Report: Ids Evasion room

Title Page

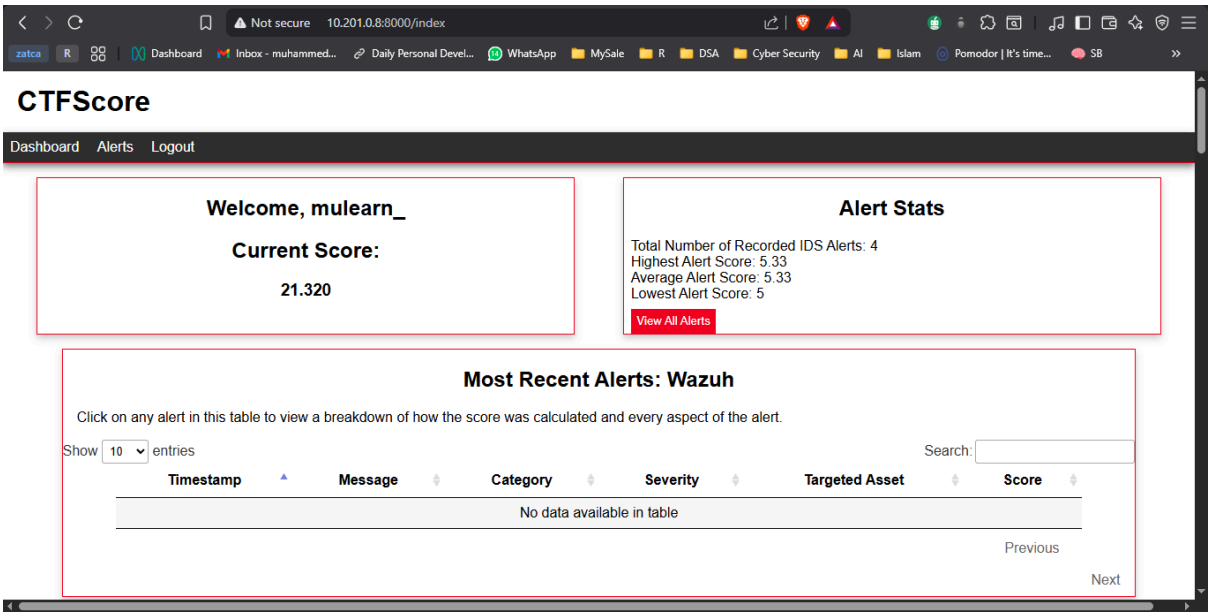
- Prepared for: Mulearn Bootcamp
- Prepared by: Jaseel K
- Date: 2025-10-25

Introduction

Intrusion Detection Systems (IDS) serve as critical sentinels, designed to monitor network or system activities for malicious policies or violations. This report details a practical exploration into IDS evasion, specifically focusing on a series of steps undertaken to bypass such defenses within a controlled environment.

Methodology

1. Deployed the target machine and createed an account and loged into the system at http://10.201.0.8:8000, in preparation for future tasks.



2. Answered the question by reading the context

Answer the questions below

What IDS detection methodology relies on rule sets?

signature-based detection

✓ Correct Answer

3. Answered the question and ran the following command **nmap -sV 10.201.0.8** against the target at **10.201.0.8**

Answer the questions below

What widely implemented protocol has an adverse effect on the reliability of NIDS?

