

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 Nikto

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

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

```
$ nikto --help
```

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

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

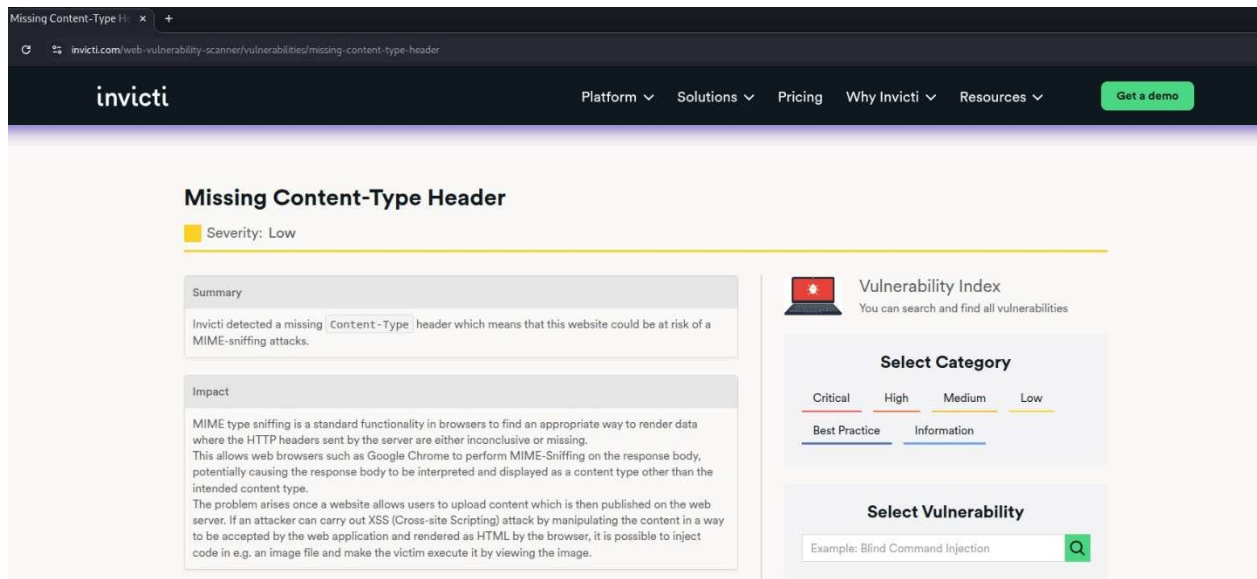


```
(kali@kali)-[~]
$ nikto -h scanme.nmap.org
- Nikto v2.5.0

+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2025-12-26 11:56:48 (GMT0)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: 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/
```

- 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/>**.
- 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
```

```
(kali@kali)~$ nikto -h https://nmap.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
+ Target IP: 50.116.1.184
+ Target Hostname: nmap.org
+ Target Port: 443

+ SSL Info: Subject: /CN=insecure.com
            Ciphers: ECDHE-RSA-AES128-GCM-SHA256
            Issuer: /C=US/O=Let's Encrypt/CN=R12
+ Start Time: 2025-12-26 12:02:29 (GMT0)

