Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

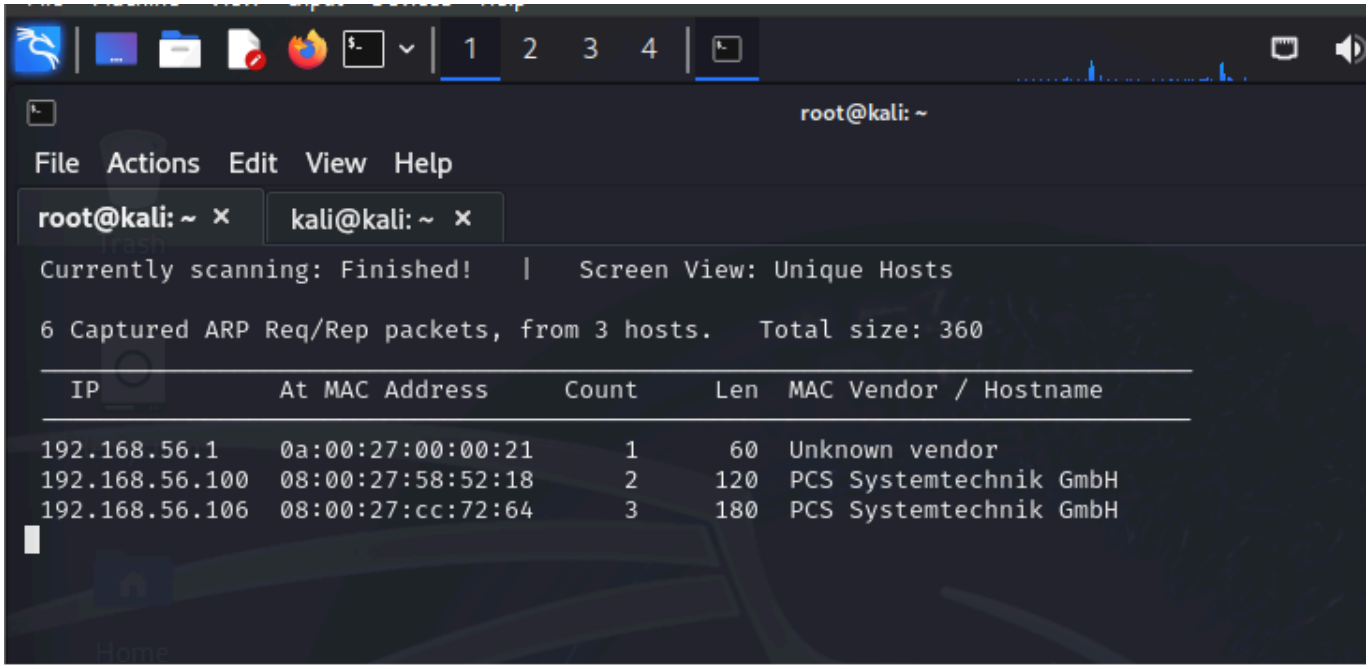
Name: Prajin P K

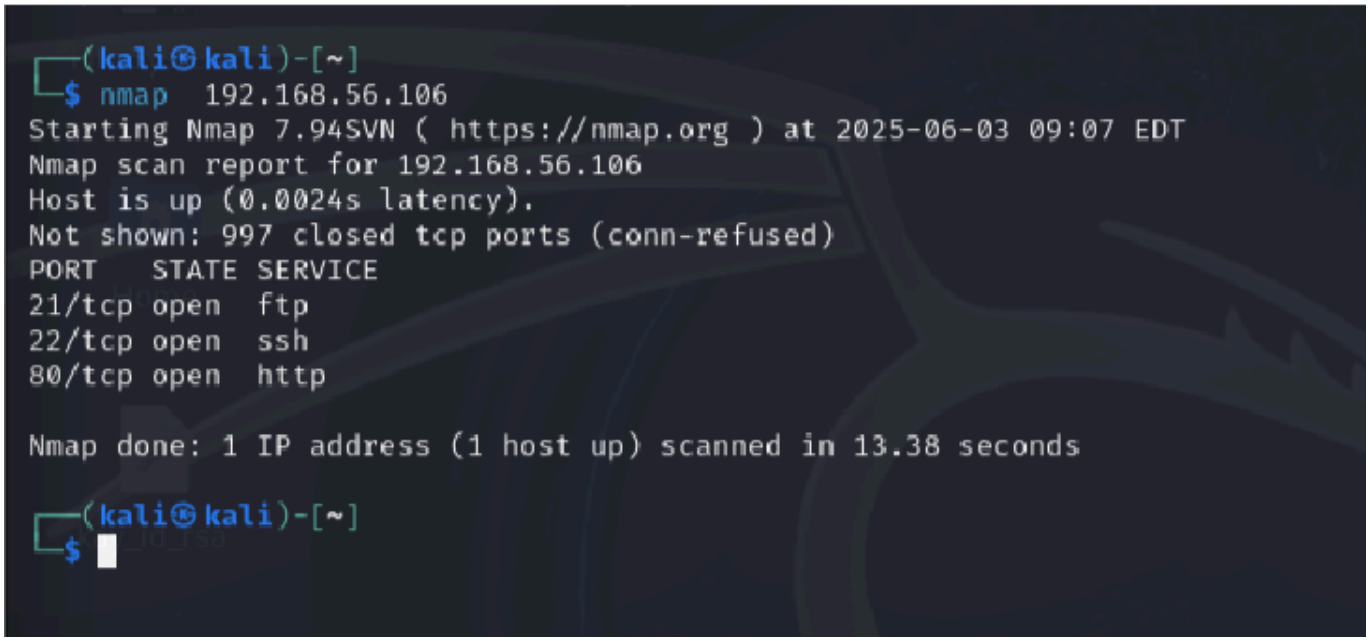
Date: June 3, 2025

This document provides a detailed walkthrough of the penetration testing steps conducted on the target machine with IP 192.168.56.106. Each section includes reconnaissance, enumeration, exploitation, and post-exploitation activities, along with observations, tools used, and relevant screenshots.

1. Recon & Scanning

