

GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

PRACTICAL – 4

Aim : Labs of Vulnerability Assessment using OpenVAS

Finding the Vulnerability of Kali Linux :

Step 1 : Starting the OpenVAS Virtual Machine

```
Welcome to Greenbone OS 22.04.3 (tty1)

The web interface is available at:

    http://192.168.235.140

gsm login: _
```

Step 2 : Starting the Kali Linux Virtual Machine

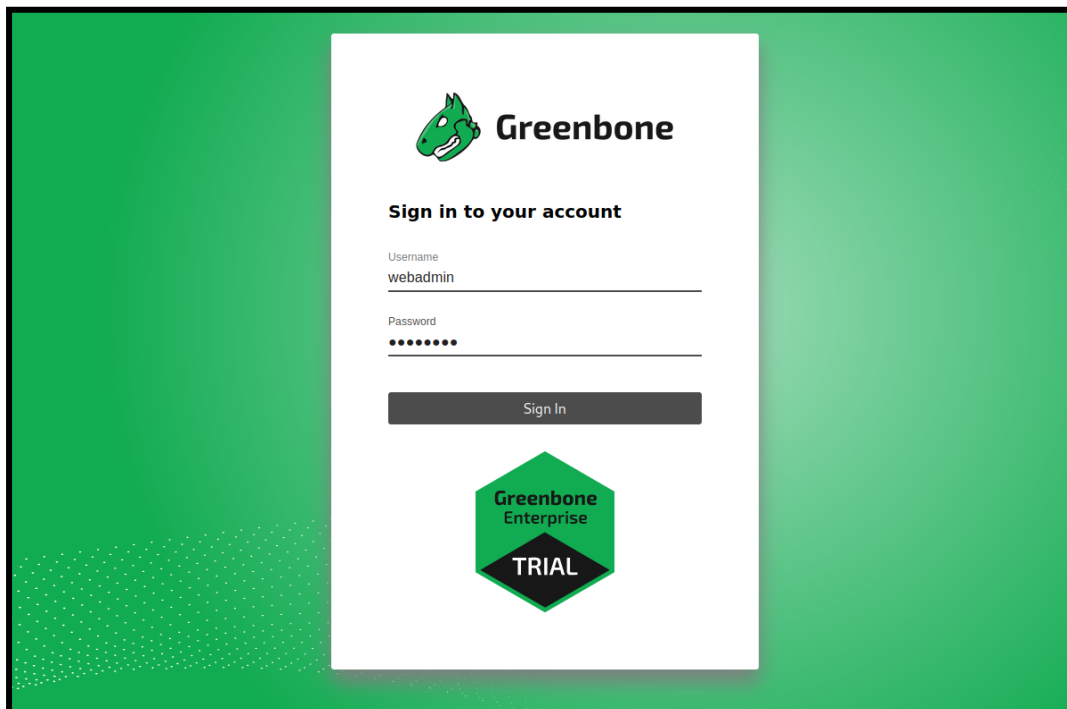


Step 3 : Go to the Web interface of the OpenVAS

Open Browser and visit the link <http://192.168.235.140> which is given in the OpenVAS Virtual Machine. In case of Warning page, Go to Advanced > Accept Risk and Continue