+ Server: Apache/2.4.6 (CentOS)
+ /: 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/
```

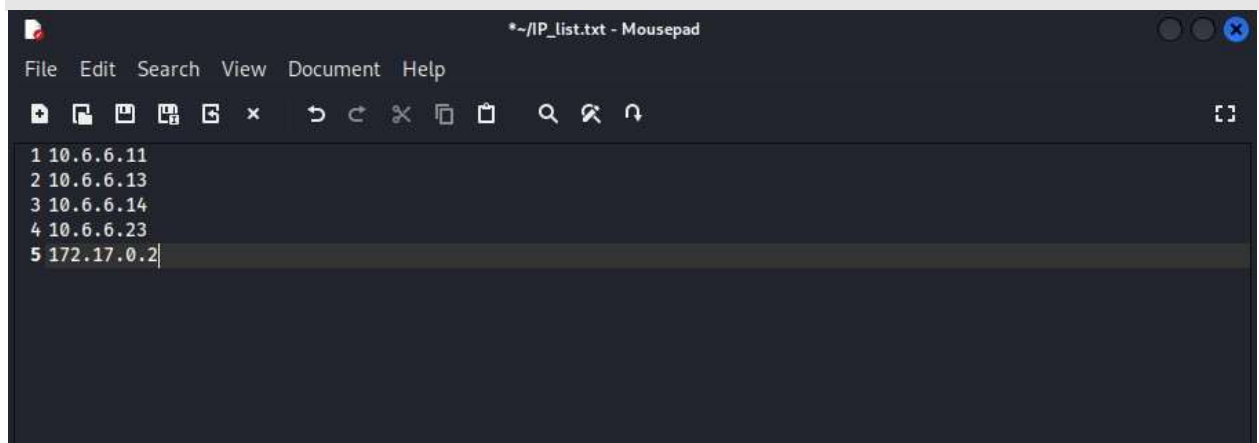
Part 2: Use Nikto to Scan Multiple Web Servers

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

- a. To scan multiple web 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.

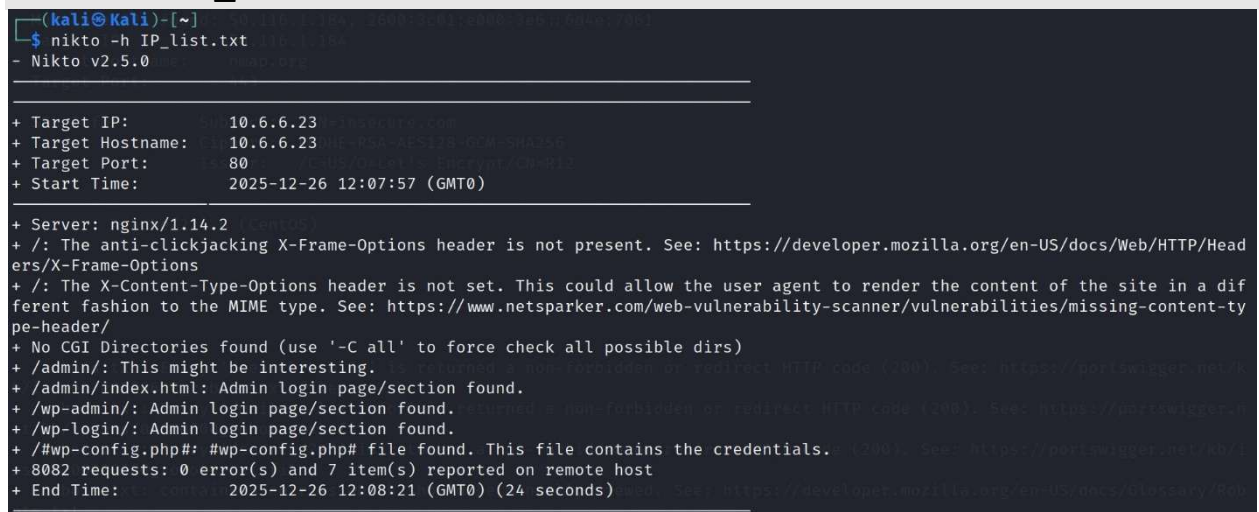
- b. To open the MousePad application, click Applications >Favorites >Text Editor. Copy and paste the following list of IP addresses into the document and save this document to the home directory with the name "IP_list.txt".

```
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 Nikto 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 contain specific QUERY strings. See: OSVDB-12184
+ /?PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /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. See: 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 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.

VULNERABILITIES

NVD Vulnerability Search

For a phrase search, use " "

Keyword: CVE-1999-0678

Items per page: 25 1-1 of 1

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-1999-0678		1999-01-17	MITRE	A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.

Items per page: 25 1-1 of 1

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
```

```
(kali@kali)~$ nikto -h 172.17.0.2 -o scan_results.htm
- Nikto v2.5.0

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2025-12-26 12:22:37 (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.
```

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

