Preparing Kali Linux VM for OpenVas Greenbone

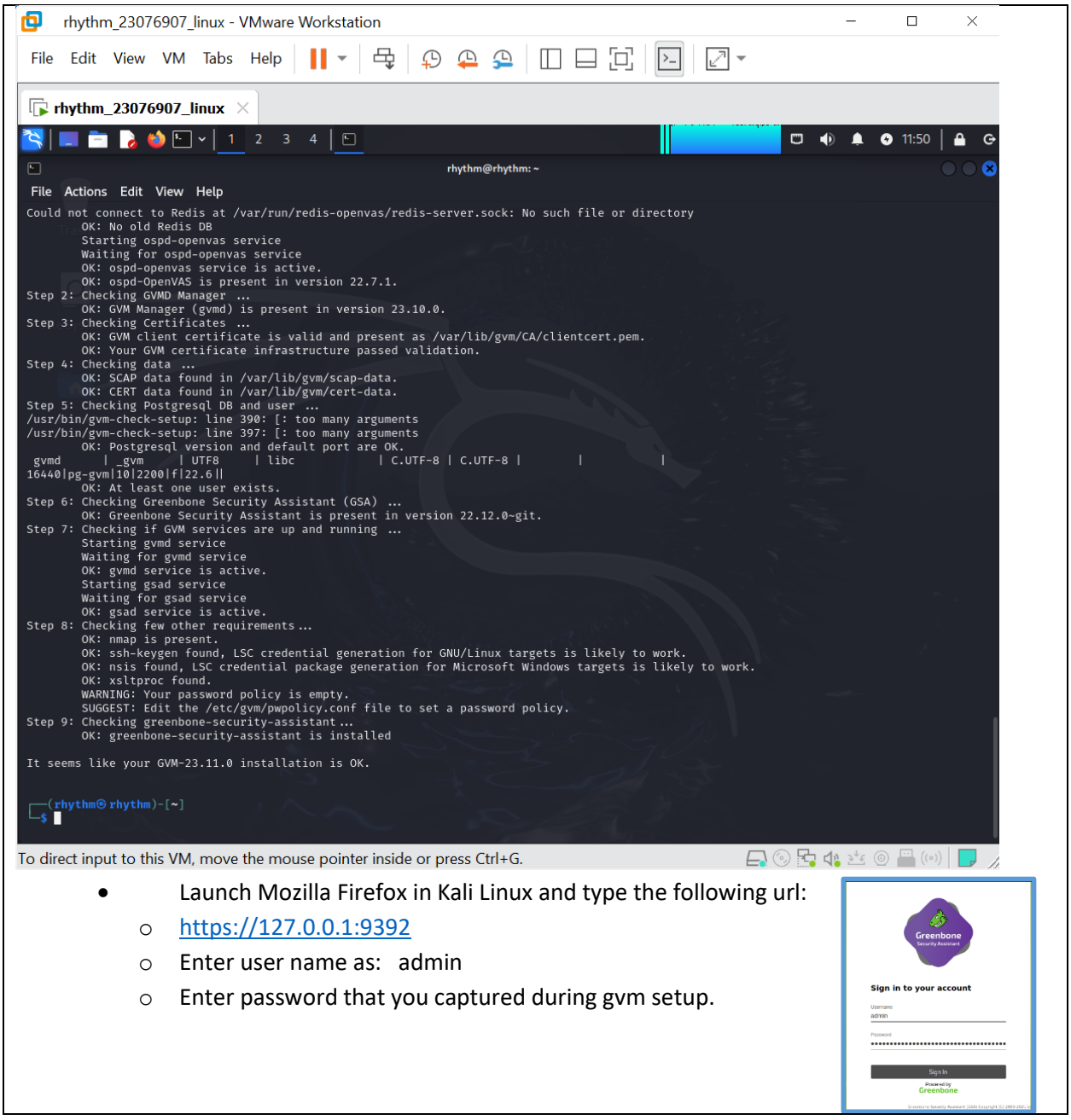
Upgrade Kali Linux 2021.3 to 2021.4 (Optional)

In this activity, you will use manual tools to gather OSINT. You may use Windows or Linux tools; however, we recommend using a Kali Linux virtual or physical machine for exercises like this to increase your familiarity with Linux and the Kali toolsets.

