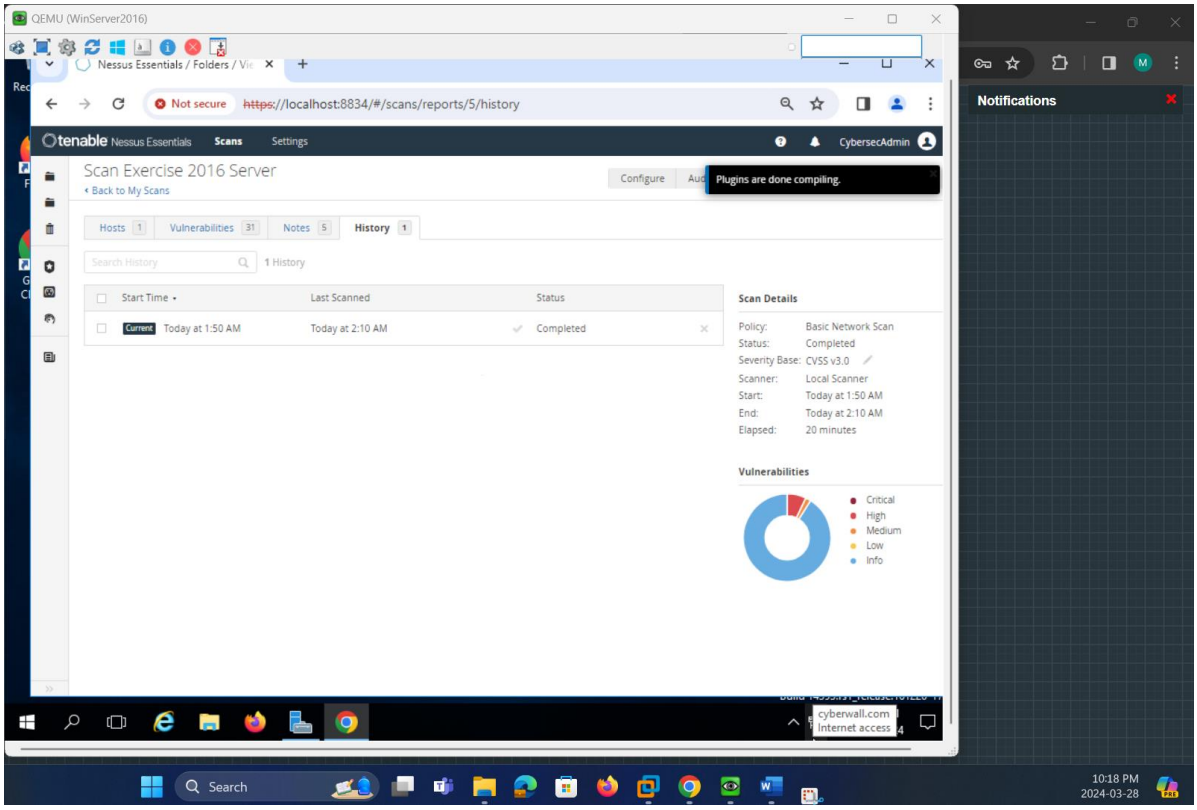

QEMU (WinServer2016)
Nessus Essentials / Folders / Vi
Not secure https://localhost:8834/#/scans/reports/5/hosts
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Missing Authentication for Critical Function in Ad...
Read More
an Exercise 2016 Server
ck to My Scans
Plugins are done compiling.
Hosts 1
Vulnerabilities 31
Notes 5
History 1
1 Host
Host
Vulnerabilities
192.168.1.20
1088
Scan Details
Policy: Basic Network Sca
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:50 AM
End: Today at 2:10 AM
Elapsed: 20 minutes
Vulnerabilities
Critic
High
Medi
Low
Info
2:15 AM
3/29/2024
Notifications
Search
10:15 PM
2024-03-28