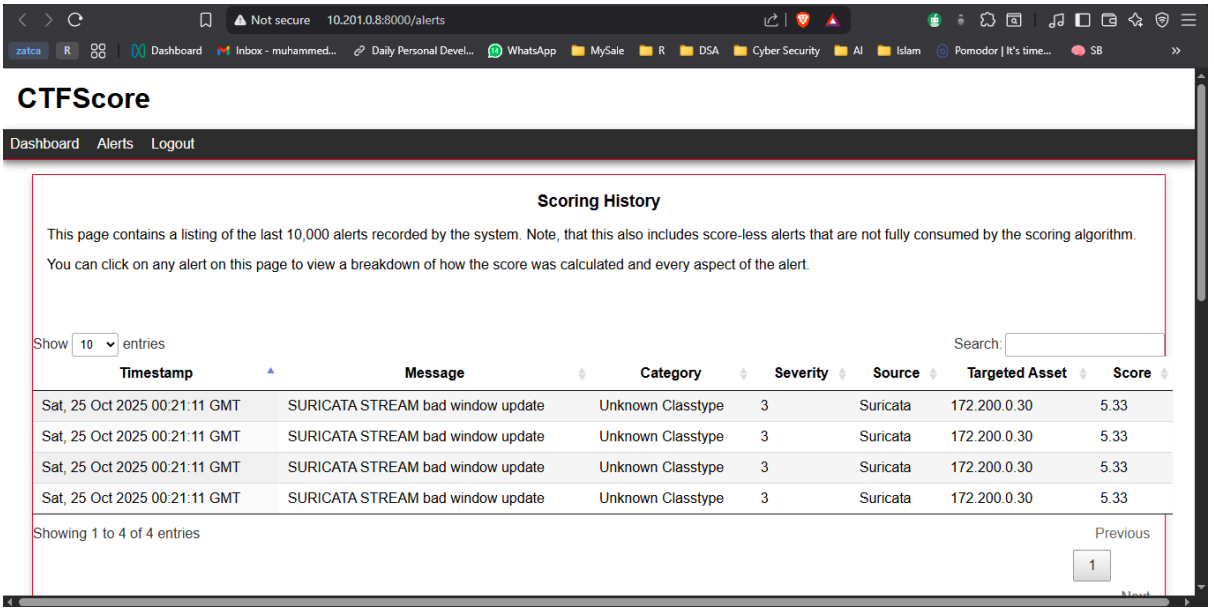
TLS

✓ Correct Answer Hint

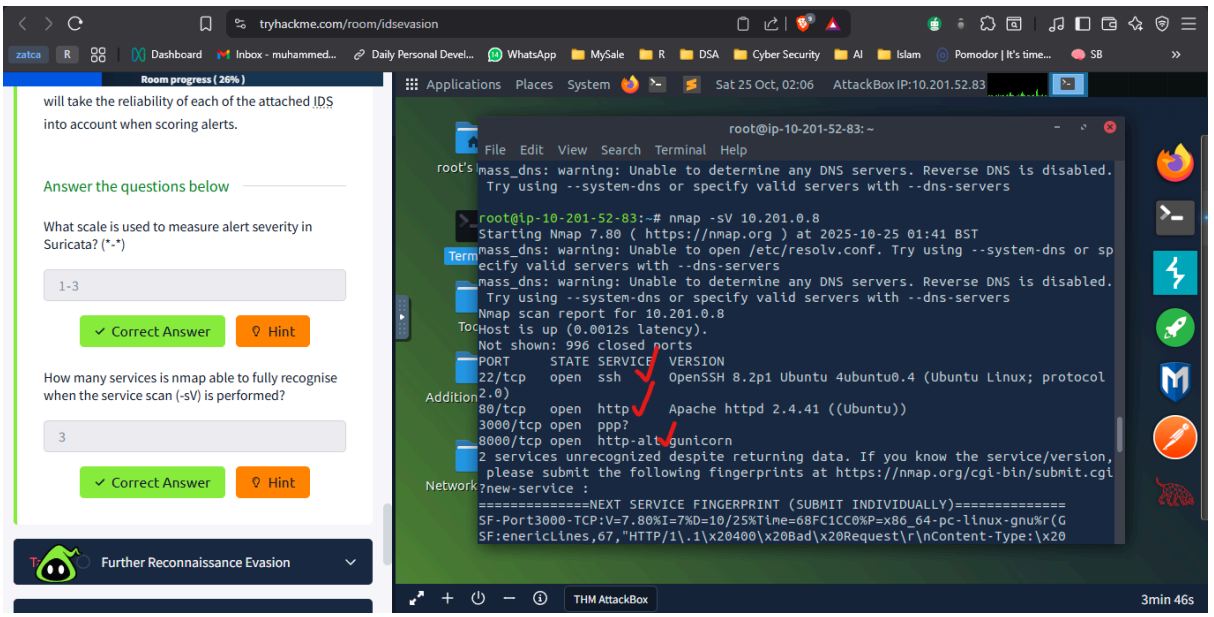
Experiment by running tools against the target and viewing the resultant alerts. Is there any unexpected activity?

