

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_23076907_linux

rhythm@rhythm: ~

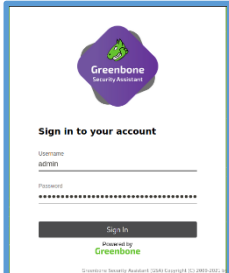
```
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting osdp-openvas service
Waiting for osdp-openvas service
OK: osdp-openvas service is active.
OK: osdp-OpenVAS is present in version 22.7.1.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvmd) 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.
gvmd | _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 gvmd service
Waiting for gvmd service
OK: gvmd 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/pwppolicy.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.

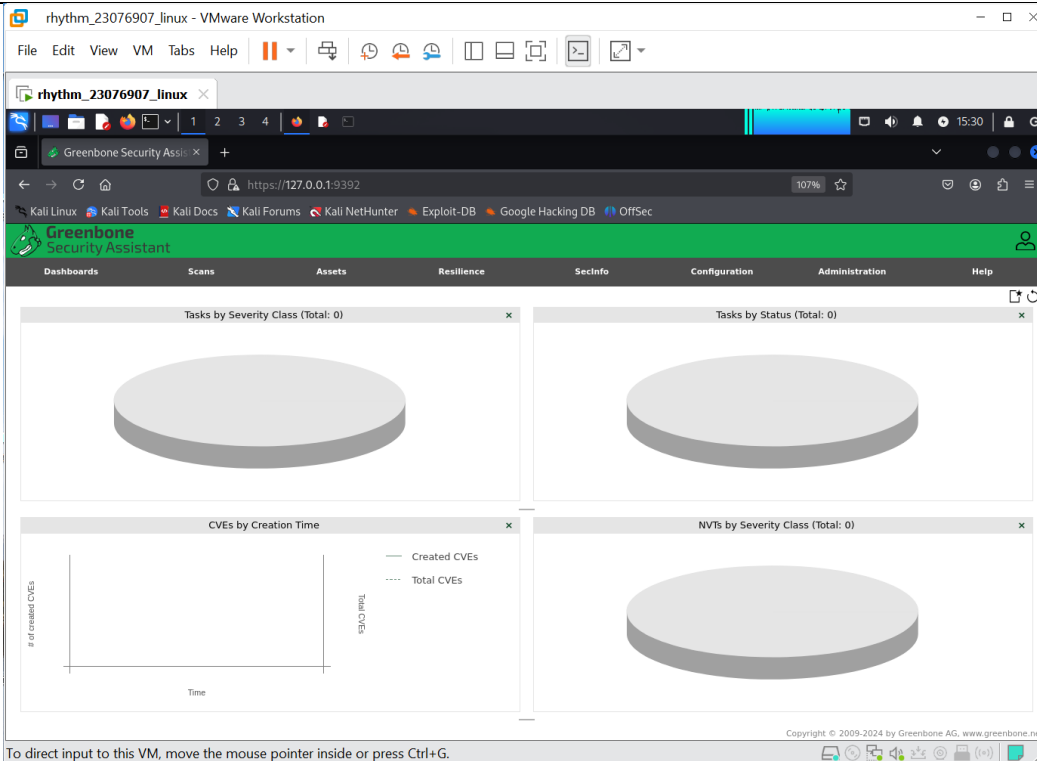
(rhythm@rhythm)-[~]
```

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 gvm setup.



The image shows the Greenbone Security Assistant login page. It features the Greenbone logo at the top, followed by the text "Sign in to your account". Below this, there are input fields for "Username" (with "admin" entered) and "Password" (with a masked password). A "Sign In" button is located at the bottom of the form. The footer of the page includes the text "Powered by Greenbone" and a small copyright notice.



