Greenbone

Sign in to your account

Username

Password

Sign In

Lab - Using the GVM Vulnerability Scanner

Objectives

In this lab, you will complete the following objectives:

- Part 1: Scan a Host for Vulnerabilities
- Part 2: Exploit a Vulnerability Found by GVM

Background / Scenario

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.

In this lab you will scan a well-known vulnerable host, Metasploitable, and then determine how to formulate attacks to take advantage of the vulnerabilities.

Required Resources

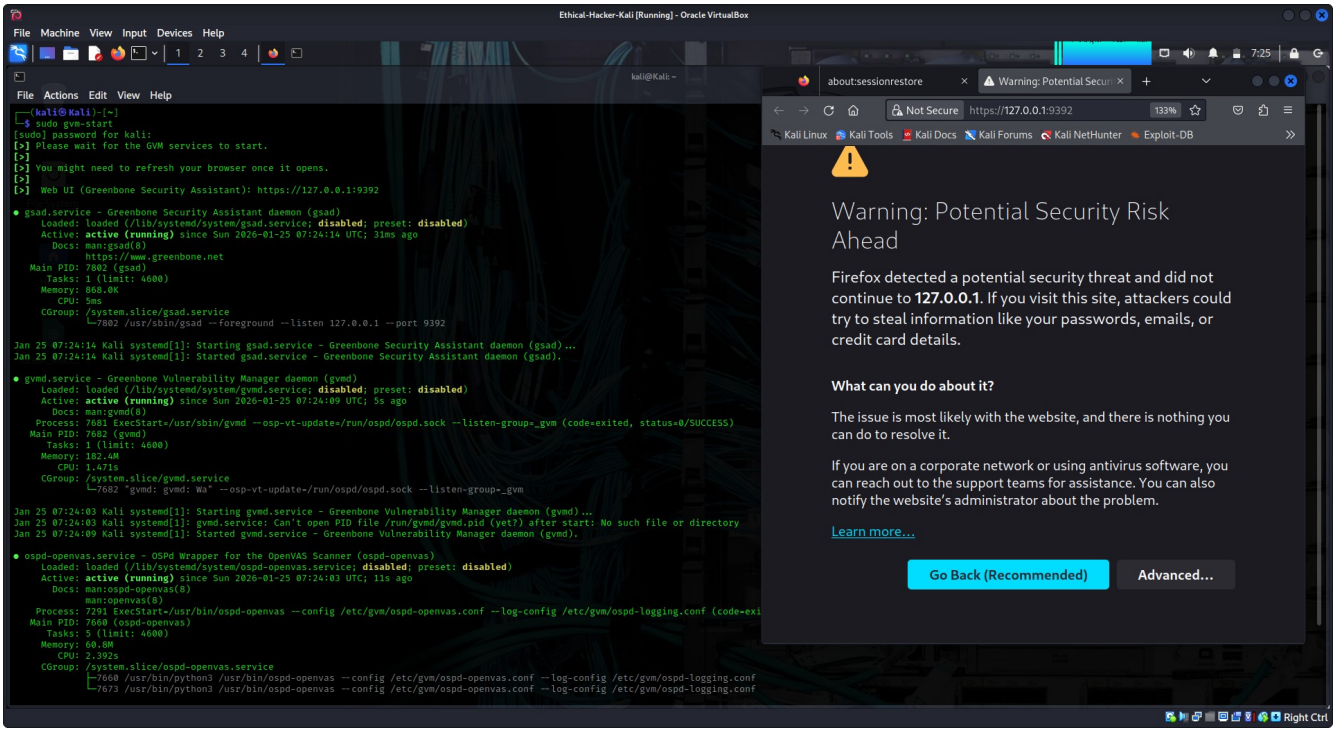
- Kali VM customized for the Ethical Hacker course
- Internet access

Instructions

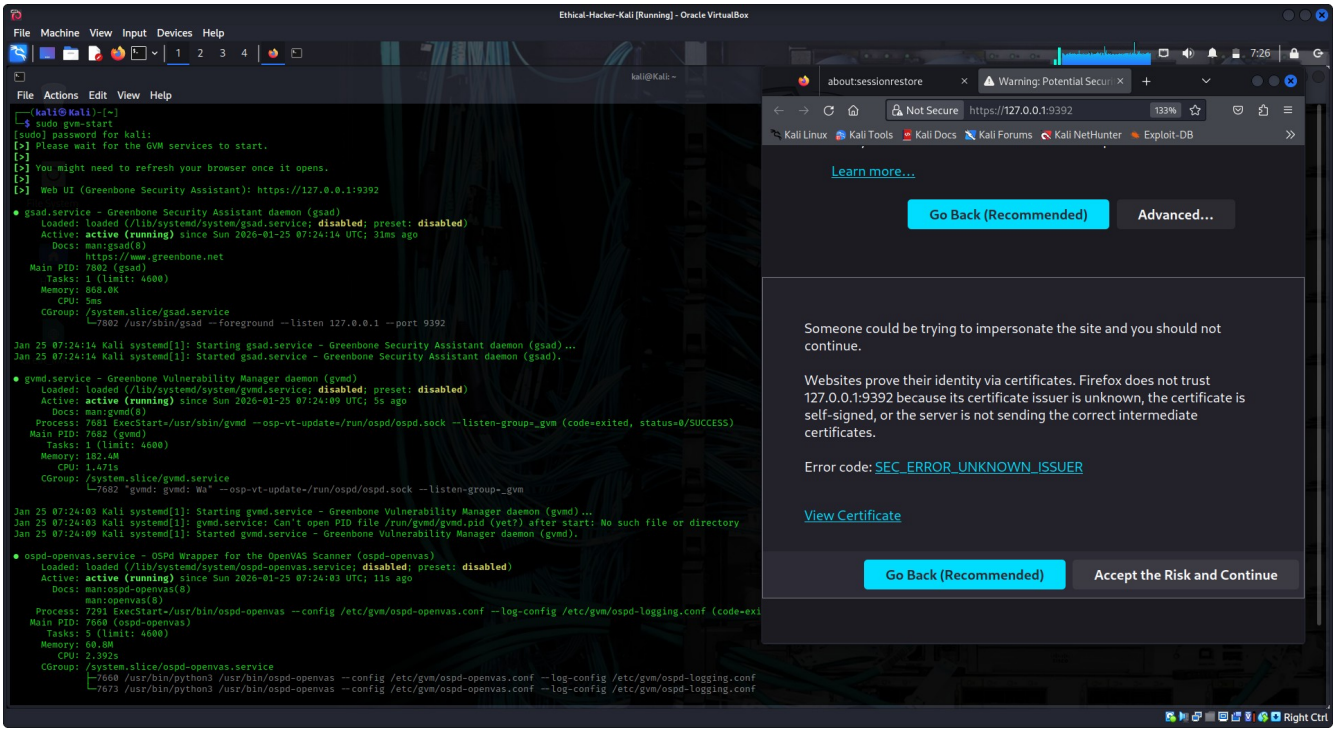
Part 1: Scan a Host for Vulnerabilities

Step 1: Start GVM services.

