Lab - Vulnerability Scanning with Kali Tools

Objectives

In this lab, you will explore network vulnerability scanning tools and use them to perform a vulnerability scan on a target host.

- Perform network scans with Nmap.
- Use Greenbone Vulnerability Management to perform a vulnerability scan.

Background / Scenario

In a previous lab, you used Nmap to enumerate a host computer that was creating unusual traffic on the network. In this lab, you will use Nmap and Greenbone Vulnerability Management (GVM) to scan the system to identify potential vulnerabilities.

Required Resources

- Kali VM customized for the Ethical Hacker course
- Internet access

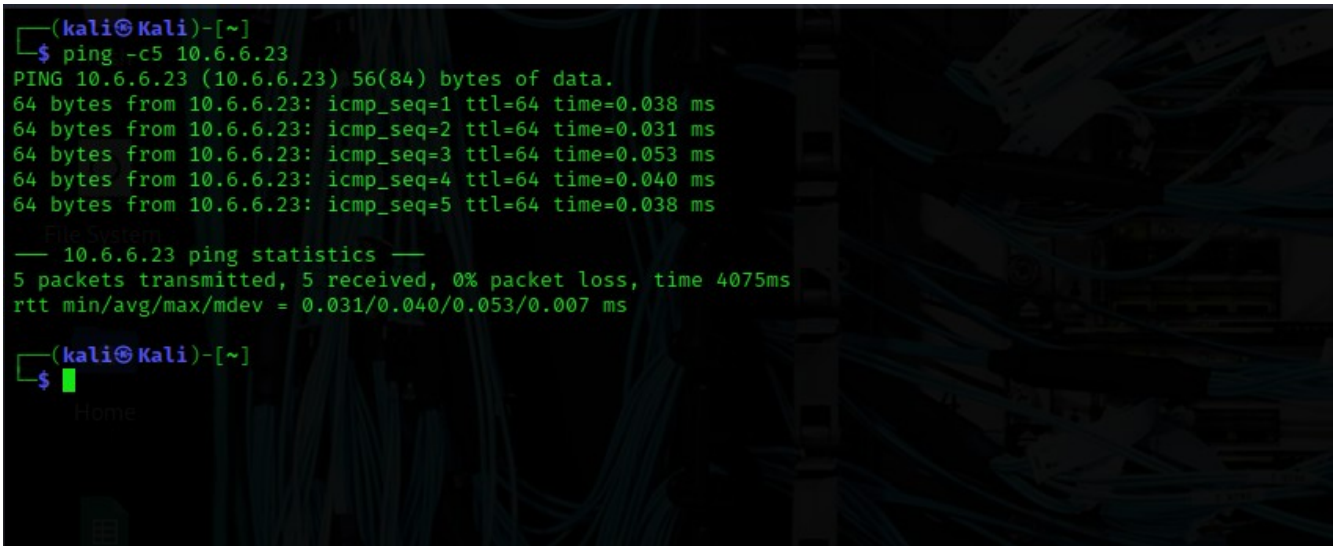
Instructions

Part 1: Run a Nmap Scan on a Target Computer

In this part, you will use Nmap and NSE scripts to uncover potential vulnerabilities in a target host.

Step 1: Start and login to the Kali virtual machine.

a. Start and log into the Kali virtual machine.
b. Start a terminal session. Expand the terminal window to a full screen. Use the **ping** command to determine if the computer with the address **10.6.6.23** or **gravemind.vm** is reachable over the network.

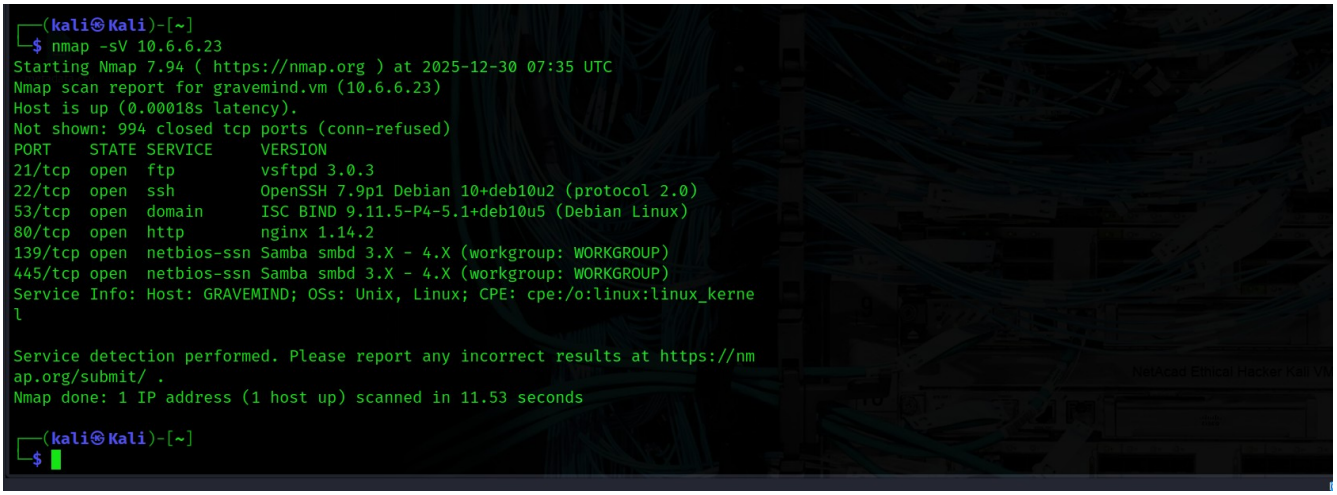


The **-c5** option tells the ping command to stop after five tries. In Linux, when a **-c** option is not specified the **ping** command will continue indefinitely until **CTRL-C** is issued.

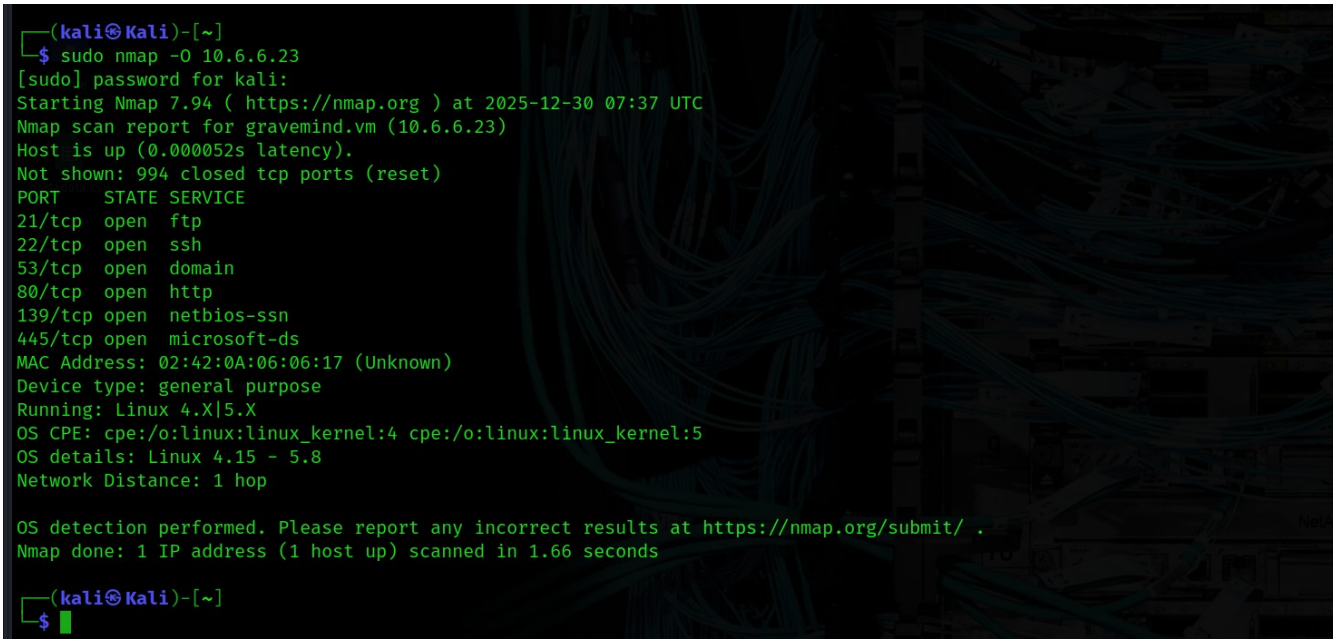
Step 2: Identify open ports and services.