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

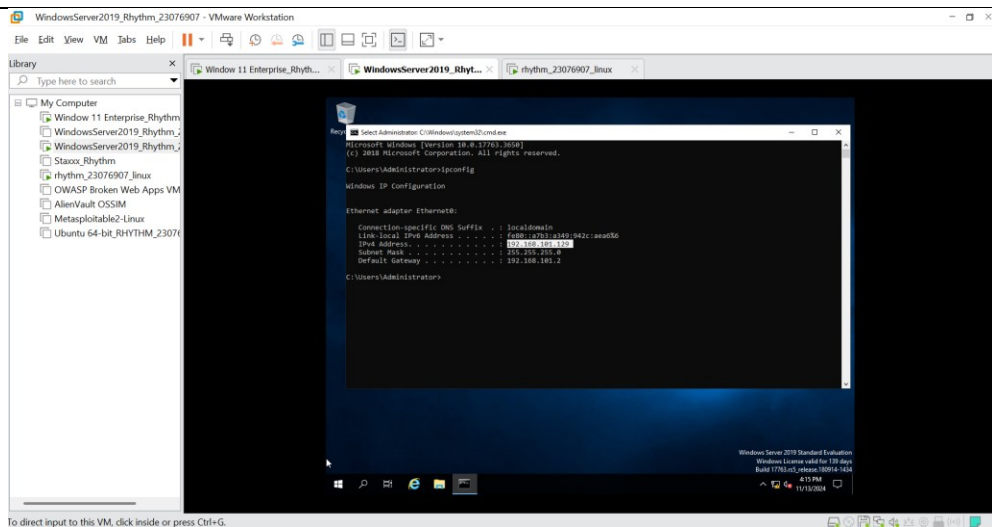
Activity 2: Vulnerability/Exposure Testing and Reporting (Linux)

- 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.

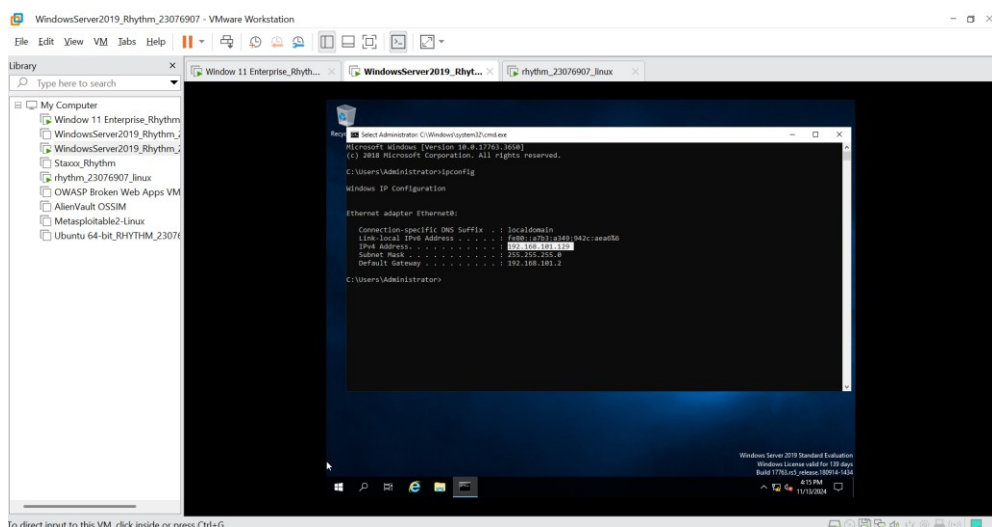
- Get the ip address of any both VMs (Windows 10 Enterprise and Windows Server 2019 evaluation).