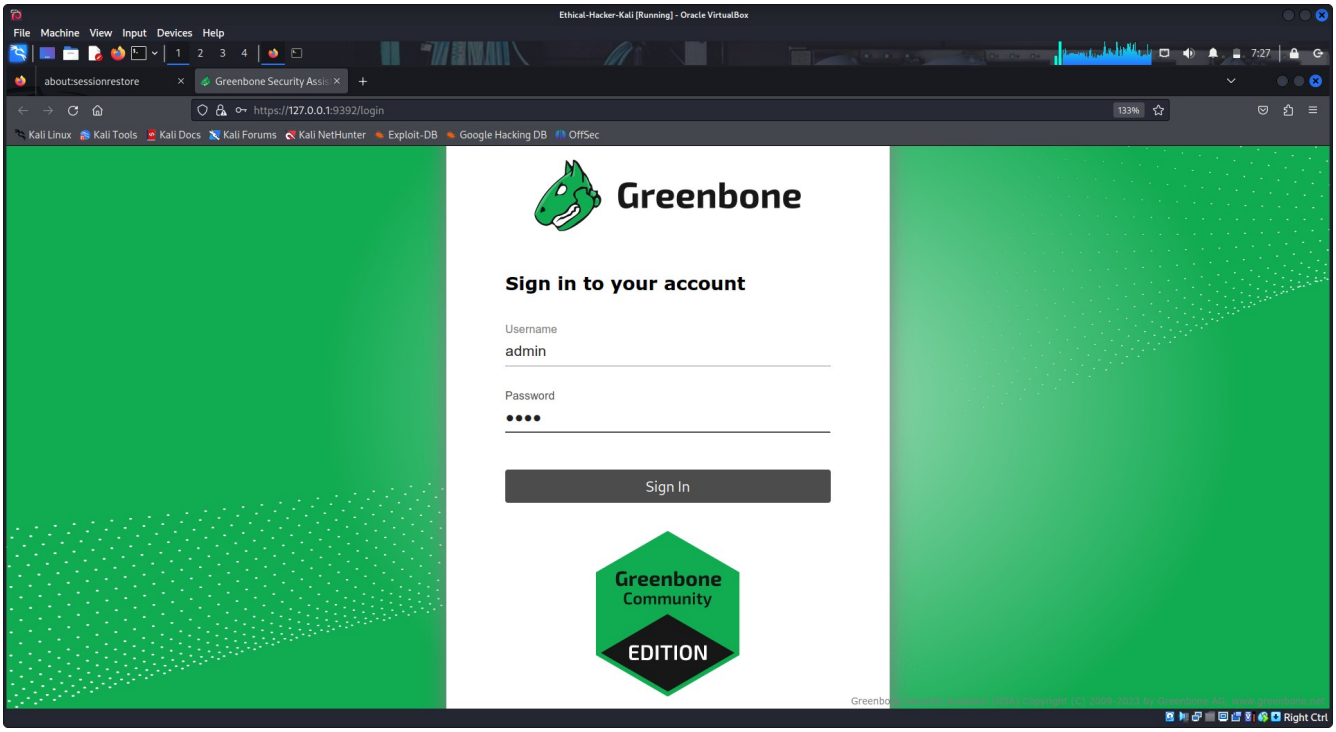
a. Start the GVM scanner using the **sudo gvm-start** command. You can also access the **gvm-start** script using the Applications menu on the Kali desktop, **Kali ->02-Vulnerability Analysis -> gvm start**.



You will receive a warning pop up on your browse, click on **Advanced** then click on **Accept Risk and Continue**



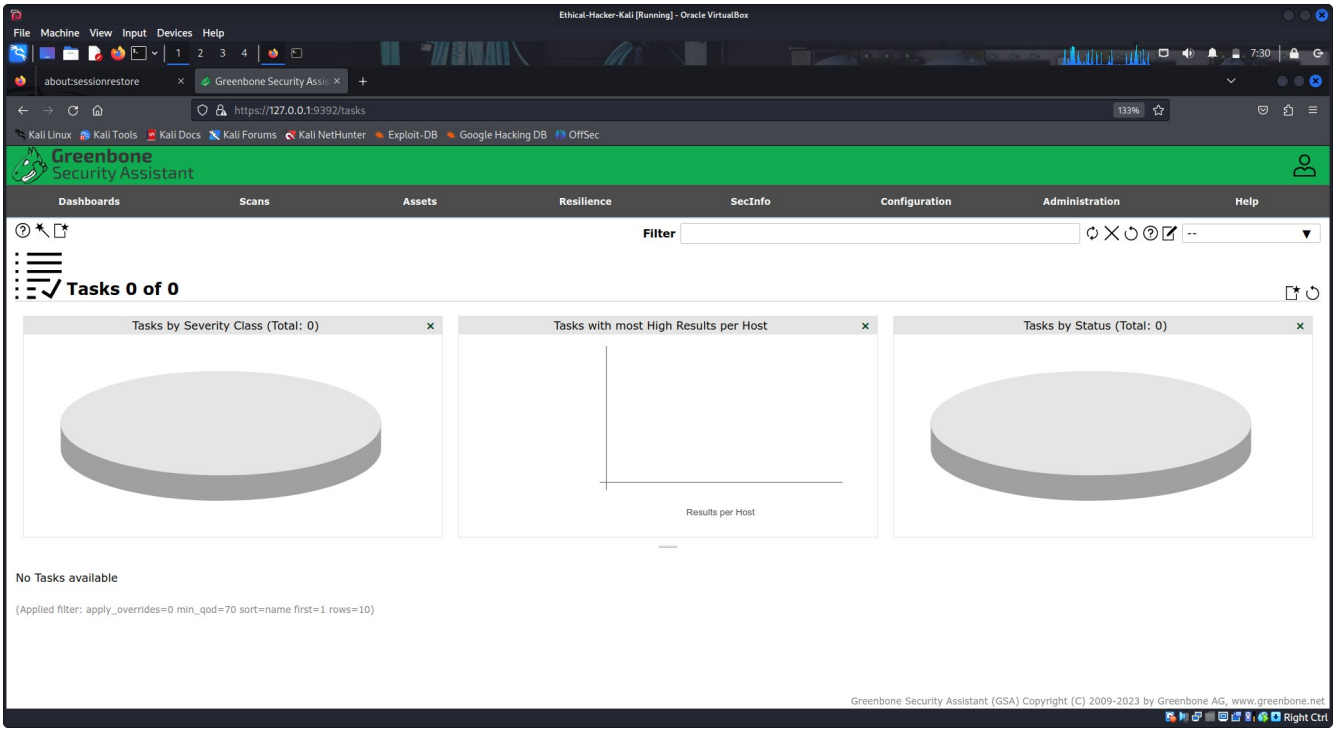
In the Greenbone Security Assistant login box, enter **admin** as the username and **kali** as the password.