Review the results of a Nmap scan on the host with the IP address 10.6.6.23.

a. Execute a ping scan of the target host using the **nmap -sV** command. Note the list of ports and applications that are discovered on the host. All the ports are Open



Identify the operating system running on the target computer using the **nmap -O** command. The OS is: **Linux 4.15 - 5.8**

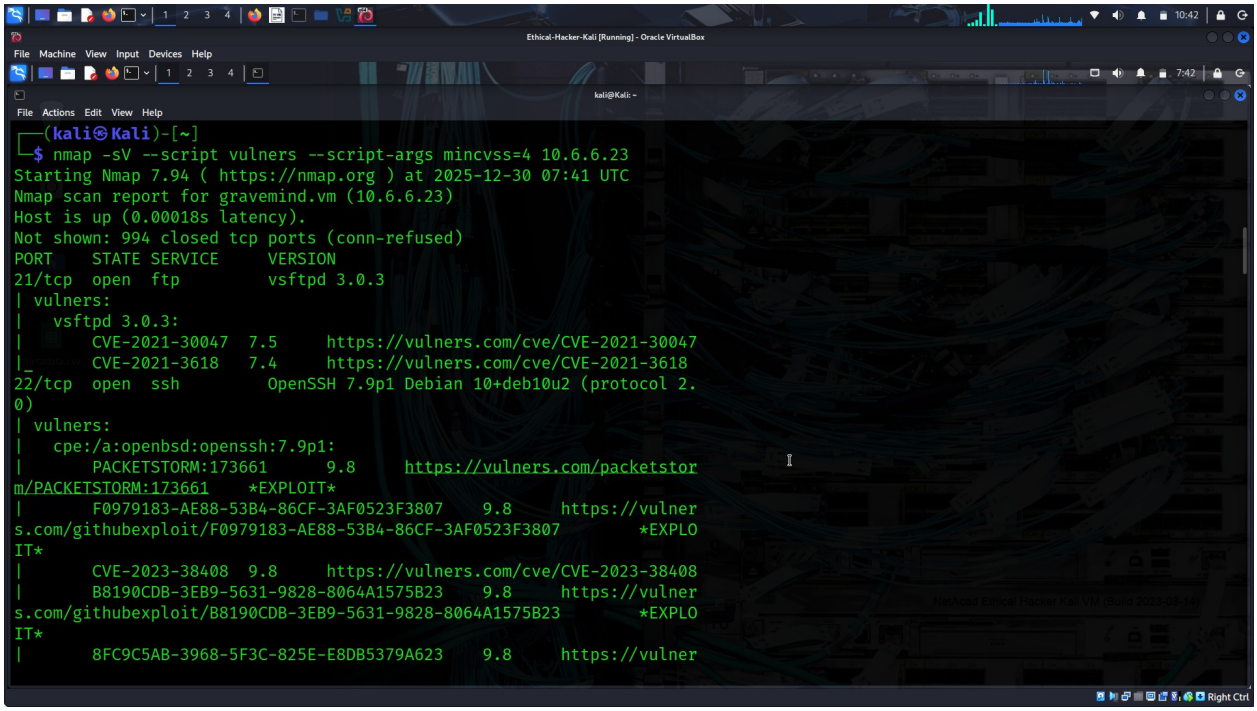


Step 3: Use the Nmap Vulners script to scan for vulnerabilities.

The Vulners script displays known vulnerabilities and the corresponding CVE. The Vulners script uses the open port and software version information to search for common platform enumeration (CPE) names that relate to the identified service. It then makes a request to a remote server to find out if any known vulnerabilities exist for that CPE.

a. Use the **nmap –script** command to launch the **vulners** script. The syntax for the command is **nmap -sV --script vulners [--script-args mincvss=<arg_val>] <target>** where the script argument **mincvss** restricts the output to only those CVEs that have a higher CVSS score than the one specified in the argument.

The vulnerabilities reported will be those with a CVE score equal to or higher than 4. The output of the command should look similar to what is shown below:

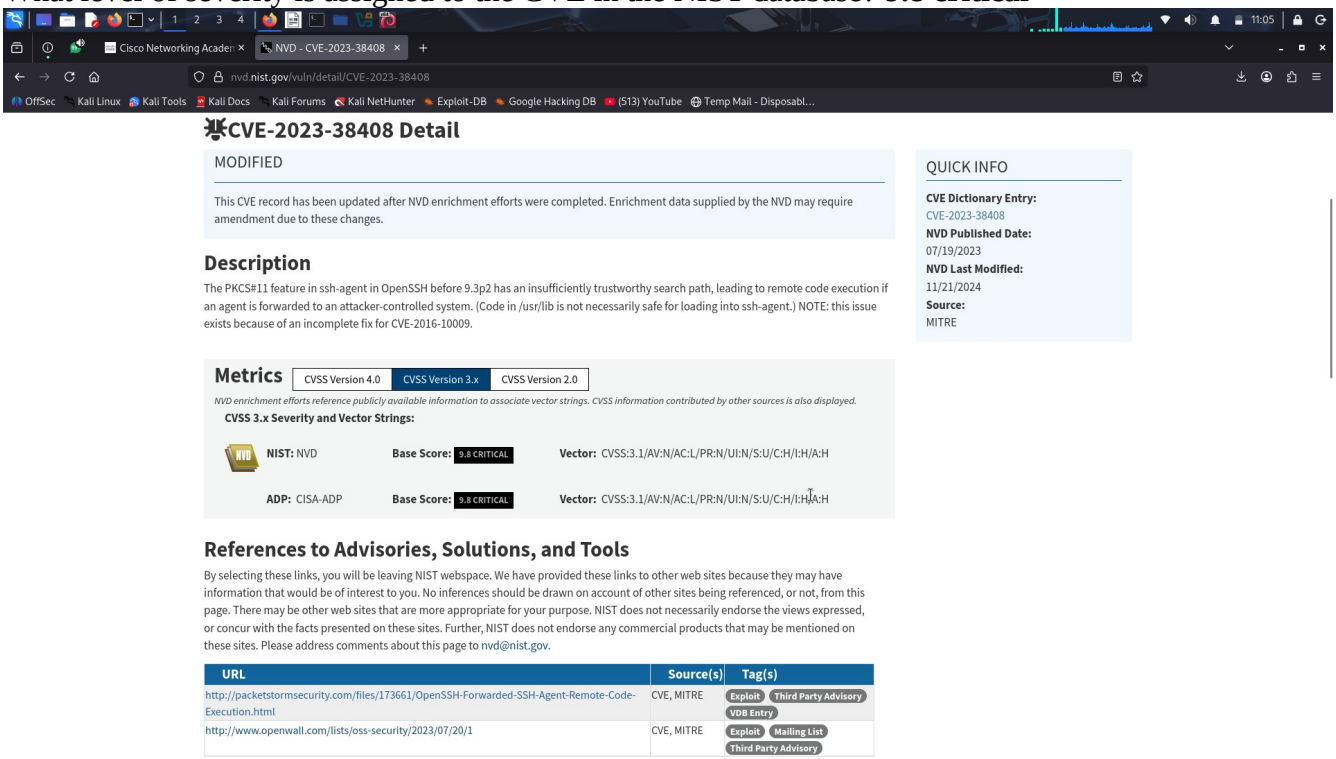


From the above scan we can identify that **OpenSSH service** has known exploited vulnerabilities

The CVE associated with the known level 5 and above vulnerability is the: **CVE-2023-38408**

Use the National Vulnerability Database at NIST to learn more about the identified vulnerability and how it can be exploited. https://nvd.nist.gov/vuln/detail/CVE-2023-38408

What level of severity is assigned to the CVE in the NIST database? **9.8 critical**



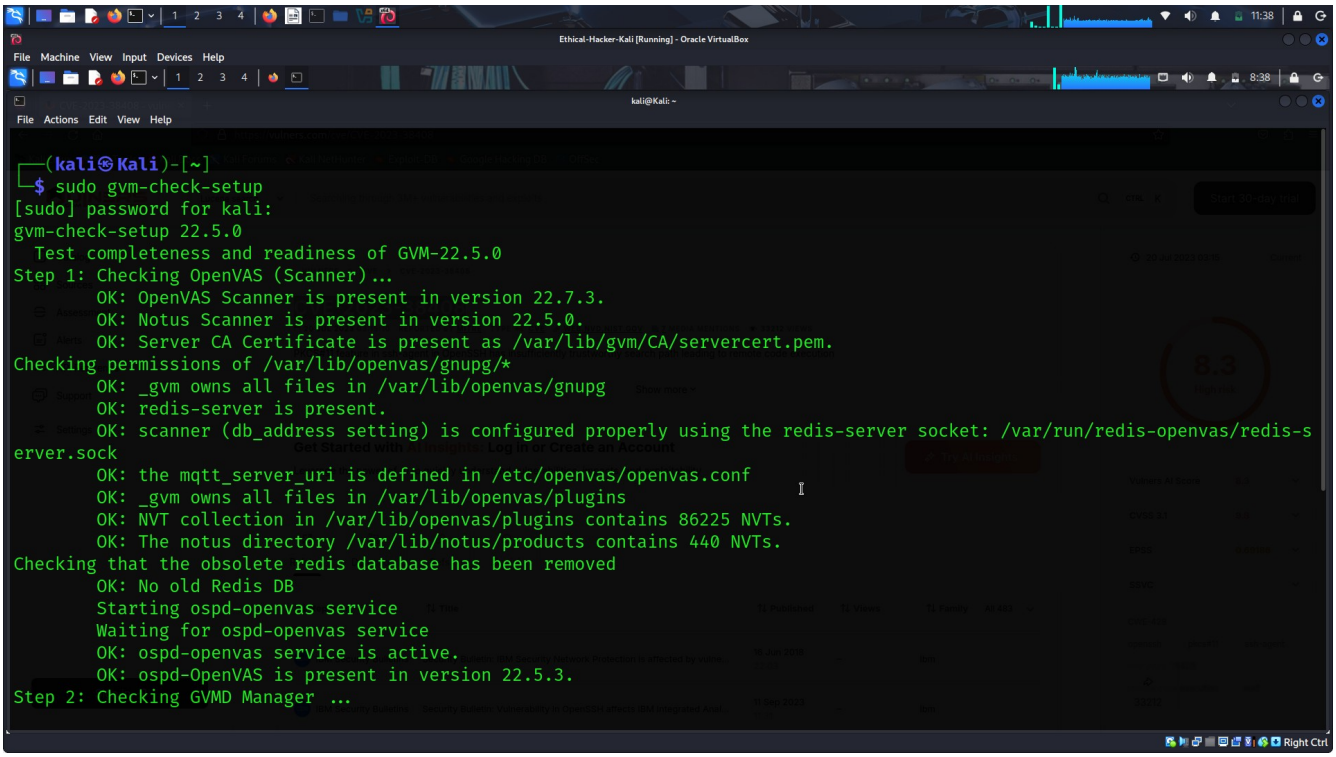
Part 2: Use GVM to Scan for Vulnerabilities

GVM is part of the Open Source Vulnerability Management suite of products produced by Greenbone Networks GmbH. The GVM scanner is one of the most widely used open-source vulnerability scanners. Unlike Nmap, GVM uses a graphical user interface to initiate scans and report vulnerability scan results.