WINDOW 11 ENTERPRISE



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

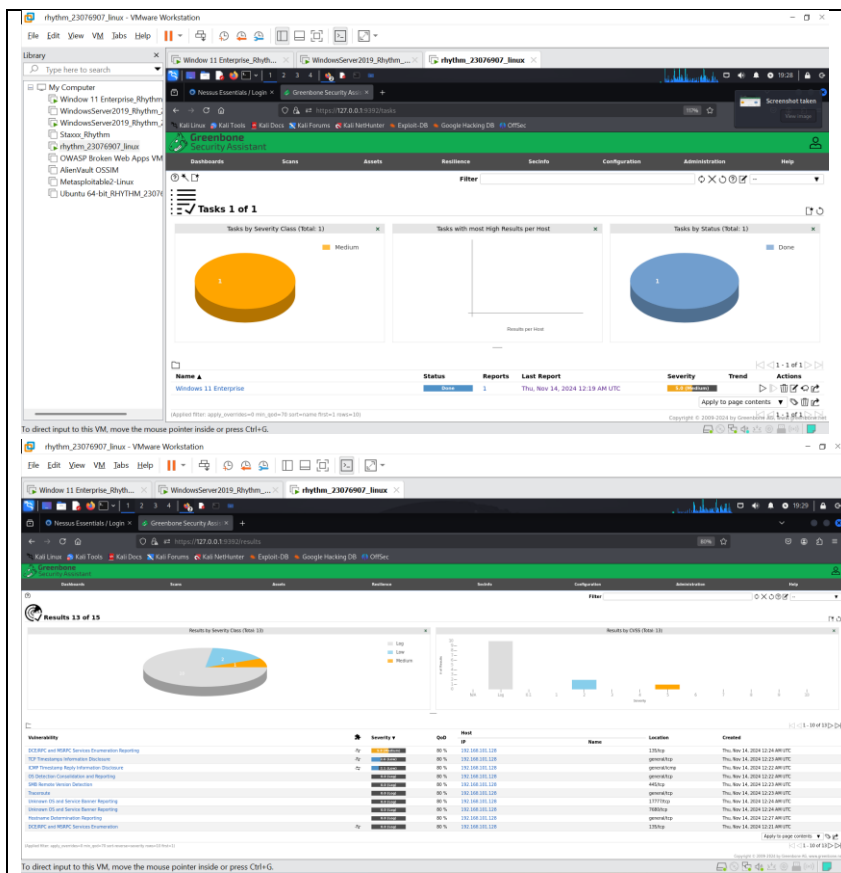
WINDOWS SERVER 2019



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

rhythm_23076907_linux - VMware Workstation

File Edit View VM Tabs Help

Window 11 Enterprise_Rhythm... WindowsServer2019_Rhythm... rhythm_23076907_linux

Nessus Essentials / Login x Greenbone Security Assis x

https://127.0.0.1:9392/results 80%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Results 31 of 32

Results by Severity Class (Total: 31)

Results by CVSS (Total: 31)

Results by CVSS (Total: 31)

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

1 - 10 of 31

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

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

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

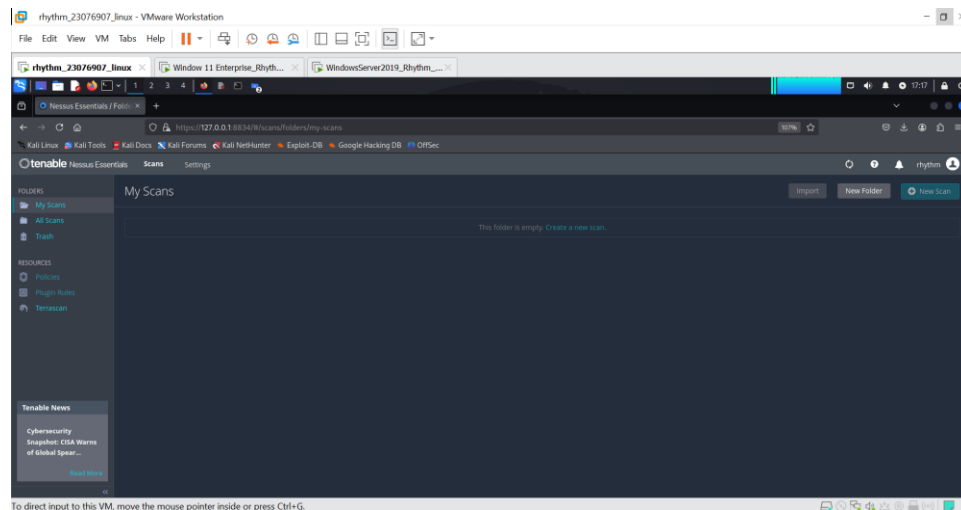
Visit the Nessus download page (<https://www.tenable.com/products/nessus/select-your-operating-system#download>) and download the appropriate version of Nessus for your system.