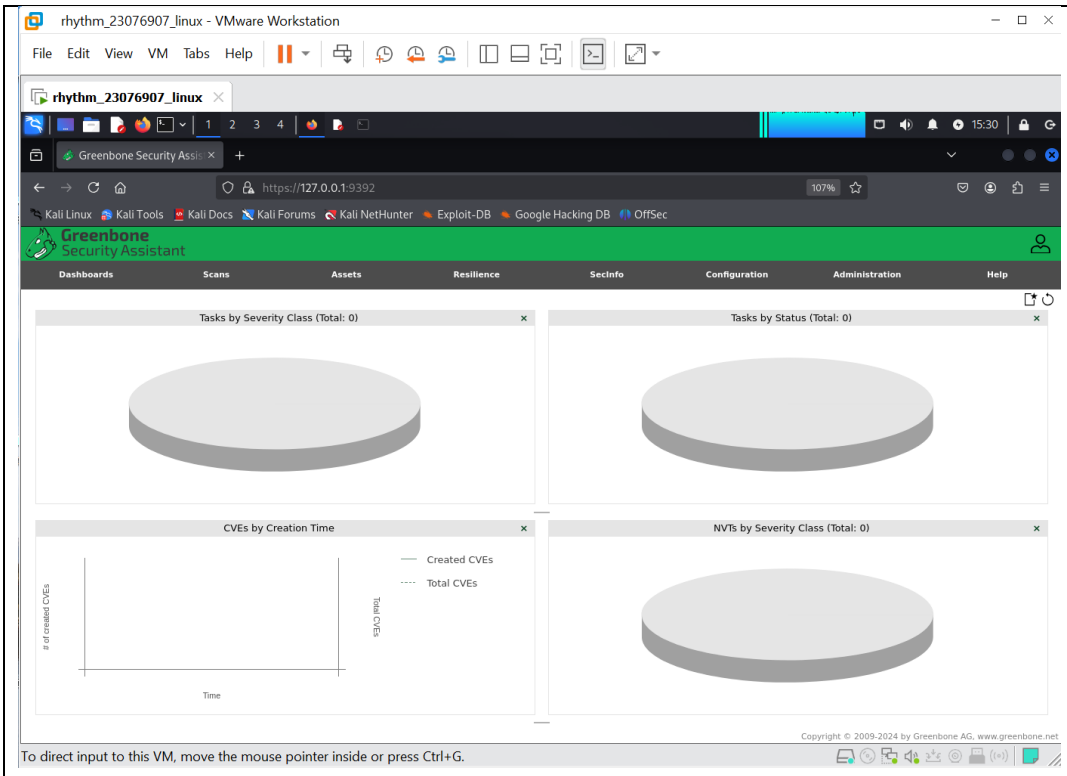
- if you are currently running Kali Linux 2021.3, you can easily upgrade it to Kali Linux 2021.4
- Getting the current version
  - lsb_release -a
- Ensure the Kali Linux Repositories are in Place
  - grep -vE "^#|^$" /etc/apt/sources.list
    Sample Output: deb http://http.kali.org/kali kali-rolling main contrib non-free
- If the repos are not set, then run the command below to update
  - echo 'deb http://http.kali.org/kali kali-rolling main contrib non-free' > /etc/apt/sources.list
- Run system Update
  - sudo apt update
- Upgrade Kali Linux 2021.3 to 2021.4
  - sudo apt full-upgrade --auto-remove
    The apt full-upgrade command performs the function of upgrade but will remove currently installed packages if this is needed to upgrade the system as a whole.
- Reboot the System
  - sudo systemctl -i reboot
- Verify Kali Linux 2021.3 Upgrade to Kali Linux 2021.4
  - lsb_release -a

Activity 1: Installing GVM

- Type the following command in terminal at Kali Linux:
  - sudo apt isntall gvm
  - sudo gvm-setup (You must capture the password during this setup)
  - sudo gvm-check-setup **(Take the screen shot)**



- Launch Mozilla Firefox in Kali Linux and type the following url:
  - https://127.0.0.1:9392
  - Enter user name as: admin
  - Enter password that you captured during gvm setup.



Do not forget to save the password here for future use. Or alternatively you may create a gvm user with an easy password.

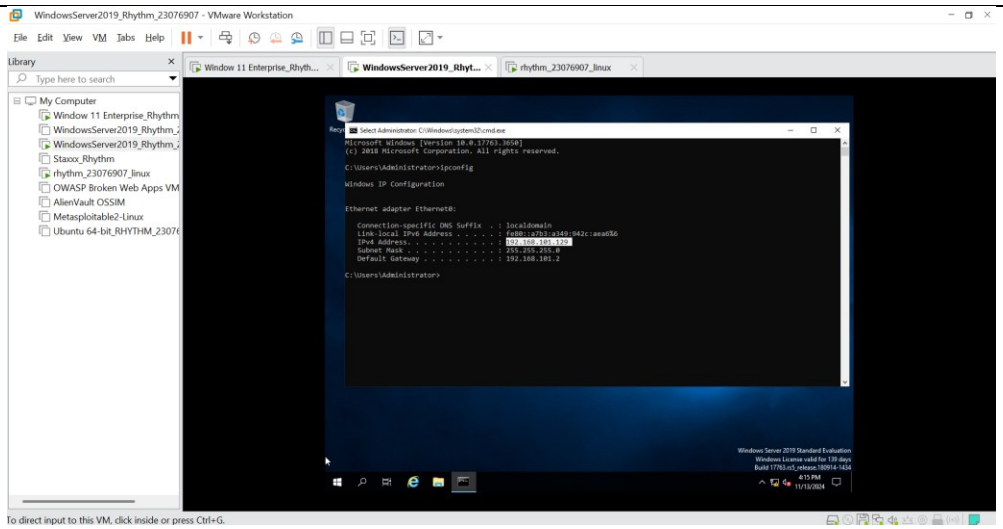
Activity 2: Vulnerability/Exposure Testing and Reporting (Linux)

- Launch the other two VMs installed in Lab.1 (Windows 10 Enterprise Evaluation and Windows Server 2019 Evaluation). Record the IP addresses that are assigned to both VMs. **Turn off the fire walls completely for both Windows based VMs.** Watch the following you tube vide:
  - OpenVas-Greenbone