Step 1: Verify the GVM Product Installation.

Before beginning any scan, it is important to verify that GVM is correctly installed and that the files it uses to identify vulnerabilities are up-to-date.

a. Verify the setup of the GVM service using the **sudo gvm-check-setup** command. This command verifies that the setup completed correctly and the necessary files are available. The verification will flag any issues that need fixing and will provide the commands to use to fix the issues.

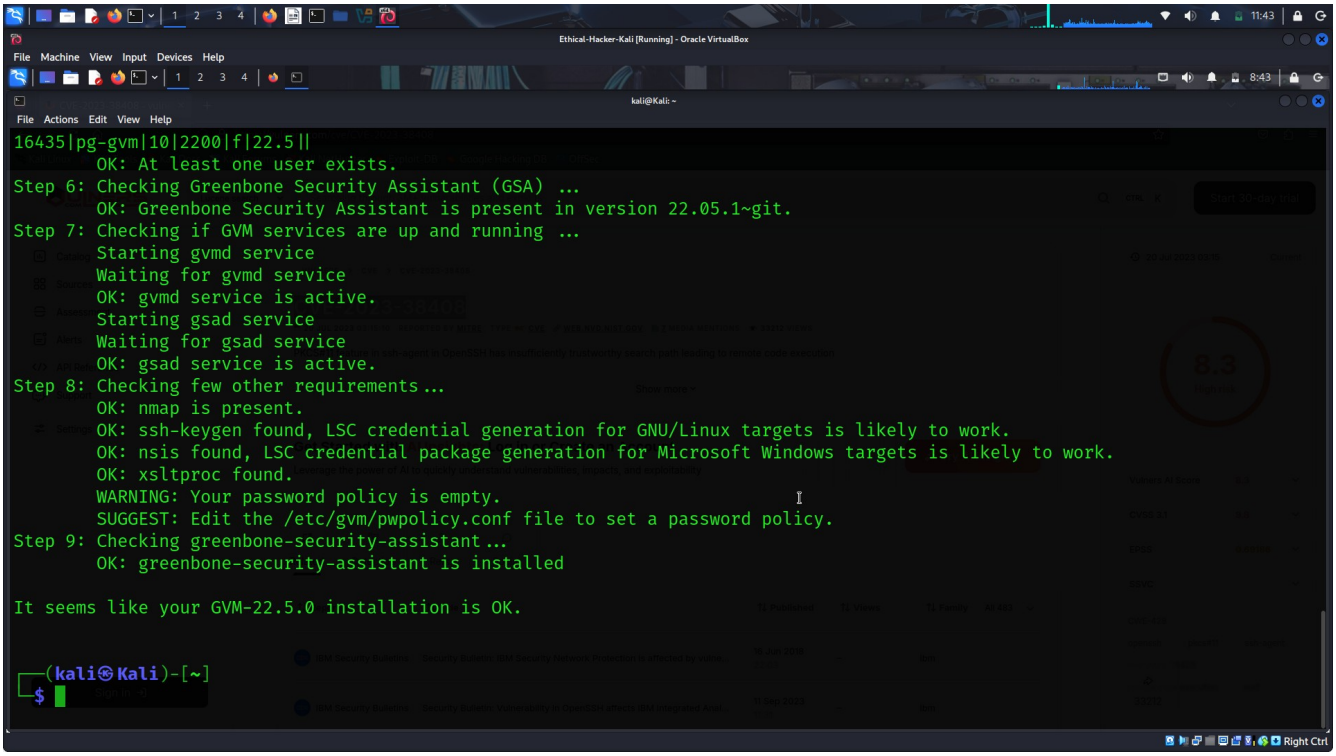


```
        OK: ospd-OpenVAS is present in version 22.5.3.
Step 2: Checking GVMD Manager ...
        OK: GVM Manager (gvmd) is present in version 22.5.5.
Step 3: Checking Certificates ...
C = DE, L = Osnabrueck, O = GVM Users, CN = Ethical-Hacker-Kali.vm
error 10 at 0 depth lookup: certificate has expired
error /var/lib/gvm/CA/clientcert.pem: verification failed
        OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
        ERROR: Your GVM certificate infrastructure did NOT pass validation.
        FIX: Run 'sudo runuser -u _gvm -- gvm-manage-certs -a'.

 ERROR: Your GVM-22.5.0 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.


┌──(kali㉿Kali)-[~]
└─$
```

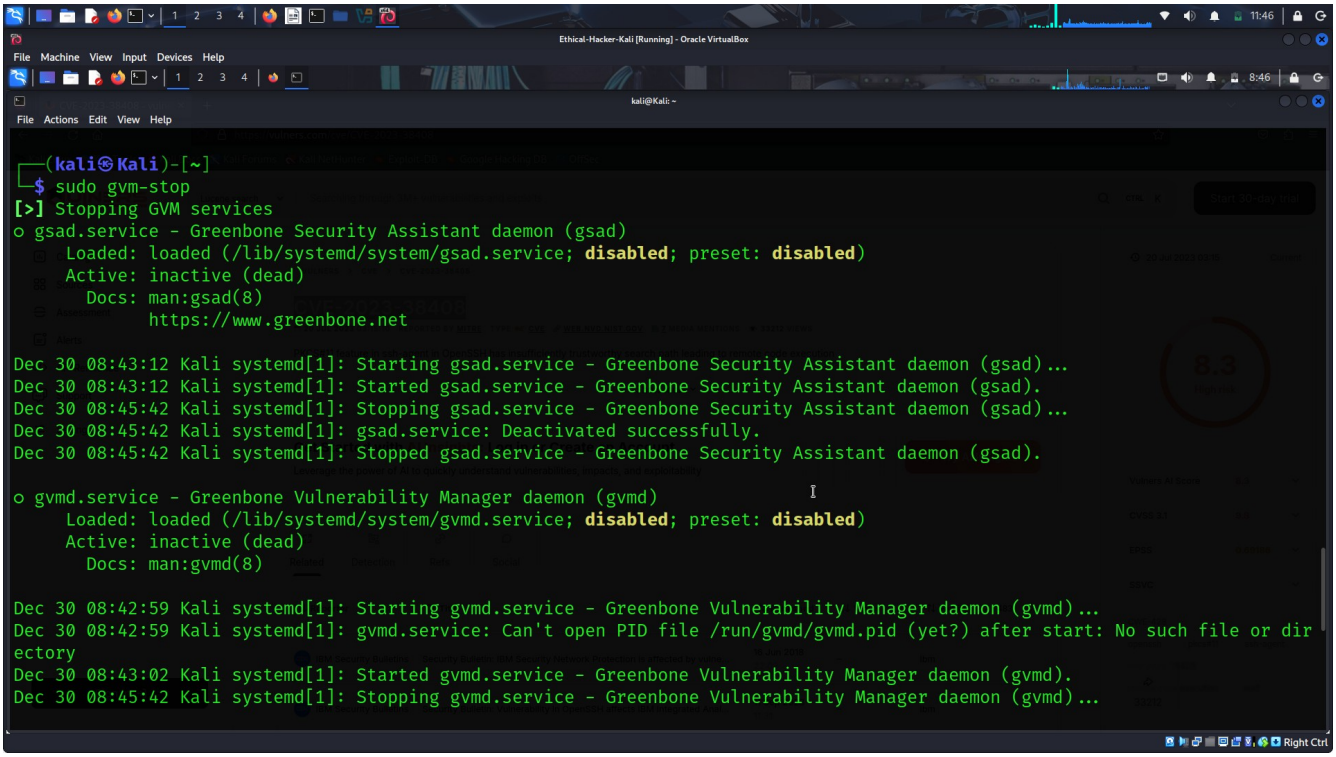
If there are issues, execute the suggested command to fix the problem

```
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
┌──(kali㉿Kali)-[~]
└─$ sudo runuser -u _gvm -- gvm-manage-certs -a
Existing certificate infrastructure found, aborting.
Use '-f' parameter to overwrite existing certificates.

┌──(kali㉿Kali)-[~]
└─$ sudo runuser -u _gvm -- gvm-manage-certs -af
Generated private key in /tmp/tmp.szj2dhMrPG/cakey.pem.
Generated self signed certificate in /tmp/tmp.szj2dhMrPG/cacert.pem.
Installed private key to /var/lib/gvm/private/CA/cakey.pem.
Installed certificate to /var/lib/gvm/CA/cacert.pem.
Generated private key in /tmp/tmp.szj2dhMrPG/serverkey.pem.
Generated certificate request in /tmp/tmp.szj2dhMrPG/serverrequest.pem.
Signed certificate request in /tmp/tmp.szj2dhMrPG/serverrequest.pem with CA certificate in /var/lib/gvm/CA/cacert.pem to gene
rate certificate in /tmp/tmp.szj2dhMrPG/servercert.pem
Installed private key to /var/lib/gvm/private/CA/serverkey.pem.
Installed certificate to /var/lib/gvm/CA/servercert.pem.
Generated private key in /tmp/tmp.szj2dhMrPG/clientkey.pem.
Generated certificate request in /tmp/tmp.szj2dhMrPG/clientrequest.pem.
Signed certificate request in /tmp/tmp.szj2dhMrPG/clientrequest.pem with CA certificate in /var/lib/gvm/CA/cacert.pem to gene
rate certificate in /tmp/tmp.szj2dhMrPG/clientcert.pem
Installed private key to /var/lib/gvm/private/CA/clientkey.pem.
Installed certificate to /var/lib/gvm/CA/clientcert.pem.
Removing temporary directory /tmp/tmp.szj2dhMrPG.

┌──(kali㉿Kali)-[~]
```