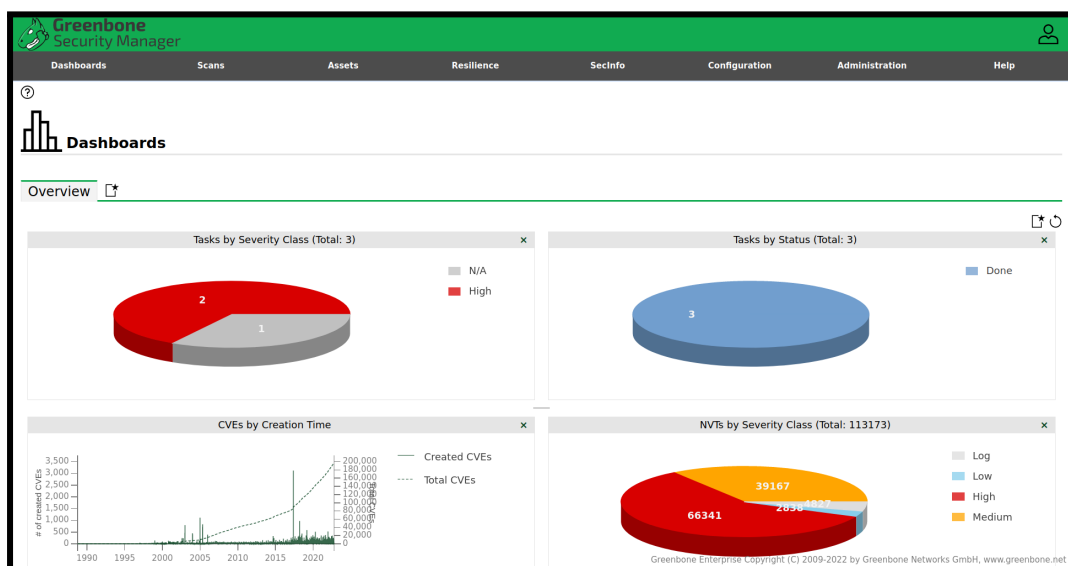
Step 4 : Login Page

Login into the OpenVAS using the username and password as **webadmin**



Step 5 : Dashboard Page

We can see the Dashboard Page in which we have overview of the previous scans with all their Severity



Step 6 : Starting the Machine which we use for Vulnerable Scanning

Starting Metasploitable 3 Virtual Machine and getting its IP Address

Name : Sanjay Sukhwani

Enrollment Number : 20012021053

Batch : B.tech(IT) - AB12

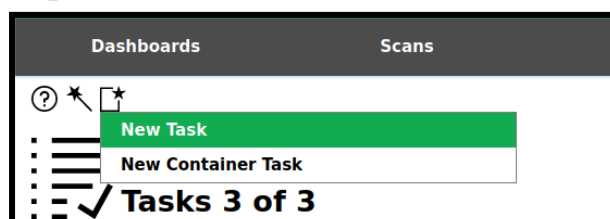
```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:71:6c:74
          inet addr:192.168.235.129  Bcast:192.168.235.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe71:6c74/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4792 (4.6 KB)  TX bytes:7570 (7.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

```

Step 7 : New tasks



Step 9 : Creating New Target

We have to create the target for which we are scanning the system

New Target

Name

Metasploitable2_053

Comment

This is a Metasploitable Target Form

Hosts

Manual

192.168.235.129

From file

Browse...

No file selected.

Exclude Hosts

Manual

From file

Browse...

No file selected.

Allow simultaneous scanning via multiple IPs

Yes

No

Port List

All IANA assigned TCP

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

--

on port

22

SMB

--

ESXi

--

SNMP

--

Cancel

Save

Step 10 : Creating New Task

Now we will fill in the details like Name of our scanning, Comment, Short Description about the Scanning, Hosts . In Hosts, we will select the target to do scan on it

New Task

Name

Sanjay-Metasploitable2

Comment

This is A Vulnerability Scanning for Metasploitable 2

Scan Targets

Metasploitable2_053

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70

%

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Order for target hosts

Sequential

Maximum concurrently executed NVTs per host

4

Maximum concurrently scanned hosts

20

Cancel

Save

Step 11 : Task Running

New Task

Name ▲	Status
MyScanMetasploitable3	Done
OpenVAS	Done
openvas scanning	Done
Sanjay-Metasploitable2 (This is A Vulnerability Scanning for Metasploitable 2)	New

Task Requested

Name ▲	Status
MyScanMetasploitable3	Done
OpenVAS	Done
openvas scanning	Done
Sanjay-Metasploitable2 (This is A Vulnerability Scanning for Metasploitable 2)	Requested

Task Running

Name ▲	Status
MyScanMetasploitable3	Done
OpenVAS	Done
openvas scanning	Done
Sanjay-Metasploitable2 (This is A Vulnerability Scanning for Metasploitable 2)	94 %

Task Done

Name ▲	Status
MyScanMetasploitable3	Done
OpenVAS	Done
openvas scanning	Done
Sanjay-Metasploitable2 (This is A Vulnerability Scanning for Metasploitable 2)	Done

Step 12 : Gather Information about the Target and Task

Reports of Severity and Status

[From Reports Page under Scans Menu]

Status	Task	Severity	High	Medium	Low	Log	False Pos.
Done	Sanjay-Metasploitable2	10.0 (High)	25	40	5	90	0
Done	openvas scanning	10.0 (High)	1	0	0	32	0
Done	OpenVAS	10.0 (High)	1	0	0	32	0
Done	MyScanMetasploitable3	N/A	0	0	0	0	0


