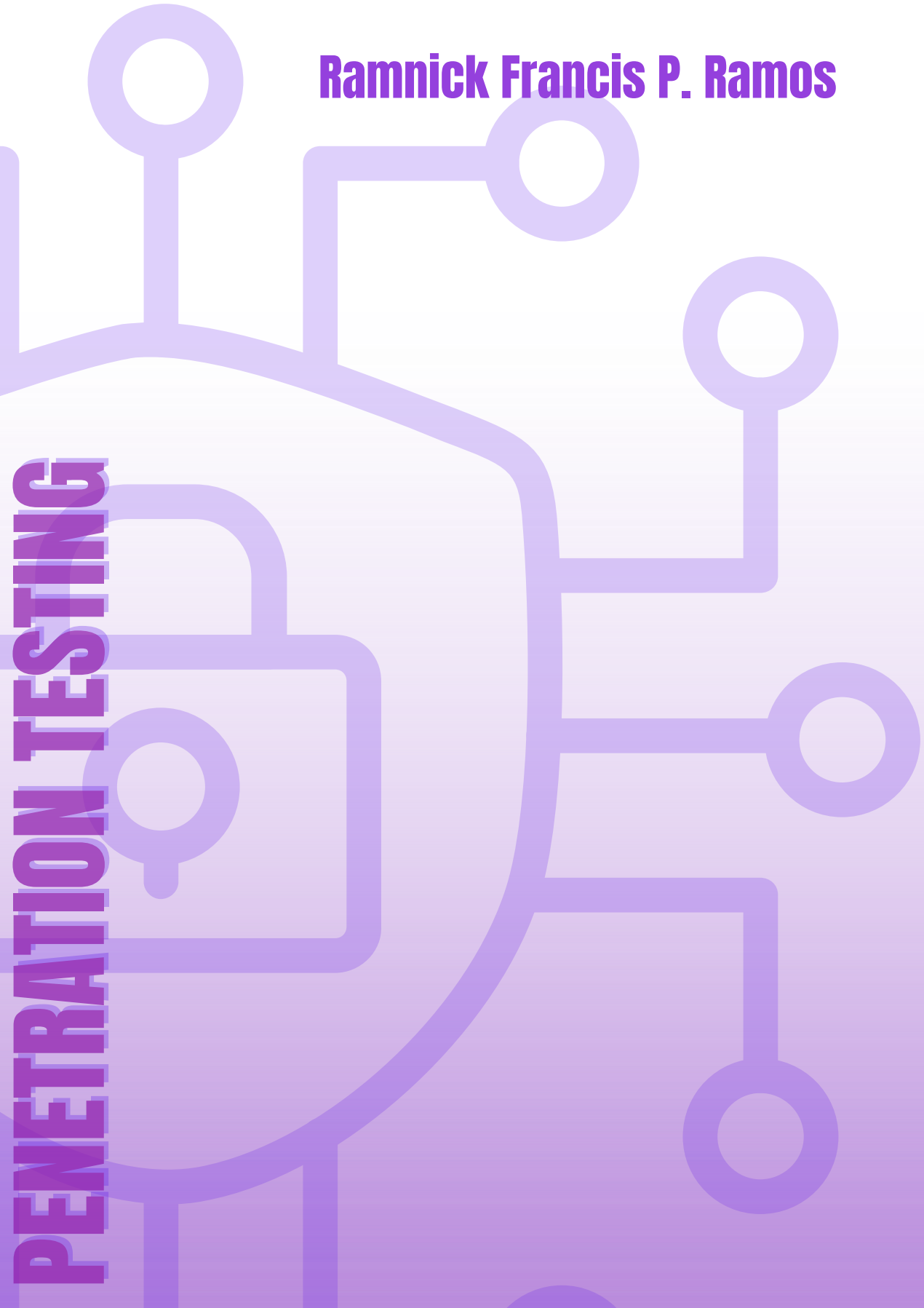
FTP Vulnerability Exploitation on PenTestLab VM