and then re-run the **gvm-check-setup** command. When all issues are addressed, the command outputs the string "**It seems like your GVM [*version*] installation is OK.**"



b. Just for this activity, stop the GVM service so you can observe the startup output.



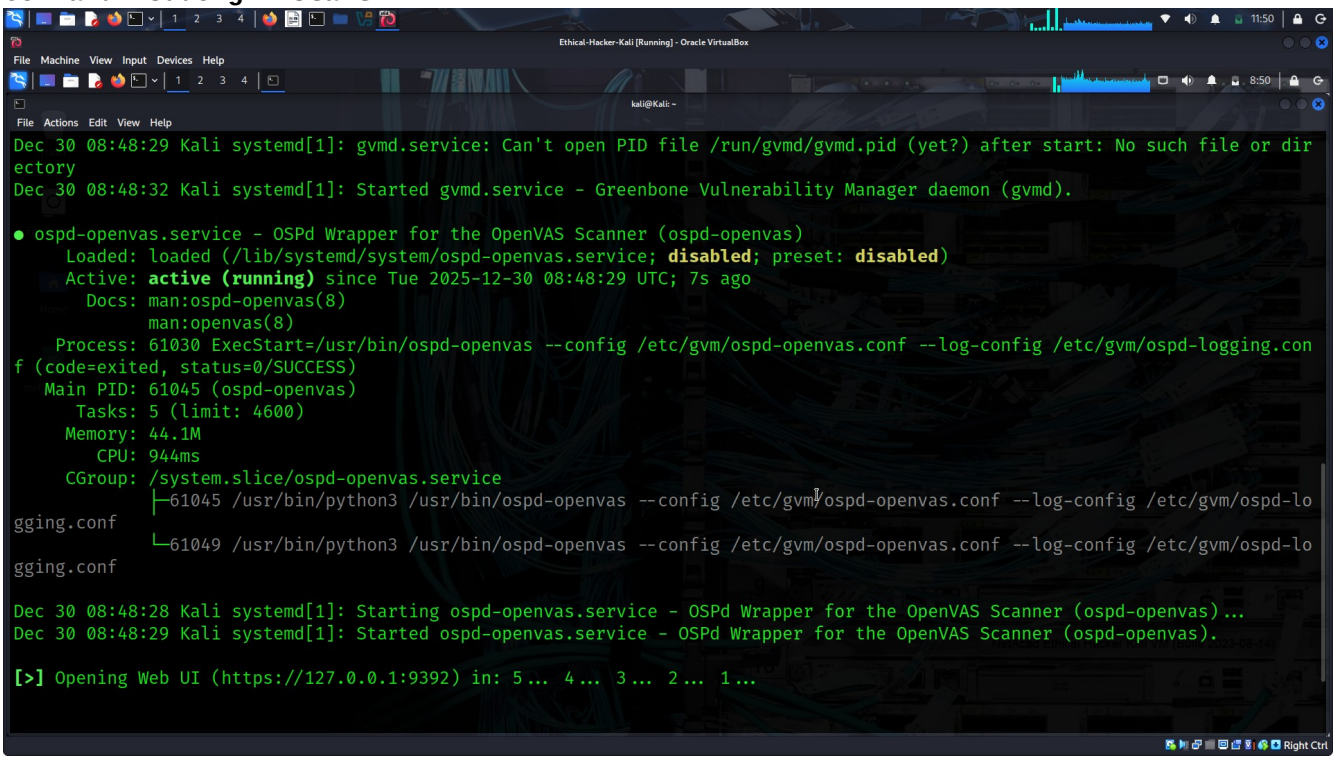
Step 2: Open the GVM Scanner GUI.

a. Start the GVM scanner using the **sudo gvm-start** command. You can also access the **gvm-start** script using the Applications menu on the Kali desktop, **Kali ->02-Vulnerability Analysis ->**

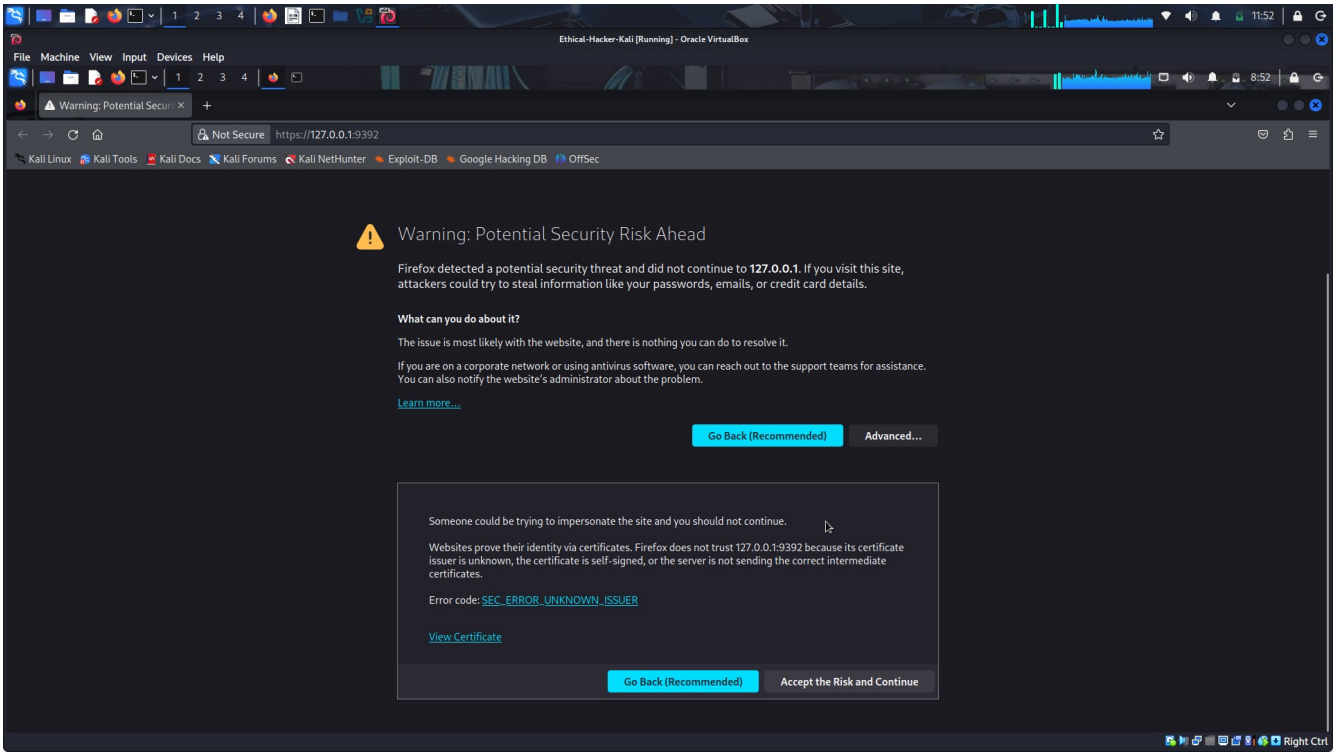
gvm start. It is possible that GVM may already be running as a result of the check setup process.

The output of the command should be similar to what is shown below. At the end of the output, a message that the scanner is loading in Firefox will appear.