```
(kali@kali)~$ pwd
/home/kali

(kali@kali)~$ ls
CVE-2019-15107  IP_list.txt  Public  external-service.gnmap  external.nmap  folder2  kali_folder2  text_file.txt
Desktop        Music        Templates  external-service.nmap  external.xml  folder3  mitm-saved.pcap
Documents      OTHER        Videos    external-service.xml  floder1       folder4  packetdump.pcap
Downloads      Pictures     badfile.txt  external.gnmap        folder        ip_list.txt  scan_results.htm
```

- 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
```

```
(kali㉿kali)-[~]
└─$ sudo gvm-start
[sudo] password for kali:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-12-26 12:45:43 UTC; 20ms ago
     Docs: man:gsad(8)
           https://www.greenbone.net
   Main PID: 46258 (gsad)
     Tasks: 1 (limit: 6841)
    Memory: 2.0M
       CPU: 13ms
    CGroup: /system.slice/gsad.service
            └─46258 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

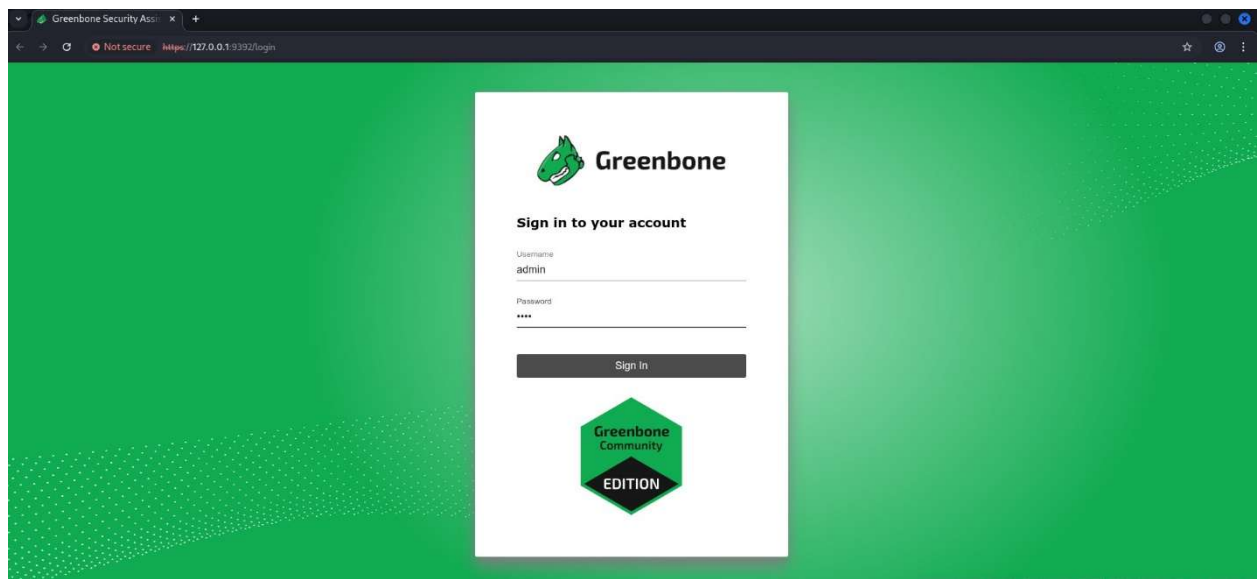
Dec 26 12:45:43 Kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Dec 26 12:45:43 Kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
```

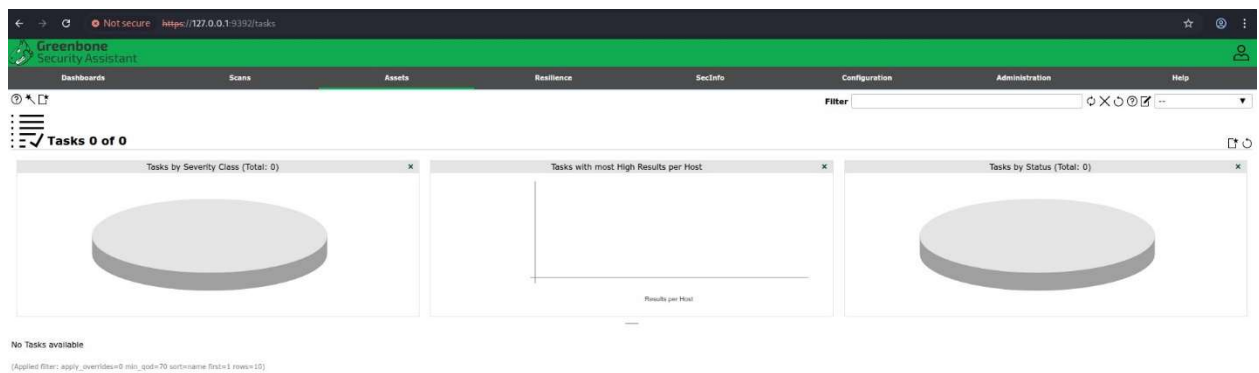
- b. Next, enter admin as the username and kali as the password in the login box.

```
Username: admin
```

