Website Vulnerability Scanning with Nikto and GVM

Note: These labs are performed based on the lab work provided in "Module 6.1: Overview of Web Application-Based Attacks" in the "Ethical Hacking" Course provided by CISCO.

Website vulnerability scanning is an automated process that systematically examines a website or web application to identify security issues, technical flaws, or misconfigurations.

Cybersecurity professionals or penetration testers often use specialized tools, such as Nikto and GVM, to assess various layers of security.

Lab 1- Website Vulnerability Scanning Nitkto

Nikto is a command-line, open-source tool created especially to identify web server vulnerabilities. It is well-known for being "**noisy**"—it doesn't attempt to conceal its presence, which makes it a great tool for determining whether your security measures, such as an intrusion detection system, are truly operational.

In this lab, we will complete the following actions:

- Launch Nikto and Perform a Basic Scan
- Use Nikto to Scan Multiple Web Servers
- Investigate Website Vulnerabilities
- Export Nikto Results to a File

Required Resources

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

Part 1: Launch Nikto and Perform a Basic Scan

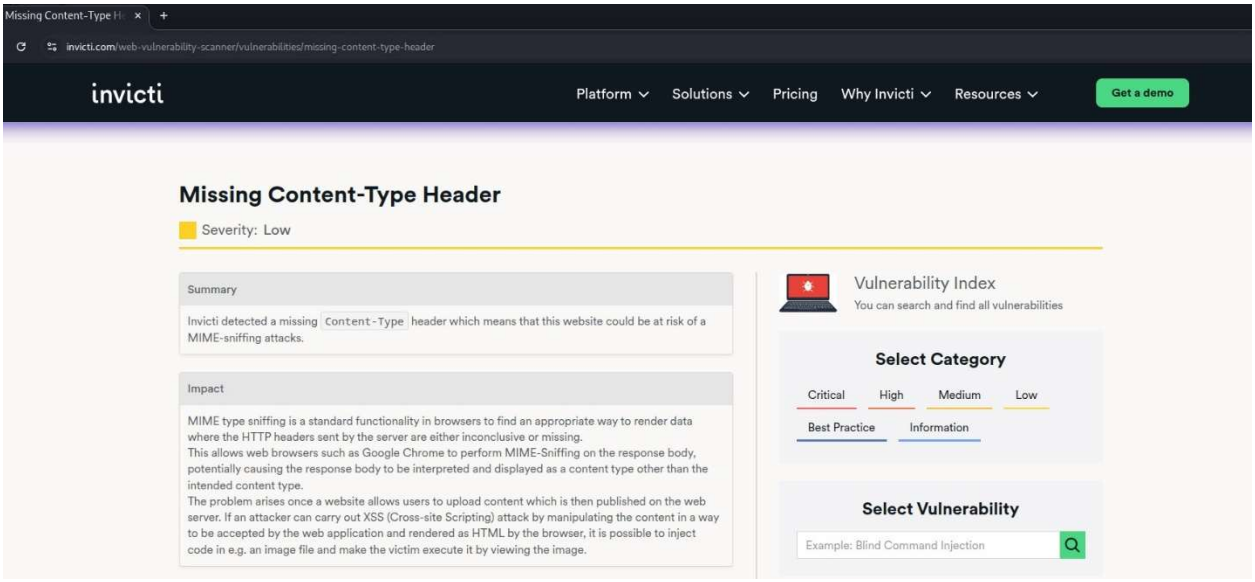
a. First of all, log in to the Kali system with the username kali and the password kali.
b. Launch Nikto using the Application > Vulnerability Analysis > nikto choice on the menu, or we can directly launch this tool from the command line.
c. Next, use the nikto --help command to view the help file that helps us to know about the tool in detail.

```
$ nikto --help
```

d. Now, use Nikto to perform a basic scan on the **scanme.nmap.org** website.

```
$ nikto -h scanme.nmap.org
```

e. The scan result shows that the vulnerability "**X-Content-Type-Options header is not set"**. Open Firefox and navigate to the link presented on the scan result: **https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/.**
f. On the webpage, we can view the summary, impact, remediation advice, and the associated vulnerability classification links.



g. By default, Nikto scans for port 80 web services. If we need to scan domains with HTTPS enabled, we must specify the -ssl flag to scan port 443:

```
$ nikto -h https://nmap.org -ssl
```

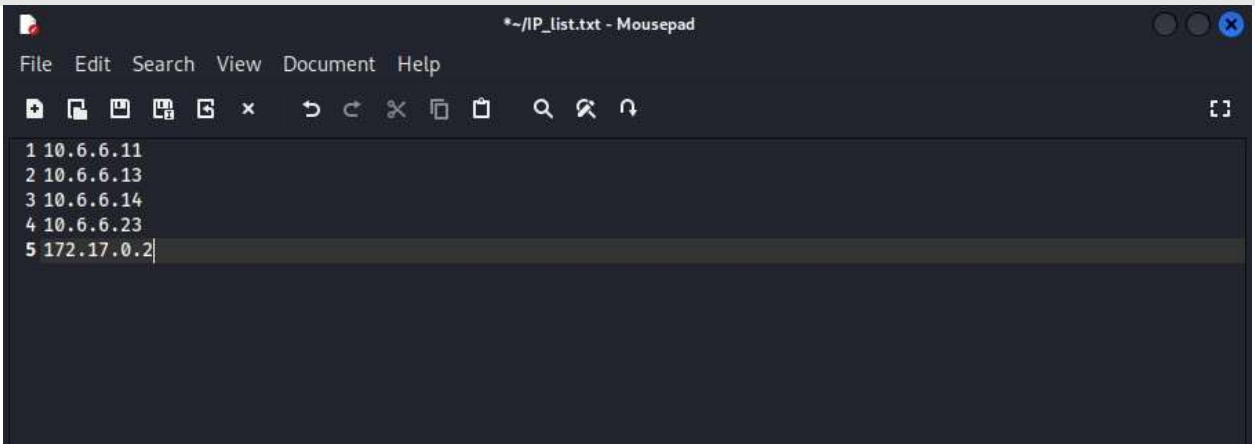
Part 2: Use Nikto to Scan Multiple Web Servers

We can also use Nikto to scan servers on the internal virtual networks to look for vulnerable web servers.

a. To scan multiple we servers, we should first create a text file to list the IP addresses that we want to scan. Then we use the built-in **MousePad** application in Kali to create the file.