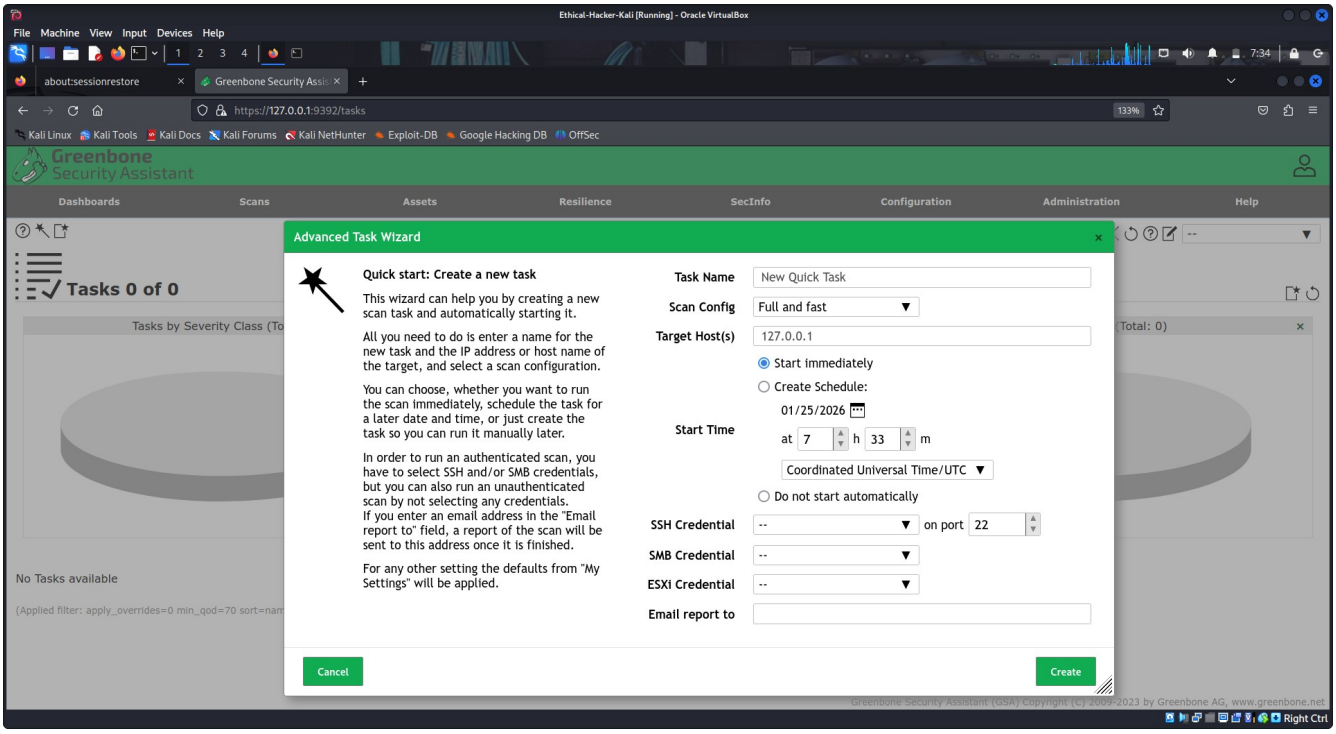
Step 2: Scan a host.

In this step, you will scan the Metasploitable vulnerable host using the GVM scanner. This scan may take some time, so be prepared to wait at least 20 or more minutes for it to complete.

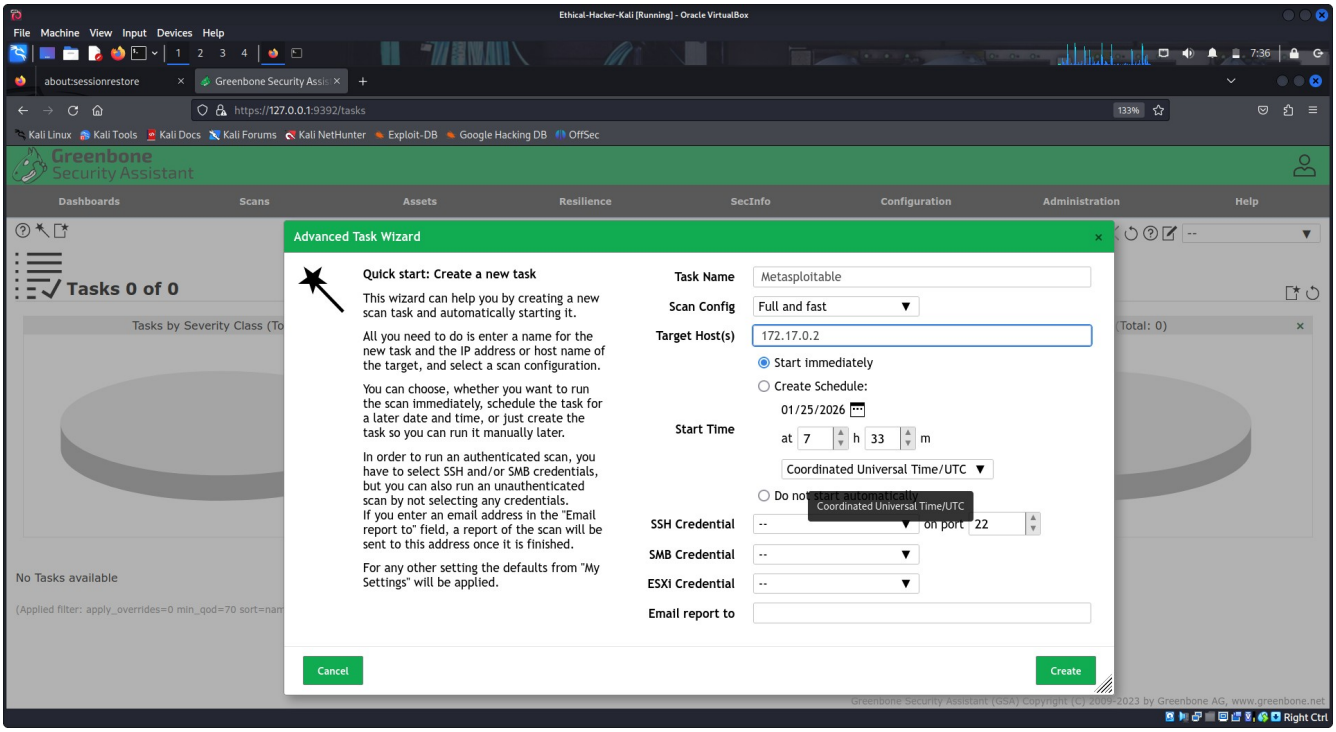
The GVM Scanner application GUI should open in the browser. Select **Scans -> Tasks** from the menu bar.