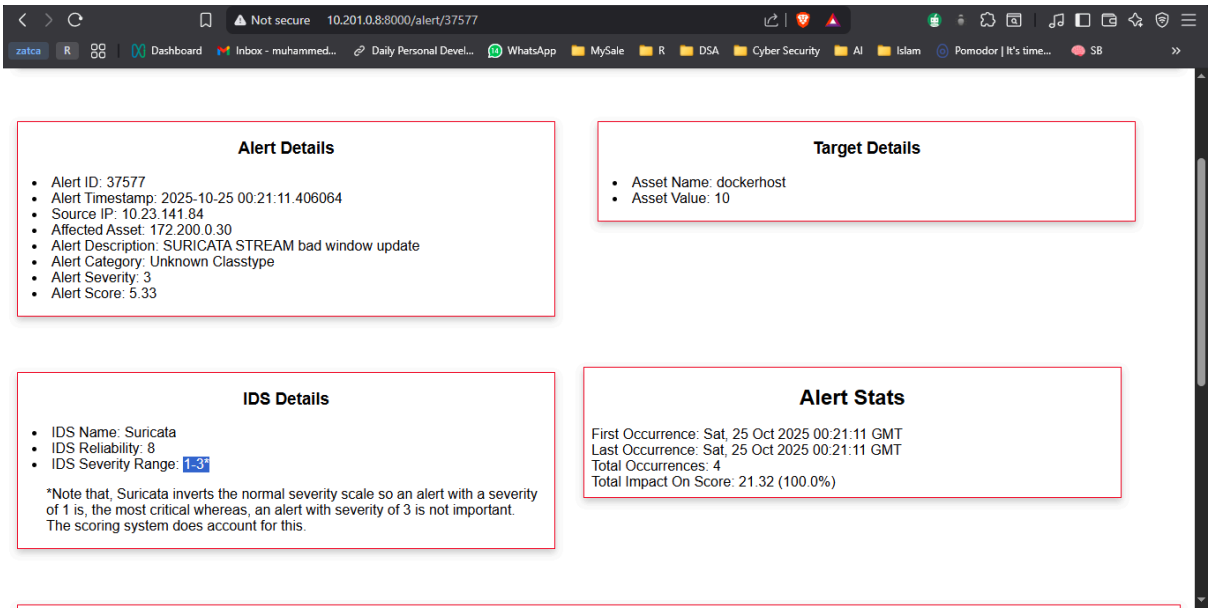
No answer needed

✓ Correct Answer Hint

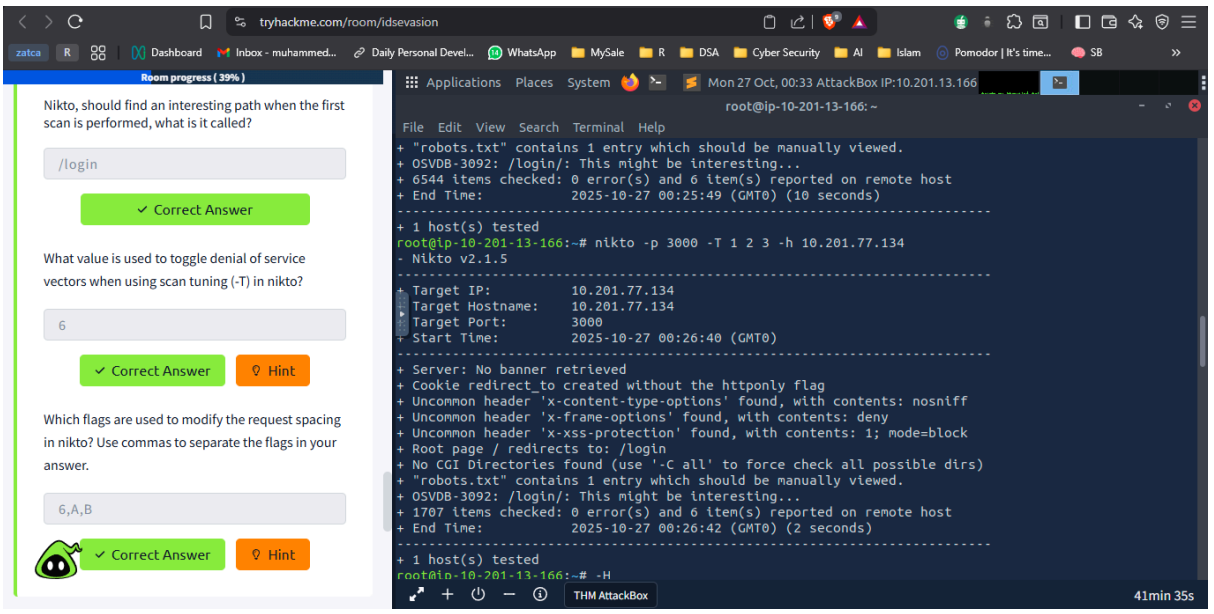


4. The severity range was mentioned in the alert detail page and there three services nmap able to fully recognise port 3000 was not able to fully recognise.