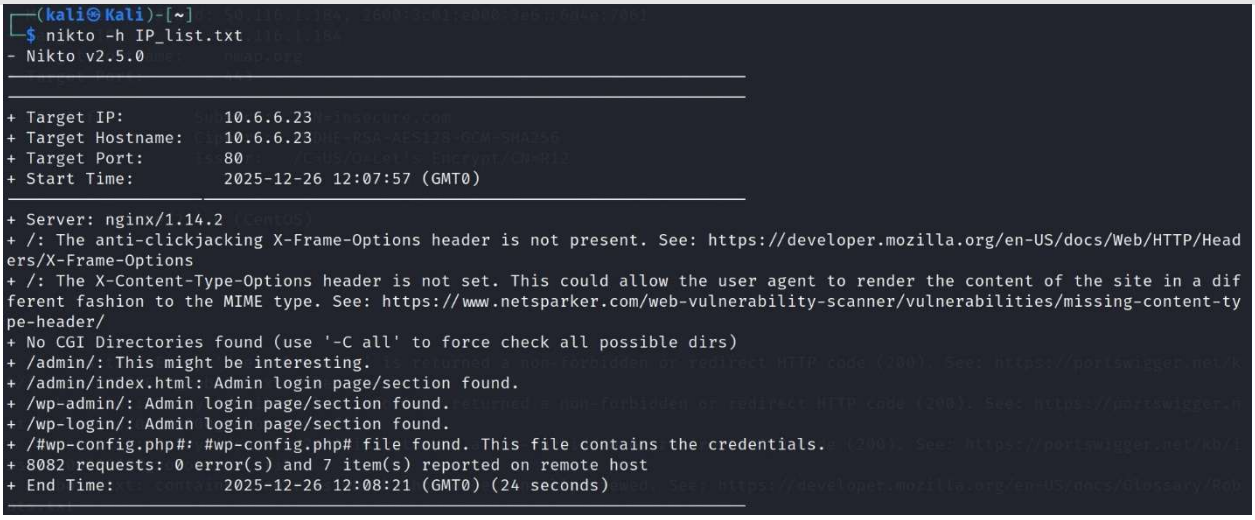
b. To open the MousePad application, click Applications >Favorites >Text Editor. Copy and paste the following list of IP addresses into the document and save this document to the home directory with the name “IP_list.txt”.

```
10.6.6.11
10.6.6.13
10.6.6.14
10.6.6.23
172.17.0.2
```



b. Now, run the scan using the **nikto -h IP_list.txt** command.

```
$ nikto -h IP_list.txt
```



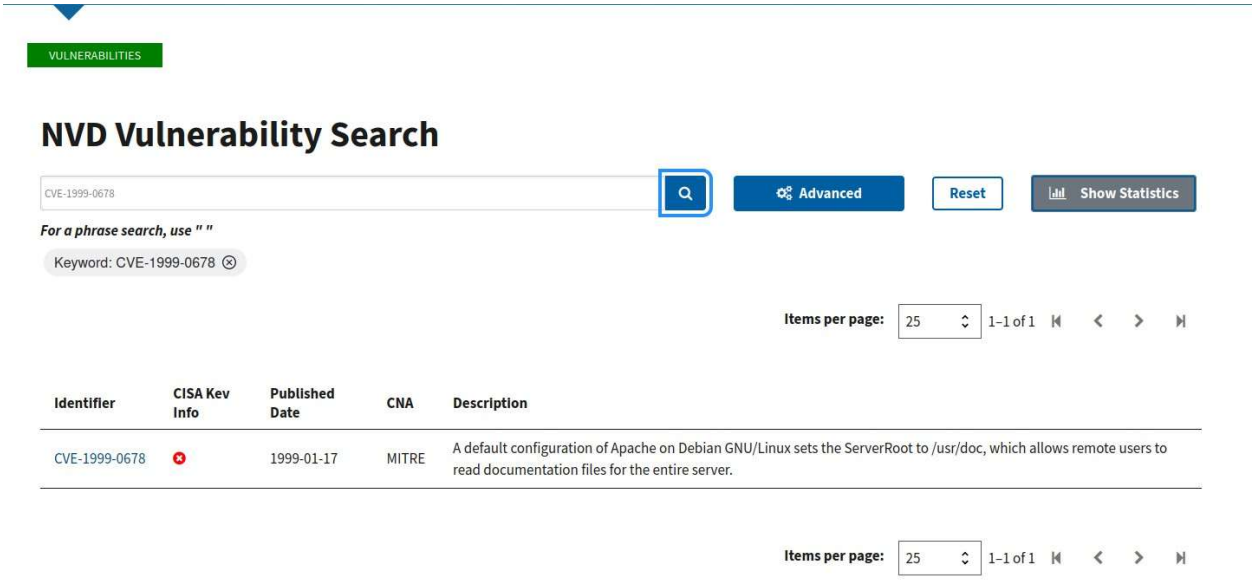
Part 3: Investigate Website Vulnerabilities

We can investigate website vulnerabilities with the use of information provided by Nitko that it uncovers during its scans.

a. Now, review the information that Nikto reported for the **172.17.0.2** web server. The CVEs listed in the output are **CVE-1999-0678** and **CVE-2003-1418**. We can use the CVE links in the Nikto output to find more information about the vulnerabilities.

```
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-
0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that co
ntain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that co
ntain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that co
ntain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that co
ntain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hos
ts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 1115138, size
: 40540, mtime: Tue Dec  9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. S
ee: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorize
d hosts.
```

b. Next, use the National Vulnerability Database (https://nvd.nist.gov) to find additional information on the CVEs. We can find here the remediation measures needed to close each vulnerability.