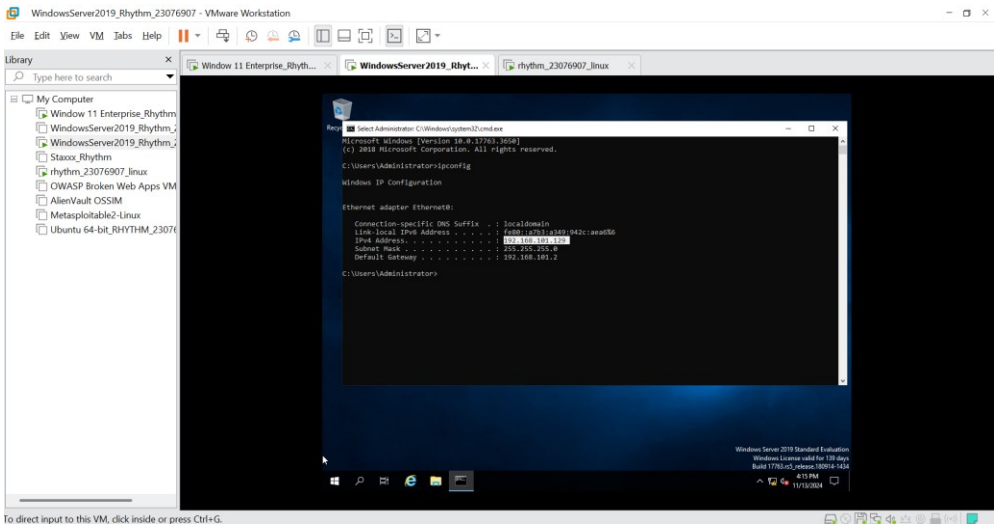
You may wish to create task(s) to use scanner to scan your local computer and/or targeted computers, use instant wizard for immediate scan.

- Get the ip address of any both VMs (Windows 10 Enterprise and Windows Server 2019 evaluation).

WINDOW 11 ENTERPRISE



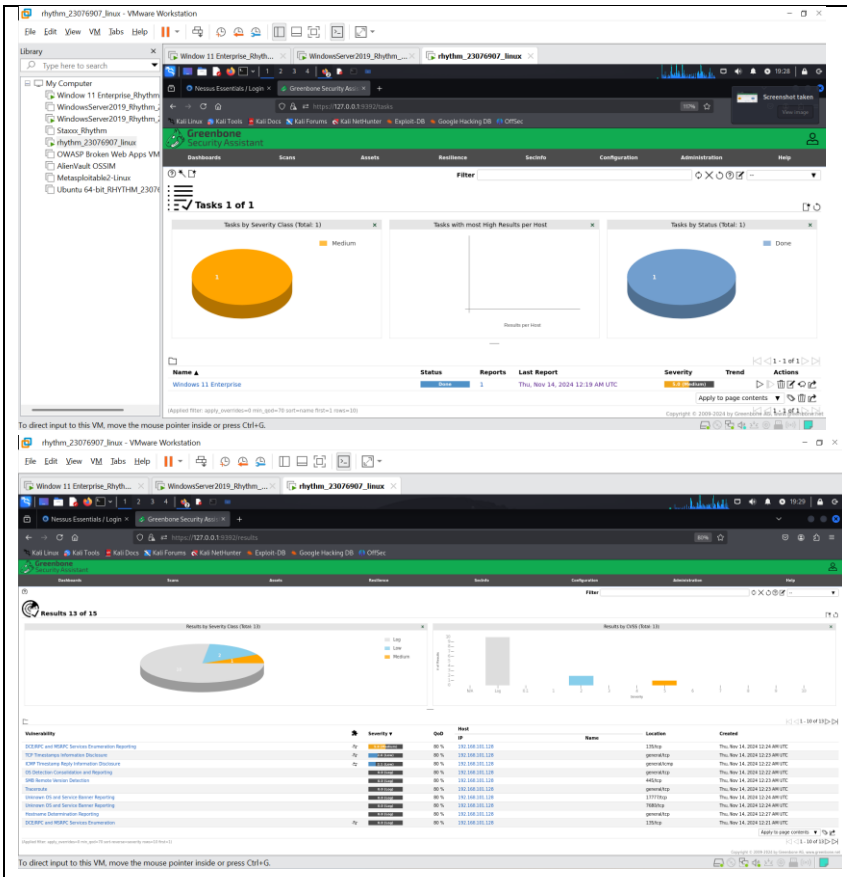
WINDOWS SERVER 2019



- Create new task for both VMs and scan the vulnerabilities.
- Creating New Target
- Review reports of each device based on the device's IP address
- Report how many vulnerabilities discovered, severity of each, QoD of each and what is the operating system (include version) of each IP address scanned in this lab?
- Summarize in report the top three vulnerabilities for each address

- Review your results under reports, results, vulnerabilities.

  In windows Case:



Windows 11 Enterprise Evaluation (IP: 192.168.101.128)

- **Operating System**: Windows 11 Enterprise
- **Total Vulnerabilities**: 15
- **Severity Breakdown**:
    - High: 0
    - Medium: 1
    - Low: 2
- **Quality of Detection (QoD)**: 80 %