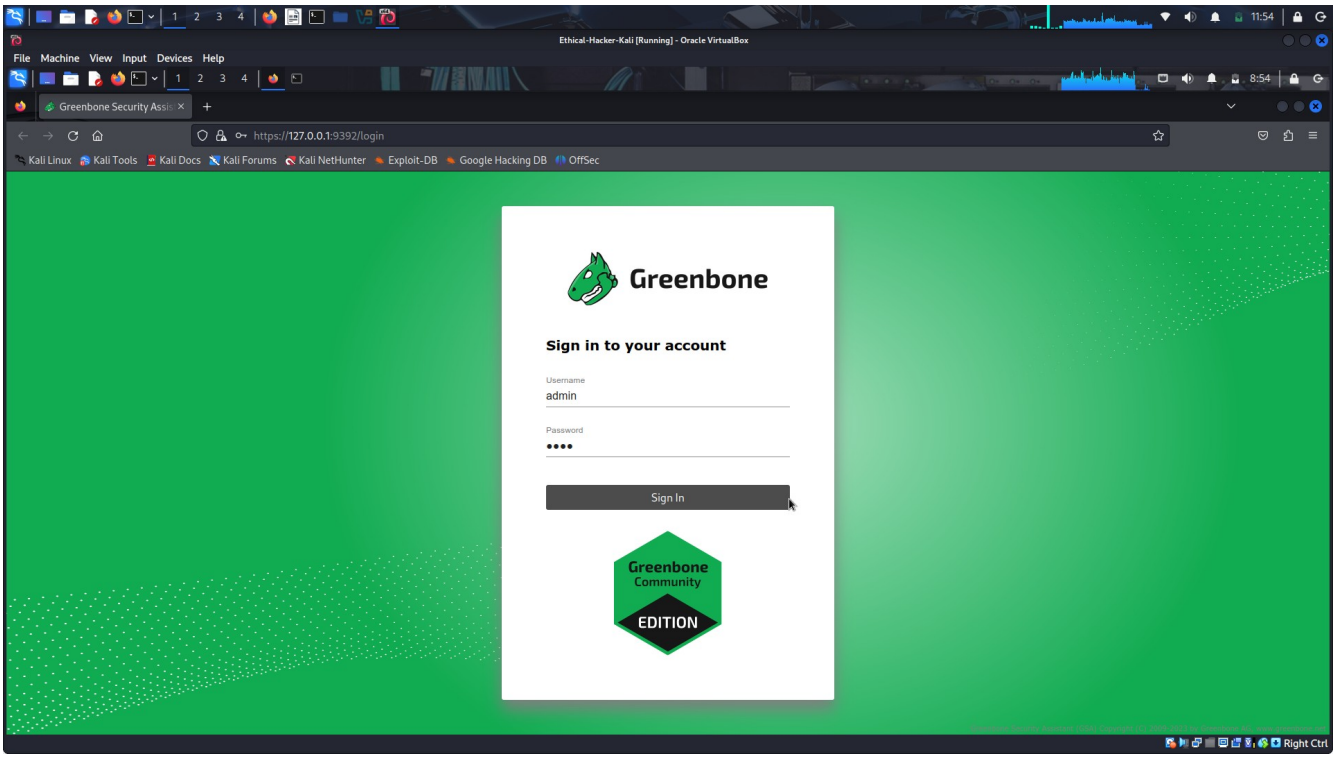
Command: sudo gvm-start



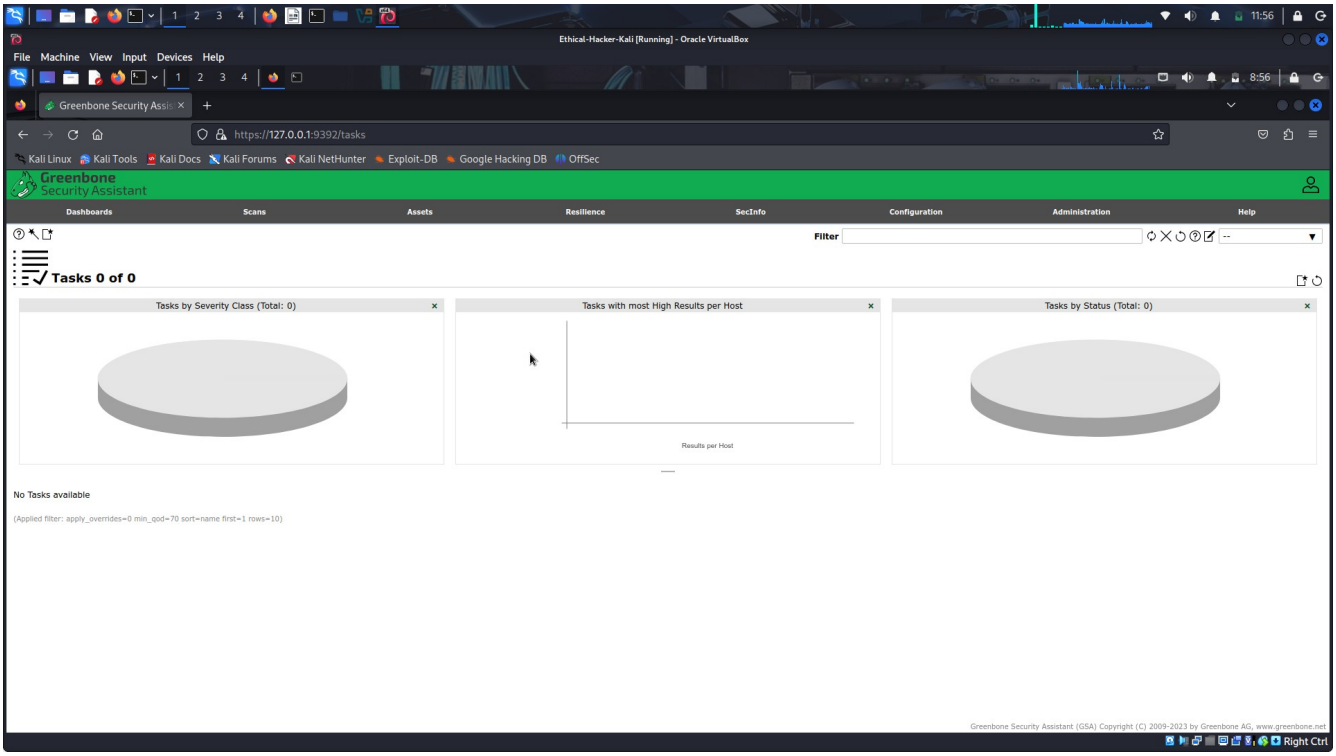
A browser window will open with a security warning that can be ignored. If the browser does not automatically open, start your browser manually and navigate to **https://127.0.0.1:9392**. Click the **Advanced** button and scroll down and accept the risk on the warning screen to proceed.



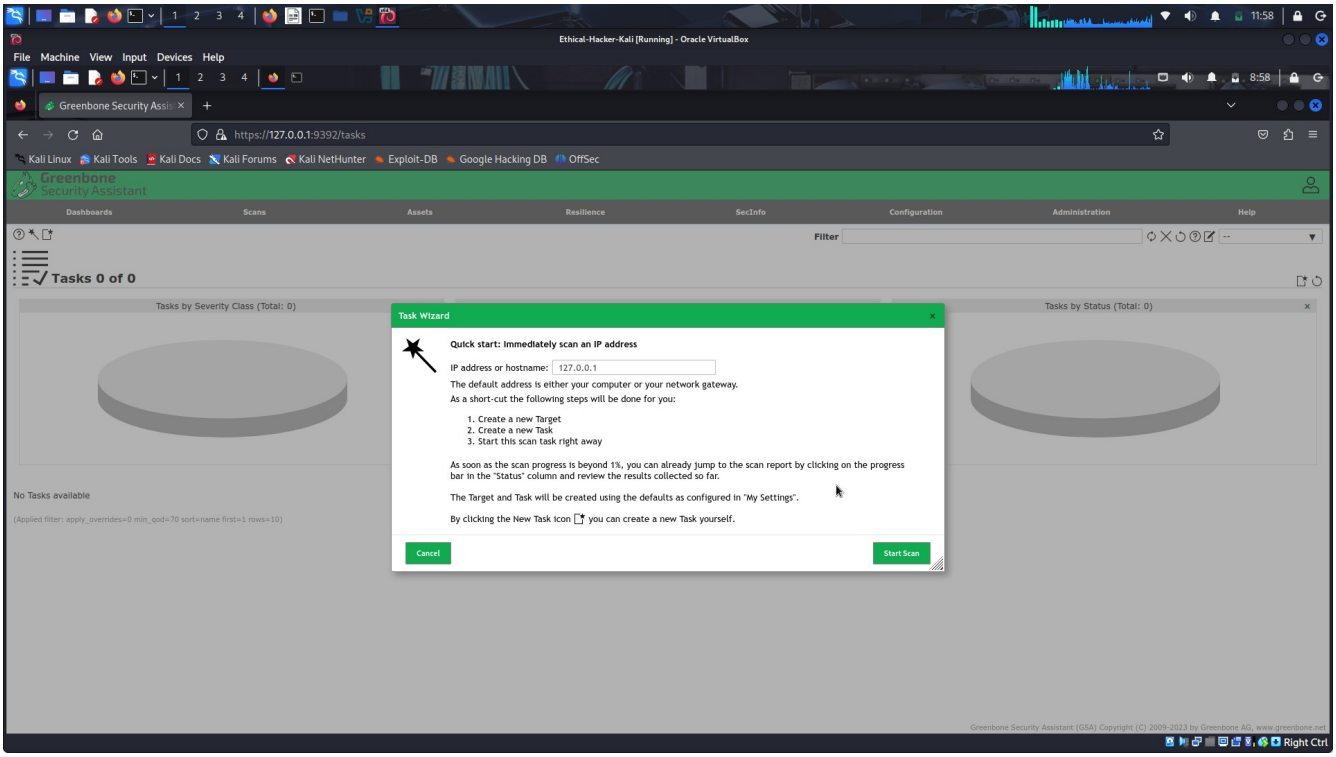
In the Greenbone Security Assistant login box, enter **admin** as the username and **kali** as the password.



