Task 4

by ashfin

Vulnerability assessment

Challenge Information

. VM Setup: Vulnerable VM imported via the Drive-provided OVA.

· Attacker Machine: Kali Linux 2025.2

o IP: 192.168.56.102

· Target Machine: Ubuntu 14.04

o IP: 192.168.56.101

.

Objective: Download and run the provided OVA VM in VirtualBox,

perform a vulnerability assessment, exploit the system, and

document each step in a professional report.

Tools Used:

. Nmap - Service & version detection

. Metasploit Framework (msf6) - Exploitation

. Browser (Firefox) - Web directory analysis

. Manual Enumeration - Validation

1. Environment Setup:

. Imported the OVA file from the provided link into VirtualBox.

. Ensured both the Kali VM and the target VM were on

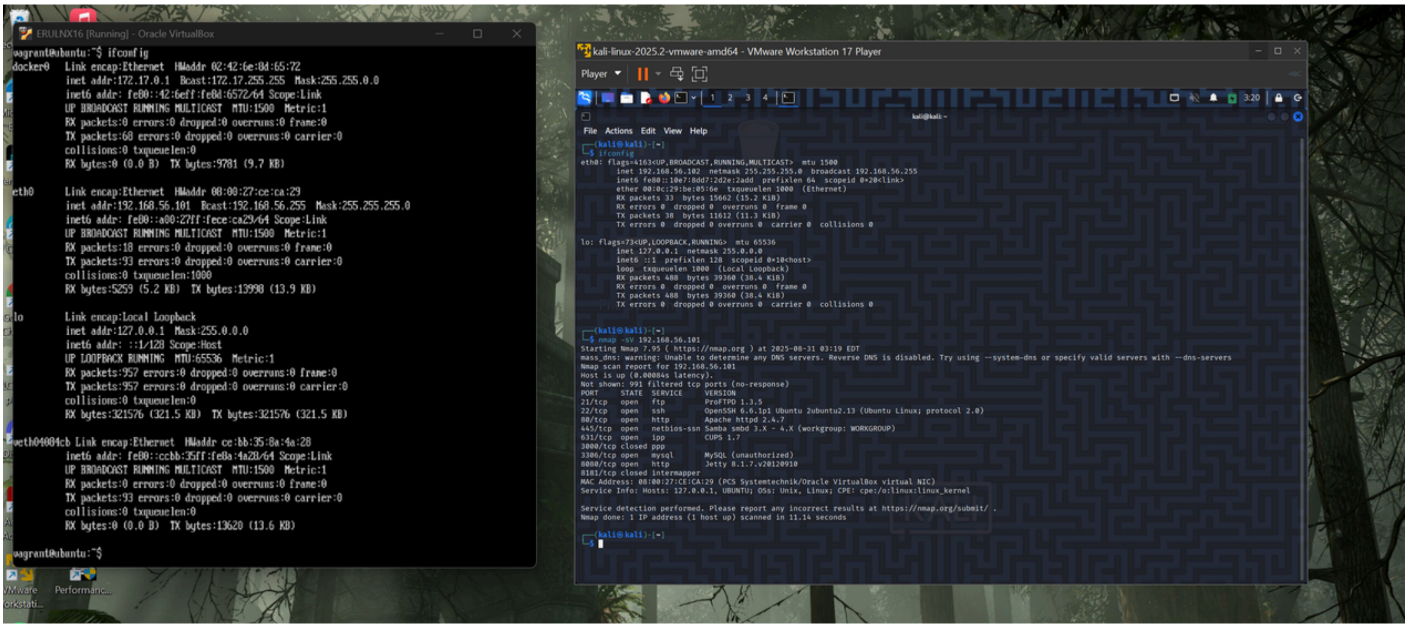
Host-Only Network for direct communication.