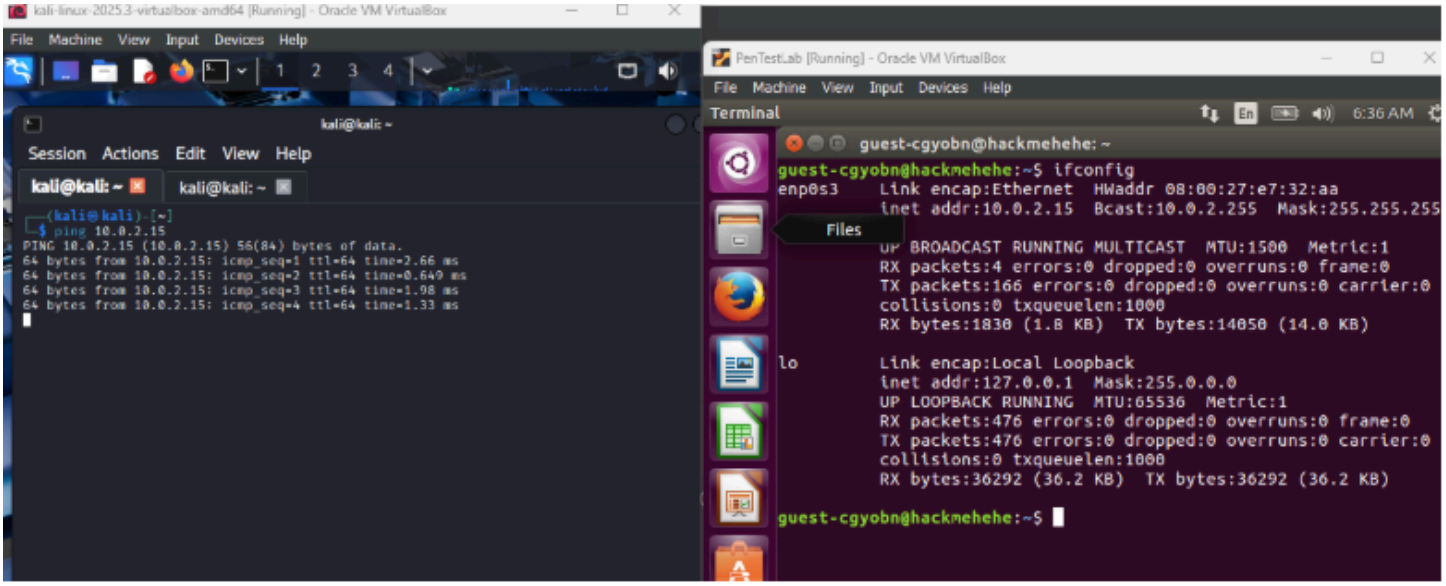
Ramnick Francis P. Ramos



PENETRATION TESTING

Executive Summary

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



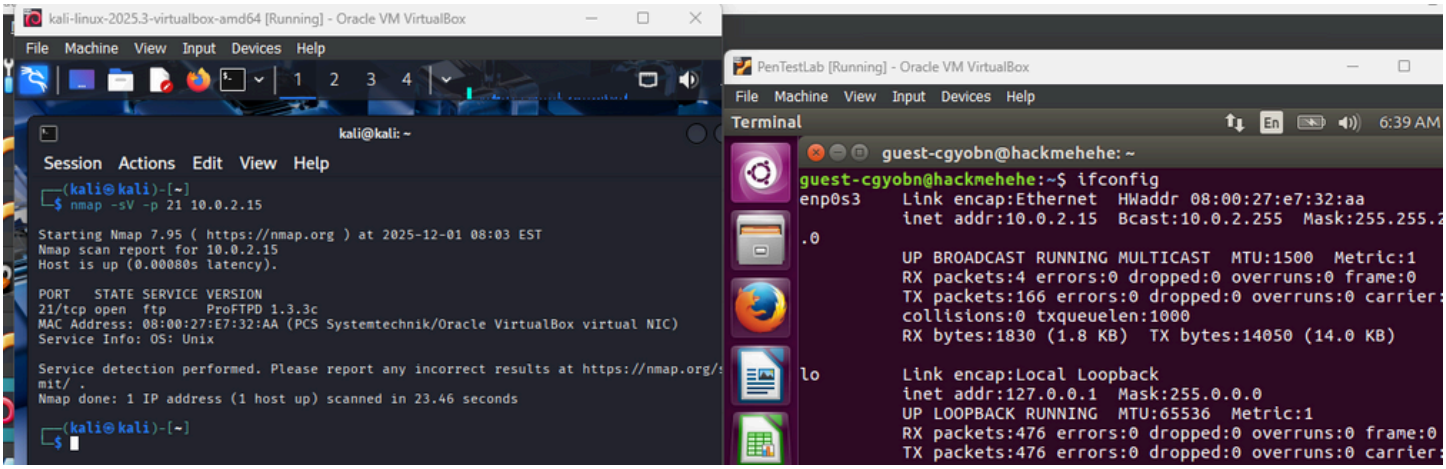
The objectives of the penetration test is to examine the attack surfaces of the machine through exploiting the vulnerabilities in the **FTP service** running on the machine.

