Lab - Vulnerability Scanning with Kali Tools

Objectives

In this lab, you will explore network vulnerability scanning tools and use them to perform a vulnerability scan on a target host.

- Perform network scans with Nmap.
- Use Greenbone Vulnerability Management to perform a vulnerability scan.

Background / Scenario

In a previous lab, you used Nmap to enumerate a host computer that was creating unusual traffic on the network. In this lab, you will use Nmap and Greenbone Vulnerability Management (GVM) to scan the system to identify potential vulnerabilities.

Required Resources

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

Instructions

Part 1: Run a Nmap Scan on a Target Computer

In this part, you will use Nmap and NSE scripts to uncover potential vulnerabilities in a target host.

Step 1: Start and login to the Kali virtual machine.

a. Start and log into the Kali virtual machine.
b. Start a terminal session. Expand the terminal window to a full screen. Use the **ping** command to determine if the computer with the address **10.6.6.23** or **gravemind.vm** is reachable over the network.

```
┌──(kali㉿Kali)-[~]
└─$ ping -c5 10.6.6.23
```

The **-c5** option tells the ping command to stop after five tries. In Linux, when a **-c** option is not specified the **ping** command will continue indefinitely until **CTRL-C** is issued.

Step 2: Identify open ports and services.

Review the results of a Nmap scan on the host with the IP address 10.6.6.23.

a. Execute a ping scan of the target host using the **nmap -sV** command. Note the list of ports and applications that are discovered on the host.

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV 10.6.6.23
```

What ports are currently open on the target computer?

Answer Area

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

b. Identify the operating system running on the target computer using the **nmap -O** command.

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 10.6.6.23
```

What operating system is the target computer running?

Answer Area

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

Step 3: Use the Nmap Vulners script to scan for vulnerabilities.

The Vulners script displays known vulnerabilities and the corresponding CVE. The Vulners script uses the open port and software version information to search for common platform enumeration (CPE) names that relate to the identified service. It then makes a request to a remote server to find out if any known vulnerabilities exist for that CPE.

a. Use the **nmap –script** command to launch the **vulners** script. The syntax for the command is **nmap -sV --script vulners [--script-args mincvss= <arg_val>] <target>** where the script argument **mincvss** restricts the output to only those CVEs that have a higher CVSS score than the one

specified in the argument.

The vulnerabilities reported will be those with a CVE score equal to or higher than 4. The output of the command should look similar to what is shown below:

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV --script vulners --script-args mincvss=4 10.6.6.23


Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 14:01 MST
Nmap scan report for 10.6.6.23
Host is up (0.0000040s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.9p1:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com
/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com
/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    5.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6111   5.8     https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2019-16905  4.4     https://vulners.com/cve/CVE-2019-16905
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6110   4.0     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   4.0     https://vulners.com/cve/CVE-2019-6109
|_      PACKETSTORM:151227      0.0     https://vulners.com/packetstorm
/PACKETSTORM:151227      *EXPLOIT*
53/tcp  open  domain      ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp  open  http        nginx 1.14.2
|_http-server-header: nginx/1.14.2
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 02:42:0A:06:06:17 (Unknown)
Service Info: Host: 868CF29B394C; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.15 seconds
```

Which service is identified as having known exploited vulnerabilities associated with it?

Answer Area

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

Which CVE is associated with the known level 5 or above vulnerability?

Answer Area

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

b. Use the National Vulnerability Database at NIST to learn more about the identified vulnerability and how it can be exploited. (https://nvd.nist.gov/vuln/search)

What level of severity is assigned to the CVE in the NIST database?

Answer Area

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

Part 2: Use GVM to Scan for Vulnerabilities

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.

Step 1: Verify the GVM Product Installation.

Before beginning any scan, it is important to verify that GVM is correctly installed and that the files it uses to identify vulnerabilities are up-to-date.

a. Verify the setup of the GVM service using the **sudo gvm-check-setup** command. This command verifies that the setup completed correctly and the necessary files are available. The verification will flag any issues that need fixing and will provide the commands to use to fix the issues.