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

The screenshot shows a VMware Workstation window titled 'rhythm_23076907_linux - VMware Workstation'. Inside the VM, a web browser is open to the Tenable Nessus Essentials interface. The browser's address bar shows the URL 'https://127.0.0.1:8834/#/scans/reports/10/hosts'. The Nessus interface displays a scan report for 'Windows 11 Enterprise'. The main content area shows a table with 1 host and 31 vulnerabilities. The right-hand panel provides scan details, including the policy 'Advanced Scan', status 'Completed', severity base 'CVSS v3.0', scanner 'Local Scanner', start time 'Today at 6:57 PM', end time 'Today at 7:02 PM', and elapsed time '5 minutes'. A donut chart shows the distribution of vulnerabilities by severity: Critical (1), High (1), Medium (1), Low (1), and Info (31).

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

rhythm_23076907_linux - VMware Workstation

File Edit View VM Tabs Help

Window 11 Enterprise_Rhyth... WindowsServer2019_Rhythm... rhythm_23076907_linux

Nessus Essentials / Folders Greenbone Security Assi...

https://127.0.0.1:8834/#/scans/reports/10/hosts/2/vulnerabilities 80%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

Windows 11 Enterprise / 192.168.101.128

Configure Audit Trail Launch Report Export

Vulnerabilities 18

Filter Search Vulnerabilities 18 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
MEDIUM	5.3			SMB Signing n...	Misc.	1		
LOW	2.1	4.2	0.8808	ICMP Timesta...	General	1		
INFO				SMB (Mult...	Windows	6		
INFO				DCE Services E...	Windows	9		
INFO				Nessus SYN sc...	Port scanners	3		
INFO				Common Platt...	General	1		
INFO				Device Type	General	1		
INFO				Ethernet Card ...	Misc.	1		
INFO				Ethernet MAC ...	General	1		
INFO				Link-Local Mult...	Service detection	1		
INFO				Nessus Scan In...	Settings	1		
INFO				OS Identification	General	1		
INFO				OS Secur...	Plugin ID: 110723 JS	1		

Host Details

IP: 192.168.101.128
 MAC: 00:0C:29:C3:F8:3D
 OS: Windows 11
 Start: Today at 6:57 PM
 End: Today at 7:02 PM
 Elapsed: 5 minutes
 KB: Download

Vulnerabilities

Donut chart showing severity breakdown: Critical (0), High (0), Medium (1), Low (1), Info (16).

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.

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

rhythm_23076907_linux - VMware Workstation

File Edit View VM Tabs Help

Window 11 Enterprise_Rhyth... WindowsServer2019_Rhythm... rhythm_23076907_linux

Nessus Essentials / Folders: x Greenbone Security Assis: x

https://127.0.0.1:8834/#/scans/reports/10/hosts/2/vulnerabilities/57608 80%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

Windows 11 Enterprise / Plugin #57608

Configure Audit Trail Launch Report Export

Vulnerabilities 18

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	192.168.101.128

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/L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/R: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:O/R:C

