

# Penetration Testing Report on Ubuntu Machine (Black Box Approach)

**Date:** September 01, 2025

**Author:** Sebin Mathew

This report documents a comprehensive black box penetration test performed on an Ubuntu 14.04 LTS machine. The assessment aimed to simulate a real-world attack by starting without prior knowledge of the system. The objective was to identify vulnerabilities, gain unauthorized access, and uncover hidden CTF flags. Where conflicts existed between two reports, details from the primary penetration test were prioritized, while technical findings from Task 4 were integrated for completeness.

## Methodology

### Methodology

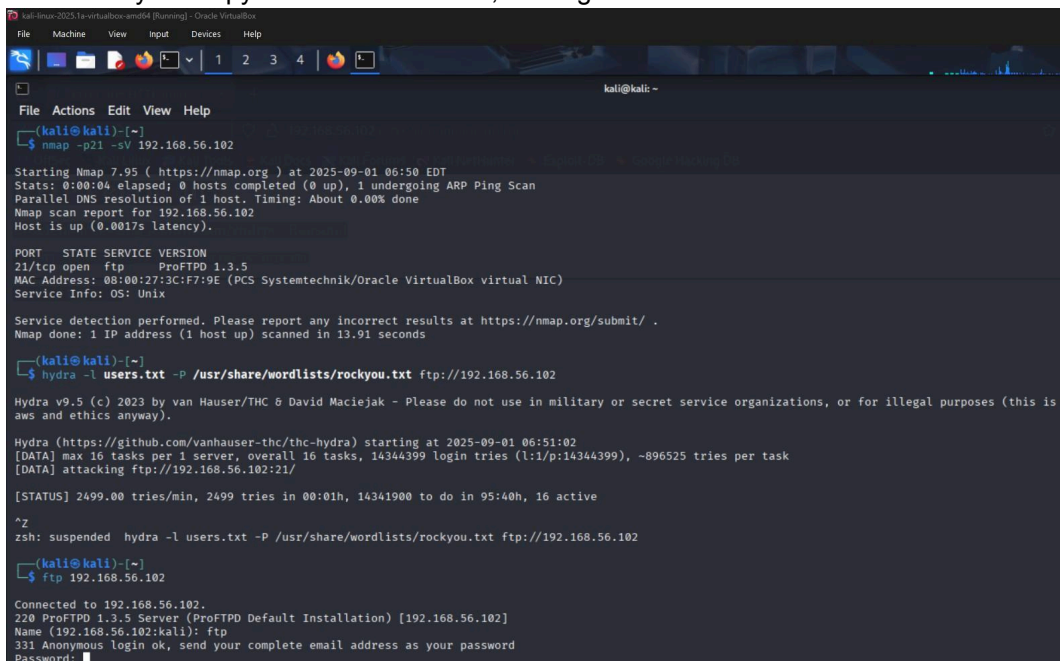
1. Host Discovery: Target IP identified using `arp -a`.
2. Port Scanning: Nmap scans identified open ports (21, 22, 80, 139, 445, 3306, 8080).
3. FTP Exploitation: FTP 7.5 vulnerability enabled username enumeration (e.g., *luke\_skywalker*).
4. SSH Access: Weak credentials allowed SSH login.
5. Privilege Escalation: Sudo misconfiguration enabled root access.
6. Enumeration: Manual and automated checks revealed web directories, Samba shares, MySQL exposure, and outdated Jetty.
7. Post-Exploitation: Retrieved hidden files, CTF flags, and confirmed persistence opportunities.

## Findings

### FTP (ProFTPD 1.3.5)

Vulnerability: `mod_copy` Remote Command Execution (CVE-2015-3306).

Allowed arbitrary file copy into web directories, leading to reverse shell as `www-data`.



```
kali@kali:~$ nmap -p21 -sV 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 06:50 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.56.102
Host is up (0.0017s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
MAC Address: 08:00:27:3C:F7:9E (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 13.91 seconds

kali@kali:~$ hydra -l users.txt -P /usr/share/wordlists/rockyou.txt ftp://192.168.56.102

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-01 06:51:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.56.102:21/

[STATUS] 2499.00 tries/min, 2499 tries in 00:01h, 14341900 to do in 95:40h, 16 active

^Z
zsh: suspended hydra -l users.txt -P /usr/share/wordlists/rockyou.txt ftp://192.168.56.102

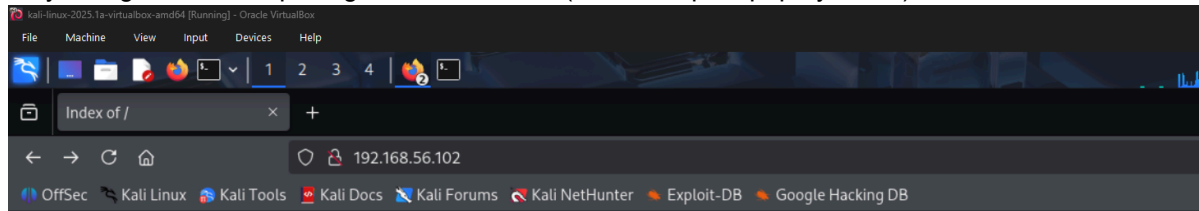
kali@kali:~$ ftp 192.168.56.102

Connected to 192.168.56.102.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.56.102]
Name (192.168.56.102:kali): ftp
331 Anonymous login ok, send your complete email address as your password
Password:
```