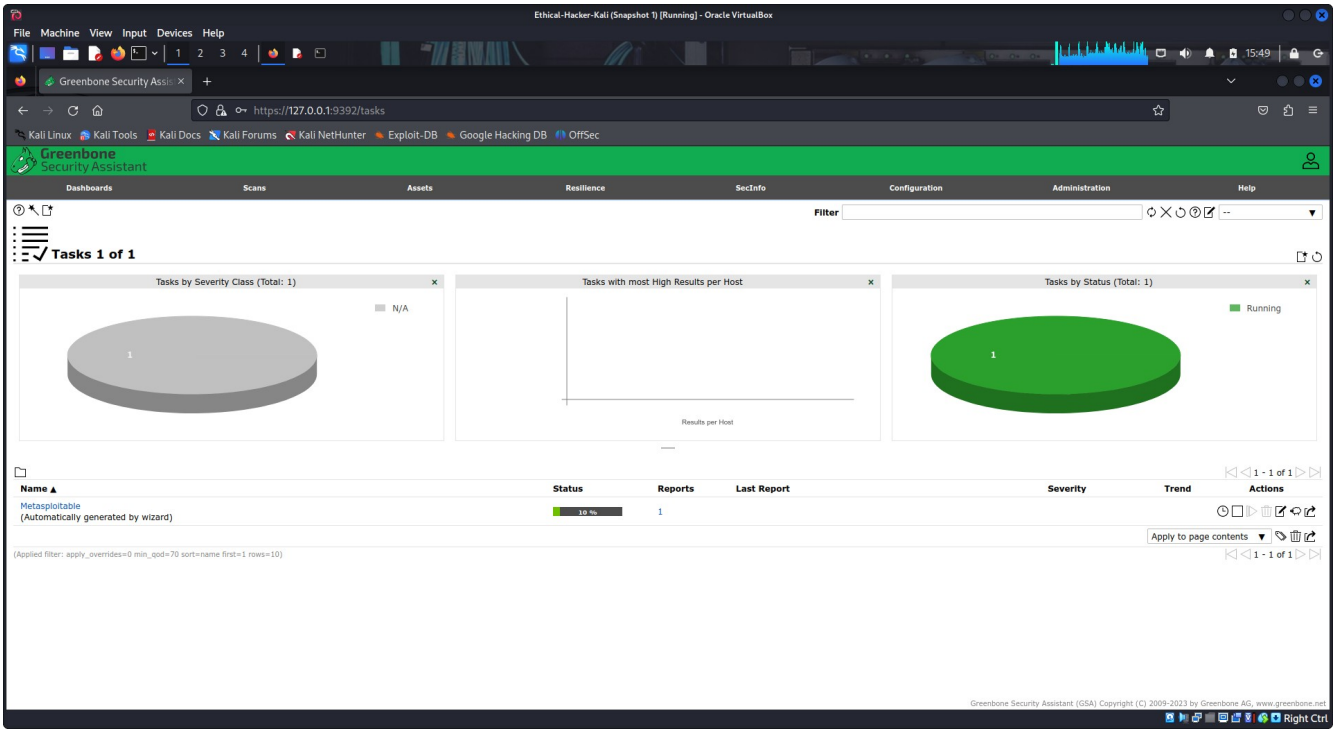
At the upper left of the **Tasks** window appear three icons. Select the **Task Wizard** icon that looks like a magic wand. Choose **Advanced Task Wizard** from the dropdown menu.



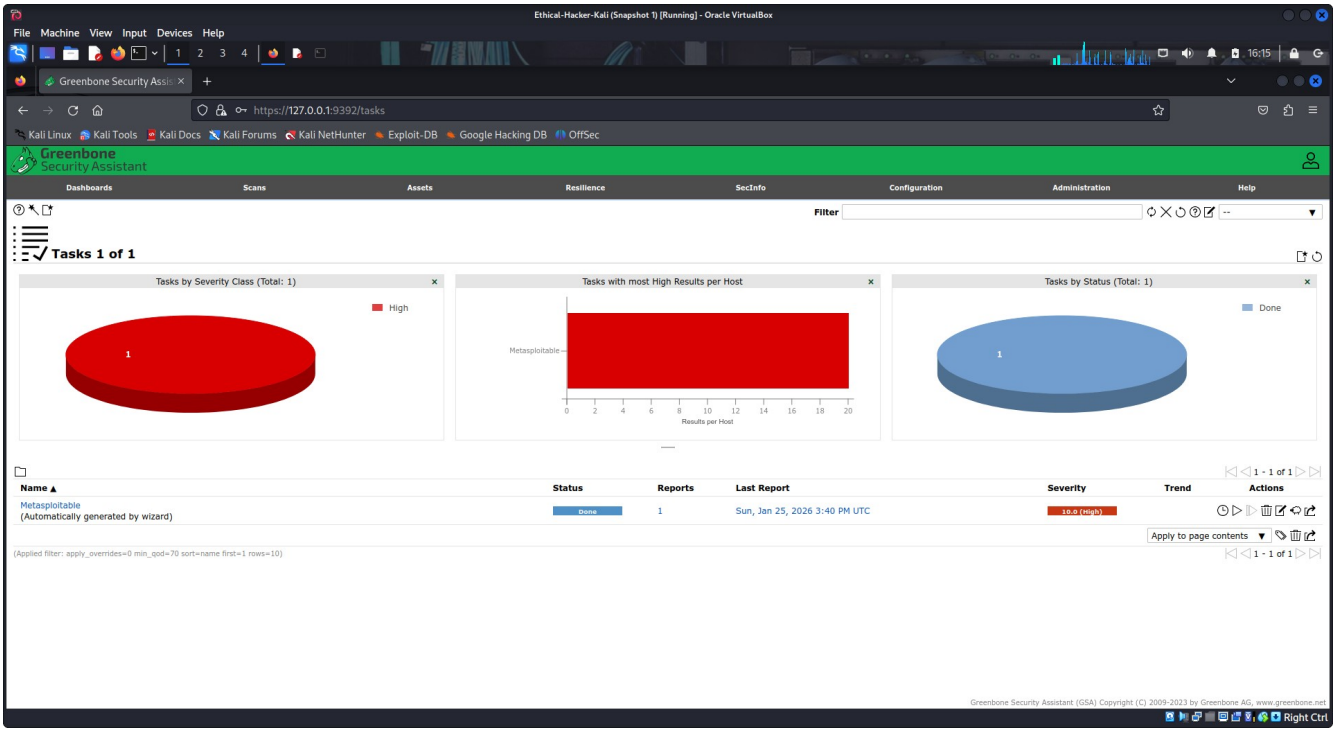
In the Advanced Task Wizard window, enter **Metasploitable** as the scan name. In the Target Host(s) field, enter the IP address of Metasploitable, **172.17.0.2**. Leave the rest of the settings unchanged and click **Create** to create the task and start the scan.



The Task window indicates the task is running. At the bottom of the window, the task Metasploitable is listed, and the status bar shows the percent complete.