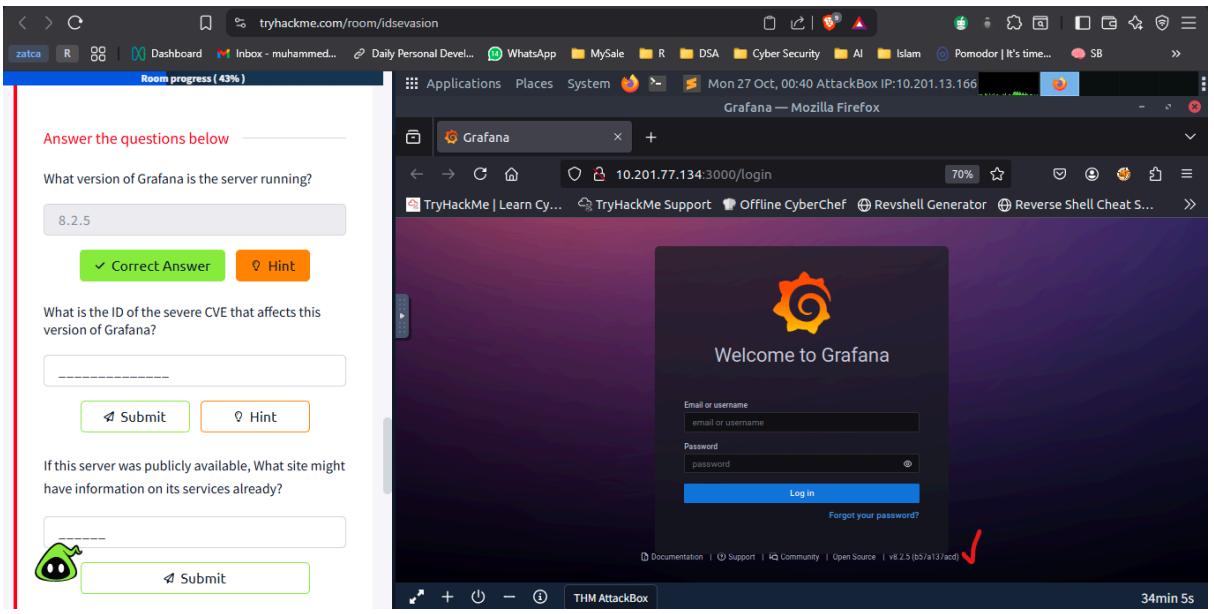




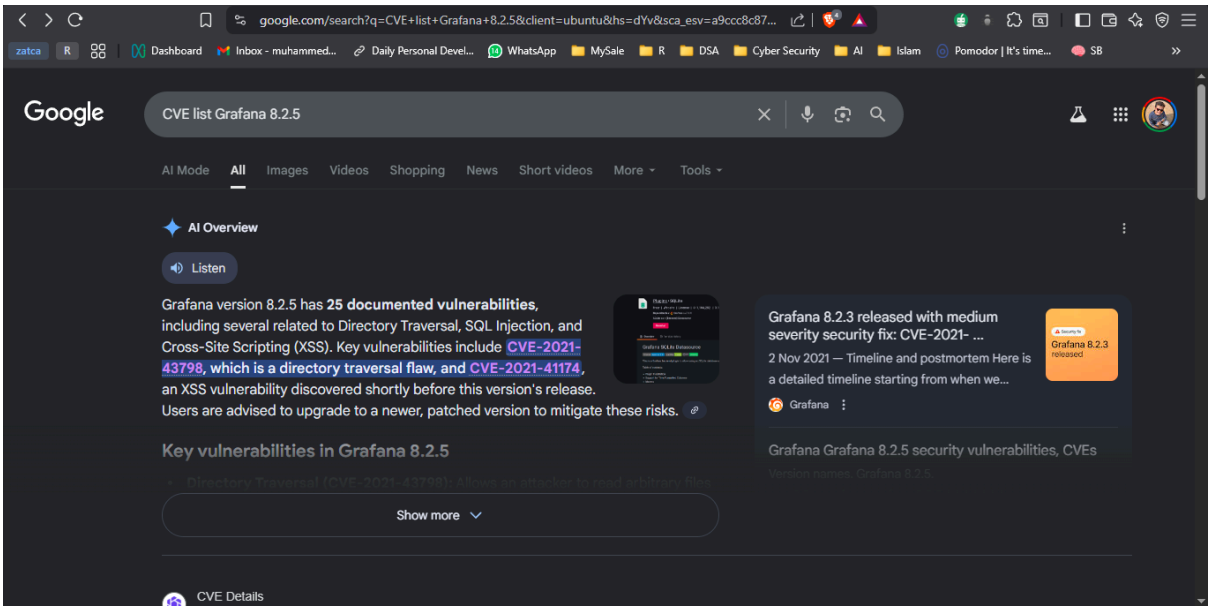
5. Performed **nikto -p 3000 -h 10.201.77.134** found an interesting path /login