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

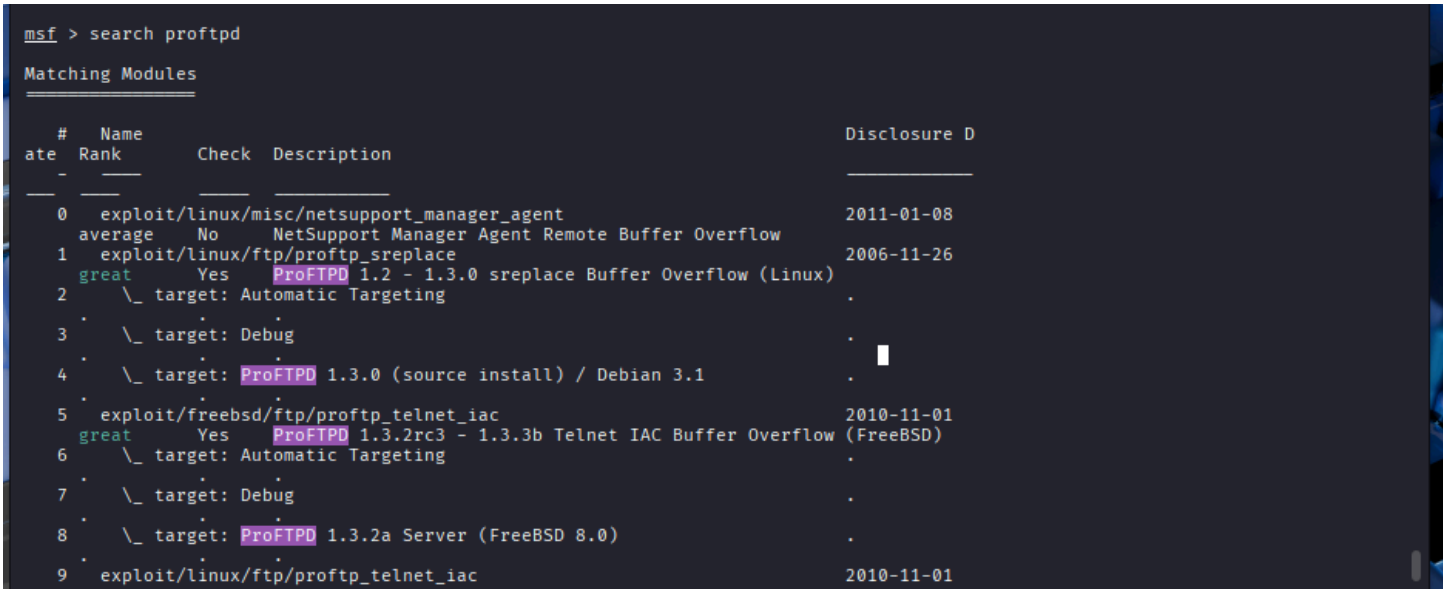
Service Enumeration



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.