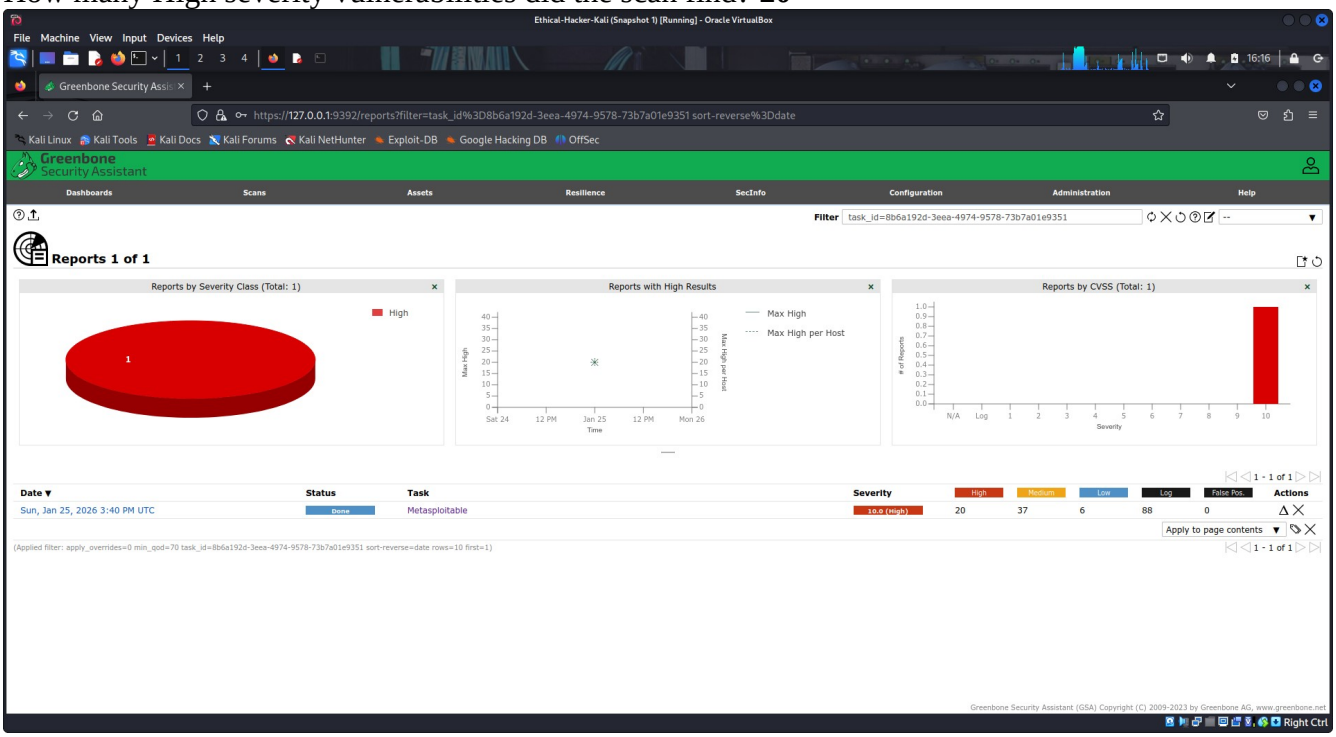


Wait until the status shows Done (100% complete). This could take 30 minutes or more.

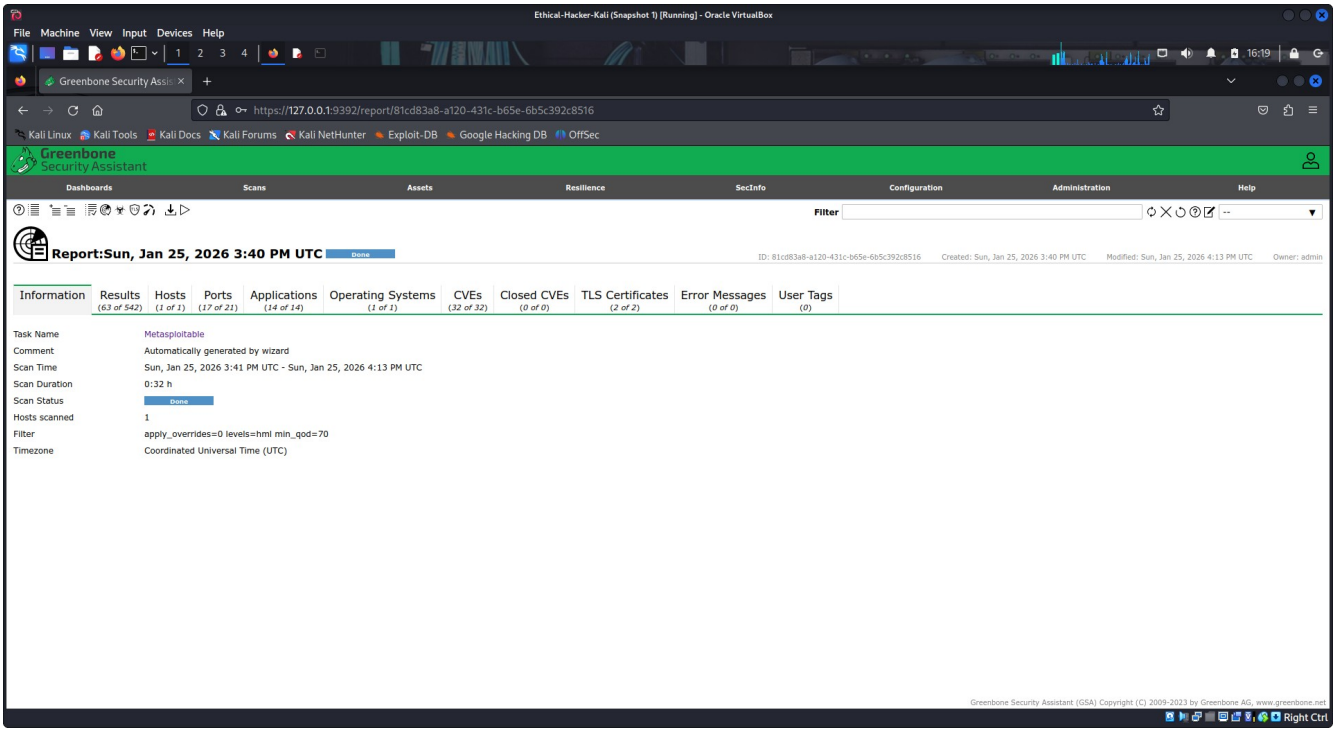


Click the number **1** under the Reports column in the Metasploitable row, next to the status indicator. The report list opens with an entry for the current day and time and the task named Metasploitable.

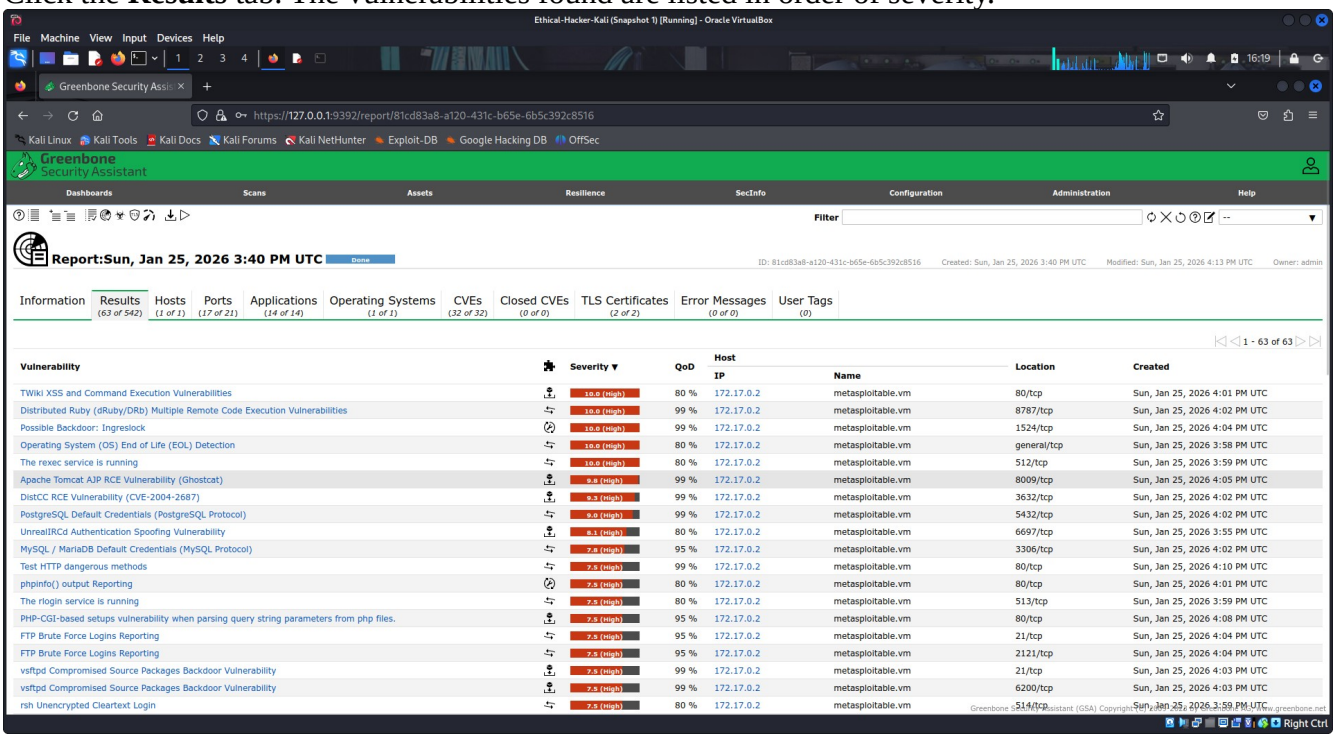
How many High severity vulnerabilities did the scan find? **20**



Open the report by clicking the **date and time link** under the Date column. The report window opens. There are eleven tabs that show various results that were found during the scan.