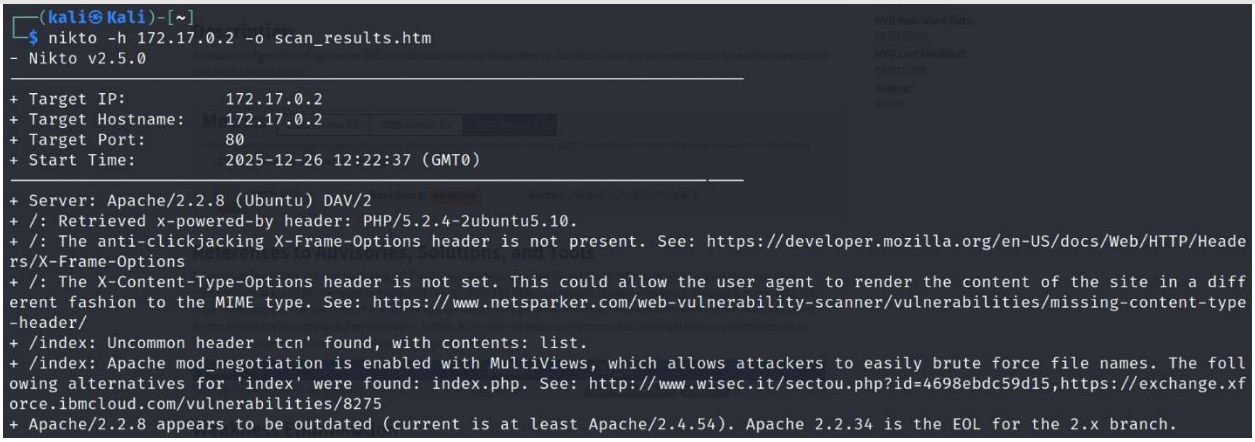


Part 4: Export Nikto Results to a File

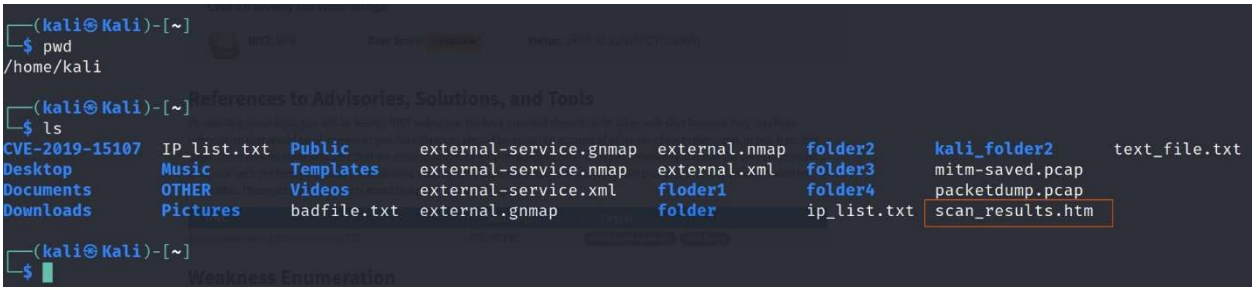
In addition to displaying the scan result on the terminal, Nikto can output the results of a scan in various formats, such as CSV, HTML, SQL, txt, and XML. Nikto can be paired with Metasploit to launch exploits against the vulnerabilities that you uncover.

a. We can use the -o flag followed by the file name to export a scan result. Now, export the results of a scan to an HTML report file named **scan_results.htm** using the following command.

```
$ nikto -h 172.17.0.2 -o scan_results.htm
```



b. The **scan_results.htm** file will be located at the **/home/kali** directory. Open it in the browser to view the generated report.



c. The -Format flag can be used to specify a text file output format that is independent of the file extension. The -Format CSV option can be used to save the file in the format of a CSV file, which is useful to import into other analysis applications.

```
$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
```

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-12-26 12:28:52 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
```

d. We can use the cat command to view the saved **scan_results.txt** file.