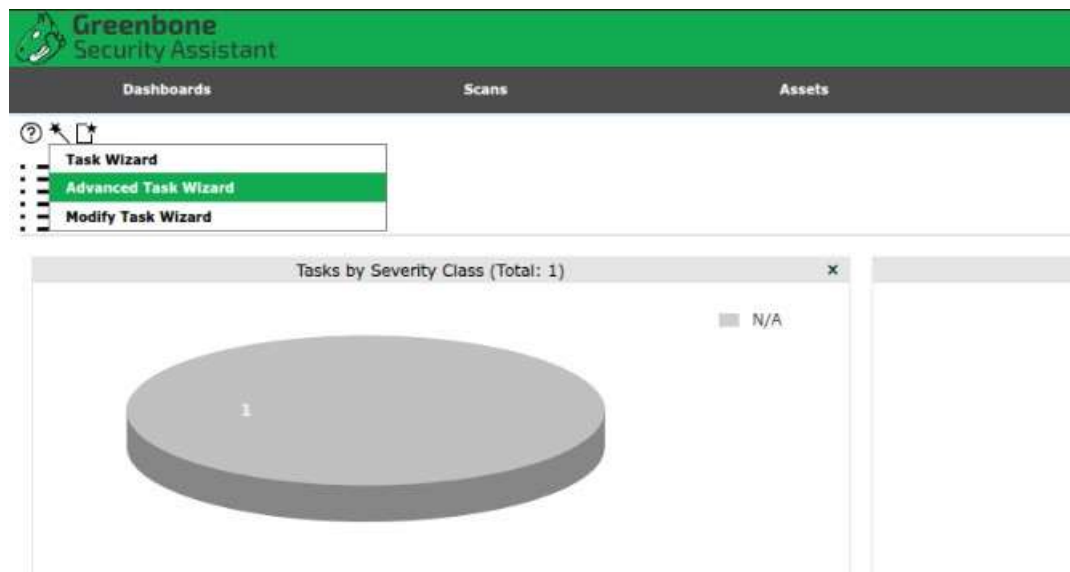
```
Password: kali
```

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



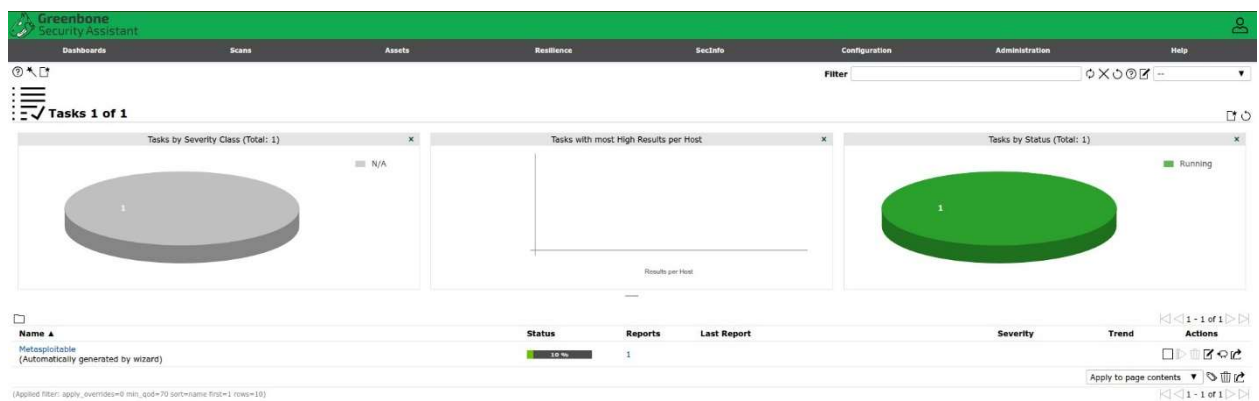
- d. At the upper left of the Tasks window appear three icons. Select the Task Wizard icon that looks like a magic wand. Choose Advanced Task Wizard from the dropdown menu.