```
┌──(kali㉿Kali)-[~]
└─$ sudo gvm-check-setup
```

Did the setup check identify any issues that must be addressed?

Answer Area

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

b. If there are issues, execute the suggested command to fix the problem and then re-run the **gvm-check-setup** command. When all issues are addressed, the command outputs the string "**It seems like your GVM [*version*] installation is OK.**".
c. Just for this activity, stop the GVM service so you can observe the startup output.

```
┌──(kali㉿Kali)-[~]
└─$ sudo gvm-stop
```

Step 2: Open the GVM Scanner GUI.

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.** It is possible that GVM may already be running as a result of the check setup process.

The output of the command should be similar to what is shown below. At the end of the output, a message that the scanner is loading in Firefox will appear.

```
┌──(kali㉿Kali)-[~]
└─$ sudo gvm-start
[>] 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 2023-03-24 18:13:28 UTC; 10ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 57707 (gsad)
      Tasks: 1 (limit: 4606)
     Memory: 912.0K
        CPU: 3ms
     CGroup: /system.slice/gsad.service
             ├─57707 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
             └─57709 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392


Mar 24 18:13:28 Kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Mar 24 18:13:28 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 Fri 2023-03-24 18:13:23 UTC; 5s ago
       Docs: man:gvmd(8)
   Process: 57631 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 57637 (gvmd)
      Tasks: 1 (limit: 4606)
     Memory: 164.6M
        CPU: 360ms
     CGroup: /system.slice/gvmd.service
             └─57637 "gvmd: gvmd: Wa" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Mar 24 18:13:23 Kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Mar 24 18:13:23 Kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: Operation not permitted
Mar 24 18:13:23 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 Fri 2023-03-24 18:13:23 UTC; 5s ago
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 57613 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=
   Main PID: 57619 (ospd-openvas)
      Tasks: 5 (limit: 4606)
     Memory: 50.2M
        CPU: 391ms
     CGroup: /system.slice/ospd-openvas.service
             ├─57619 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-
openvas.conf --log-config /etc/gvm/ospd-logging.conf
             └─57623 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-
openvas.conf --log-config /etc/gvm/ospd-logging.conf

Mar 24 18:13:22 Kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)...
Mar 24 18:13:23 Kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).

[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
```

b. A browser window will open with a security warning that can be ignored. If the browser does not automatically open, start your browser manually and navigate to **https://127.0.0.1:9392**. Click the **Advanced** button and scroll down and accept the risk on the warning screen to proceed.
c. In the Greenbone Security Assistant login box, enter **admin** as the username and **kali** as the password.

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

d. 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 **Task Wizard** from the dropdown menu.

Step 3: Scan the Target Host for Vulnerabilities

In this step you will scan the same target computer for vulnerabilities that you did with the earlier Nmap scan.

a. In the **IP address or hostname** box, enter the IP address **10.6.6.23** or **gravemind.vm**. Click the **Start Scan** button at the bottom of the screen. The scan will take a few minutes, so wait for it to complete. The status and percent complete are displayed on the screen. The scan will be finished when the status changes to **Done**.
b. Click the number under the **Reports** column while the scanning is running for the associated scan.
c. When the scan is complete, click the timestamp under the **Date** column to view the report detail.
d. The CVEs associated with the vulnerabilities that were found on the host can be viewed by clicking the **CVEs** tab. Explore the other tabs.
e. Download the report by clicking **the Download Filtered Report** button from the menu in the upper left of the report page. It has a downward-pointing arrow icon. In the settings box, choose to download the report in PDF format. After a brief delay, the PDF file should open in your browser.

Are the CVEs reported by GVM the same as the CVEs reported by the Nmap scan?

Answer Area

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

What is the severity level of the CVEs found by the GVM scan?

Answer Area

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

f. Click the other headers on the report and view the information provided. Compare this information with what you discovered in Part 1.

Step 4: Clean Up

When you are done with GVM services, use the following command to stop GVM.

```
┌──(kali㉿Kali)-[~]
└─$ sudo gvm-stop
```

Reflection Questions

1. In your opinion, which tool is easier to use? Explain.

Answer Area

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

2. It is recommended to keep the databases of vulnerabilities updated every few days. Research on the internet the necessary commands to update the GVM CVE database. Why do you think it is necessary to keep a database of all CVEs (current and past) for use by vulnerability scanners?

Answer Area

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