Initial network scan was conducted using ARP requests and Nmap. The IP addresses of the hosts in the network were identified, and the target IP 192.168.56.106 was selected for further analysis. An Nmap scan revealed that ports 21 (FTP), 22 (SSH), and 80 (HTTP) were open.

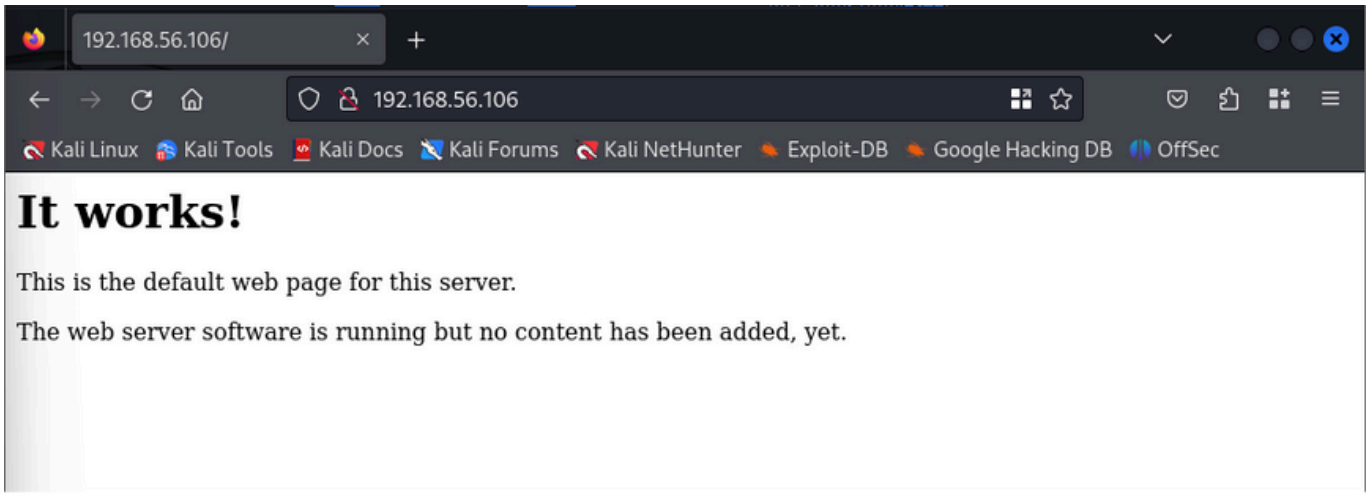




2. Enumeration

Enumeration was performed using tools such as web browser access and enum4linux. The HTTP service displayed a default Apache page, and enum4linux was used to gather information on SMB shares and

