## Incomplete 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 gvm-start
```

**Note**: You may receive the message "**GVM services are already running**." If the browser does not automatically open, start your browser manually and navigate to **https://127.0.0.1:9392**. The Greenbone Security Assistant login screen will appear in the browser.

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

```
Username: admin
Password: kali
```

## 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.

a. 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.
b. 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.
c. 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.
d. 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?

Answer Area

<!----><!---->

e. 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?

Answer Area

<!----><!---->

f. 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?

Answer Area

<!----><!---->

## 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?

Answer Area

<!----><!---->

What is the suggested mitigation for the rexec vulnerability?

Answer Area

<!----><!---->

b. 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?

Answer Area

<!----><!---->

c. 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.

d. 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?

Answer Area

<!----><!---->

e. 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?

Answer Area

<!----><!---->

f. Explore the other vulnerabilities and focus on how you might use them to exploit the 172.17.0.2 client.

## 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
```

b. Locate the **Host script results** section in the command output. Username and password combinations that were uncovered with the Nmap script are listed in this section.

List the usernames and passwords that were found.

Answer Area

<!----><!---->

## Step 2: Perform the rexec exploit.

a. 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.

```
┌──(kali㉿Kali)-[~]
└─$ sudo apt-get install rsh-client
```

b. Attempt to log in to the Metasploitable target with the username **msfadmin** using **RSH**. The syntax for the **rsh** command is **rsh -l** [*username*] [*target IP or hostname*]

```
┌──(kali㉿Kali)-[~]
└─$ rsh -l msfadmin 172.17.0.2
```

c. 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
```

d. 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: msfadmin
root@metasploitable:/home/msfadmin#
```

e. 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 **rlogin: connection closed**.

# Reflection Questions

1. What steps can you use to obtain other usernames and passwords that are not SMB users on the system once you obtain privileged access?

Answer Area

<!----><!---->

2. 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? If you are not familiar with these utilities, use an internet search engine to obtain the information.

Answer Area

<!----><!---->