Report Information in Detail :

[Click on Report Link Column in Task Page under Scans Menu]






Basic Information :

Task Name	Sanjay-Metasploitable2
Comment	This is A Vulnerability Scanning for Metasploitable 2
Scan Time	Sun, Apr 16, 2023 4:14 PM UTC - Sun, Apr 16, 2023 4:54 PM UTC
Scan Duration	0:40 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)

Operating Systems

Operating System	CPE	Hosts	Severity ▼
 Ubuntu 8.04	cpe:/o:canonical:ubuntu_linux:8.04	1	10.0 (High)

Applications in the Target Machine with Occurences and Severity

Application CPE	Hosts	Occurrences	Severity ▼
 cpe:/a:mysql:mysql:5.0.51a	1	1	9.0 (High)
 cpe:/a:postgresql:postgresql:8.3.1	1	1	9.0 (High)
cpe:/a:unrealircd:unrealircd:3.2.8.1	1	1	8.1 (High)
cpe:/a:samba:samba:3.0.20	1	1	6.0 (Medium)
 cpe:/a:apache:http_server:2.2.8	1	1	4.3 (Medium)
cpe:/a:proftpd:proftpd:1.3.1	1	1	N/A
cpe:/a:postfix:postfix	1	3	N/A
cpe:/a:oracle:mysql:5.0.51a	1	1	N/A
cpe:/a:twiki:twiki:01.Feb.2003	1	3	N/A
cpe:/a:phpmyadmin:phpmyadmin:3.1.1	1	3	N/A
cpe:/a:jquery:jquery:1.3.2	1	2	N/A
cpe:/a:isc:bind:9.4.2	1	1	N/A
 cpe:/a:php:php:5.2.4	1	3	N/A
 cpe:/a:openbsd:openssh:4.7p1	1	1	N/A

Ports Details

Port	Hosts	Severity ▼
80/tcp	1	10.0 (High)
512/tcp	1	10.0 (High)
513/tcp	1	10.0 (High)
1099/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)
3306/tcp	1	9.0 (High)
5432/tcp	1	9.0 (High)
5900/tcp	1	9.0 (High)
6697/tcp	1	8.1 (High)
21/tcp	1	7.5 (High)
22/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	6.8 (Medium)
445/tcp	1	6.0 (Medium)
23/tcp	1	4.8 (Medium)

Vulnerability Details with Severity and Location

Vulnerability		Severity ▼	QoD	Host		Location
				IP	Name	
rlogin Passwordless Login	🔓	10.0 (High)	80 %	192.168.235.129		513/tcp
TWiki XSS and Command Execution Vulnerabilities	🔓	10.0 (High)	80 %	192.168.235.129		80/tcp
Operating System (OS) End of Life (EOL) Detection	🔓	10.0 (High)	80 %	192.168.235.129		general/tcp
Possible Backdoor: Ingreslock	🔓	10.0 (High)	99 %	192.168.235.129		1524/tcp
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	🔓	10.0 (High)	95 %	192.168.235.129		1099/tcp
The rexec service is running	🔓	10.0 (High)	80 %	192.168.235.129		512/tcp
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	🔓	10.0 (High)	99 %	192.168.235.129		8787/tcp
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	🔓	9.8 (High)	99 %	192.168.235.129		8009/tcp
DistCC RCE Vulnerability (CVE-2004-2687)	🔓	9.3 (High)	99 %	192.168.235.129		3632/tcp
PostgreSQL weak password	🔓	9.0 (High)	99 %	192.168.235.129		5432/tcp
VNC Brute Force Login	🔓	9.0 (High)	95 %	192.168.235.129		5900/tcp
MySQL / MariaDB weak password	🔓	9.0 (High)	95 %	192.168.235.129		3306/tcp
UnrealIRCd Authentication Spoofing Vulnerability	🔓	8.1 (High)	80 %	192.168.235.129		6697/tcp

Information about Task :

Name	Sanjay-Metasploitable2
Comment	This is A Vulnerability Scanning for Metasploitable 2
Alterable	No
Status	Done

Target

Metasploitable2_053

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	sequential
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	40 minutes
Average Scan duration	40 minutes
Auto delete Reports	Do not automatically delete reports