

### 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 install gvm`
  - `sudo gvm-setup` (You must capture the password during this setup)
  - `sudo gvm-check-setup` (**Take the screen shot**)

rhythm\_23076907\_linux - VMware Workstation

File Edit View VM Tabs Help

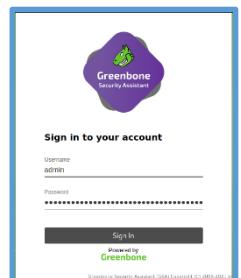
rhythm@rhythm: ~

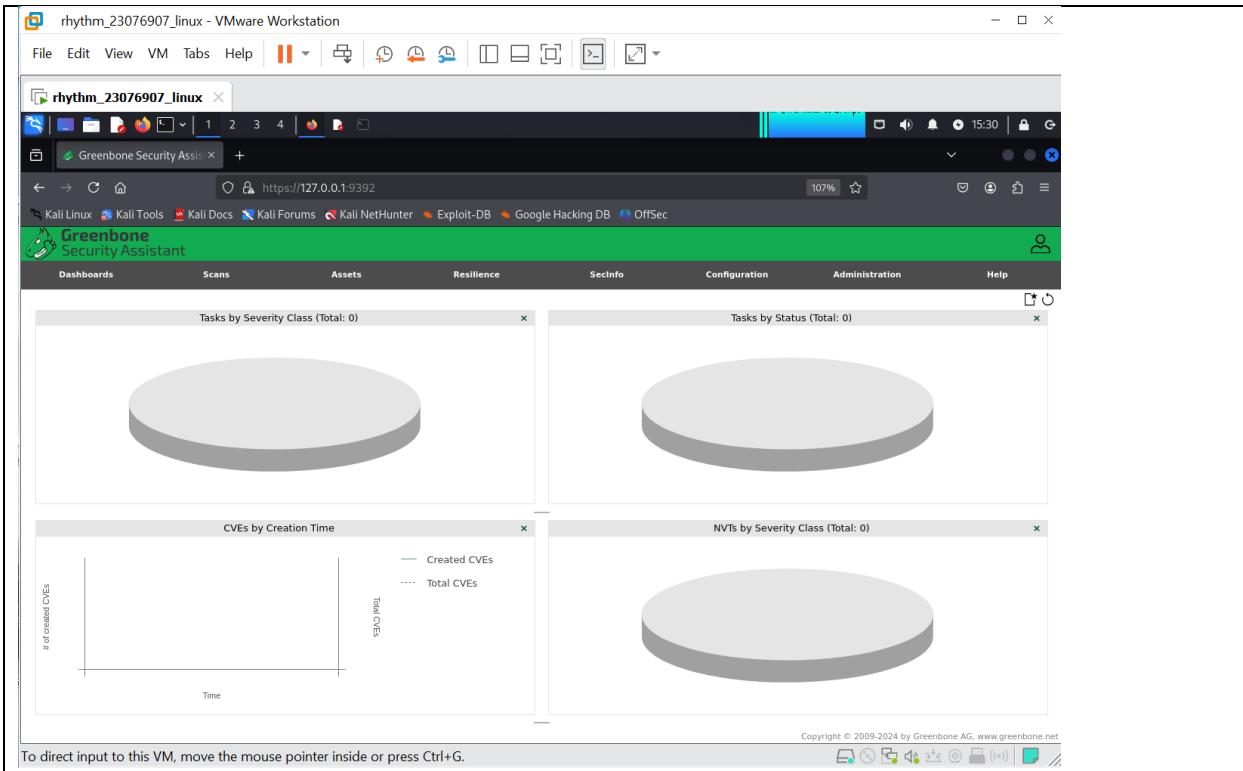
```
File Actions Edit View Help
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
    OK: No old Redis DB
    Starting ospd-openvas service
    Waiting for ospd-openvas service
    OK: ospd-openvas service is active.
    OK: ospd-OpenVAS is present in version 22.7.1.
Step 2: Checking GVM Manager ...
    OK: GVM Manager (gvmmd) is present in version 23.10.0.
Step 3: Checking Certificates ...
    OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
    OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
    OK: SCAP data found in /var/lib/gvm/scap-data.
    OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking Postgresql DB and user ...
/usr/bin/gvm-check-setup: line 390: [: too many arguments
/usr/bin/gvm-check-setup: line 397: [: too many arguments
    OK: Postgresql version and default port are OK.
    gvmmd | .gvm | UTF8 | libc | C.UTF-8 | C.UTF-8 | | |
16440|pg-gvm|10|2200|f|22.6|||
    OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
    OK: Greenbone Security Assistant is present in version 22.12.0-git.
Step 7: Checking if GVM services are up and running ...
    Starting gvmmd service
    Waiting for gvmmd service
    OK: gvmmd service is active.
    Starting gsad service
    Waiting for gsad service
    OK: gsad service is active.
Step 8: Checking few other requirements ...
    OK: nmap is present.
    OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
    OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
    OK: xsltproc found.
    WARNING: Your password policy is empty.
    SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant...
    OK: greenbone-security-assistant is installed

It seems like your GVM-23.11.0 installation is OK.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- 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 gym 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 youtube video:
  - [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

To direct input to this VM, click inside or press Ctrl+G.

## WINDOWS SERVER 2019

```

Windows Server 2019 Standard Evaluation
Windows License valid for 199 days
Build 17763.152, release.180914-1454
4:15 PM 10/10/2024

Key Select Administrator C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.3658]
(c) 2018 Microsoft Corporation. All Rights Reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

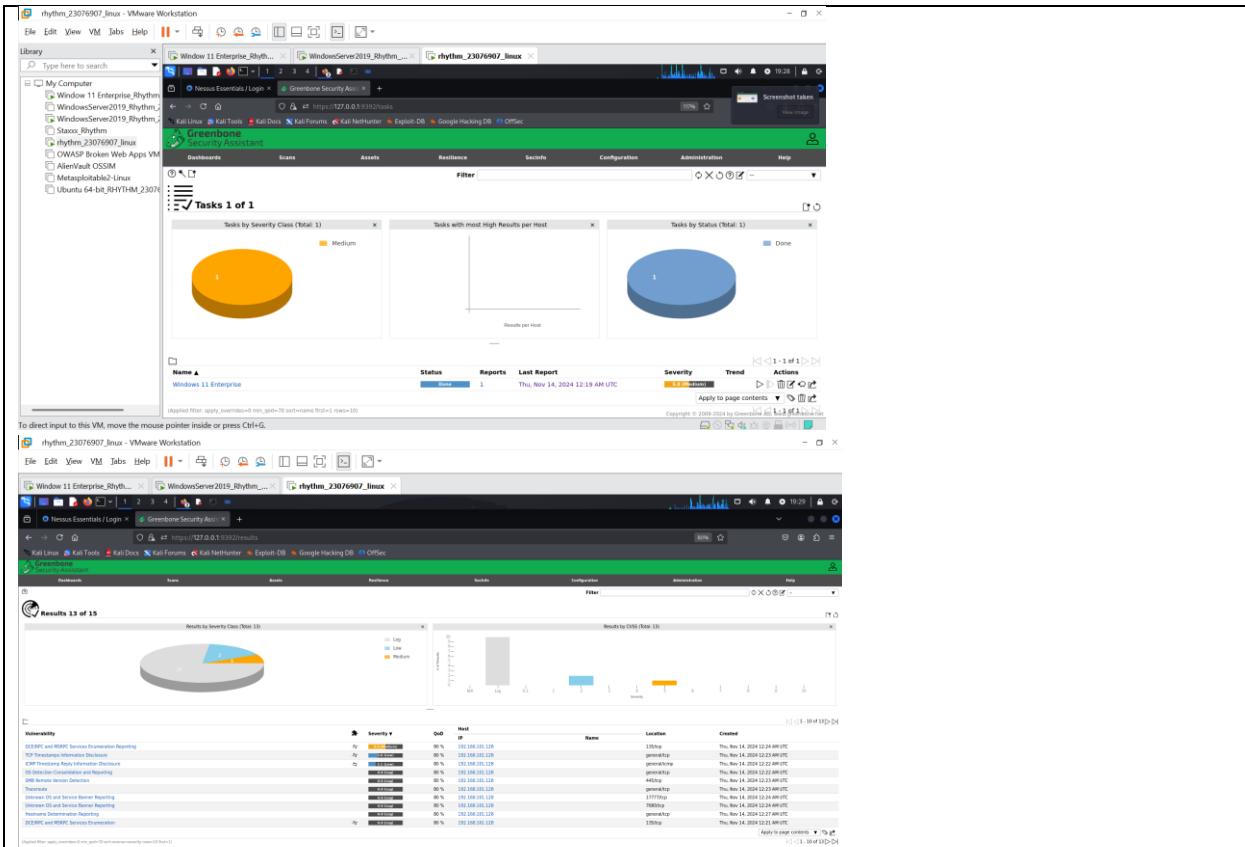
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::20c:9aff%101
IPv4 Address. . . . . : 192.168.1.101  Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1  DHCPv6 Client IPv6 Address . . . . . : 2002::10c:9ff%101
  
```

To direct input to this VM, click inside or press Ctrl+G.