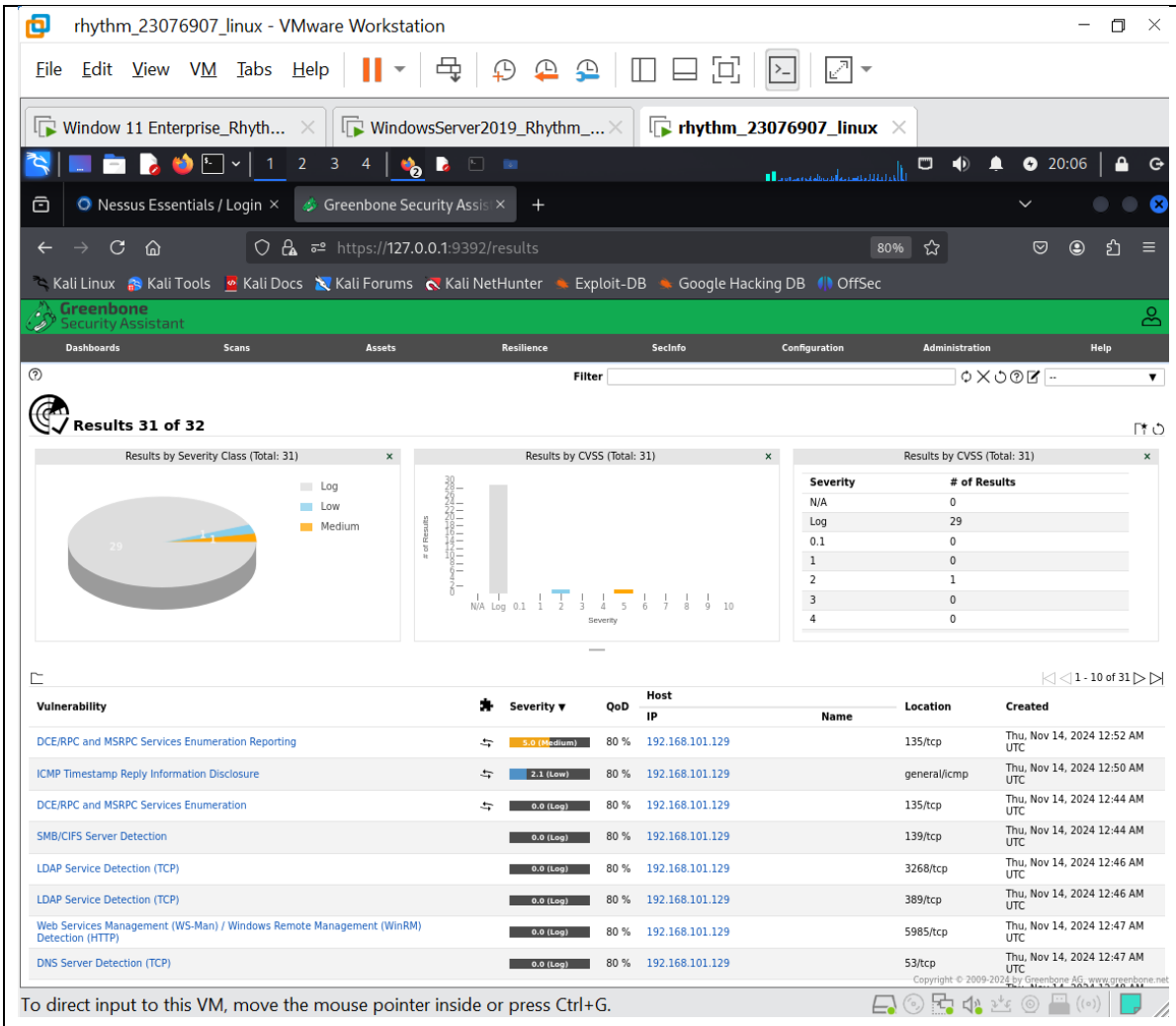
Top Three Vulnerabilities:

Vulnerability 1 – { Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.. CVSS Base 5.0, QoD 80 %}

Vulnerability 2 - [The remote host implements TCP timestamps and therefore allows to compute the uptime.CVSS Base 2.6, QoD 80%]

Vulnerability 3 - [The remote host responded to an ICMP timestamp request., CVSS Base 2.1 , QoD : 80 %]

In windows server 2019



Windows Server 2019 Evaluation (IP: 192.168.101.129)

- **Operating System**: Windows Server
- **Total Vulnerabilities**: 2
- **Severity Breakdown**:
    - High: 0
    - Medium: 1
    - Low: 1
- **Quality of Detection (QoD)**: 80 %

Top Three Vulnerabilities:

Vulnerability 1 - [Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries., CVSS Base 5.0,, QoD 80%]

Vulnerability 2 - [The remote host responded to an ICMP timestamp request., CVSS Base 2.1 QoD 80%]

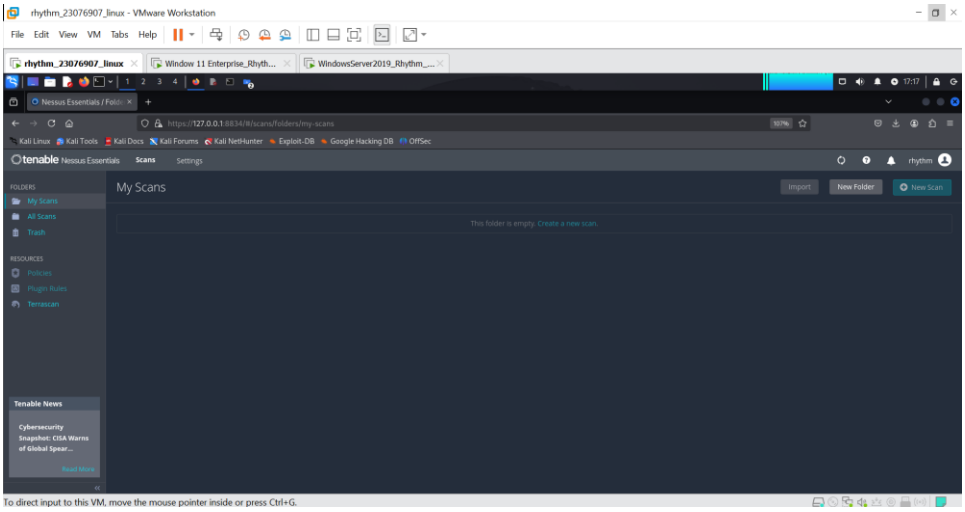
Activity 3: Installing another Vulnerability Scanner (Nessus)

In this lab, you will install the Nessus vulnerability management package on a system.
This lab requires access to a Linux system that you can use to install Nessus.