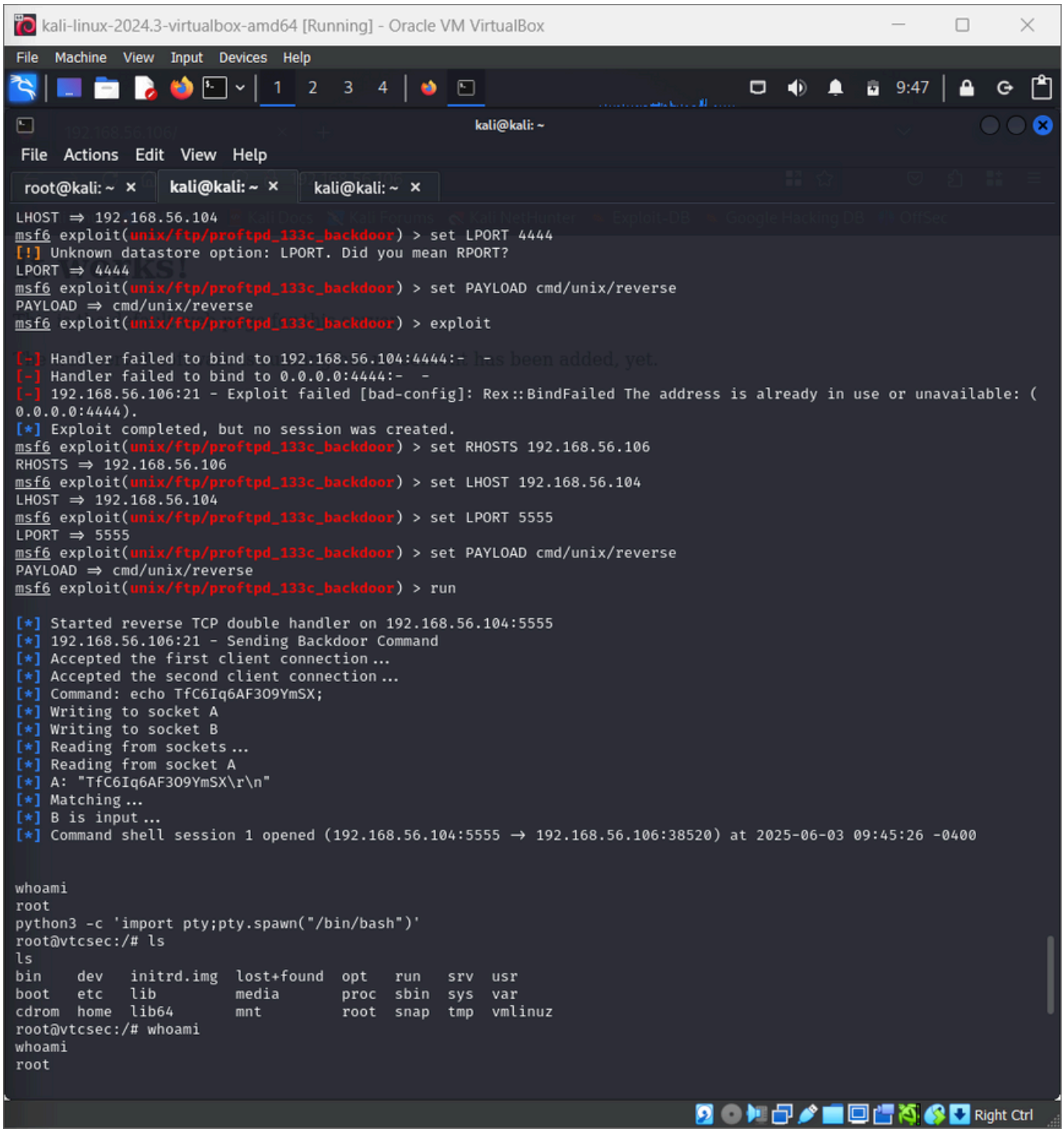
domain information. However, the enum4linux scan failed to retrieve detailed domain or session data.




```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.56.106

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jun  3 09:18:59 2025

 ========================================( Target Information )========================================

Target ........... 192.168.56.106
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.56.106 )============================


[E] Can't find workgroup/domain


 ==============================( Nbtstat Information for 192.168.56.106 )==============================

Looking up status of 192.168.56.106
No reply from 192.168.56.106

 =================================( Session Check on 192.168.56.106 )=================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

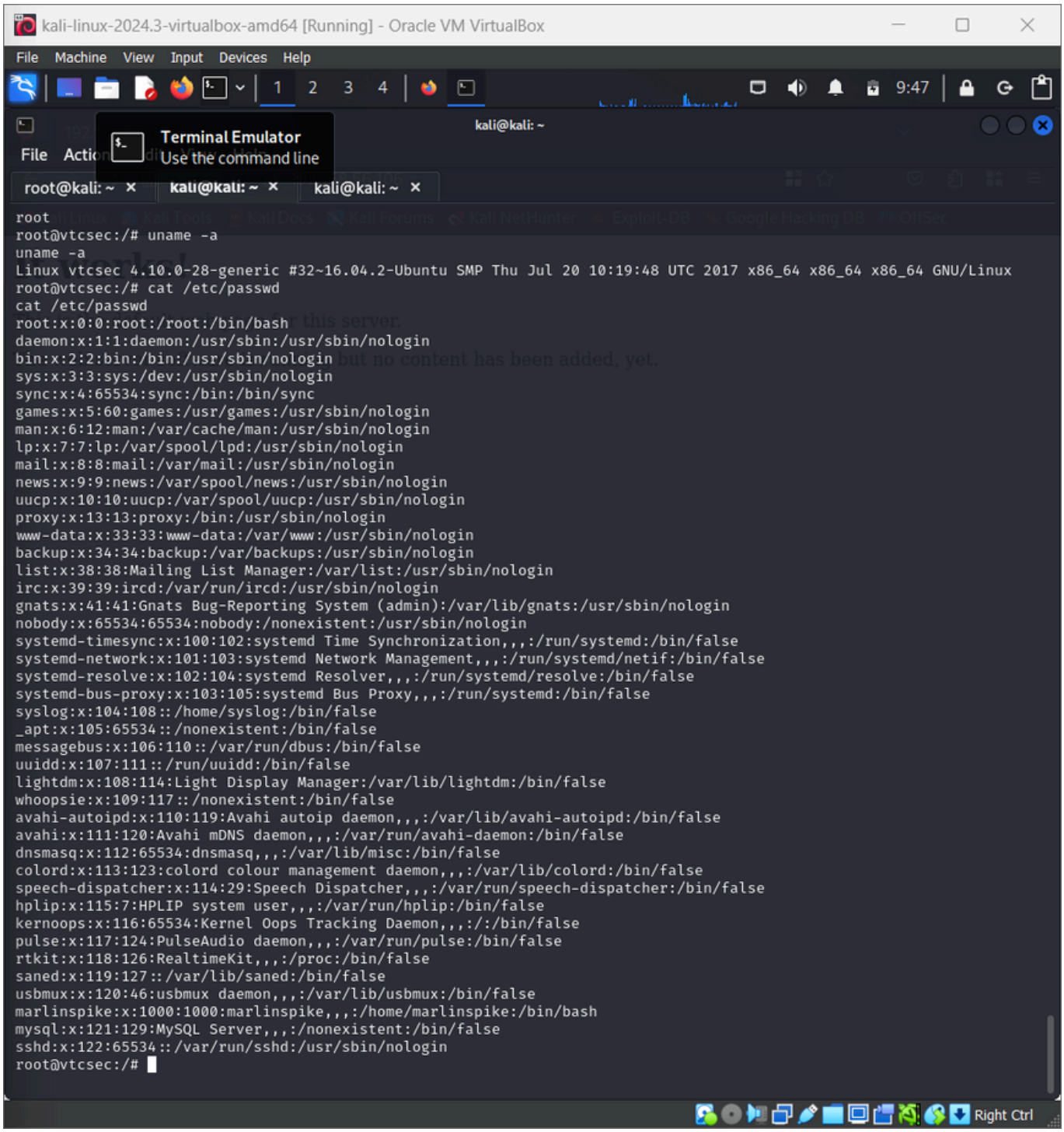
3. Exploitation

Metasploit Framework was used to exploit the target using the 'proftpd_133c_backdoor' module. A reverse TCP payload was configured, and upon execution, a session was successfully opened, granting shell access to the target.



4. Post Exploitation

Post-exploitation confirmed root access on the target system. Commands like 'whoami', 'id', and 'uname -a' were used to gather system information. Additionally, the '/etc/passwd' file was examined to enumerate users.



5. Summary

The penetration test was successful in identifying a vulnerable FTP service, exploiting it, and gaining root access to the target system. Enumeration attempts were partially successful, with limited domain information retrieved.

6. Lessons Learned

- Reconnaissance and scanning are critical to identifying attack surfaces.

- Enumeration results may vary depending on service configurations.

- Exploiting known vulnerabilities in outdated services can lead to full system compromise.

- Always verify the level of access gained during post-exploitation.

7. Suggestions for Defense

- Update and patch all services regularly.

- Disable or restrict unnecessary services such as FTP.

- Implement proper firewall rules to restrict access to critical ports.

- Monitor network traffic for suspicious activity and set up intrusion detection systems.