- 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

Screenshot of the Greenbone Security Assistant interface showing results for the VM 'rhythm\_23076907\_linux'. The interface includes a navigation bar with tabs for File, Edit, View, VM, Tabs, Help, and various icons. The main window displays three panels: 'Results by Severity Class (Total: 31)', 'Results by CVSS (Total: 31)', and a detailed list of vulnerabilities.

**Results by Severity Class (Total: 31)**

- Log: 29
- Low: 1
- Medium: 1

**Results by CVSS (Total: 31)**

Severity	# of Results
N/A	0
Log	29
0.1	0
1	0
2	1
3	0
4	0

**Vulnerability List**

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.101.129	135/tcp	Thu, Nov 14, 2024 12:52 AM UTC	
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.101.129	general/icmp	Thu, Nov 14, 2024 12:50 AM UTC	
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	80 %	192.168.101.129	135/tcp	Thu, Nov 14, 2024 12:44 AM UTC	
SMB/CIFS Server Detection	0.0 (Log)	80 %	192.168.101.129	139/tcp	Thu, Nov 14, 2024 12:44 AM UTC	
LDAP Service Detection (TCP)	0.0 (Log)	80 %	192.168.101.129	3268/tcp	Thu, Nov 14, 2024 12:46 AM UTC	
LDAP Service Detection (TCP)	0.0 (Log)	80 %	192.168.101.129	389/tcp	Thu, Nov 14, 2024 12:46 AM UTC	
Web Services Management (WS-Man) / Windows Remote Management (WinRM) Detection (HTTP)	0.0 (Log)	80 %	192.168.101.129	5985/tcp	Thu, Nov 14, 2024 12:47 AM UTC	
DNS Server Detection (TCP)	0.0 (Log)	80 %	192.168.101.129	53/tcp	Thu, Nov 14, 2024 12:47 AM UTC	

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

### 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

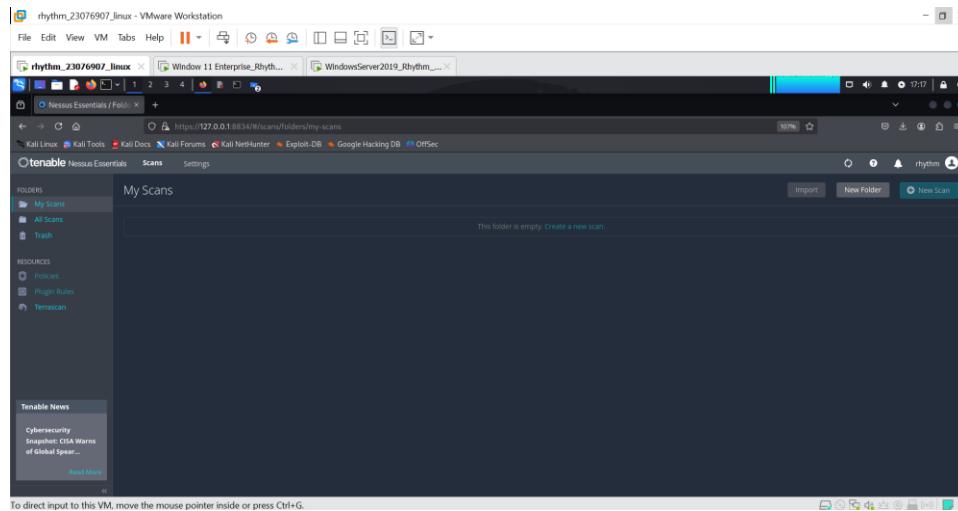
Visit the Nessus download page (<https://www.tenable.com/products/nessus/select-your-operating-system#download>) and download the appropriate version of Nessus for your system.