```
┌──(kali㉿Kali)-[~]
└─$ cat scan_results.txt
"Nikto - v2.5.0/"
"172.17.0.2","172.17.0.2","80","","","","Apache/2.2.8 (Ubuntu) DAV/2"
"172.17.0.2","172.17.0.2","80","","GET","/","Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10."
"172.17.0.2","172.17.0.2","80","https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options","GET","/","The anti-clickjacking X-Frame-Options header is not present."
"172.17.0.2","172.17.0.2","80","https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/","GET","/","The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type."
"172.17.0.2","172.17.0.2","80","","GET","/index","Uncommon header 'tcn' found, with contents: list."
"172.17.0.2","172.17.0.2","80","http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275","GET","/index","Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php."
"172.17.0.2","172.17.0.2","80","","HEAD","/","Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch."
"172.17.0.2","172.17.0.2","80","","BTHIRZYZ","/","Web Server returns a valid response with junk HTTP methods which may cause false positives."
"172.17.0.2","172.17.0.2","80","https://owasp.org/www-community/attacks/Cross_Site_Tracing","TRACE","/","HTTP TRACE method is active which suggests the host is vulnerable to XST."
"172.17.0.2","172.17.0.2","80","","GET","/phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>","/phpinfo.php: Output from the phpinfo() function was found."
"172.17.0.2","172.17.0.2","80","","GET","/doc/","Directory indexing found."
"172.17.0.2","172.17.0.2","80","CVE-1999-0678","GET","/doc/","The /doc/ directory is browsable. This may be /usr/doc."
```

Lab 2- Website Vulnerability Scanning GVM

Greenbone Vulnerability Management (GVM), formerly known as OpenVAS, is a large, enterprise-level network vulnerability management system. It has a collection of services that collaborate to scan thousands of devices on a network with advanced features, in contrast to the lightweight Nikto.