The GVM Scanner application GUI should open in the browser. Select **Scans -> Tasks** from the menu bar. At the upper left of the **Tasks** window appear three icons.



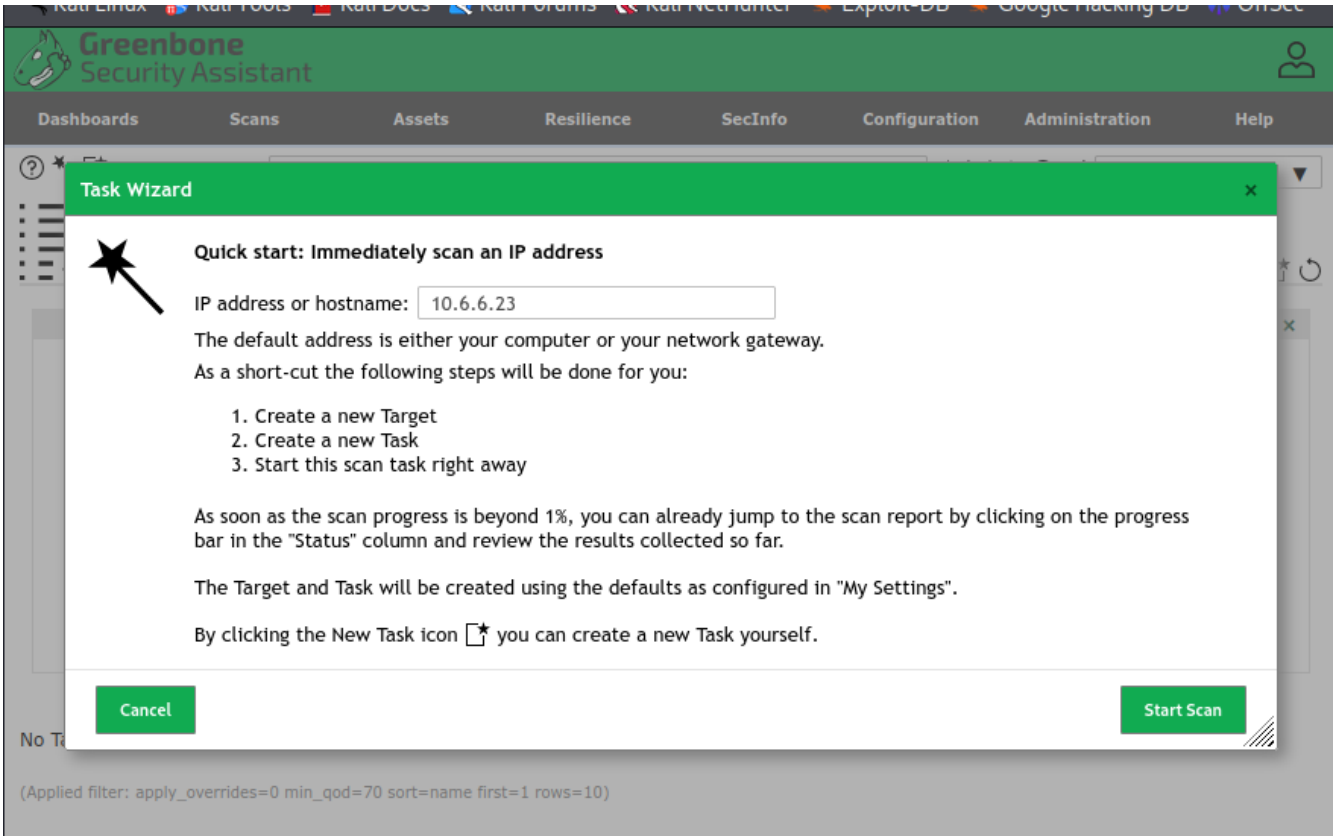
Select the **Task Wizard** icon that looks like a magic wand. Choose **Task Wizard** from the dropdown menu.



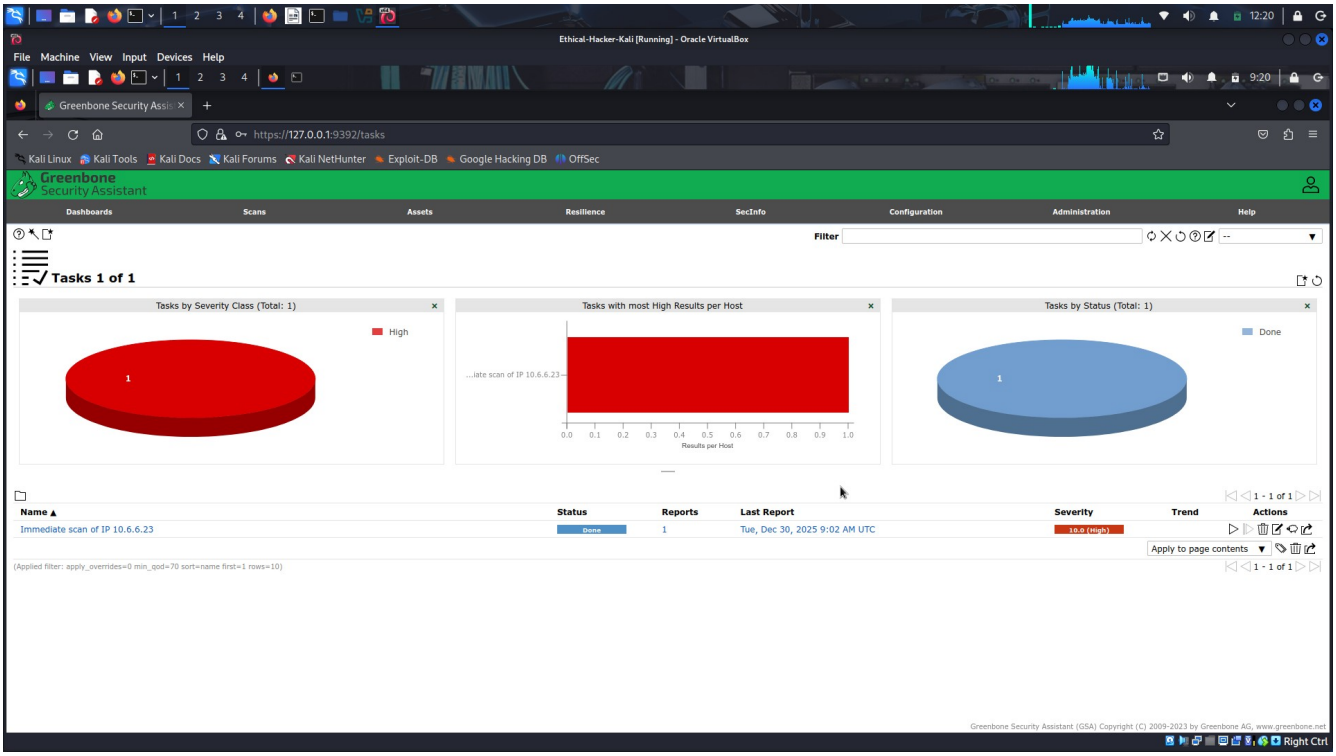
Step 3: Scan the Target Host for Vulnerabilities

In this step you will scan the same target computer for vulnerabilities that you did with the earlier Nmap scan.

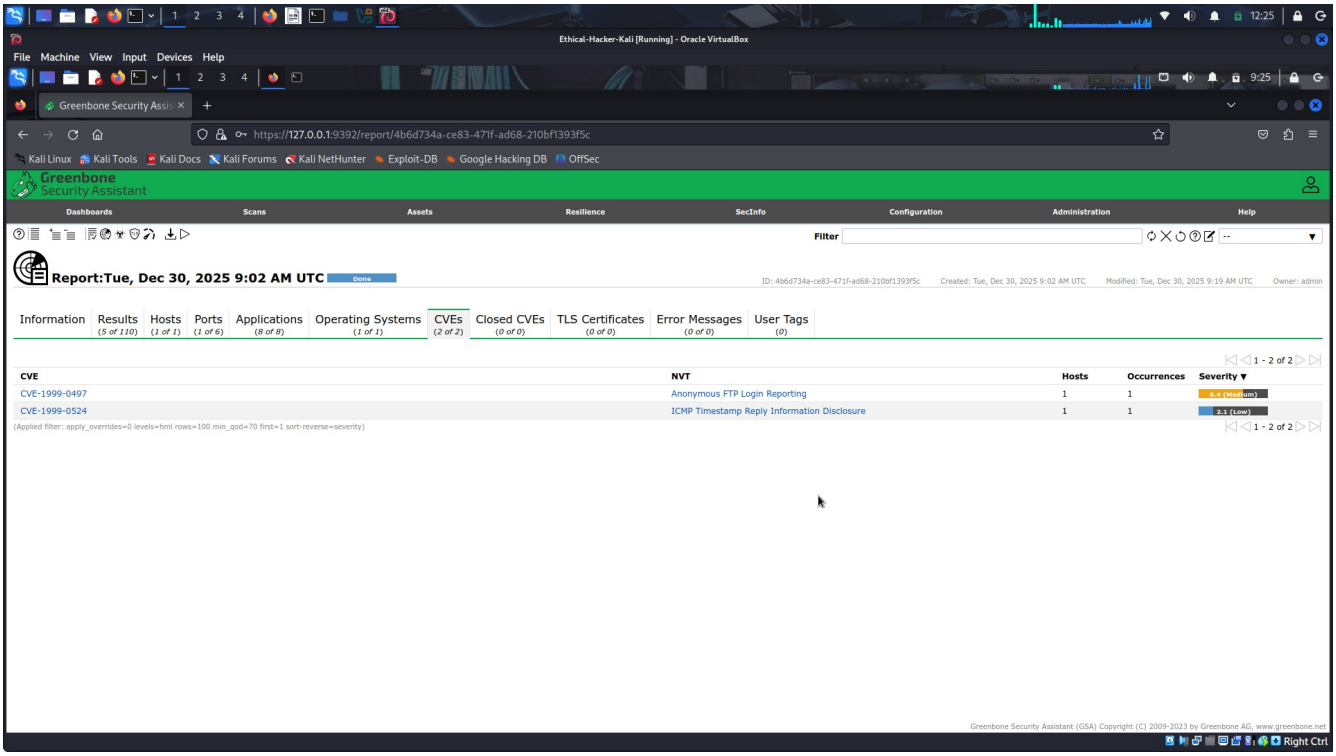
a. In the **IP address or hostname** box, enter the IP address **10.6.6.23** or **gravemind.vm**. Click the **Start Scan** button at the bottom of the screen.