Step 1: Obtain a Nessus Home Activation Code
Visit the Nessus website (https://www.tenable.com/products/nessus-home) and fill out the form to obtain an activation code. Save the email containing the code for use during the installation and activation process.

Step 2: Download Nessus and Install It on Your System
Visit the Nessus download page (https://www.tenable.com/products/nessus/select-your-operating-system#download) and download the appropriate version of Nessus for your system.
Initializing Nessus

Install Nessus following the documentation available at:
https://docs.tenable.com/nessus/Content/InstallNessusLinux.htm
Verify that your installation was successful by logging into your Nessus server. **Take the screen shot.**



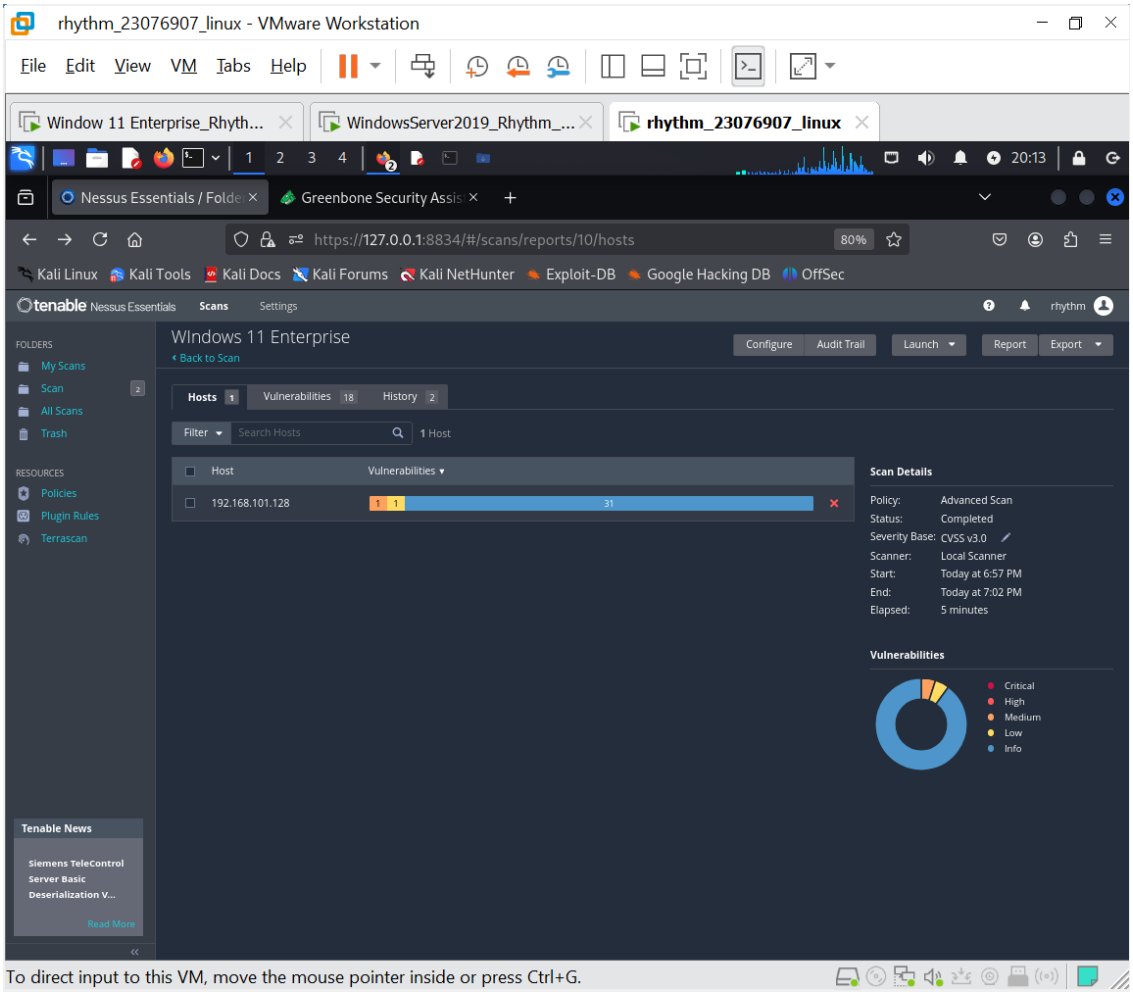
Activity 4: Nessus Vulnerability Scanning