- 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.

The screenshot shows the 'Advanced Task Wizard' window. On the left, there's a 'Quick start: Create a new task' section with a star icon and explanatory text. The right side contains the following fields: 'Task Name' (Metasploitable), 'Scan Config' (Full and fast), 'Target Host(s)' (172.17.0.2), 'Start Time' (12/26/2025 at 12:54 m), 'SSH Credential' (empty), 'SMB Credential' (empty), 'ESXI Credential' (empty), and 'Email report to' (empty). The 'Start immediately' radio button is selected. The 'Create' button is at the bottom right.

- 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.

The screenshot shows the Greenbone Security Assistant report for 'Metasploitable' dated 'Fri, Dec 26, 2025 12:57 PM UTC'. The report is titled 'Report: Fri, Dec 26, 2025 12:57 PM UTC'. The report shows a list of vulnerabilities under the 'Results' tab. The table has columns: Vulnerability, Severity, QoD, Host, Name, Location, and Created. The vulnerabilities are listed in descending order of severity.

Vulnerability	Severity	QoD	Host	Name	Location	Created
The rexec service is running	10.0 (high)	80 %	172.17.0.2	metasploitable-vm	512/tcp	Fri, Dec 26, 2025 1:12 PM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (high)	80 %	172.17.0.2	metasploitable-vm	general/tcp	Fri, Dec 26, 2025 1:11 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	8787/tcp	Fri, Dec 26, 2025 1:28 PM UTC
Possible Backdoor: Ingreslock	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	1524/tcp	Fri, Dec 26, 2025 1:29 PM UTC
Wiki XSS and Command Execution Vulnerabilities	10.0 (high)	80 %	172.17.0.2	metasploitable-vm	80/tcp	Fri, Dec 26, 2025 1:25 PM UTC
Apache Tomcat ASP RCE Vulnerability (Gh0st4t)	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	8009/tcp	Fri, Dec 26, 2025 1:31 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	3632/tcp	Fri, Dec 26, 2025 1:28 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	5432/tcp	Fri, Dec 26, 2025 1:27 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	10.0 (high)	80 %	172.17.0.2	metasploitable-vm	6697/tcp	Fri, Dec 26, 2025 1:10 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	10.0 (high)	95 %	172.17.0.2	metasploitable-vm	3306/tcp	Fri, Dec 26, 2025 1:27 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	10.0 (high)	99 %	172.17.0.2	metasploitable-vm	21/tcp	Fri, Dec 26, 2025 1:28 PM UTC
phpinfo() output Reporting	7.5 (high)	80 %	172.17.0.2	metasploitable-vm	80/tcp	Fri, Dec 26, 2025 1:25 PM UTC
Test HTTP dangerous methods	7.5 (high)	99 %	172.17.0.2	metasploitable-vm	80/tcp	Fri, Dec 26, 2025 1:38 PM UTC
PHP-CGI based setups vulnerability when parsing query string parameters from php files.	7.5 (high)	95 %	172.17.0.2	metasploitable-vm	80/tcp	Fri, Dec 26, 2025 1:34 PM UTC
The rlogin service is running	7.5 (high)	80 %	172.17.0.2	metasploitable-vm	513/tcp	Fri, Dec 26, 2025 1:12 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (high)	99 %	172.17.0.2	metasploitable-vm	6200/tcp	Fri, Dec 26, 2025 1:28 PM UTC
UnrealIRCd Backdoor	7.5 (high)	70 %	172.17.0.2	metasploitable-vm	6697/tcp	Fri, Dec 26, 2025 1:28 PM UTC
FTP Bruteforce Logins Reporting	7.5 (high)	95 %	172.17.0.2	metasploitable-vm	21/tcp	Fri, Dec 26, 2025 1:27 PM UTC

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

Greenbone Security Assistant

Dashboards	Scans	Assets	Resilience	SecInfo
Possible Backdoor: Ingreslock			10.0 (High)	99 % 172.17.0.2
TWiki XSS and Command Execution Vulnerabilities			10.0 (High)	80 % 172.17.0.2

Summary

TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Detection Result

Installed version: 01.Feb.2003
Fixed version: 4.2.4

Insight

The flaws are due to:

- %URLPARAM{}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH{}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Detection Method

Details: TWiki XSS and Command Execution Vulnerabilities OID: 1.3.6.1.4.1.25623.1.0.800320
Version used: 2023-07-28T05:05:23Z

Affected Software/OS

TWiki, TWiki version prior to 4.2.4.