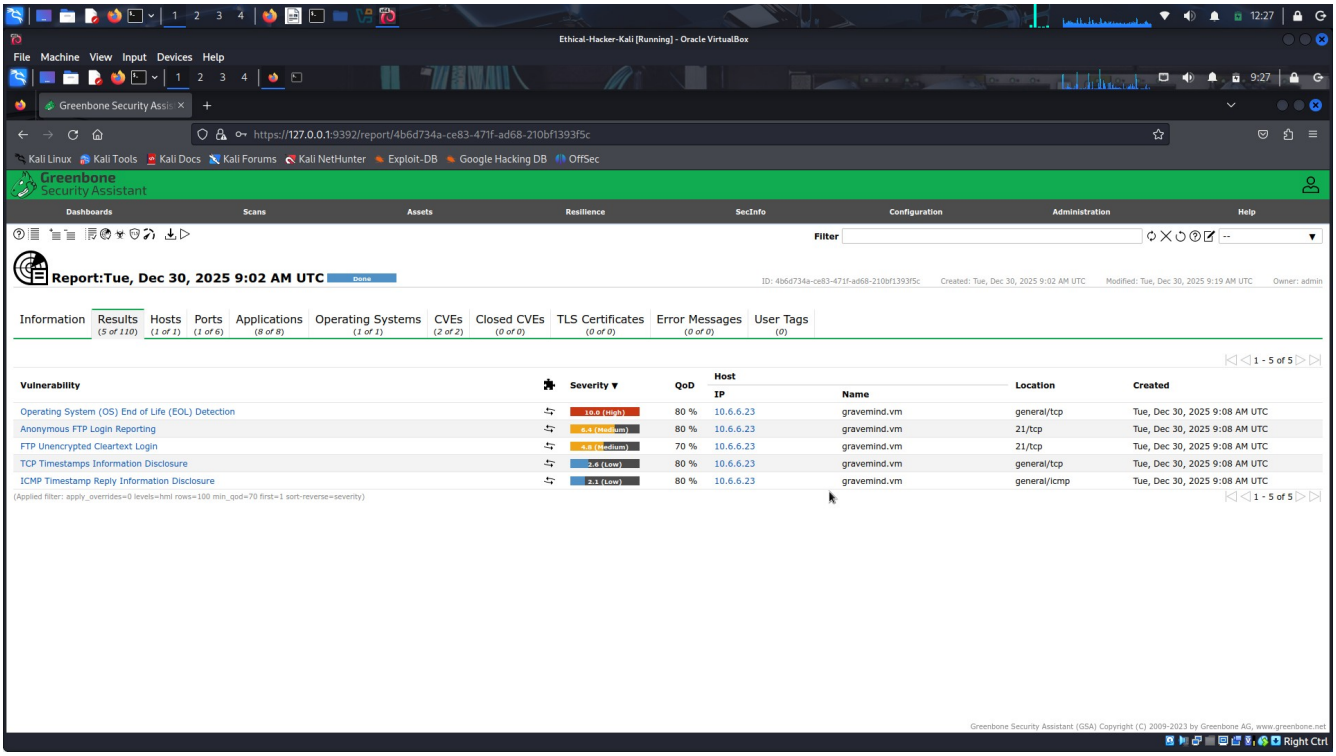
The scan will take a few minutes, so wait for it to complete. The status and percent complete are displayed on the screen. The scan will be finished when the status changes to **Done**.



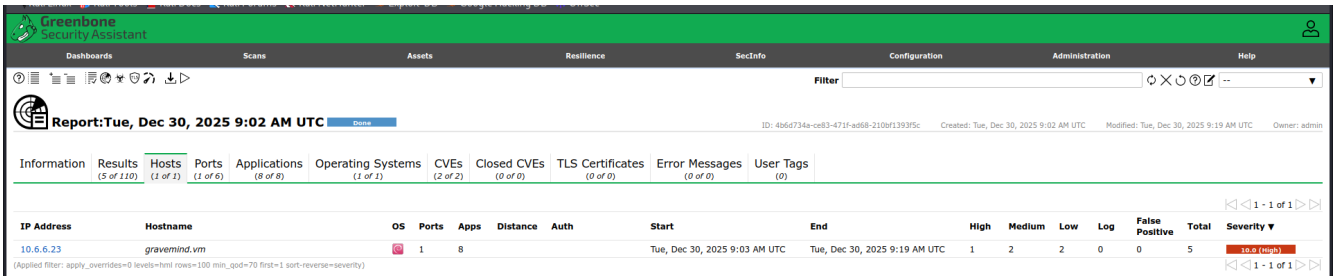
b. Click the number under the **Reports** column while the scanning is running for the associated scan.
c. When the scan is complete, click the timestamp under the **Date** column to view the report detail.
d. The CVEs associated with the vulnerabilities that were found on the host can be viewed by clicking the **CVEs** tab.



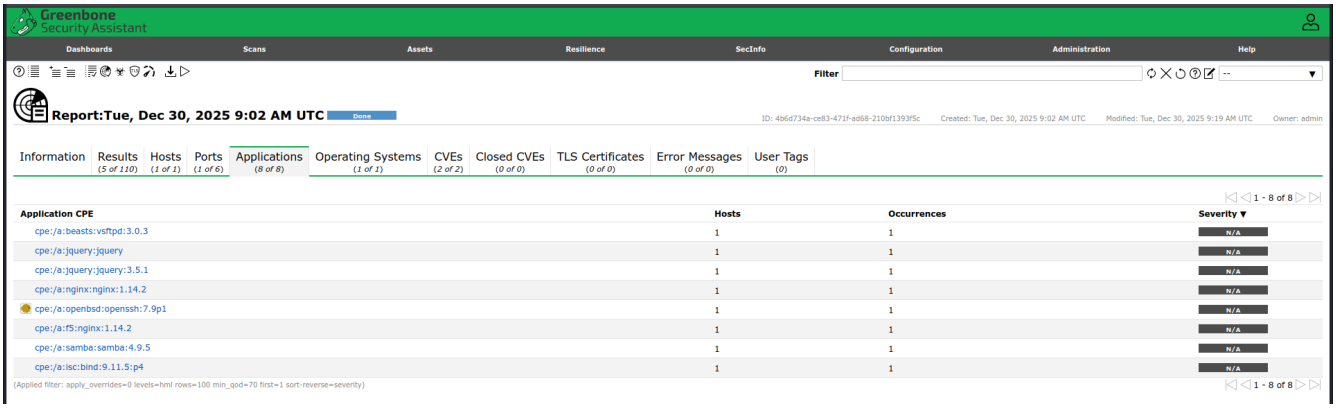
Explore the other tabs


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://127.0.0.1:9392/report/4b6d734a-ce83-471f-ad68-210bf1393f5c
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
Report:Tue, Dec 30, 2025 9:02 AM UTC
Information Results (5 of 110) Hosts (1 of 1) Ports (1 of 6) Applications (8 of 8) Operating Systems (1 of 1) CVEs (2 of 2) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)
Vulnerability Severity QoD Host IP Name Location Created
Operating System (OS) End of Life (EOL) Detection 10.0 (High) 80 % 10.6.6.23 gravemind.vm general/tcp Tue, Dec 30, 2025 9:08 AM UTC
Anonymous FTP Login Reporting 6.4 (Medium) 80 % 10.6.6.23 gravemind.vm 21/tcp Tue, Dec 30, 2025 9:08 AM UTC
FTP Unencrypted Cleartext Login 4.8 (Medium) 70 % 10.6.6.23 gravemind.vm 21/tcp Tue, Dec 30, 2025 9:08 AM UTC
TCP Timestamps Information Disclosure 2.6 (Low) 80 % 10.6.6.23 gravemind.vm general/tcp Tue, Dec 30, 2025 9:08 AM UTC
ICMP Timestamp Reply Information Disclosure 2.1 (Low) 80 % 10.6.6.23 gravemind.vm general/icmp Tue, Dec 30, 2025 9:08 AM UTC
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net
Right Ctrl