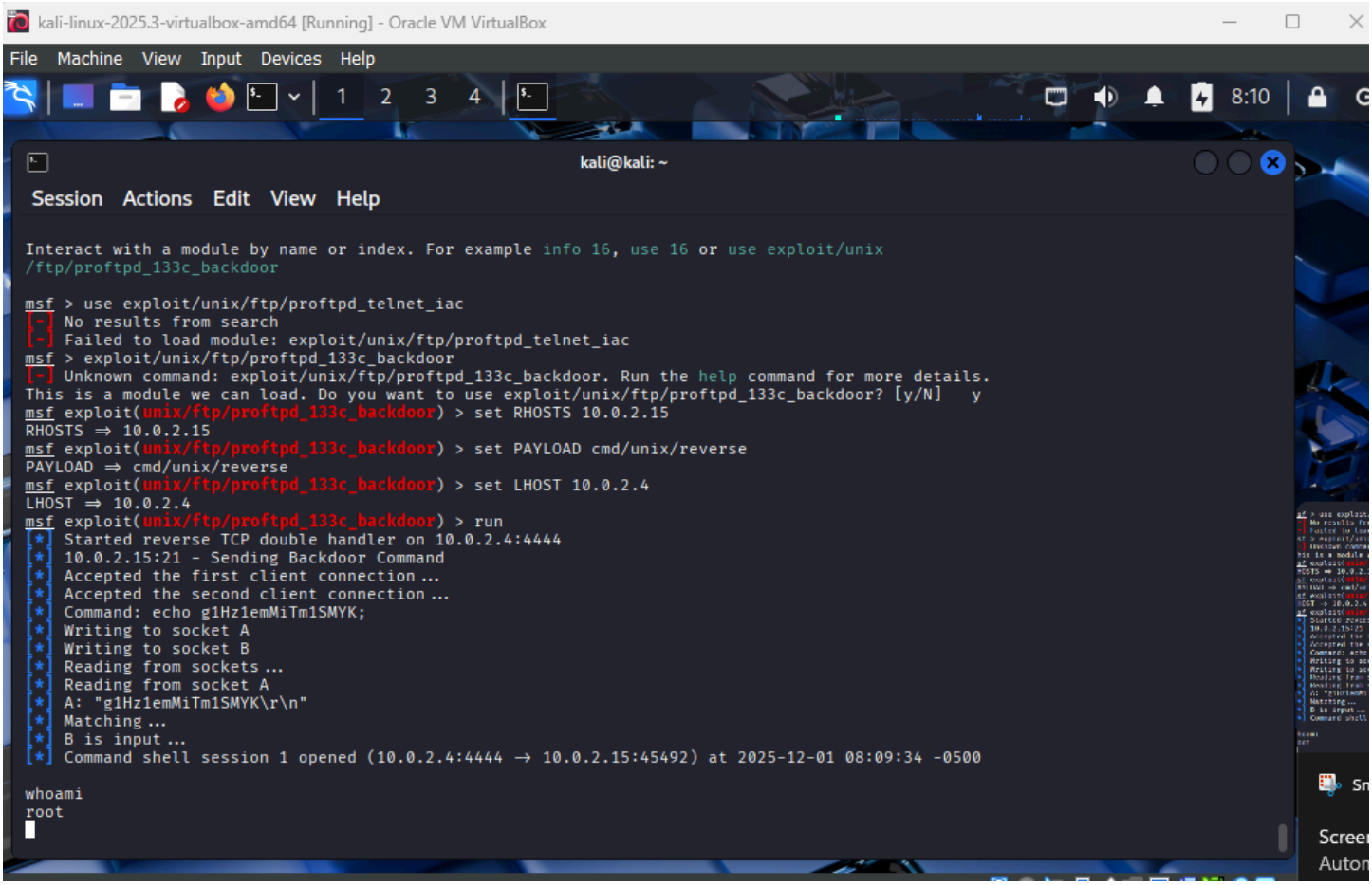
Using Metasploit, enumerated above is the possible vulnerabilities that can be exploited.

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 vulerability was chosen to be exploited.

```
   excellent  Yes     ProFTPD 1.3.5 Mod_Copy Command Execution
16  exploit/unix/ftp/proftpd_133c_backdoor                      2010-12-02
   excellent  No      ProFTPD-1.3.3c Backdoor Command Execution
```

Privilege Escalation



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**.