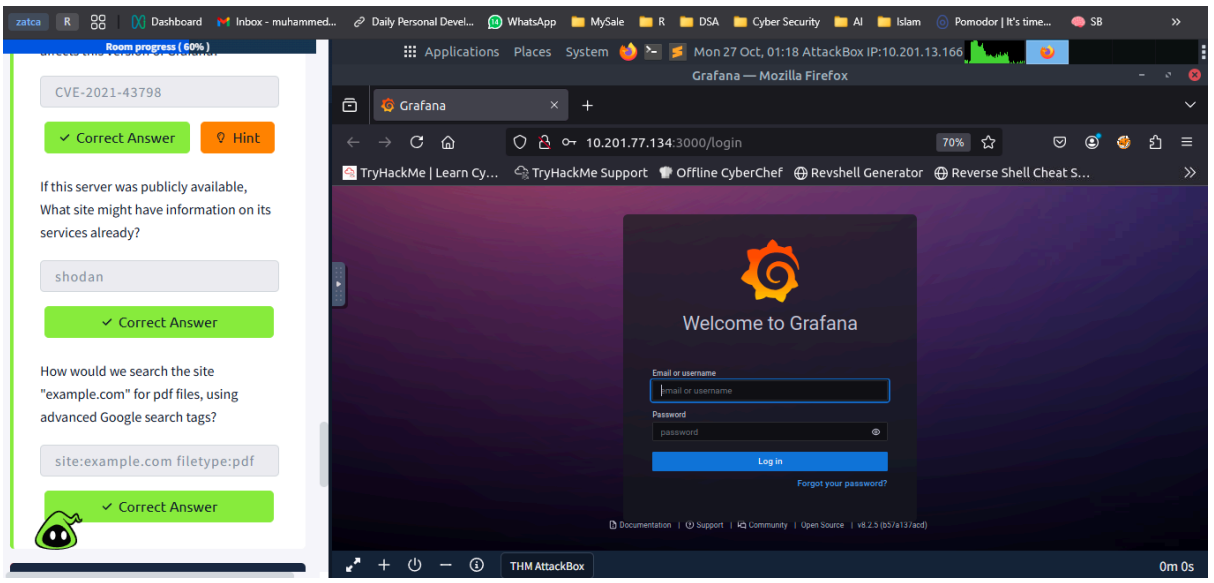


6. Opened the IP in browser and found the login page of Grafana where they have mentioned the version number.