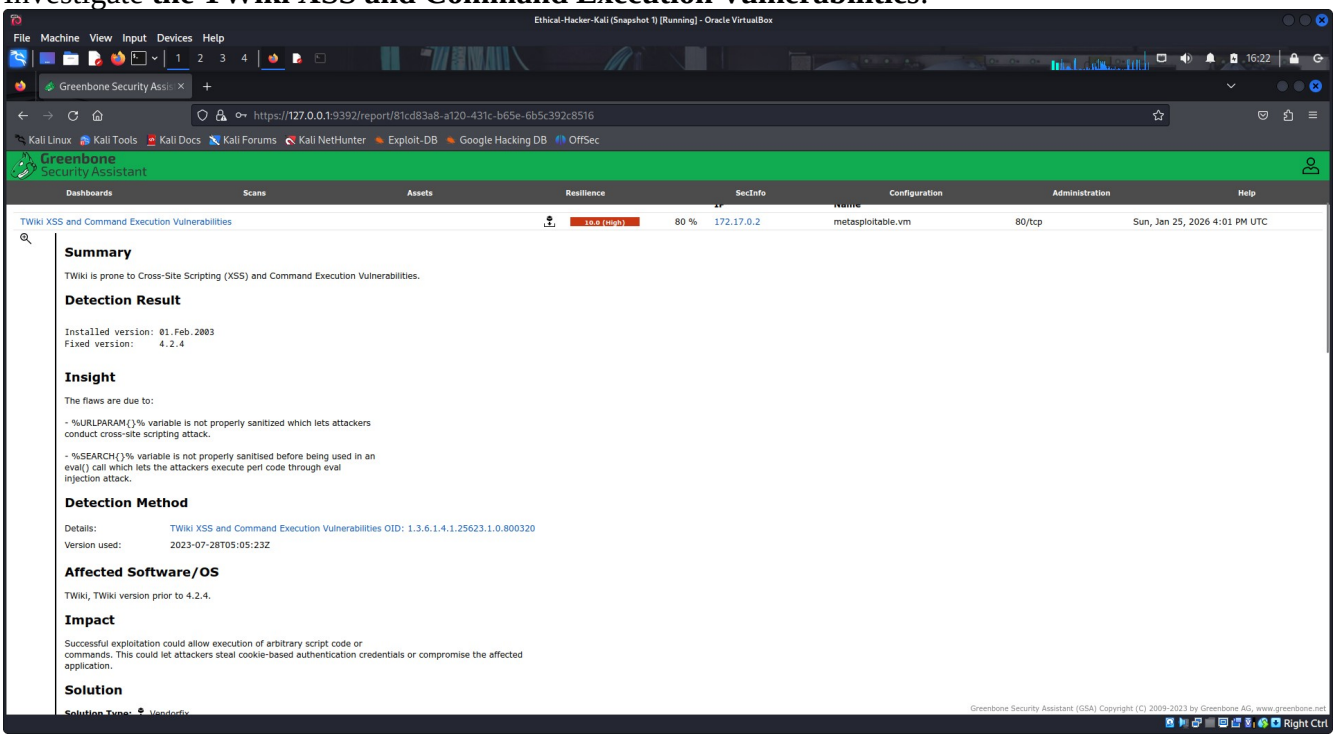
Click the **Results** tab. The vulnerabilities found are listed in order of severity.



What are some of the vulnerabilities with the highest severity score?

TWiki XSS and Command Execution Vulnerabilities
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
Possible Backdoor: Ingreslock
Operating System (OS) End of Life (EOL) Detection
The rexec service is running
Apache Tomcat AJP RCE Vulnerability (Ghostcat)
DistCC RCE Vulnerability (CVE-2004-2687)

For more information on a vulnerability, click it. GVM has explanations for the vulnerabilities it finds. Investigate **the TWiki XSS and Command Execution Vulnerabilities**.

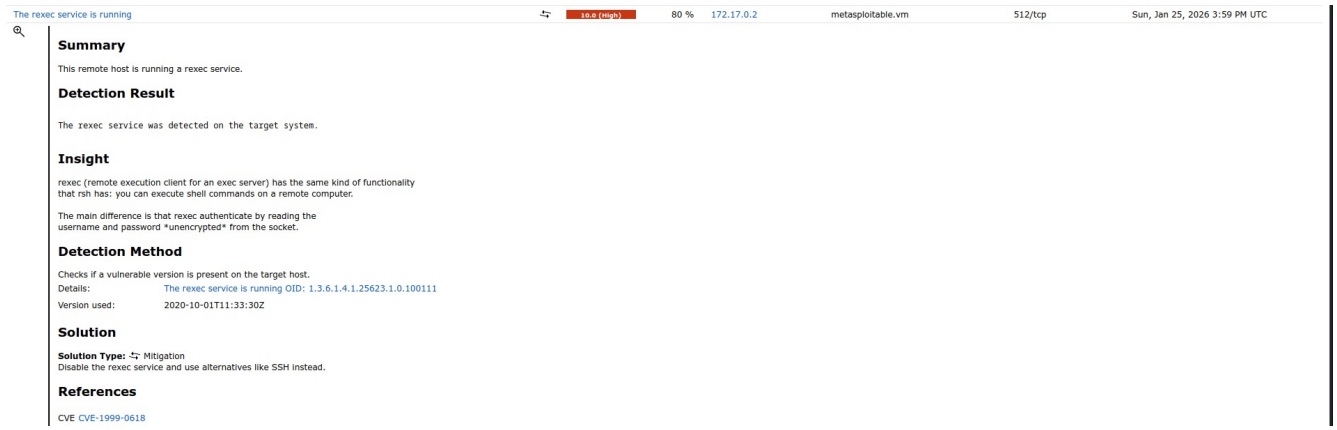


What is TWiki? How can this vulnerability be mitigated?
TWiki is an open-source enterprise wiki and web application platform. This vulnerability is present prior to version 4.2.4 of the software. Updating the software version will mitigate the vulnerability.

Step 3: Interpret the scan results.