QEMU (WinServer2016)
Nessus Essentials / Folders / Vie
Not secure
https://localhost:8834/#/scans/reports/5/vulnerabilities
tenable Nessus Essentials
Scans
Settings
CybersecAdmin
Scan Exercise 2016 Server
Back to My Scans
Configure
Audit T
Plugins are done compiling.
Hosts 1
Vulnerabilities 31
Notes 5
History 1
Filter
Search Vulnerabilities
31 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED
Microsoft Windo...
Windows
5
MIXED
SSL (Multiple Iss...
General
4
INFO
SMB (Multiple Is...
Windows
7
INFO
HTTP (Multiple I...
Web Servers
6
INFO
TLS (Multiple Iss...
Service detection
2
INFO
Netstat Portscanner (...
Port scanners
1024
INFO
DCE Services Enumer...
Windows
11
INFO
Service Detection
Service detection
8
INFO
LDAP Crafted Search ...
Misc.
2
INFO
LDAP Server Detection
Service detection
2
INFO
Additional DNS Host...
General
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:50 AM
End: Today at 2:10 AM
Elapsed: 20 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
2:17 AM
3/29/2024
Notifications
Search
10:17 PM
2024-03-28


QEMU (WinServer2016)
Nessus Essentials / Folders / Vie
Not secure
https://localhost:8834/#/scans/reports/5/vulnerabilities
tenable Nessus Essentials
Scans
Settings
CybersecAdmin
Plugins are done compiling.
INFO
LDAP Server Detection
Service detection
2
INFO
Additional DNS Host...
General
1
INFO
Authenticated Check ...
Settings
1
INFO
COM+ Internet Servic...
Windows
1
INFO
Common Platform E...
General
1
INFO
Device Type
General
1
INFO
DNS Server Detection
DNS
1
INFO
Host Fully Qualified ...
General
1
INFO
Kerberos Informatio...
Misc.
1
INFO
Nessus Scan Informa...
Settings
1
INFO
Nessus Server Detect...
Service detection
1
INFO
Nessus Windows Sca...
Settings
1
INFO
Netstat Connection I...
General
1
INFO
Network Time Protoc...
Service detection
1
INFO
OS Identification
General
1
INFO
OS Identification and...
Misc.
1
2:18 AM
3/29/2024
Notifications
Search
10:18 PM
2024-03-28


QEMU (WinServer2016)
Nessus Essentials / Folders / Vie
Not secure https://localhost:8834/#/scans/reports/5/vulnerabilities
tenable Nessus Essentials Scans Settings CybersecAdmin
Plugins are done compiling.
Notifications
INFO Host Fully Qualified ... General 1
INFO Kerberos Informatio... Misc. 1
INFO Nessus Scan Informa... Settings 1
INFO Nessus Server Detect... Service detection 1
INFO Nessus Windows Sca... Settings 1
INFO Netstat Connection I... General 1
INFO Network Time Protoc... Service detection 1
INFO OS Identification General 1
INFO OS Identification and... Misc. 1
INFO OS Security Patch As... Settings 1
INFO Server Message Bloc... Misc. 1
INFO SSL / TLS Versions Su... General 1
INFO Strict Transport Secu... Service detection 1
INFO Target Credential Stat... Settings 1
INFO WS-Management Ser... Web Servers 1
2:19 AM
3/29/2024
Search
10:19 PM
2024-03-28


QEMU (WinServer2016)
Nessus Essentials / Folders / Vie
Not secure https://localhost:8834/#/scans/reports/5/notes
tenable Nessus Essentials Scans Settings CybersecAdmin
Plugins are done compiling.
Notifications
Scan Exercise 2016 Server
Back to My Scans
Configure
Hosts 1 Vulnerabilities 31 Notes 5 History 1
Search Notes
5 Notes
Scan Notes
DNS Issue
Unable to resolve log4shell-generic-eQXIHFBmfIEcZgof3Gyk.r.nessus.org, please check your DNS configuration or retry the scan later
DNS Issue
Unable to resolve log4shell-generic-H0q5HR5F3vz5gkcG2QE3.r.nessus.org, please check your DNS configuration or retry the scan later
DNS Issue
Unable to resolve log4shell-generic-hF3ImDNhsI5MRxXUkJcs.r.nessus.org, please check your DNS configuration or retry the scan later
Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.
Portscanner Max Ports Exceeded
Warning: portscanners have found more than 1024 ports open for target 192.168.1.20, and the number of reported ports has been truncated to 1024 (threshold controlled by scanner preference portscanner.max_ports). Usually this is due to intervening network equipment intercepting and responding to connection requests as a countermeasure against portscanning or other potentially malicious activity. Since this negatively impacts both scan accuracy and performance, you may want to adjust your network security configuration to disable this behavior for vulnerability scans.
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:50 AM
End: Today at 2:10 AM
Elapsed: 20 minutes
2:17 AM
3/29/2024
Search
10:17 PM
2024-03-28