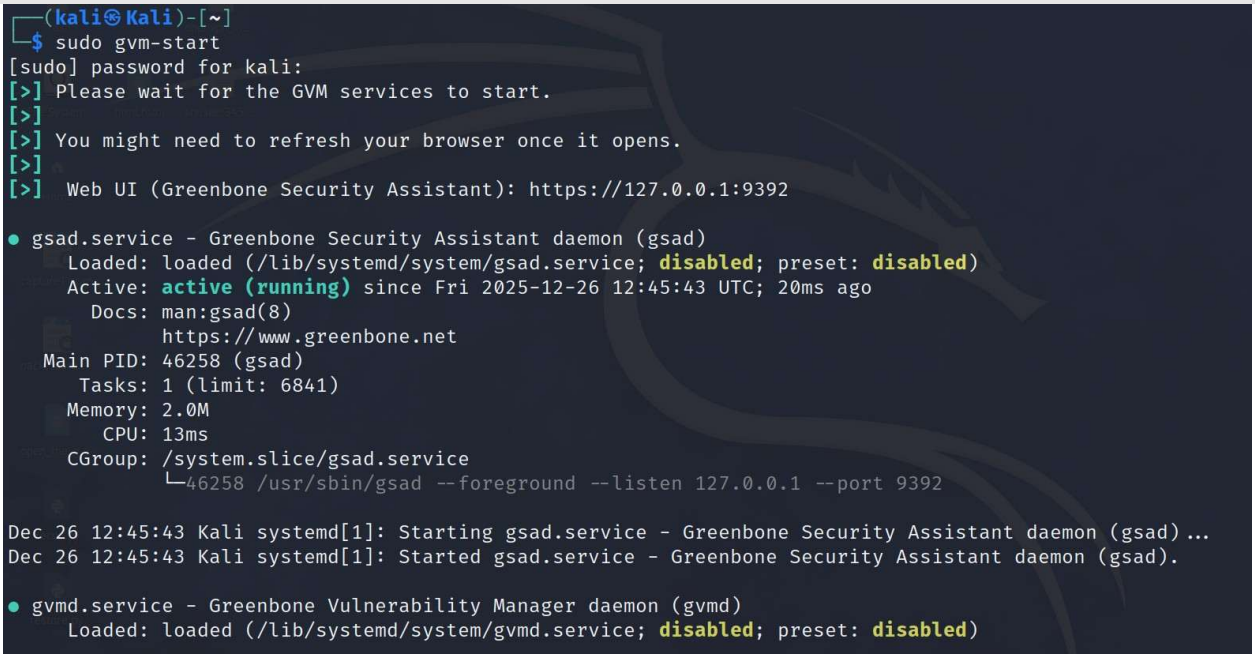
In this lab, we will complete the following activities:

- Scan a Host for Vulnerabilities

Scanning Host for Vulnerabilities

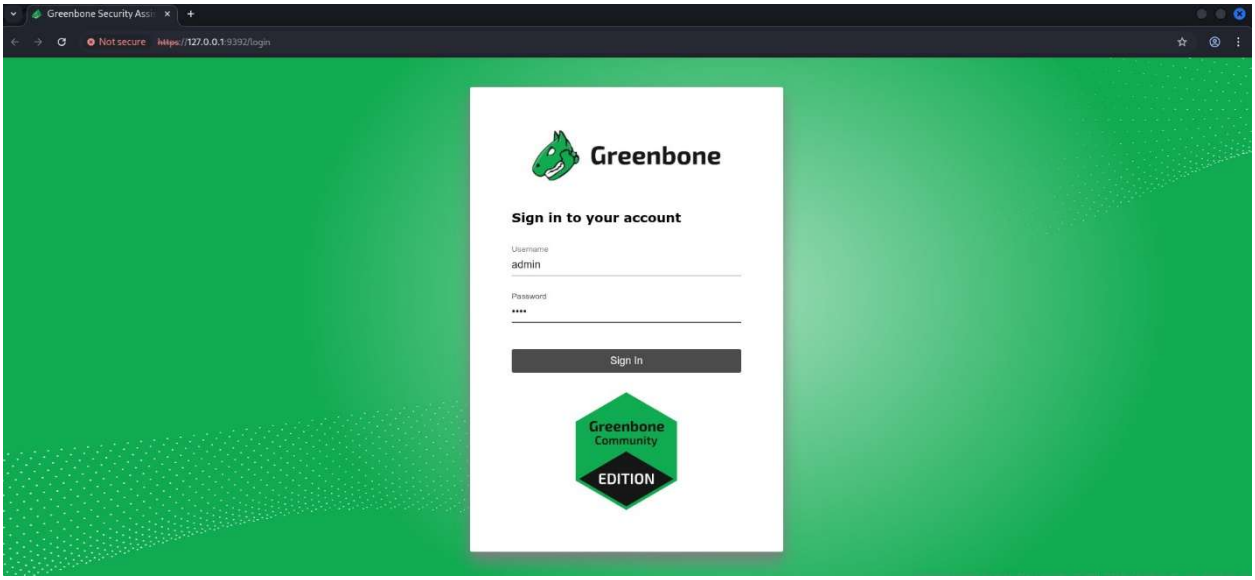
a. Start the GVM scanner using the **sudo gvm-start** command. You can also access the gvm-start script using the Applications menu on the Kali desktop. For this, go to Kali > 02-Vulnerability Analysis > gvm start.

$ sudo gvm-start

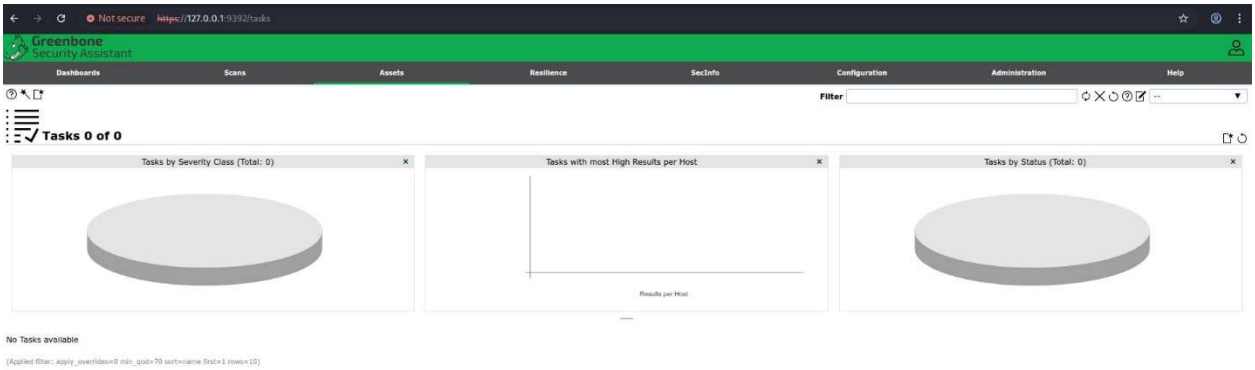


b. Next, enter admin as the username and kali as the password in the login box.

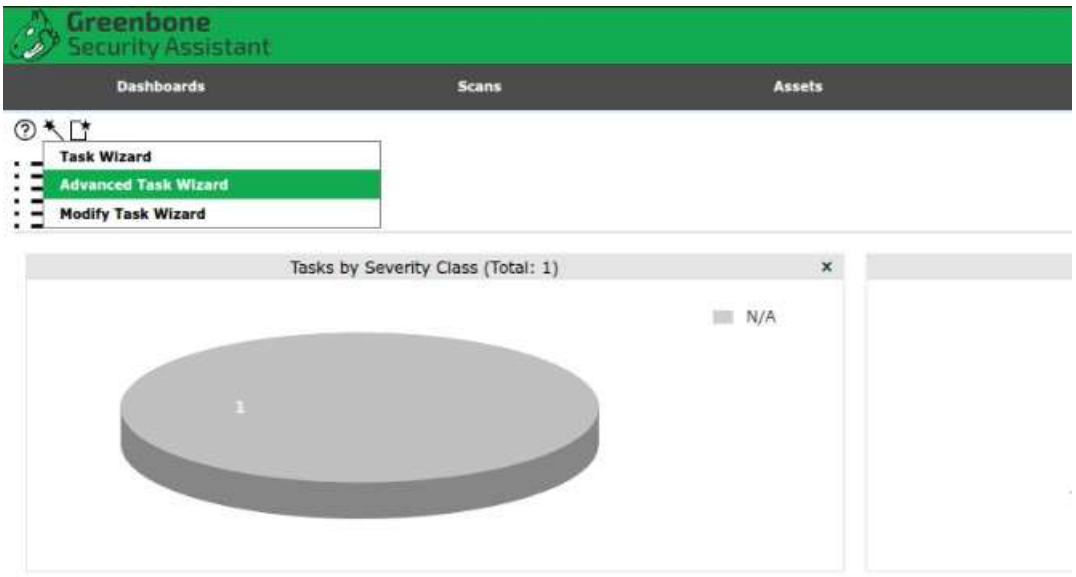
Username: admin
Password: kali



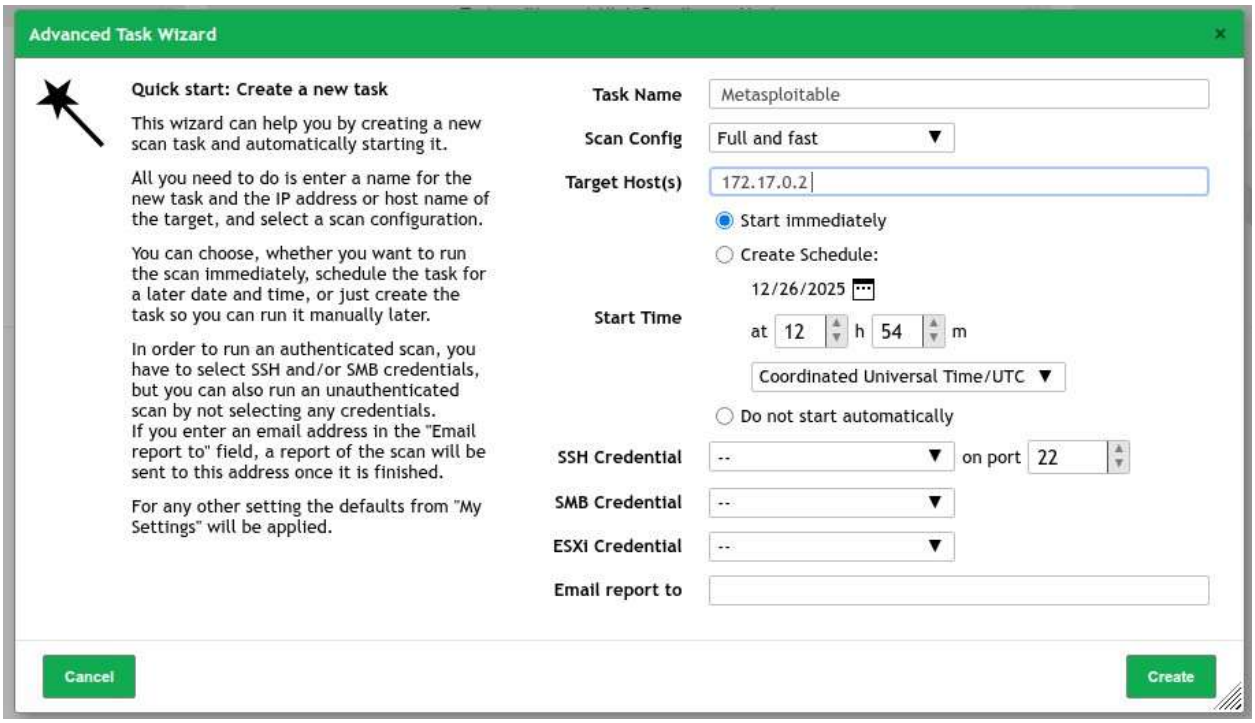
c. The GVM Scanner application GUI will be opened in the browser. Now, select **Scans** and then **Tasks** from the menu bar.



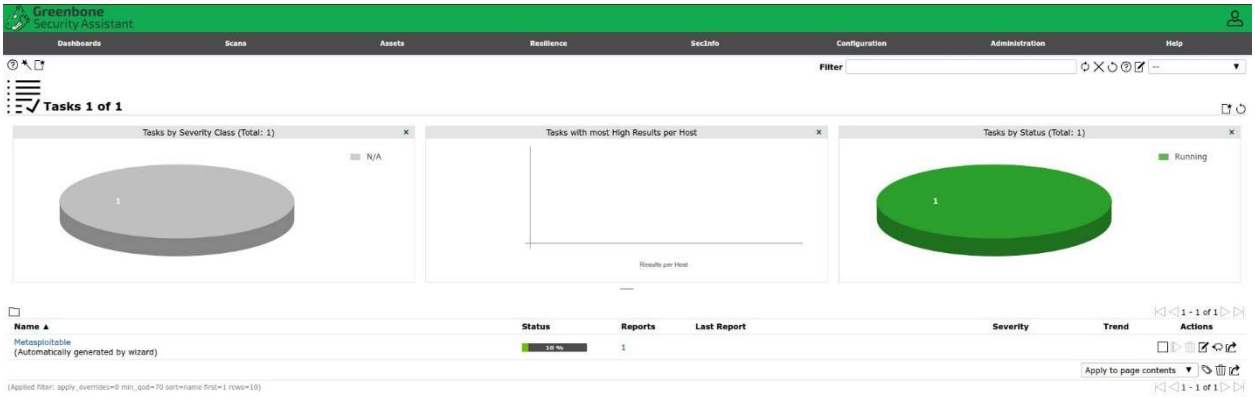
