UNIVERSITI MALAYSIA TERENGGANU

UMT

COURSE:

CSF3404 : CYBER SECURITY

PROGRAMME:

BACHELOR OF COMPUTER SCIENCE (SOFTWARE ENGINEERING) WITH HONOURS

LECTURER:

SIR FAKHRUL ADLI BIN MOHD ZAKI

CLASS:

K3

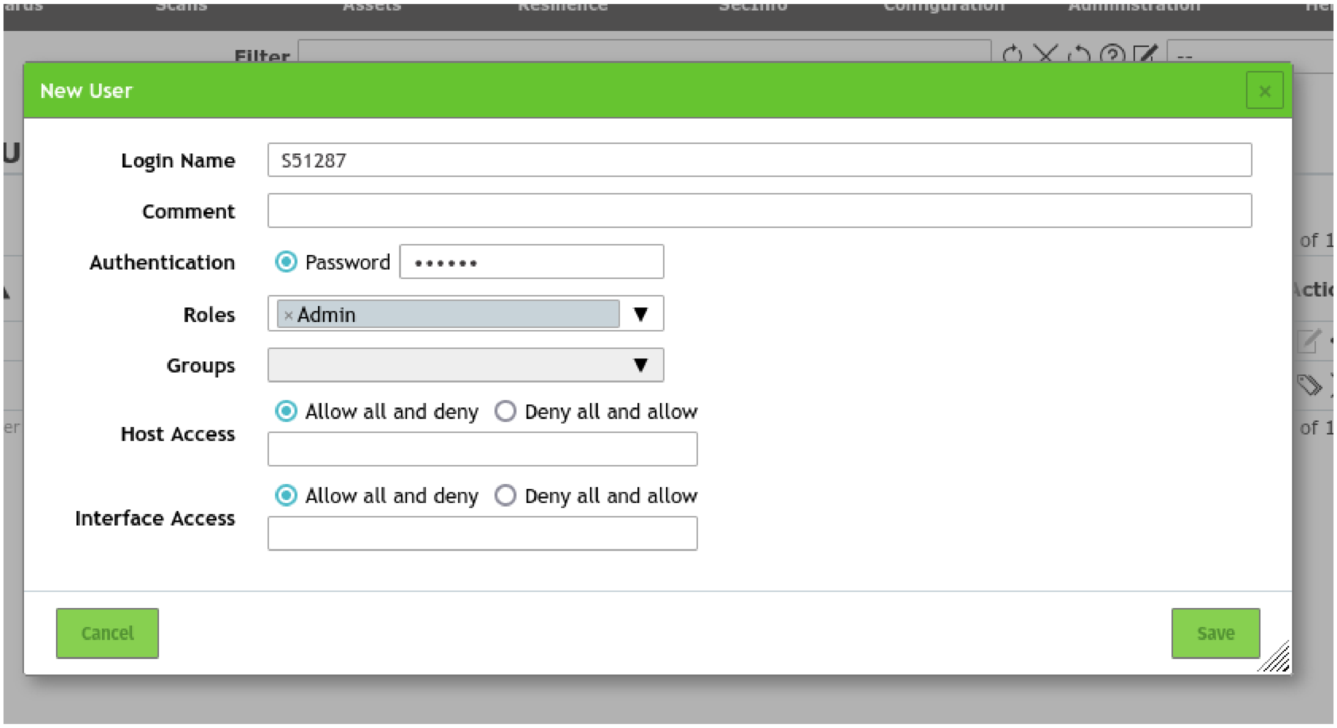
TOPIC:

LAB 6 : Scanning Vulnerabilities (Part 2)

NAME:

NAME	MATRIC NUMBER
MOHAMAD HAFIZ HAZIQ BIN MOHAMAD NAZRI	S51287

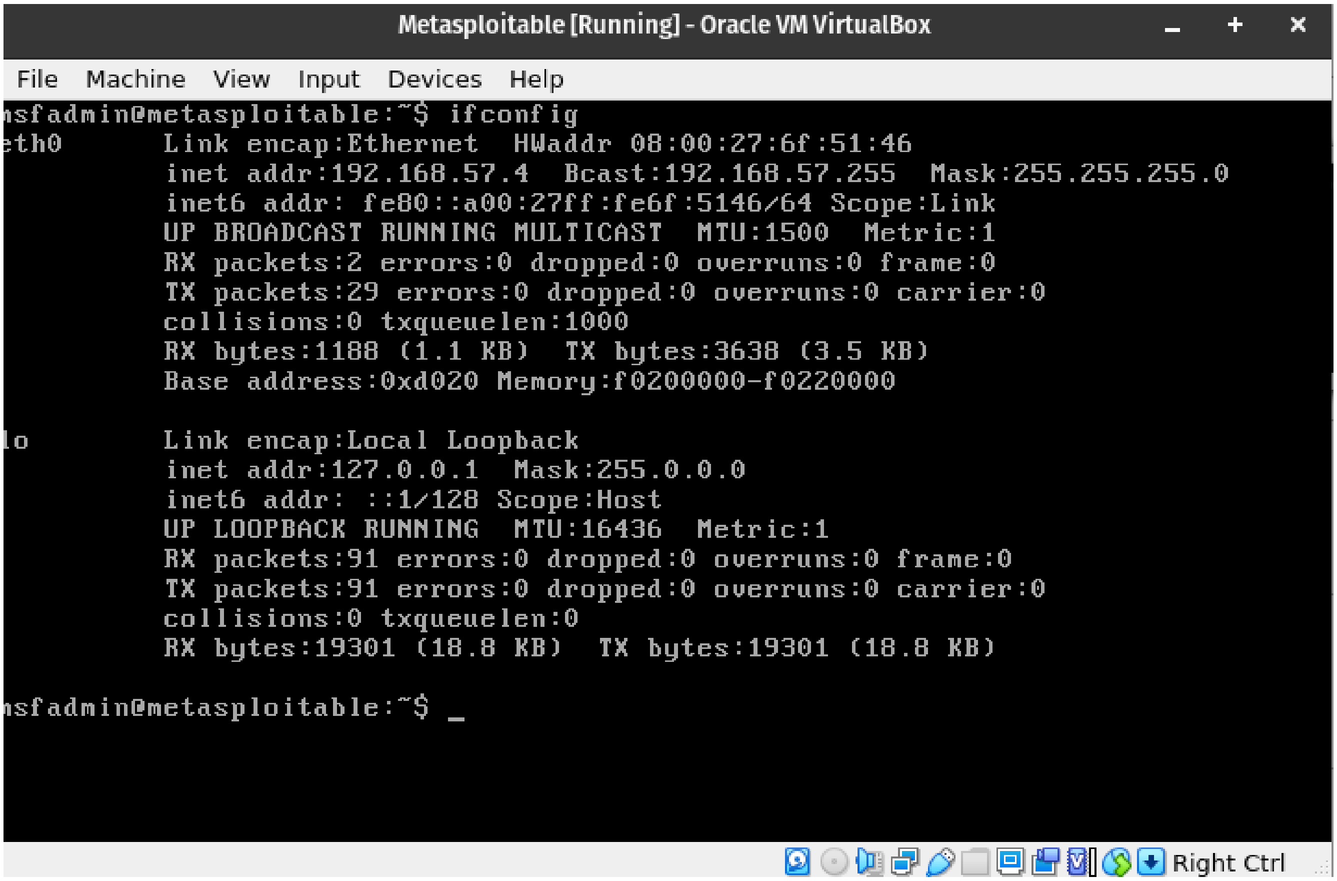
Task 1: Running Green Bone Security Manager (GSM)



New User

Login Name	S51287
Comment	
Authentication	● Password ••••••
Roles	× Admin ▼
Groups	▼
Host Access	● Allow all and deny ○ Deny all and allow
Interface Access	● Allow all and deny ○ Deny all and allow