#### 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

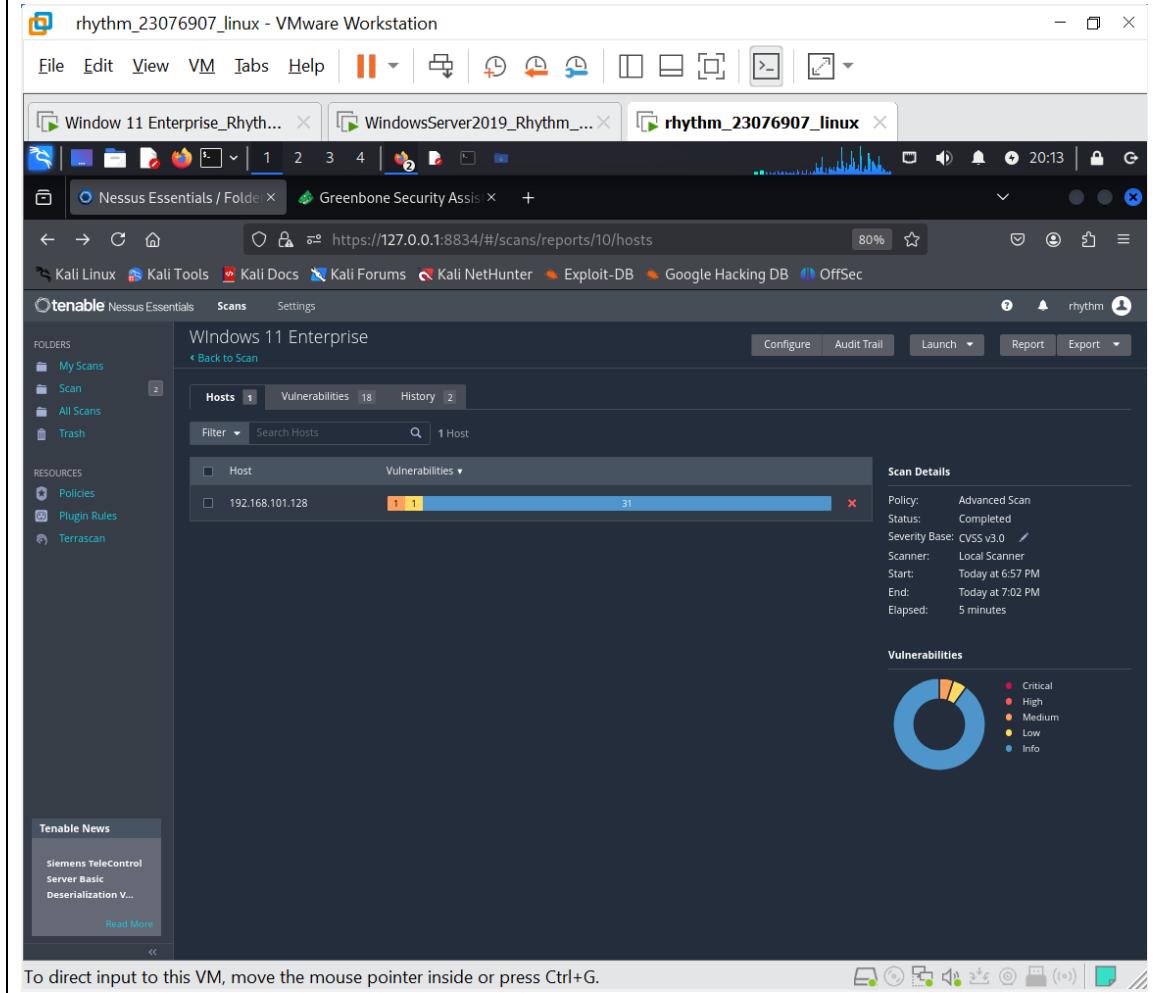
In this lab, you will run a vulnerability scan against a server of your choice. It is important to note that you should never run a vulnerability scan without permission.