d. At the upper left of the Tasks window appear three icons. Select the Task Wizard icon that looks like a magic wand. Choose Advanced Task Wizard from the dropdown menu.



e. When the Advanced Task Wizard window opened, enter **Metasploitable** as the scan name. In the Target Host(s) field, we should enter the IP address of Metasploitable, which was **172.17.0.2** for this lab. Leave the rest of the settings unchanged and click **Create** to create the task and start the scan.

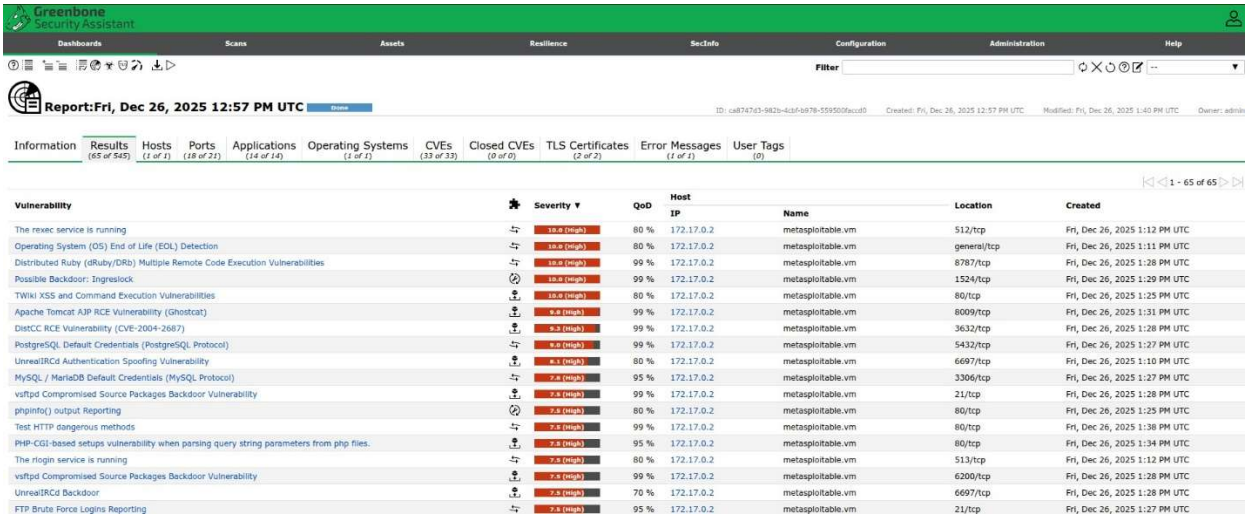


f. The Task window indicates the task is running when the scan was started. At the bottom of the window, the task Metasploitable will be listed, and the status bar shows the percent complete.

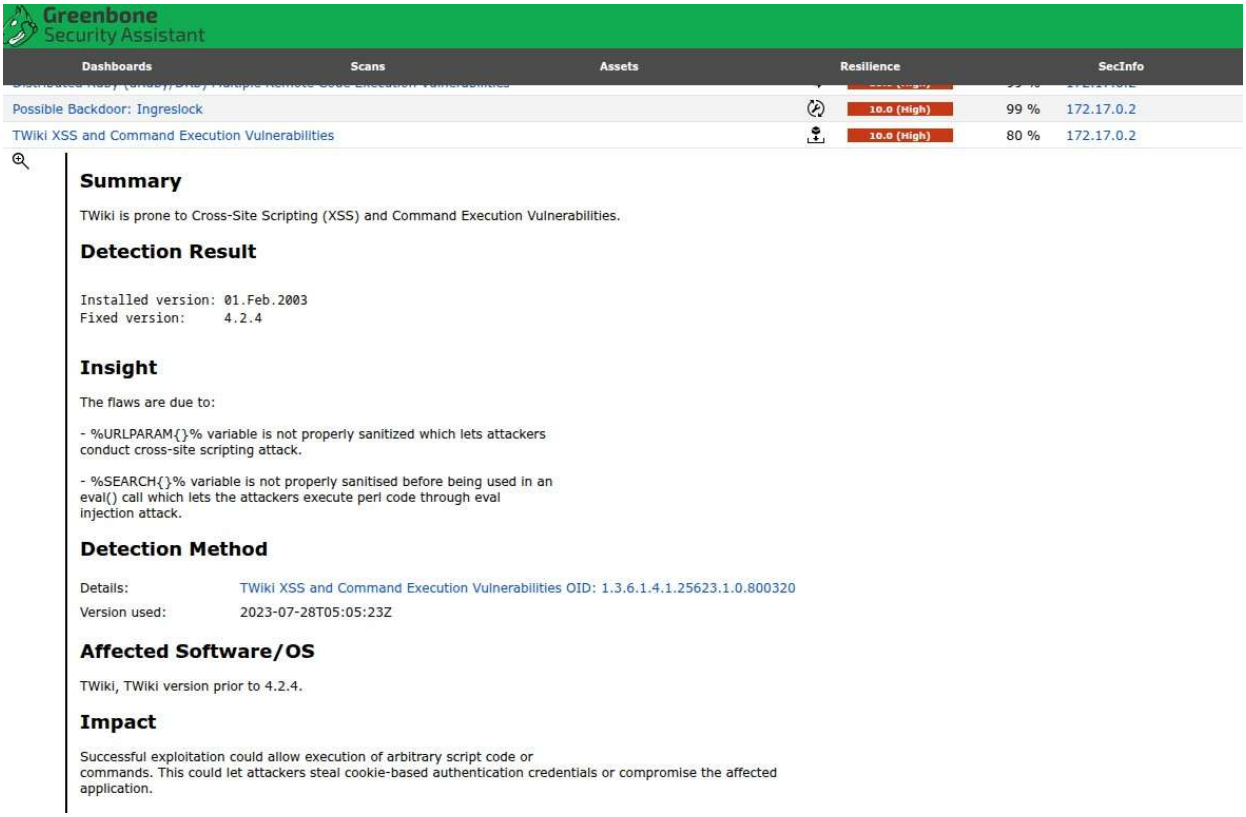


g. Now, click the number “1” under the Reports column in the Metasploitable row, next to the status indicator.

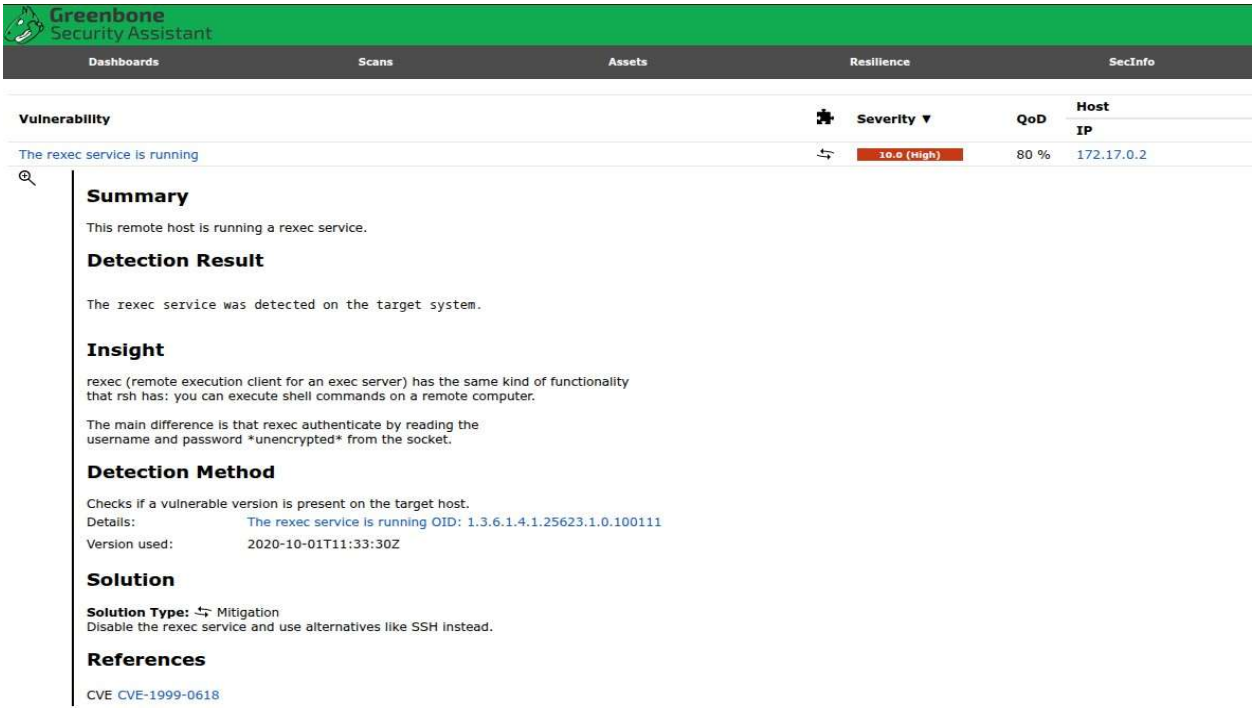
h. Next, open the report by clicking the date and time link located under the Date column. The vulnerabilities found will be listed in order of severity after clicking on the results tab.