Vulnerability Information

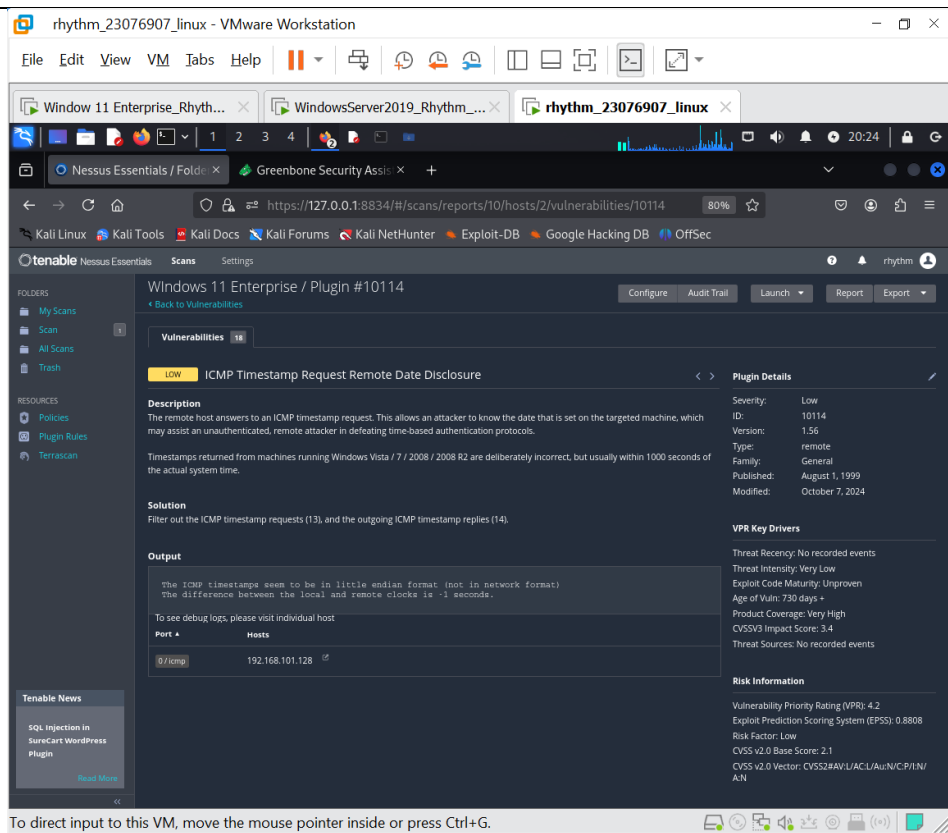
Exploit Available: true
Exploit Ease: Exploits are available

Tenable News

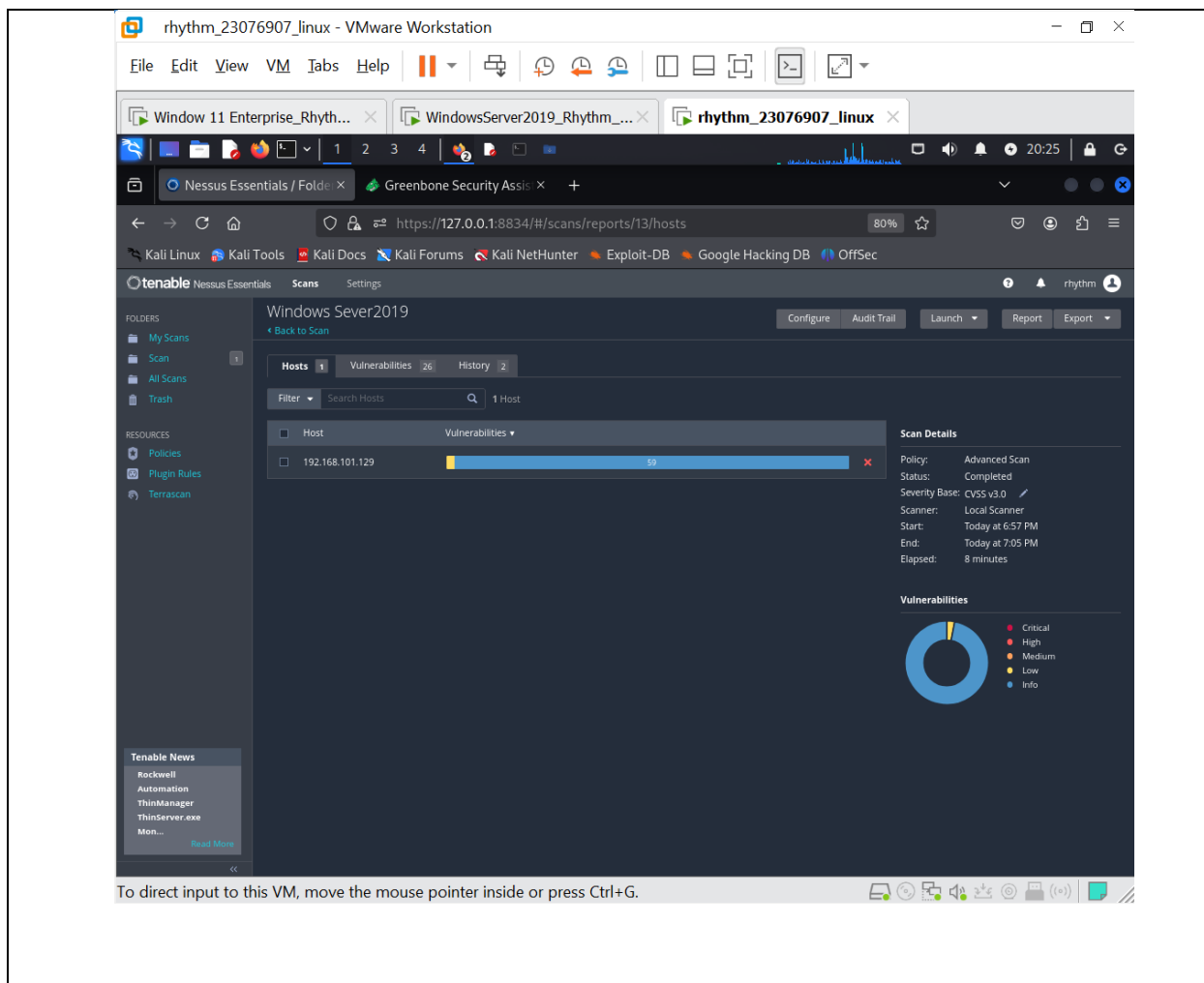
GCP 1st Gen Cloud Functions Cross Account Code Exe...
Read More