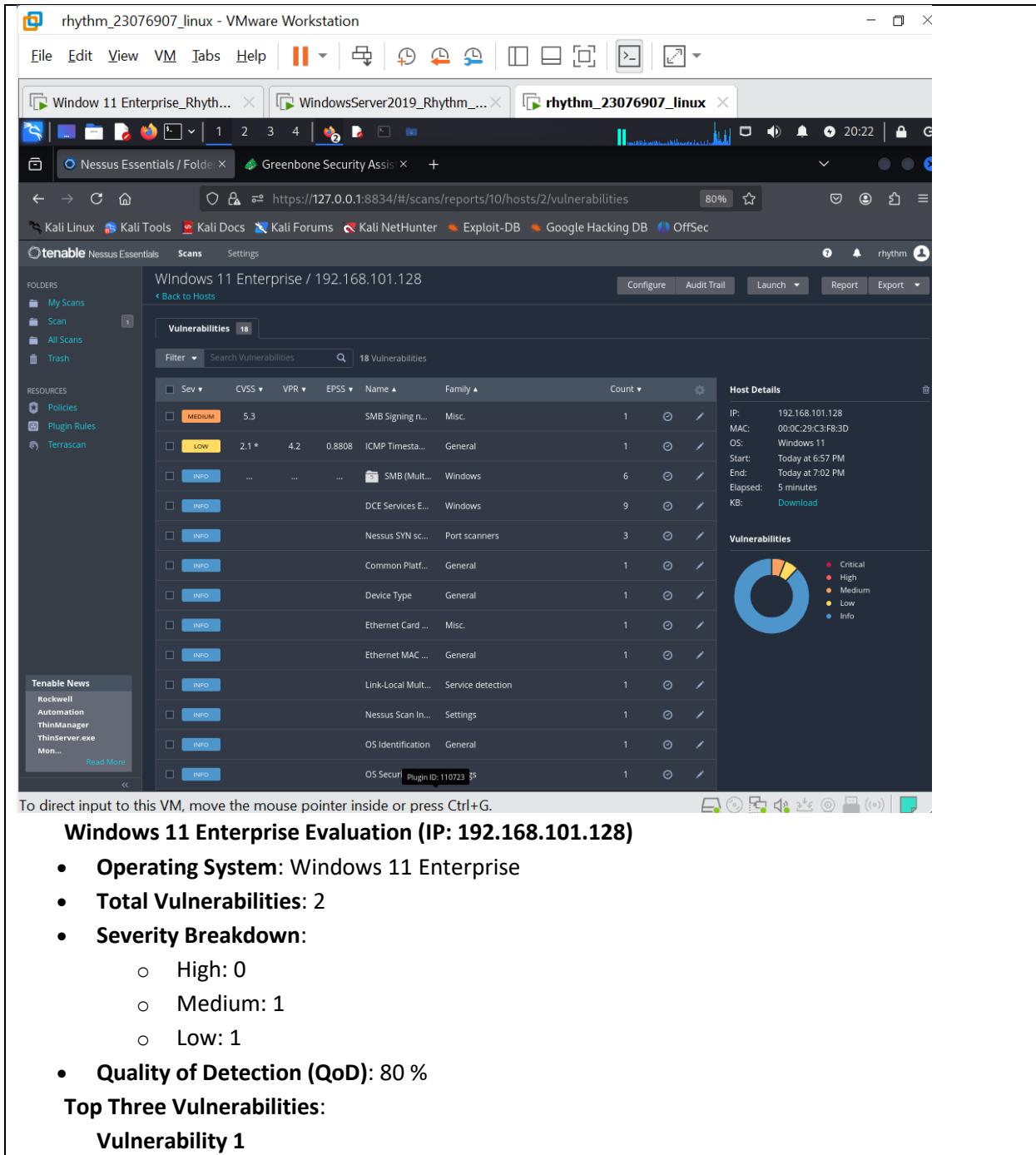
You will need access to both your vulnerability scanning Server/Window VMs that you built in Activity previously and a target server for your scan. You also may wish to scan your home network as an