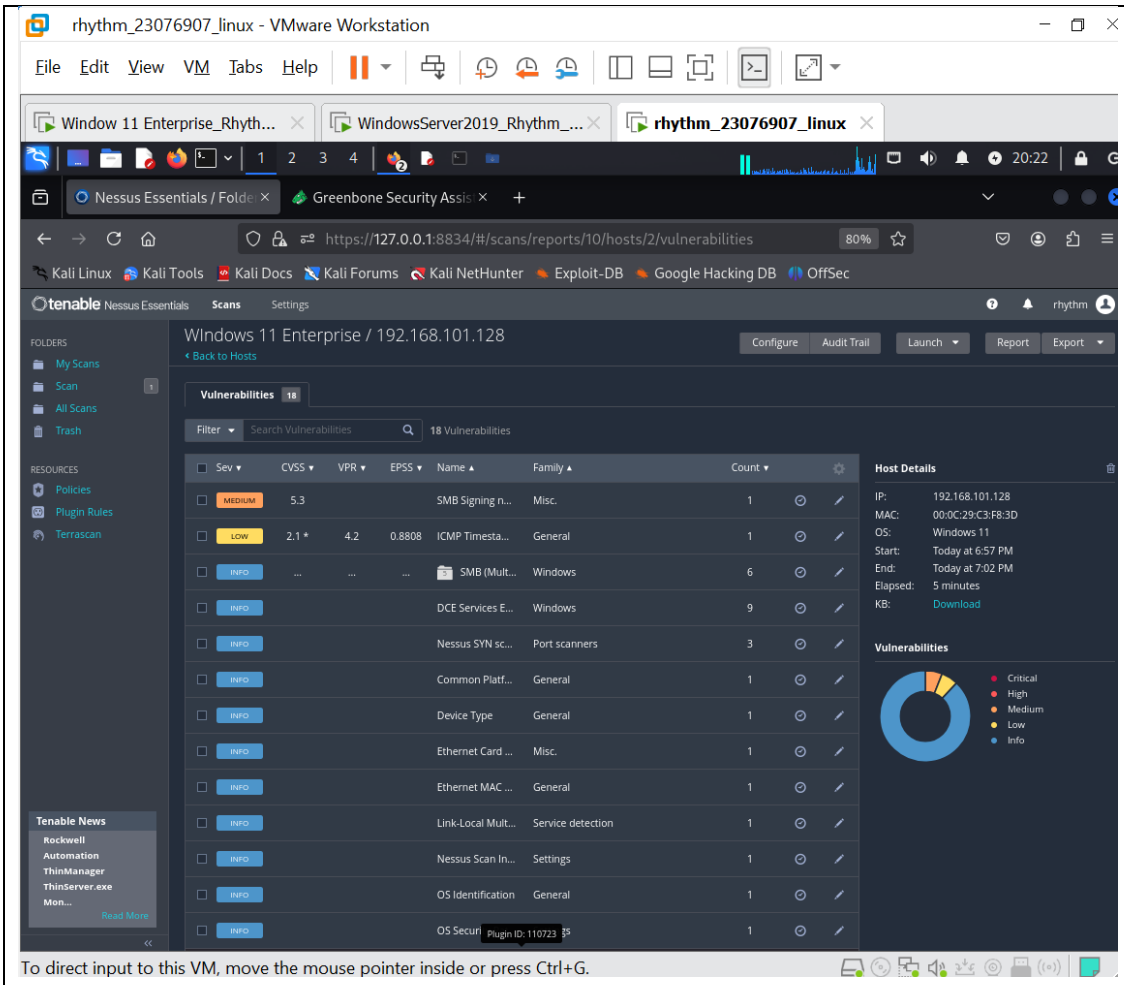
In this lab, you will run a vulnerability scan against a server of your choice. It is important to note that you should never run a vulnerability scan without permission
You will need access to both your vulnerability scanning Server/Window VMs that you built in Activity previously and a target server for your scan. You also may wish to scan your home network as an

alternative. You might be surprised at some of the vulnerabilities that you find lurking in your “smart” home devices! **Turn off the fire walls completely for both Windows based VMs.**

- Conduct a vulnerability scan against your windows server 2019 and windows 10 enterprise VM and save the resulting report. If you need assistance, consult the Nessus documentation. You will need the report from this vulnerability scan to complete the activities in the **next lab(s)**.