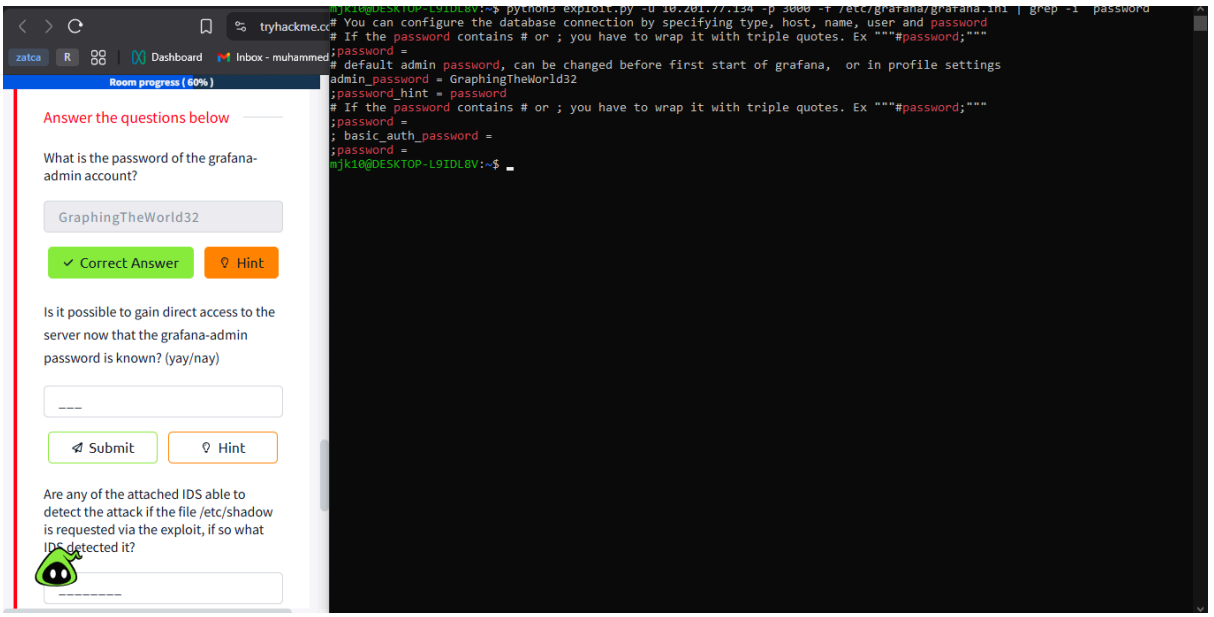


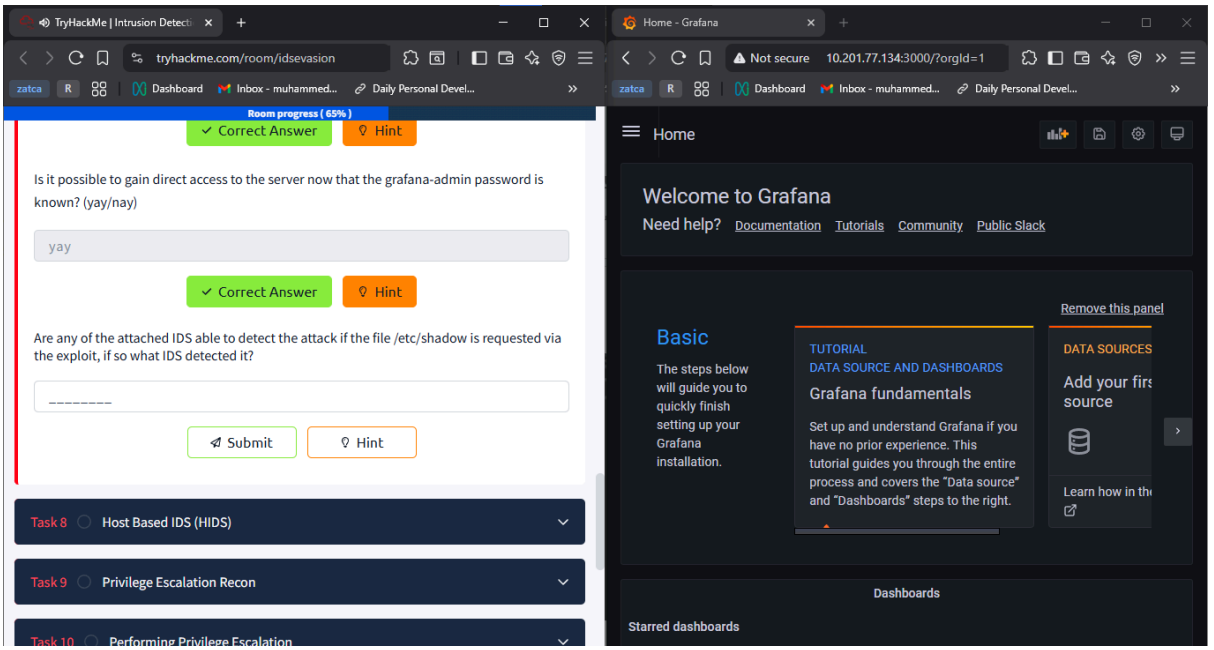
With a google search was able to find the ID of the severe CVE.