## Nmap Scan Result

### Apache (2.4.7)

Directory listing enabled, exposing sensitive folders (/chat, /drupal, /phpmyadmin).



### Index of /

Name	Last modified	Size	Description
<a href="#">chat/</a>	2020-10-29 19:37	-	
<a href="#">drupal/</a>	2011-07-27 20:17	-	
<a href="#">? payroll_app.php</a>	2020-10-29 19:37	1.7K	
<a href="#">phpmyadmin/</a>	2013-04-08 12:06	-	

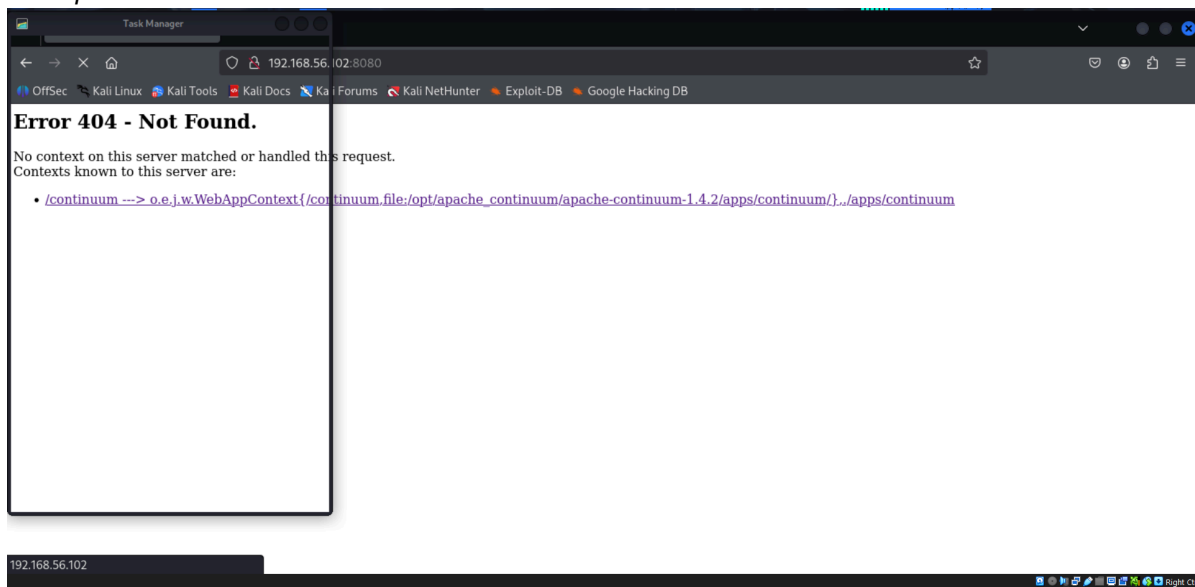
Apache/2.4.7 (Ubuntu) Server at 192.168.56.102 Port 80

## FTP Exploitation Evidence

### Samba (3.x)

Null sessions possible, message signing disabled, leading to information disclosure.

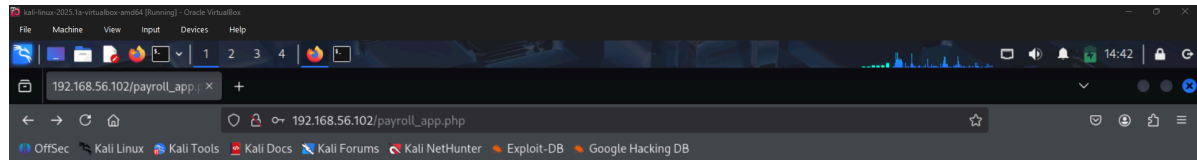
## Metasploit Reverse Shell




## MySQL

Remote access enabled without proper restrictions, exposing database service.