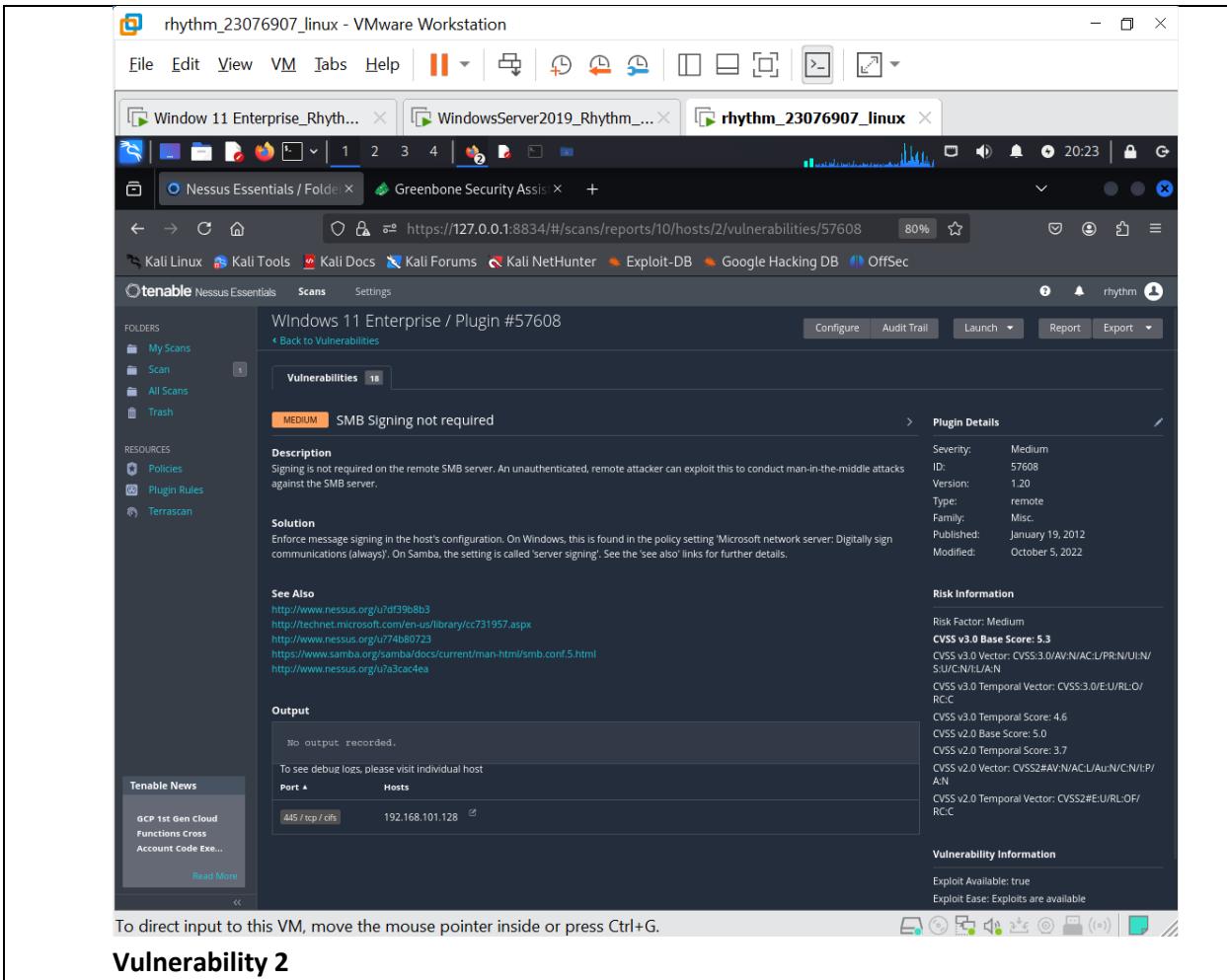
alternative. You might be surprised at some of the vulnerabilities that you find lurking in your “smart” home devices! **Turn off the fire walls completely for both Windows based VMs.**