Impact

Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

- 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.

Greenbone Security Assistant

Dashboards	Scans	Assets	Resilience	SecInfo
Vulnerability			Severity ▼	QoD Host IP
The rexec service is running			10.0 (High)	80 % 172.17.0.2

Summary

This remote host is running a rexec service.

Detection Result

The rexec service was detected on the target system.

Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticates by reading the username and password *unencrypted* from the socket.

Detection Method

Checks if a vulnerable version is present on the target host.
Details: The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111
Version used: 2020-10-01T11:33:30Z

Solution

Solution Type: Mitigation
Disable the rexec service and use alternatives like SSH instead.

References

CVE CVE-1999-0618

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

The screenshot shows the Greenbone Security Assistant interface. At the top, there's a green header with the logo and navigation tabs: Dashboards, Scans, Assets, and Resilience. Below the header, there's a sidebar with icons for help, settings, and a search bar. The main content area displays the CVE details for CVE-1999-0618. The 'Information' tab is selected, showing the CVE ID and a description: 'The rexec service is running.' Below this, the 'CVSS' section lists various scores and vectors: Base Score 10.0 (High), Base Vector AV:N/AC:L/Au:N/C:C/I:C/A:C, Access Vector NETWORK, Access Complexity LOW, Authentication NONE, Confidentiality Impact COMPLETE, Integrity Impact COMPLETE, and Availability Impact COMPLETE. The 'References' section lists a MISC URL: https://www.cve.org/CVERecord?id=CVE-1999-0618. The 'Vulnerable Products' section is empty. The 'NVTs addressing this CVE' section shows 'The rexec service is running'.

Greenbone Security Assistant

Dashboards Scans Assets Resilience

🔍 **CVE: CVE-1999-0618**

Information User Tags (0)

Description

The rexec service is running.

CVSS

Base Score **10.0 (High)**
Base Vector **AV:N/AC:L/Au:N/C:C/I:C/A:C**
Access Vector **NETWORK**
Access Complexity **LOW**
Authentication **NONE**
Confidentiality Impact **COMPLETE**
Integrity Impact **COMPLETE**
Availability Impact **COMPLETE**

References

MISC <https://www.cve.org/CVERecord?id=CVE-1999-0618>

Vulnerable Products

NVTs addressing this CVE

The rexec service is running

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

The screenshot shows the Greenbone Security Assistant interface with the 'Ports' tab selected. The main content area displays a table of open ports on the Metasploitable system. The table has columns for Port, Hosts, and Severity. The ports listed are: 512/tcp, 80/tcp, 1524/tcp, 8787/tcp, 8080/tcp, 3632/tcp, 5432/tcp, 6667/tcp, 3306/tcp, 6200/tcp, 2121/tcp, 21/tcp, 514/tcp, 513/tcp, 25/tcp, 445/tcp, 22/tcp, and 23/tcp. The severity for most ports is 'High' (red), while for 25/tcp, 445/tcp, 22/tcp, and 23/tcp, it is 'Medium' (yellow).

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Fri, Dec 26, 2025 12:57 PM UTC

ID: ca8747d3-982b-4d3f-6978-539590fa0c80 Created: Fri, Dec 26, 2025 12:57 PM UTC Modified: Fri, Dec 26, 2025 1:40 PM UTC Owner: admin

Port	Hosts	Severity
512/tcp	1	High
80/tcp	1	High
1524/tcp	1	High
8787/tcp	1	High
8080/tcp	1	High
3632/tcp	1	High
5432/tcp	1	High
6667/tcp	1	High
3306/tcp	1	High
6200/tcp	1	High
2121/tcp	1	High
21/tcp	1	High
514/tcp	1	High
513/tcp	1	High
25/tcp	1	Medium
445/tcp	1	Medium
22/tcp	1	Medium
23/tcp	1	Medium

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