7. Interpretation of Nessus Basic Scan on Windows 2016 Server VM

The screenshots uploaded are from a Nessus vulnerability scan report for a Windows Server 2016 virtual machine (VM). Nessus is a widely used cybersecurity tool that helps in identifying vulnerabilities, misconfigurations, and potential risks within network environments. An overview of the information typically contained the report are the following:

1. **Hosts Tab:** Shows the IP address of the scanned host(s) and a summary of vulnerabilities categorized by their risk levels.
2. **Vulnerabilities Tab:** Details the specific vulnerabilities found. They are categorized by severity levels, indicated by color codes (red for critical, orange for high, etc.), and are usually assigned a Common Vulnerabilities and Exposures (CVE) number along with a Common Vulnerability Scoring System (CVSS) score. It often includes details like the vulnerability name, the family it belongs to, and the number of times it was found (count).
3. **Notes Tab:** Contains additional information or warnings about the scan. For example, it might indicate DNS resolution issues or problems with the scan itself, like if it was unable to complete certain checks or if performance issues were detected.
4. **History Tab:** Offers information about the scan sessions, including start and end times, as well as the status (completed, aborted, etc.) of each scan.

Specifically, for the Windows Server 2016 VM, the report included:

- Vulnerabilities related to the Windows OS, services running on the server, and applications installed.
- Information on any misconfigurations or default configurations that may be insecure.
- Recommendations for patches or updates that should be applied to secure the system.
- Findings on any default credentials or weak passwords that may be in use.

The information provided in these reports is critical for maintaining the security posture of your systems, allowing you to address vulnerabilities before they can be exploited by malicious actors. It's crucial to review the details of each identified vulnerability and follow up with the necessary remediation steps, such as applying patches, updating configurations, or removing unnecessary services.

Findings:

- The Nessus scan has been completed successfully, identifying various vulnerabilities, and providing detailed insight into the security posture of the Windows Server 2016 VM.
- The vulnerabilities are organized by severity, indicating that there is a mixture of low, medium, and high-severity vulnerabilities, but it seems there are no critical issues based on the pie chart.
- The scan has detected issues such as SSL/TLS vulnerabilities, which may indicate outdated protocols or weak ciphers, and Windows-related vulnerabilities that may involve patch management or configuration settings.
- Some service-specific vulnerabilities and detections, such as those related to LDAP and DNS, suggest potential misconfigurations or outdated software versions that could be exploited.
- The notes and history indicate that the scan was completed without interruptions and provide traceability for the scan execution.

8. Conclusion

- Immediate attention is required to address the high and medium-severity vulnerabilities to reduce the risk of potential exploitation.
- It is recommended to investigate and remediate the vulnerabilities in accordance with the provided Nessus severity ratings and descriptions.
- Some issues may require patching software to the latest versions, modifying configurations for services like SSL/TLS, LDAP, and DNS, and reinforcing security settings where defaults may be insufficient.
- Regular follow-up scans after remediation efforts are essential to ensure all issues have been addressed and to maintain an ongoing awareness of the server's security posture.
- Documentation of actions taken and any deviations from recommended remediations should be recorded for compliance purposes and future reference.

Next Steps:

- Prioritize the vulnerabilities based on their severity, the value of the assets affected, and the potential impact on the business.
- Begin remediation with high-severity issues and follow best practices for patch management and system hardening.
- Retest the system after remediations to ensure that vulnerabilities have been resolved and no new issues have arisen.
- Consider a comprehensive review of security policies and practices to prevent similar vulnerabilities in the future.

The actual steps for remediation will depend on the specifics of each vulnerability and the operational context of the server in your environment. It’s important to balance the need for security with the potential impact on service availability and business operations.