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

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 / Folders Greenbone Security Assis

https://127.0.0.1:8834/#/scans/reports/13/hosts/2/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

Windows Sever2019 / 192.168.101.129

Configure Audit Trail Launch Report Export

Vulnerabilities 26

Filter Search Vulnerabilities 26 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Host Details
Low	2.1*	4.2	0.8808	ICMP Timesta...	General	1	IP: 192.168.101.129 MAC: 00:0C:29:3A:25:74 OS: Microsoft Windows Start: Today at 6:57 PM End: Today at 7:05 PM Elapsed: 8 minutes KB: Download
Info	SMB (Mult...	Windows	7	
Info	HTTP (Mult...	Web Servers	2	
Info	DCE Services E...	Windows	13	
Info	Nessus SYN sc...	Port scanners	12	
Info	DNS Server Det...	DNS	2	
Info	LDAP Crafted S...	Misc.	2	
Info	LDAP Server D...	Service detection	2	
Info	Service Detecti...	Service detection	2	
Info	Additional DNS...	General	1	
Info	Common Platt...	General	1	
Info	Device Type	General	1	
Info	Ethernet Card ...	Misc.	1	

Tenable News

ivanti Avalanche WLAvalancheService.exe V6.4.4.0 M...

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

Vulnerability 1

rhythm_23076907_linux - VMware Workstation

File Edit View VM Tabs Help

Window 11 Enterprise_Rhyth... WindowsServer2019_Rhythm... rhythm_23076907_linux

Nessus Essentials / Folders Greenbone Security Assis

https://127.0.0.1:8834/#/scans/reports/13/hosts/2/vulnerabilities/10114

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

Windows Sever2019 / Plugin #10114

Configure Audit Trail Launch Report Export

Vulnerabilities 26

LOW ICMP Timestamp Request Remote Date Disclosure

Plugin Details

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Output

This host returns non-standard timestamps (high bit is set). The ICMP timestamp might be in little endian format (not in network format). The difference between the local and remote clocks is ~2 seconds.

To see debug logs, please visit individual host

Port	Hosts
0/icmp	192.168.101.129 10

Severity: Low

ID: 10114

Version: 1.56

Type: remote

Family: General

Published: August 1, 1999

Modified: October 7, 2024

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days+

Product Coverage: Very High

CVSS3 Impact Score: 3.4

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.2

Exploit Prediction Scoring System (EPSS): 0.8808

Risk Factor: Low

CVSS v2.0 Base Score: 2.1

CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:P/IN/A:N

Tenable News

Cybersecurity Snapshot CISA Warns of Global Spear...

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