2. Enumeration & Discovery

2.1 - Service Scan

. Command: nmap -sV 192.168.56.102

. Result: 21/tcp open ftp ProFTPD 1.3.5



ERULNX16 [Running] - Oracle VirtualBox
VMware Workstati...
Performanc...
kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
kali@kali: ~
File
Actions
Edit
View
Help

```
vagrant@ubuntu:~$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:6e:8d:65:72
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:6eff:fe8d:6572/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:9781 (9.7 KB)

eth0      Link encap:Ethernet  HWaddr 08:00:27:ce:ca:29
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fece:ca29/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5259 (5.2 KB)  TX bytes:13998 (13.9 KB)

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:65536  Metric:1
          RX packets:957 errors:0 dropped:0 overruns:0 frame:0
          TX packets:957 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:321576 (321.5 KB)  TX bytes:321576 (321.5 KB)

veth04084cb Link encap:Ethernet  HWaddr ce:bb:35:8a:4a:28
          inet6 addr: fe80::ccbb:35ff:fe8a:4a28/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:13620 (13.6 KB)

vagrant@ubuntu:~$
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::10e7:8dd7:2d2e:2add  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:be:05:6e  txqueuelen 1000  (Ethernet)
        RX packets 33  bytes 15662 (15.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 11612 (11.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 488  bytes 39360 (38.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 488  bytes 39360 (38.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-31 03:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00084s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:CE:CA:29 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU; 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 11.14 seconds

┌──(kali㉿kali)-[~]
└─$
```

2.1 - Service Notes

. FTP (ProFTPD 1.3.5): Vulnerable to mod_copy RCE (CVE-2015-3306).

. HTTP (Apache 2.4.7): Directory listing enabled -+ info disclosure.

· Samba (4.3.11): Message signing disabled -+ MITM risk.

. CUPS (1.7): PUT method allowed -+ possible file upload.

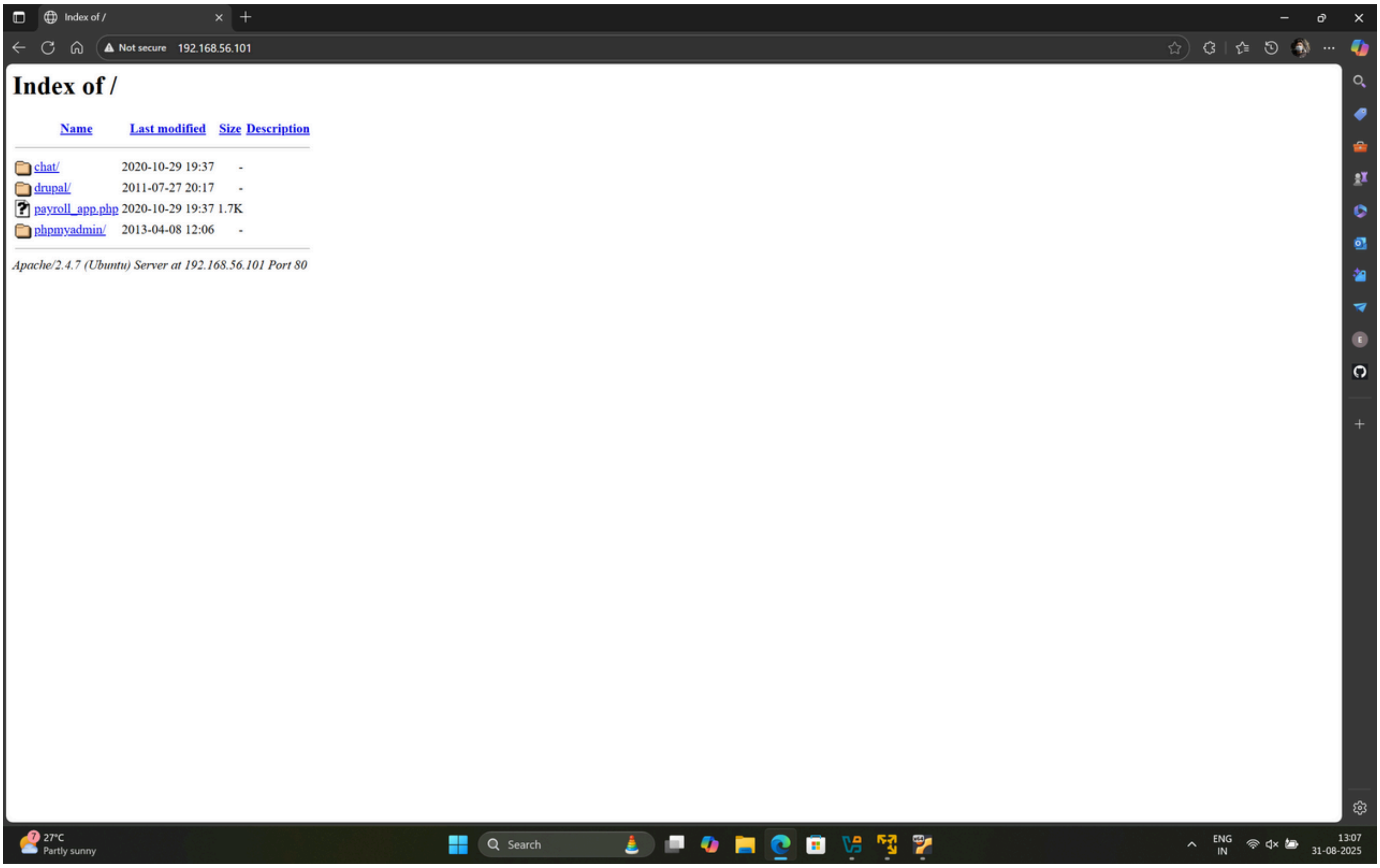
. MySQL: Externally accessible -+ brute-force/credential risk.