- 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

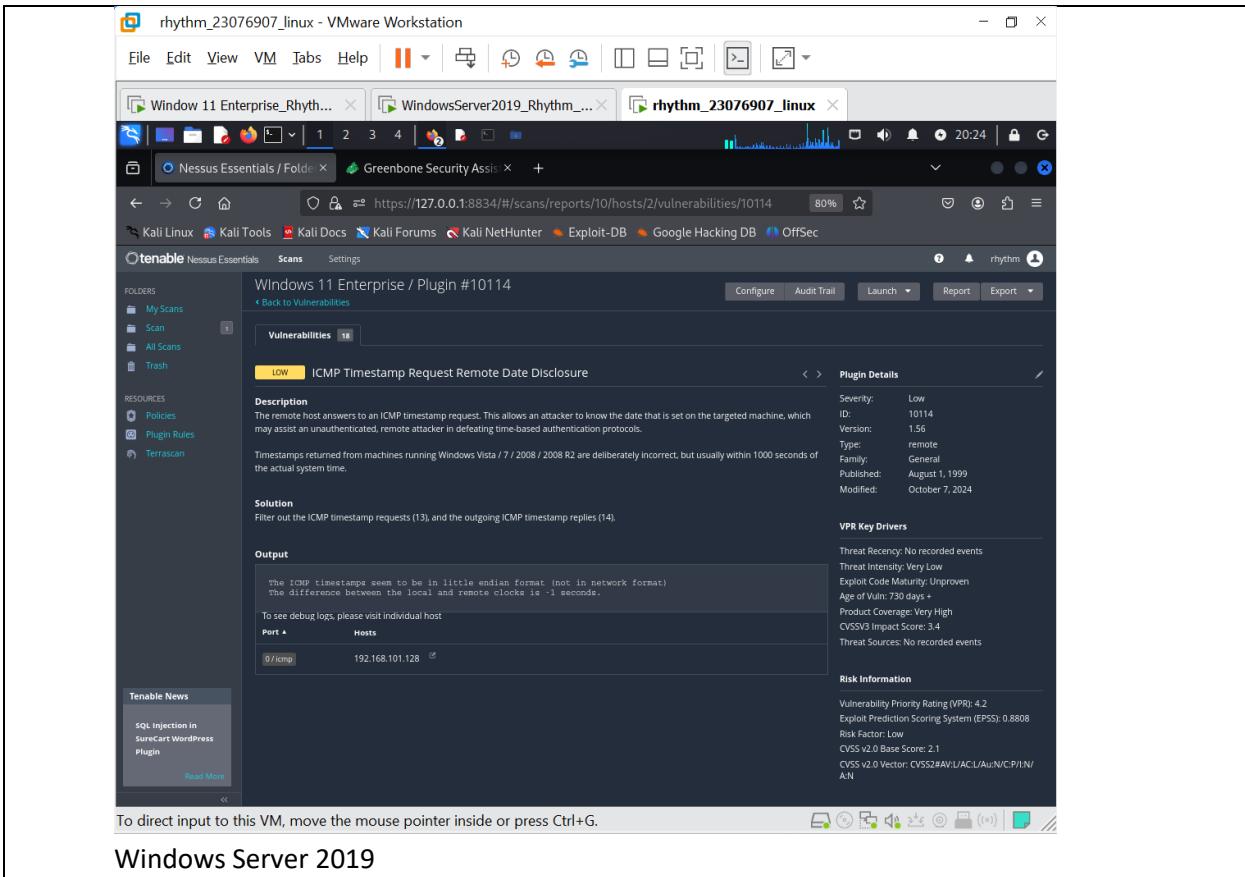






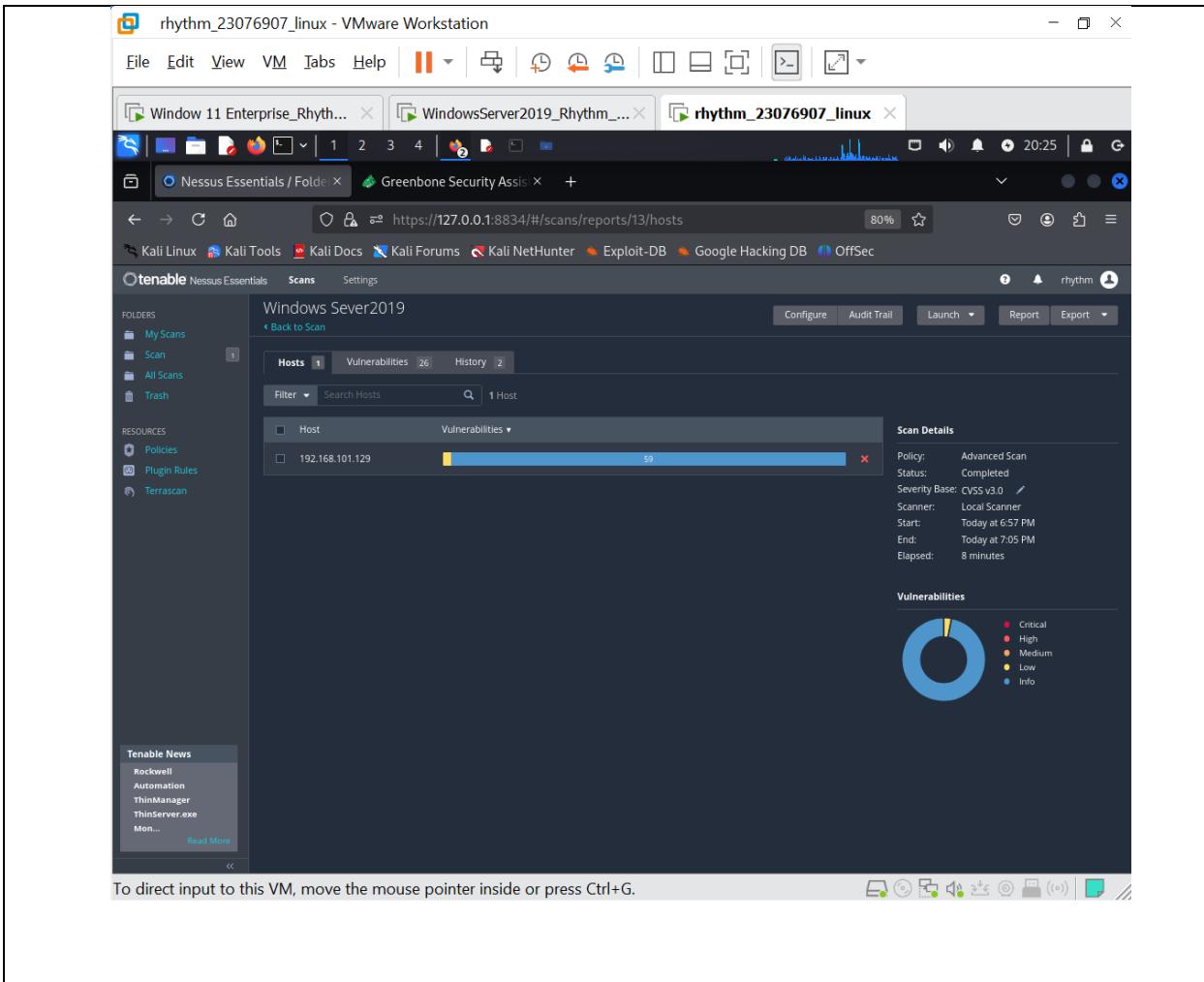
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Vulnerability 2



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Windows Server 2019



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Vulnerability 1

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