### Web Directory Listing

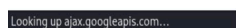
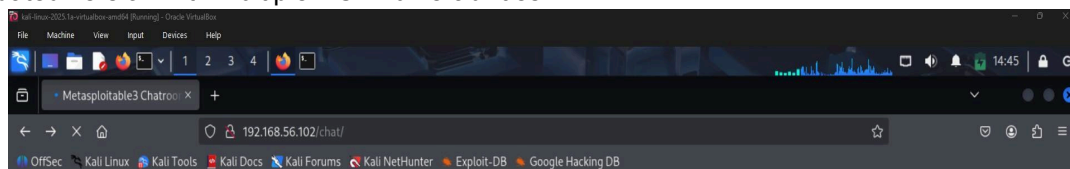


## Payroll Login



### ***Jetty (8.1.7)***

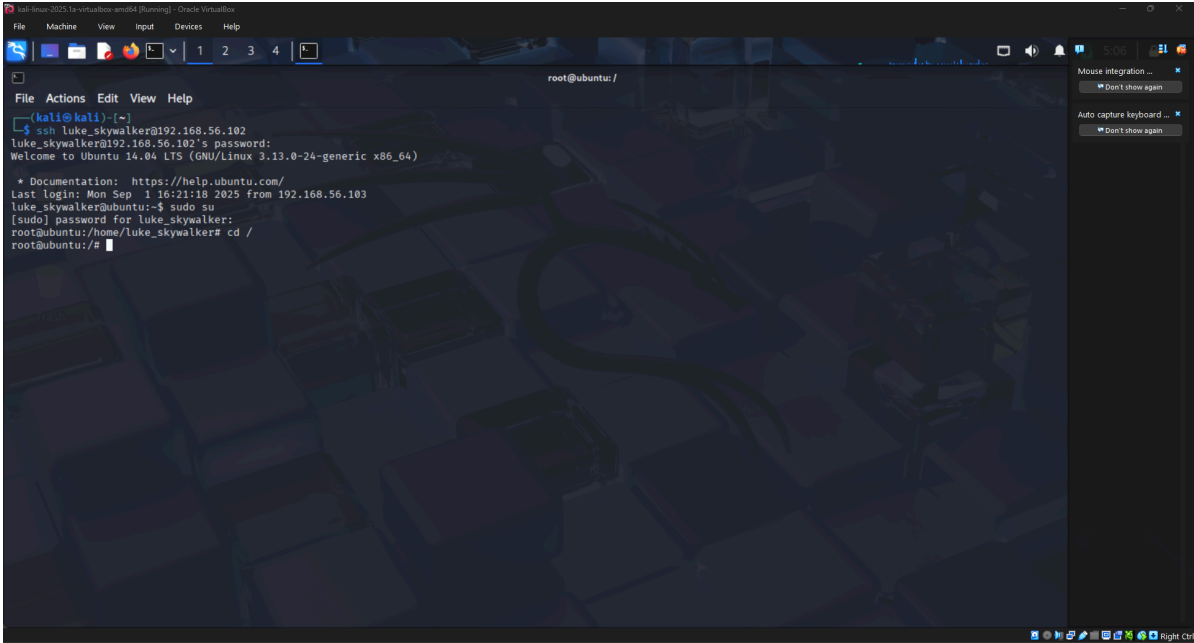
Outdated version with multiple RCE vulnerabilities.



## Samba / MySQL Enumeration

## SSH

Weak credentials (user: luke\_skywalker, pass: like\_my\_father\_beforeme) allowed login and privilege escalation to root.



### CTF Flag Discovery

## Hidden Files & Flags

Multiple CTF flags found (e.g., VolgaCTF{15de975cfd8a8b36ff14c9ec9d1c72ef}). Hidden and suspicious files discovered, some likely containing steganography.

## Risk Assessment

Service	Vulnerability	CVE	Risk Level	CVSS v3.1
ProFTPD 1.3.5	mod_copy RCE	CVE-2015-3306	Critical	9.8
Apache 2.4.7	Directory Listing	N/A	Medium	5.3
Samba 3.x	Null session, no signing	N/A	High	7.4
MySQL	Remote access exposed	N/A	High	7.5
Jetty 8.1.7	Outdated, multiple RCEs	Multiple	High	8.1
SSH	Weak credentials & sudo abuse	N/A	Critical	9.8

## Recommendations

- Upgrade or patch vulnerable services (ProFTPD, Apache, Samba, Jetty, MySQL).
- Disable unnecessary directory listings and null sessions.
- Enforce strong SSH credentials and enable multi-factor authentication.
- Restrict remote access with firewall rules.
- Migrate to the updated OS versions.
- Audit suspicious files and monitor log

## Conclusion

The Ubuntu machine was compromised using a chain of misconfigurations and known vulnerabilities. Attackers could easily gain root access and extract sensitive information. Addressing outdated software, enforcing secure authentication, and applying hardening practices will significantly improve security posture.