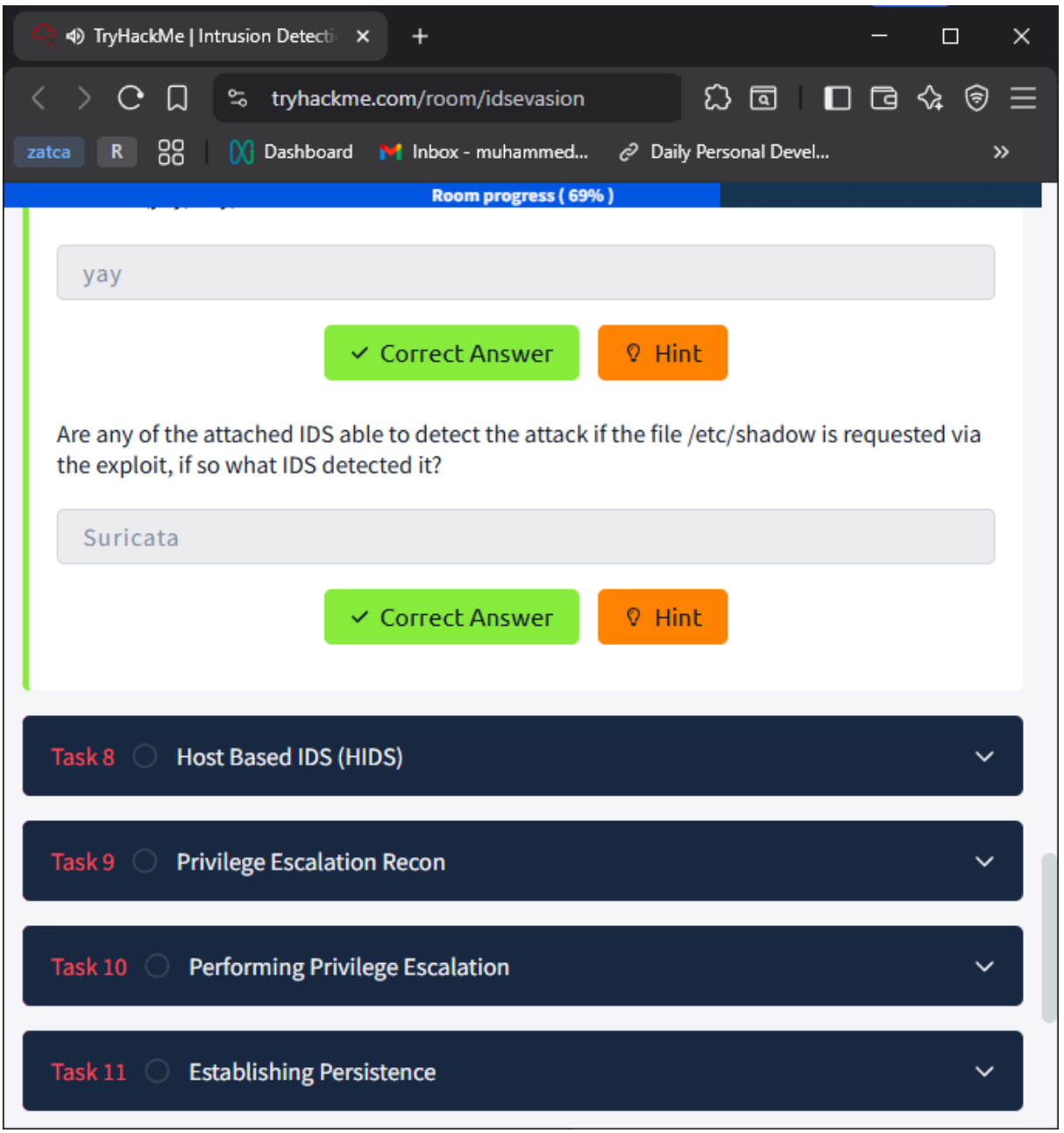




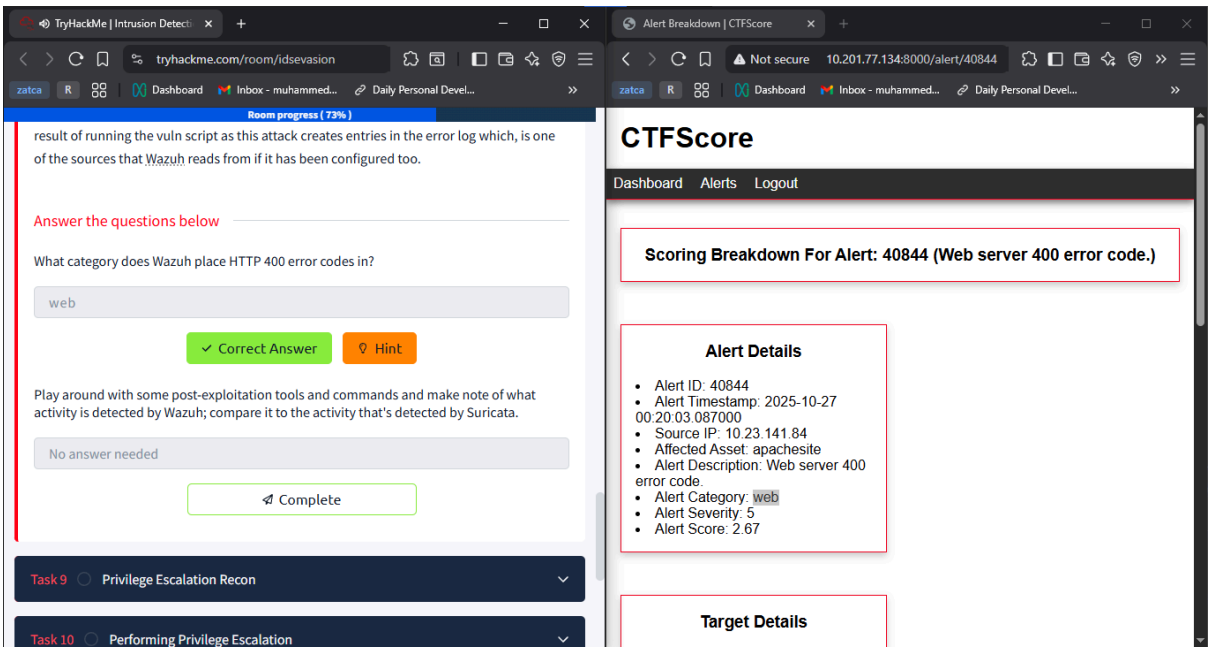
7. By running the python exploit script was able to find the password of grafana-admin account