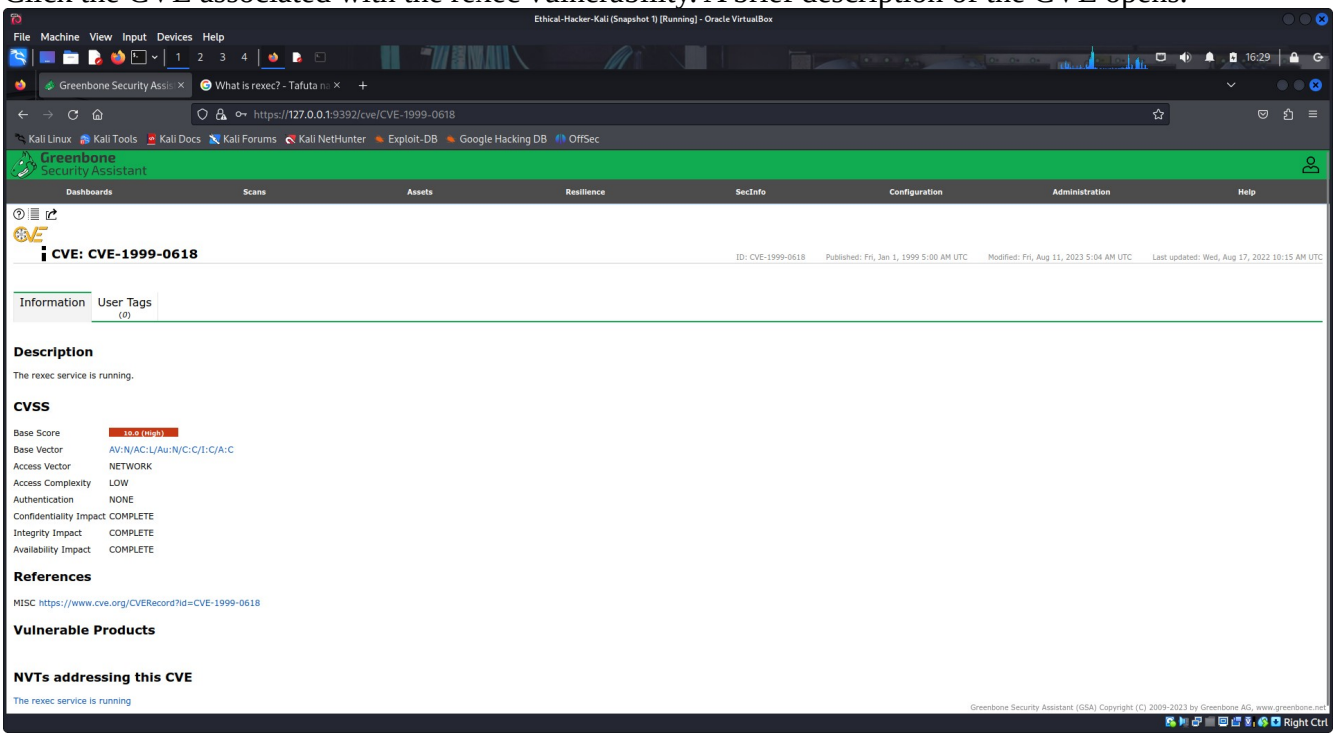
GVM provides a detailed description of the vulnerabilities including methods to mitigate each vulnerability.

a. Click the **The rexec service is running** vulnerability listed in the Results tab. GVM provides a summary of the finding and additional details. The Insight section explains a little about the vulnerability and the Solution section gives mitigation suggestions.



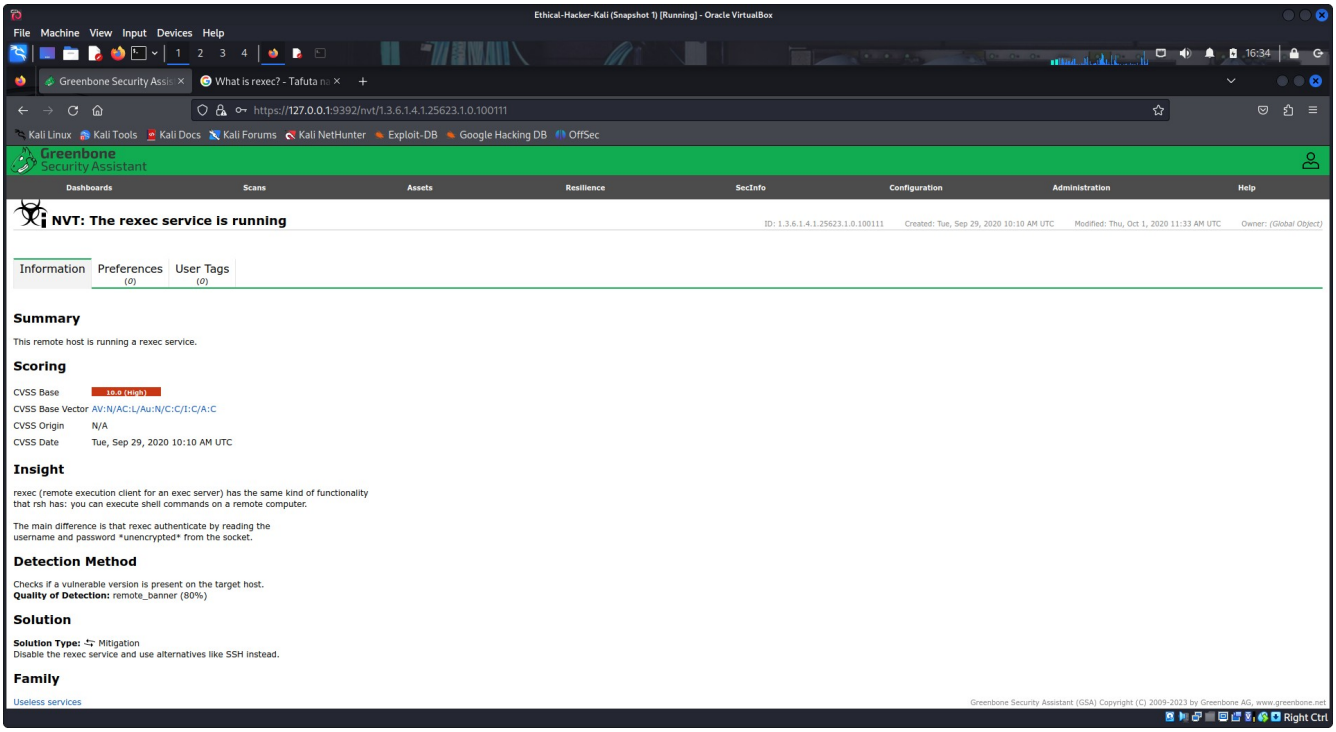
What is rexec? **Is an outdated and insecure command execution protocol that allows users to execute shell commands on a remote machine**

What is the suggested mitigation for the rexec vulnerability? **Disable the rexec service and use alternatives like SSH instead.**
Click the CVE associated with the rexec vulnerability. A brief description of the CVE opens.