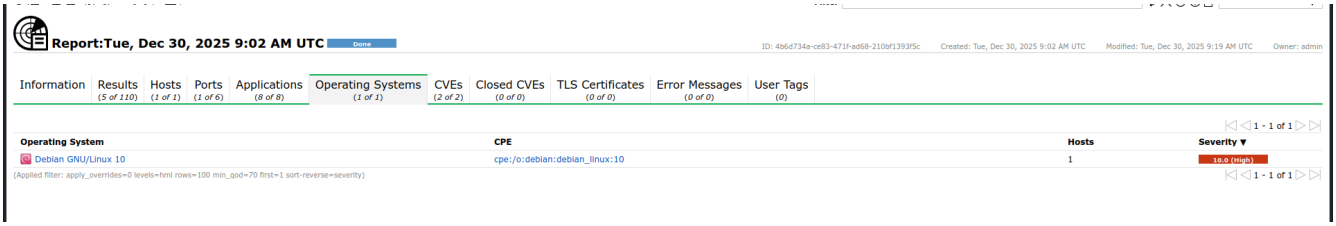
hosts


Greenbone Security Assistant
Report:Tue, Dec 30, 2025 9:02 AM UTC
Information Results (5 of 110) Hosts (1 of 1) Ports (1 of 6) Applications (8 of 8) Operating Systems (1 of 1) CVEs (2 of 2) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)
IP Address Hostname OS Ports Apps Distance Auth Start End High Medium Low Log False Positive Total Severity
10.6.6.23 gravemind.vm 1 8 Tue, Dec 30, 2025 9:03 AM UTC Tue, Dec 30, 2025 9:19 AM UTC 1 2 2 0 0 5 10.0 (High)

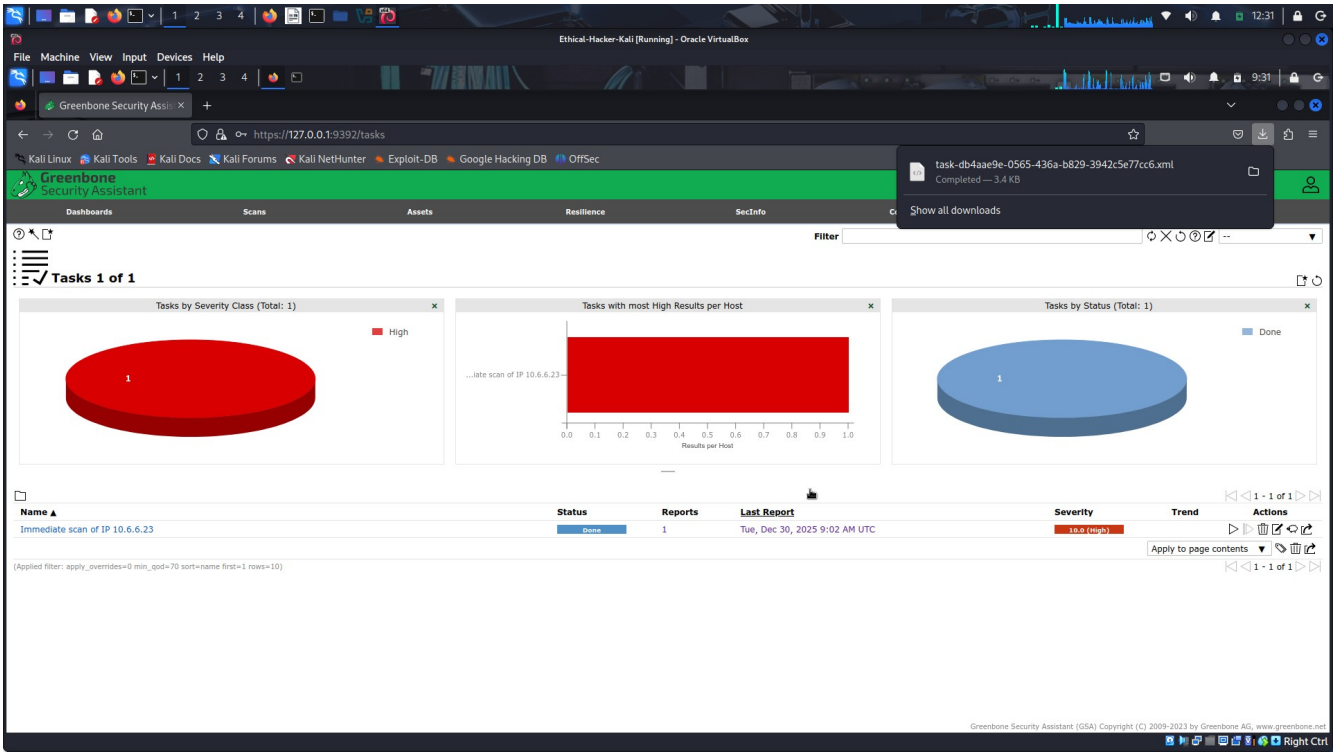
app:


Greenbone Security Assistant
Report:Tue, Dec 30, 2025 9:02 AM UTC
Information Results (5 of 110) Hosts (1 of 1) Ports (1 of 6) Applications (8 of 8) Operating Systems (1 of 1) CVEs (2 of 2) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)
Application CPE Hosts Occurrences Severity
cpe:/a:beasts:vsftpd:3.0.3 1 1 N/A
cpe:/a:jquery:jquery 1 1 N/A
cpe:/a:jquery:jquery:3.5.1 1 1 N/A
cpe:/a:nginx:nginx:1.14.2 1 1 N/A
cpe:/a:openbsd:openssh:7.9p1 1 1 N/A
cpe:/a:f5:nginx:1.14.2 1 1 N/A
cpe:/a:samba:samba:4.9.5 1 1 N/A
cpe:/a:isc:bind:9.11.5:p4 1 1 N/A

OS:



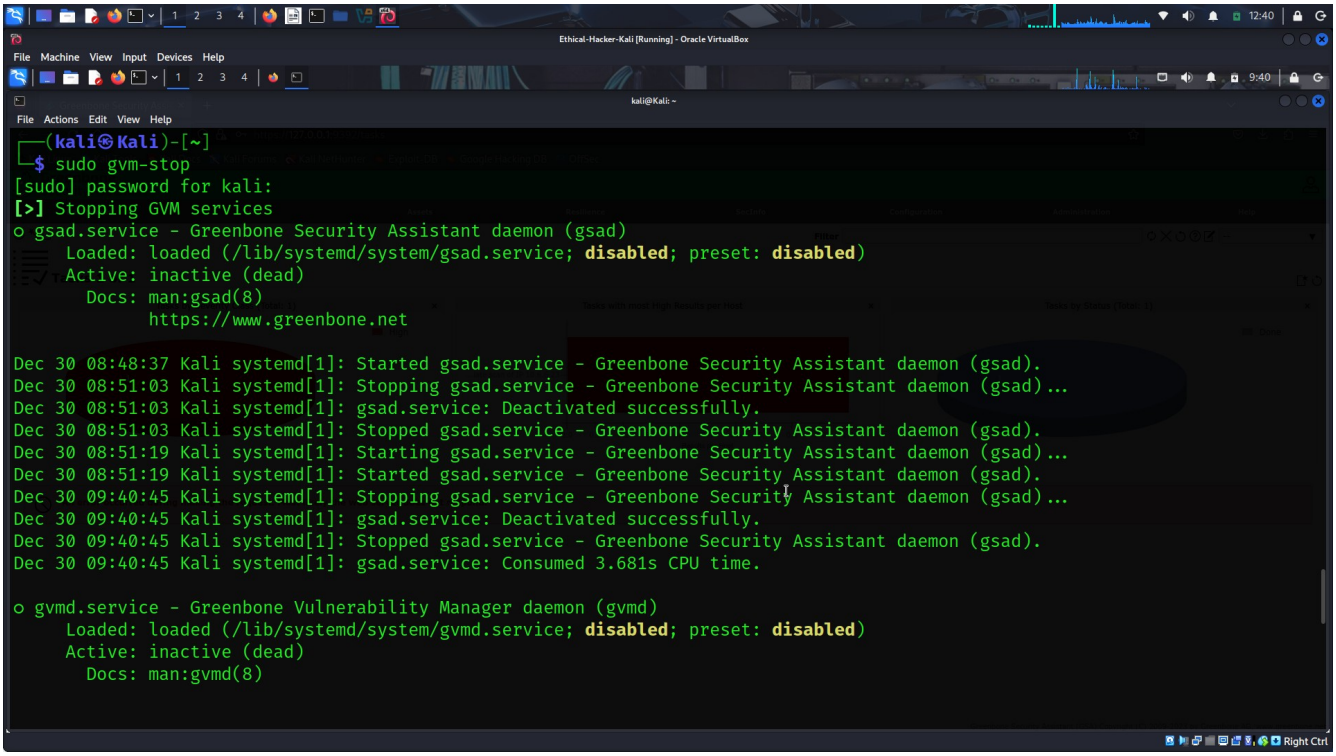
e. Download the report by clicking **the Download Filtered Report** button from the menu in the upper left of the report page. It has a downward-pointing arrow icon. In the settings box, choose to download the report in PDF format. After a brief delay, the PDF file should open in your browser.



Are the CVEs reported by GVM the same as the CVEs reported by the Nmap scan? **No. The two scanning tools may use different vulnerability databases to make their identifications.**

Step 4: Clean Up

When you are done with GVM services, use the following command to stop GVM. **sudo gvm-stop**



NOTE: New exploits and vulnerabilities are discovered every day. Not all systems are patched and up-to-date on security. Therefore, it is necessary to keep both new and older CVEs in the database.