. Jetty (8.1.7): Outdated -+ known RCE exploits.

- Web Directory Listing

. Purpose: Identify web applications/files accessible via HTTP.

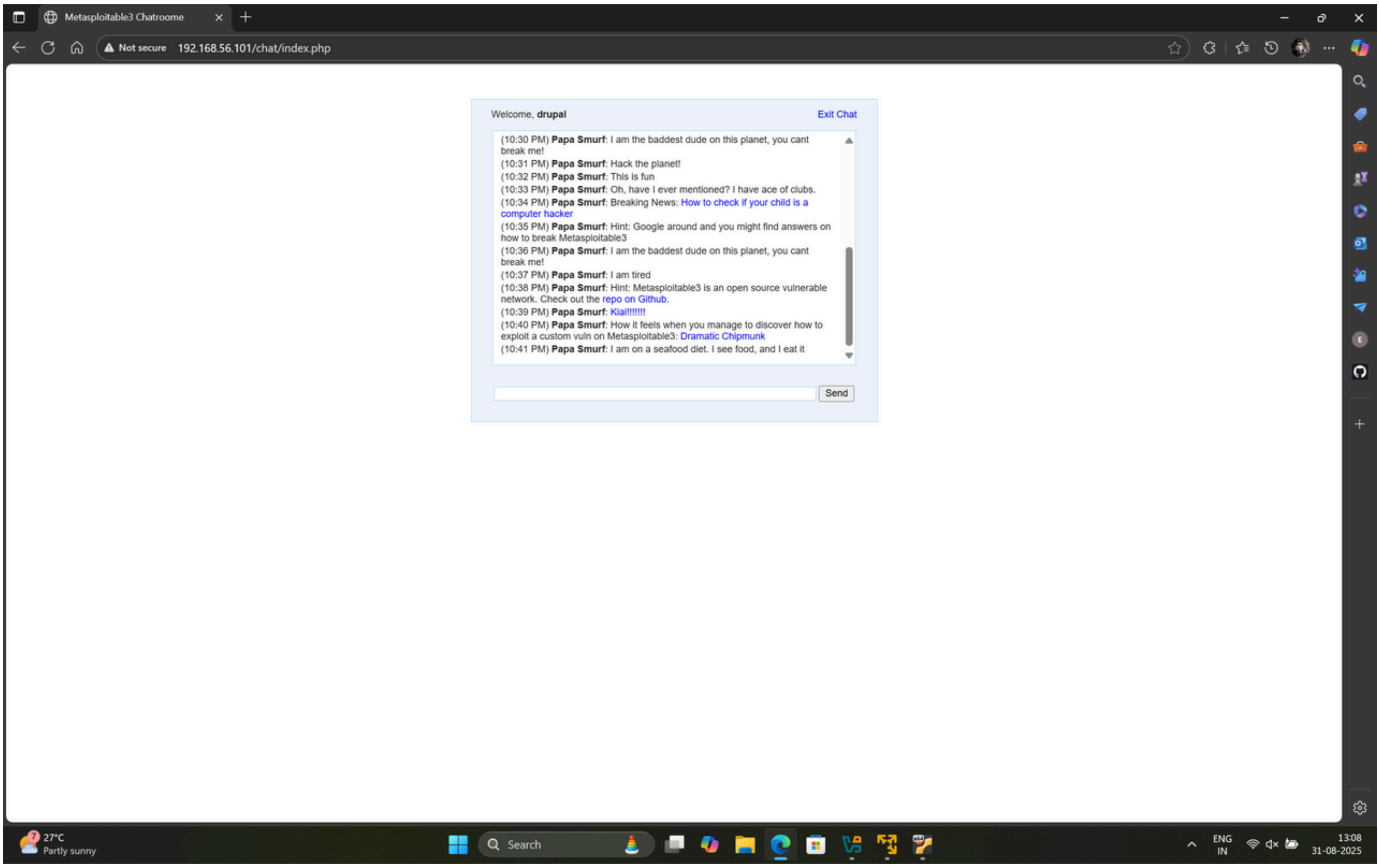
Visited http://192.168.56.102/ in a browser and confirmed directory listing exists.



Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.101 Port 80



Welcome, **drupal** Exit Chat

(10:30 PM) **Papa Smurf**: I am the baddest dude on this planet, you cant break me!
(10:31 PM) **Papa Smurf**: Hack the planet!
(10:32 PM) **Papa Smurf**: This is fun
(10:33 PM) **Papa Smurf**: Oh, have I ever mentioned? I have ace of clubs.
(10:34 PM) **Papa Smurf**: Breaking News: How to check if your child is a computer hacker
(10:35 PM) **Papa Smurf**: Hint: Google around and you might find answers on how to break Metasploitable3
(10:36 PM) **Papa Smurf**: I am the baddest dude on this planet, you cant break me!
(10:37 PM) **Papa Smurf**: I am tired
(10:38 PM) **Papa Smurf**: Hint: Metasploitable3 is an open source vulnerable network. Check out the repo on Github.
(10:39 PM) **Papa Smurf**: Kiai!!!!!!!
(10:40 PM) **Papa Smurf**: How it feels when you manage to discover how to exploit a custom vuln on Metasploitable3: Dramatic Chipmunk
(10:41 PM) **Papa Smurf**: I am on a seafood diet. I see food, and I eat it

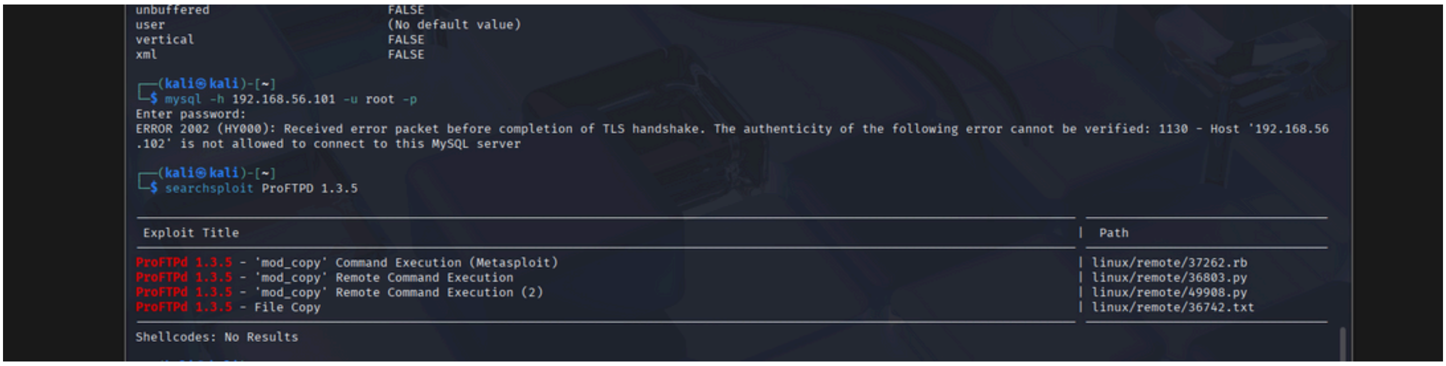
Send

Exploitation

The ProFTPD allows unauthorized file copying on the server. Found relevant Metasploit

module via:

Command: searchsploit ProFTPD 1.3.5



```
unbuffered                         FALSE
user                               (No default value)
vertical                           FALSE
xml                                FALSE

┌──(kali㉿kali)-[~]
└─$ mysql -h 192.168.56.101 -u root -p
Enter password:
ERROR 2002 (HY000): Received error packet before completion of TLS handshake. The authenticity of the following error cannot be verified: 1130 - Host '192.168.56
.102' is not allowed to connect to this MySQL server

┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.5
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                         | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                               | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                           | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                                         | linux/remote/36742.txt
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Conclusion

This assessment confirmed that the target VM contains multiple critical vulnerabilities, ProFTPD enabled file copying.