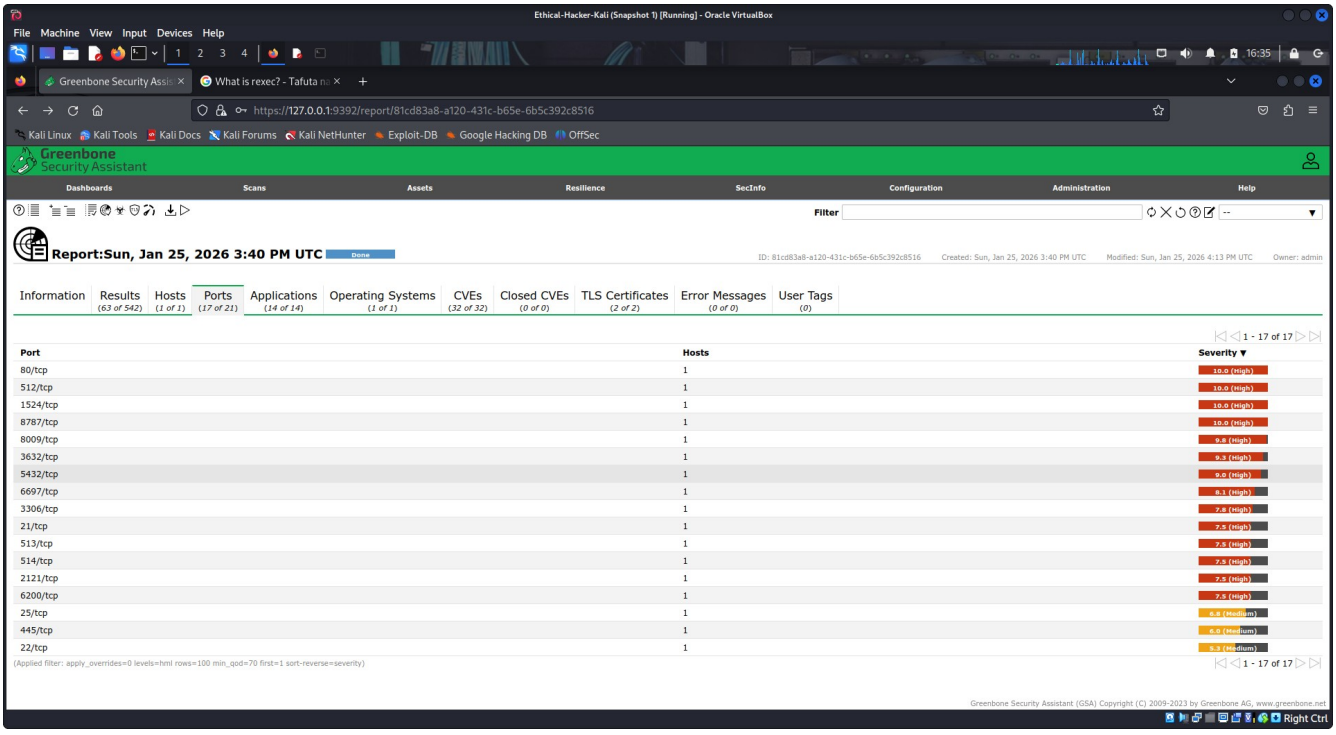
What is the CVSS Access Complexity rating of this vulnerability? Does this mean it is easy or difficult to exploit this vulnerability? **low: meaning it is easy to exploit**

You can obtain additional information about the **Network Vulnerability Test (NVT)** that discovered this CVE by clicking the NVT at the bottom of the CVE window. An **NVT** is a script that can be executed to check for specific vulnerabilities, including CVEs.



Click the back arrow in the browser to return to the report screen. The rexec services typically run on TCP ports 512, 513, or 514.

What rexec port is currently open on the Metasploitable system? **512**
Select the Ports tab to view the open ports on the Metasploitable system.
Are SMB services currently running on the client? How do you know? **Yes, port 445 is open**



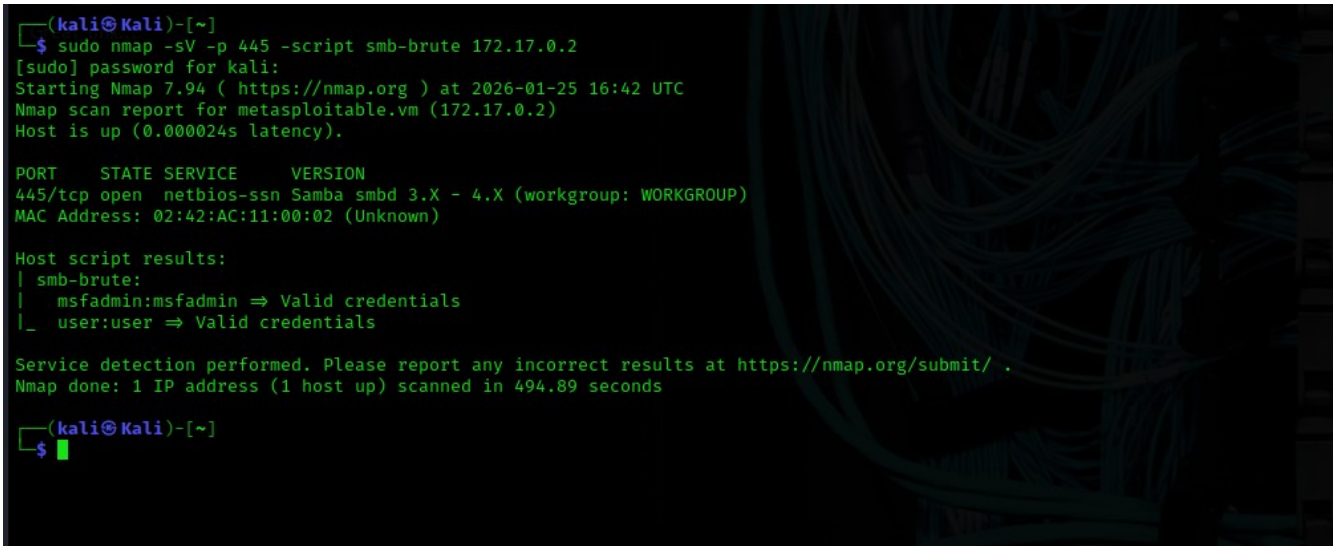
Part 2: Exploit a Vulnerability Found by GVM

After a vulnerability is discovered with the GVM scanner, it is possible to formulate an attack strategy to exploit a vulnerability. You discovered and investigated a rexec vulnerability. In this part, you will formulate an attack strategy and perform an exploit against the target.

Step 1: Perform reconnaissance against the target.

Administrators and other users often reuse passwords, use weak passwords, or fail to change the default credentials for a service. From a previous lab, we learned about vulnerabilities in SMB. We will use Nmap to see if we can learn anything from SMB about accounts that we might be able to use with rexec.

a. There are multiple scripts available to find valid usernames using Nmap. One of the most common is the SMB username script. It is a common practice to synchronize OS Users with SMB (Samba or Windows) users. Use the Nmap script **smb-brute** to find users and to attempt to brute force passwords.



List the usernames and passwords that were found.
msfadmin:msfadmin
user:user

Step 2: Perform the rexec exploit.

To access the Metasploitable target to exploit the rexec vulnerability, you will need a remote shell client. Use **apt-get** to install a remote shell (RSH) client on the Kali Linux VM. In this case **rsh** could not install so I opted to ssh

Attempt to log in to the Metasploitable target with the username **msfadmin** using **ssh**. The syntax for the **ssh** command is ssh@**[*username*] [*target IP or hostname*]**

```
┌──(kali㉿Kali)-[~]
└─$ ssh msfadmin@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? YES
Warning: Permanently added '172.17.0.2' (DSA) to the list of known hosts.
msfadmin@172.17.0.2's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Jul 16 21:04:01 2017
msfadmin@metasploitable:~$
```

The login is successful. The prompt changes to the msfadmin user at the remote computer. Use the **pwd** command to determine the remote directory.

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$
```

Attempt to gain root access to Metasploitable using the **sudo su** command. When prompted for a password enter the **msfadmin** password that you uncovered earlier.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin#
```

At this point, you have full root access to the target computer and can execute commands, upload or download files, or add users. Type **exit** twice to return to the Kali CLI. A message should appear that says **Connection to 172.17.0.2 closed.**

```
root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ exit
logout
Connection to 172.17.0.2 closed.

┌──(kali㉿Kali)-[~]
└─$
```

What steps can you use to obtain other usernames and passwords that are not SMB users on the system once you obtain privileged access? **copy the /etc/passwd and /etc/shadow files**

What capabilities of the **Unshadow** and **John the Ripper** utilities would you use to obtain the credentials of the users once you have the passwd and shadow files? **Unshadow can combine the two files and the resulting file can be used by John the Ripper to find the clear text passwords.**