Windows 11 Enterprise



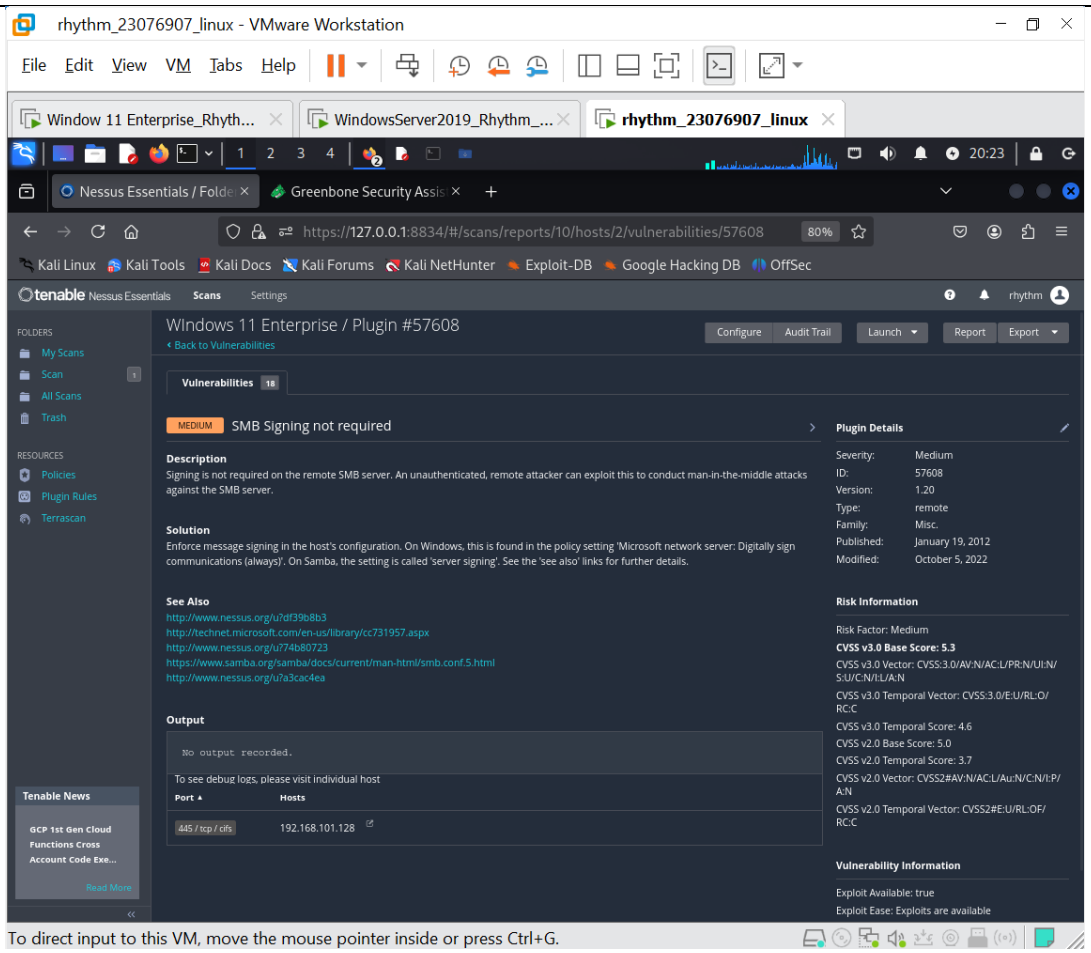


Windows 11 Enterprise Evaluation (IP: 192.168.101.128)

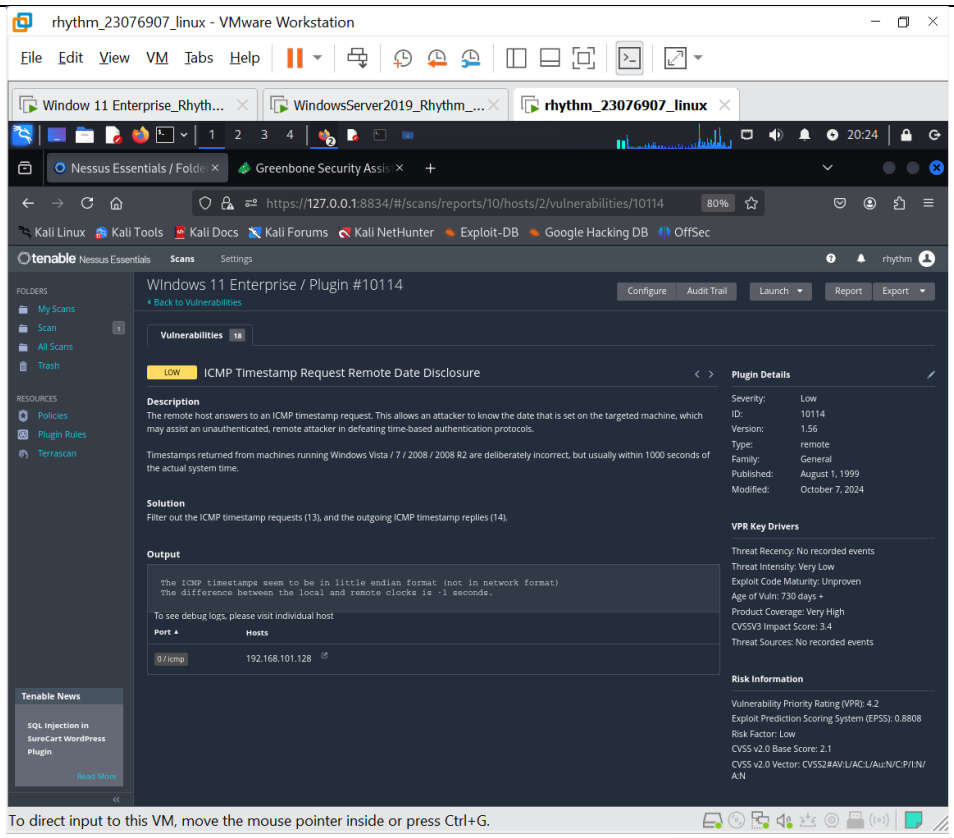
- **Operating System**: Windows 11 Enterprise
- **Total Vulnerabilities**: 2
- **Severity Breakdown**:
  - High: 0
  - Medium: 1
  - Low: 1
- **Quality of Detection (QoD)**: 80 %

Top Three Vulnerabilities:

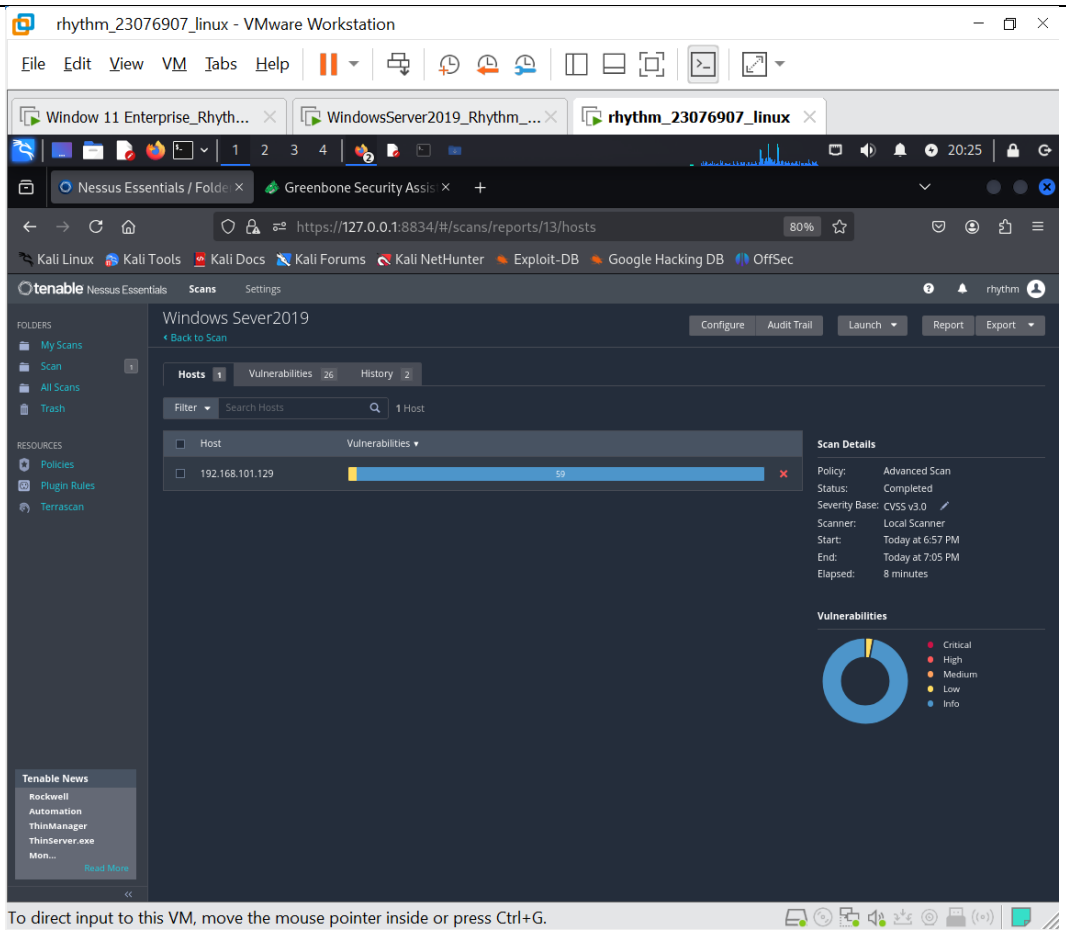
Vulnerability 1

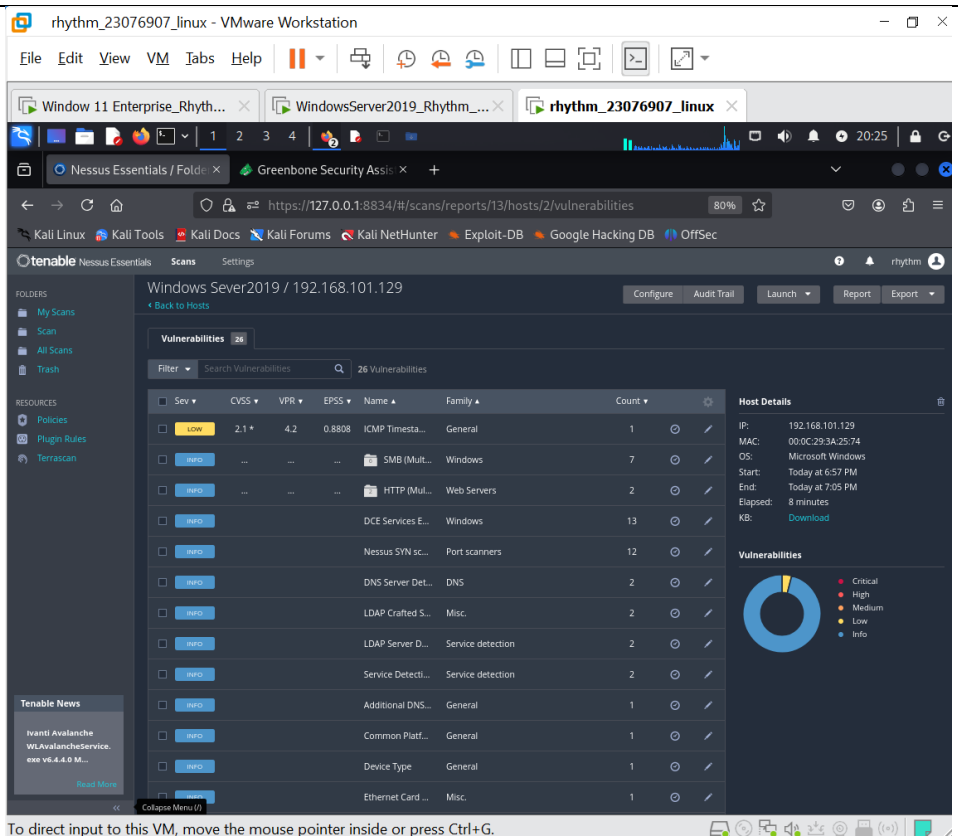


Vulnerability 2



Windows Server 2019


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
Window 11 Enterprise_Rhyth...
WindowsServer2019_Rhythm_...
rhythm_23076907_linux
Nessus Essentials / Folde
Greenbone Security Assis
https://127.0.0.1:8834/#/scans/reports/13/hosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
rhythm
FOLDERS
My Scans
Scan
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Windows Sever2019
Back to Scan
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 26
History 2
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.101.129
59
Scan Details
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:57 PM
End: Today at 7:05 PM
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Rockwell Automation ThinManager ThinServer.exe Mon...
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Vulnerability 1