Task 2: Setting Up The Network for Metasploitable



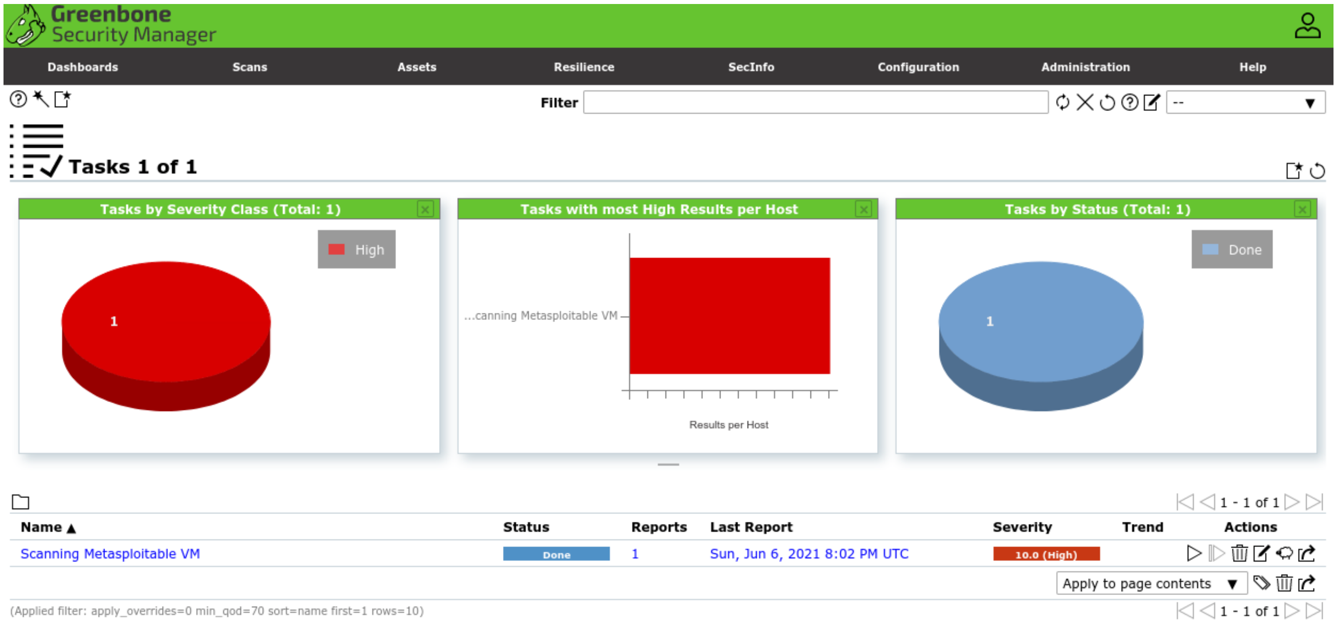
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6f:51:46
          inet addr:192.168.57.4  Bcast:192.168.57.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:5146/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

Task 3: Scanning The Vulnerabilities In Metasploitable

12.



1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scanning Metasploitable VM	Done	1	Sun, Jun 6, 2021 8:02 PM UTC	10.0 (High)		

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 1 of 1

16.

a.

Severity	Total
High	22
Medium	36
Low	2
Log	85
Grand Total	145

b. What are vulnerabilities that have the highest severities? List them.

- rlogin Passwordless Login
- TWiki XSS and Command Execution Vulnerabilities
- OS End Of Life Detection
- Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability
- Possible Backdoor: Ingreslock
- Distributed Ruby (dRuby.DRb) Multiple Remote Code Execution Vulnerabilities
- The rexec service is running

c. What is the vulnerability for port 513/tcp?

rlogin Passwordless Login

d. List three (3) vulnerabilities with medium severity.

- /doc directory browsable
- Anonymous FTP Login Report
- FTP Unencrypted Cleartext Login

e. Based on the given information by GSM, how do we solve the “VNC Brute Force” vulnerability?

Lock account for the certain amount of time if there are too many incorrect password attempts.

Reflection Questions

1. **In your own words, explain about Common Vulnerability Scanning System (CVSS) and Common Vulnerability Enumeration (CVE).**
   - CVE is a special identifier that used to catalog individual security vulnerabilities.
   - CVSS is used to get score that based on different factors to know the importance of vulnerability.

2. **Explain the difference(s) between CVSS and CVE.**

CVSS	CVE
Total score assigned to a vulnerability	List of all publicly disclosed vulnerabilities
Require NVD	Not require NVD

3. **How many severity levels are there in the CVSS version 3.0?**

   5 severity levels.

4. **Draw a table CVSS 3.0 severity levels and their score range.**

Severity	Base Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

5. **Observe the information provided at vuldb.com and answer the question below:**

   a) **List three (3) most recent vulnerabilities and their severities.**

Vulnerability	Severity
EmTec ZOC unknown vulnerability	Low
Mintty Bracketed Paste Mode unknown vulnerability	Low
Auth0 auth0-lock Sign In cross site scripting	Low

b) List three (3) latest available exploits.

- Vmware vCenter Server Virtual SAN Health Check unknown vulnerability
- BigTree CMS Settings unknown vulnerability
- Microsoft Exchange unknown vulnerability

c) List three (3) vulnerabilities in current CVSS Top 5.

- QEMU vshost-user-gpu out-of-bounds write
- Cisco SD-WAN CLI unnecessary privileges
- Linux Kernel io_uring Subsystem mem heap-based