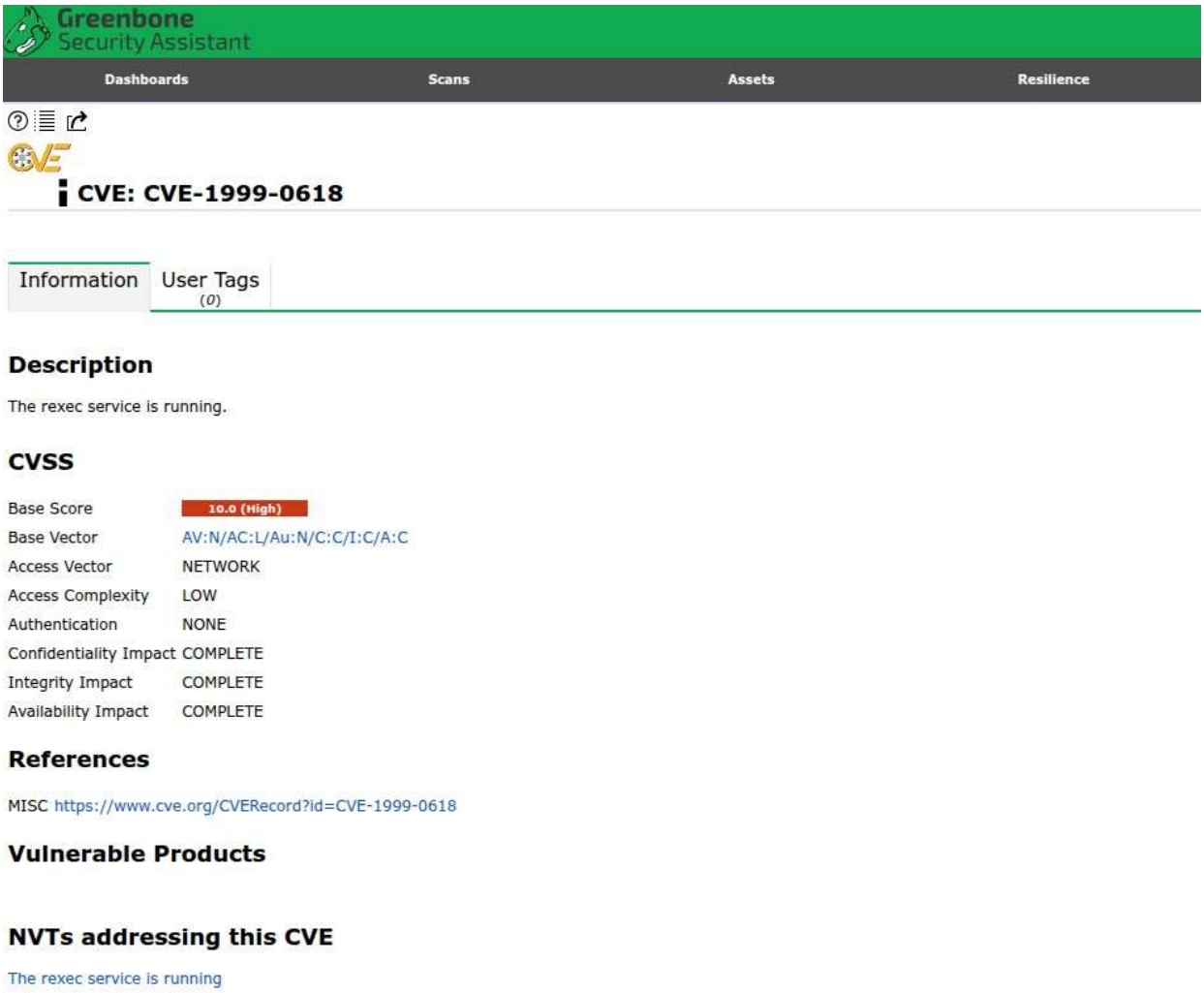
i. If you need more information on a vulnerability, click on it. GVM has explanations for these vulnerabilities. Now, click on the link “**TWiki XSS and Command Execution”** to investigate this Vulnerability.



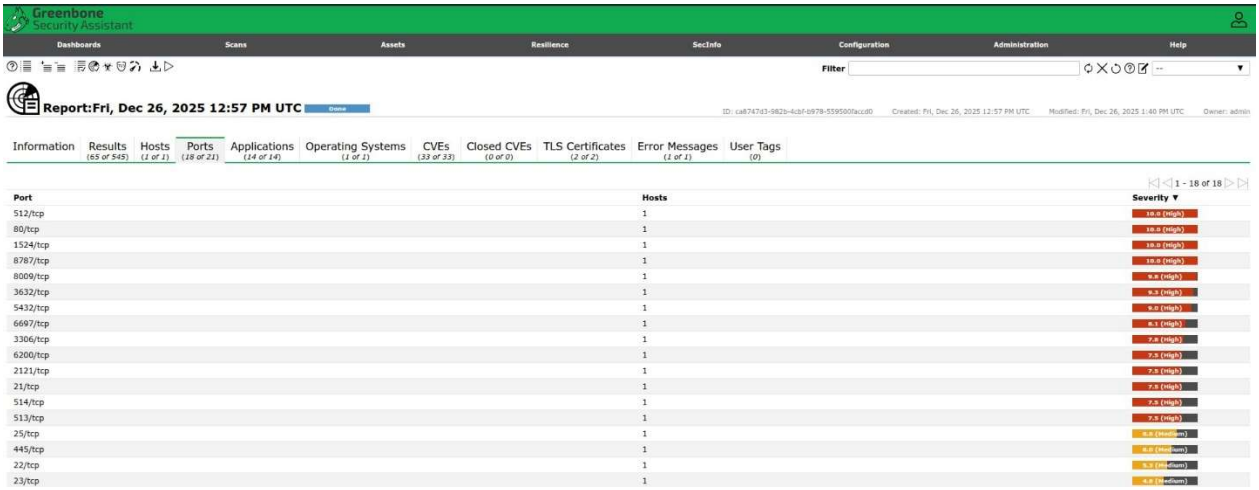
j. Now, click on the "**The rexec"** service is running vulnerability listed in the Results tab. GVM provides a summary of the findings and additional details. The Insight section explains a little about the vulnerability, and the Solution section gives mitigation suggestions.



k. If we need a brief description of the CVE, can select the CVE associated with the **rexec** vulnerability.



l. Now, select the Ports tab to view the open ports on the Metasploitable system.



m. We can explore the other vulnerabilities and focus on how we might use them to exploit the 172.17.0.2 client.