Room progress (60%)
Answer the questions below
What is the password of the grafana-admin account?
GraphingTheWorld32
Correct Answer
Hint
Is it possible to gain direct access to the server now that the grafana-admin password is known? (yay/nay)
___
Submit
Hint
Are any of the attached IDS able to detect the attack if the file /etc/shadow is requested via the exploit, if so what IDS detected it?
_____
mjk10@DESKTOP-L9IDL8V:~$ python3 exploit.py -u 10.201.77.134 -p 3000 -f /etc/grafana/grafana.ini | grep -i "password
You can configure the database connection by specifying type, host, name, user and password
If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""
;password =
# default admin password, can be changed before first start of grafana, or in profile settings
admin_password = GraphingTheWorld32
;password_hint = password
If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""
;password =
; basic_auth_password =
;password =
mjk10@DESKTOP-L9IDL8V:~$

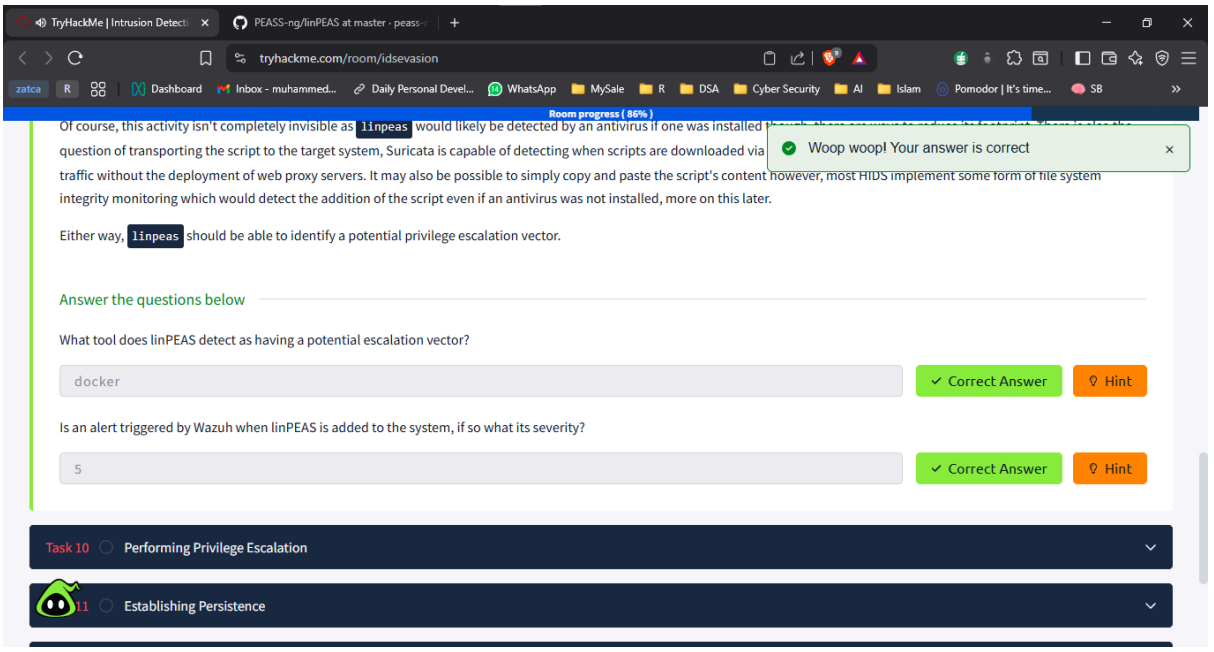

TryHackMe | Intrusion Detecti
tryhackme.com/room/idsevasion
Room progress (65%)
Correct Answer
Hint
Is it possible to gain direct access to the server now that the grafana-admin password is known? (yay/nay)
yay
Correct Answer
Hint
Are any of the attached IDS able to detect the attack if the file /etc/shadow is requested via the exploit, if so what IDS detected it?
_____
Submit
Hint
Task 8 Host Based IDS (HIDS)
Task 9 Privilege Escalation Recon
Task 10 Performing Privilege Escalation
Home - Grafana
Not secure 10.201.77.134:3000/?orgId=1
Home
Welcome to Grafana
Need help? Documentation Tutorials Community Public Slack
Remove this panel
Basic
The steps below will guide you to quickly finish setting up your Grafana installation.
TUTORIAL
DATA SOURCE AND DASHBOARDS
Grafana fundamentals
Set up and understand Grafana if you have no prior experience. This tutorial guides you through the entire process and covers the "Data source" and "Dashboards" steps to the right.
DATA SOURCES
Add your firs source
Learn how in th
Dashboards
Starred dashboards



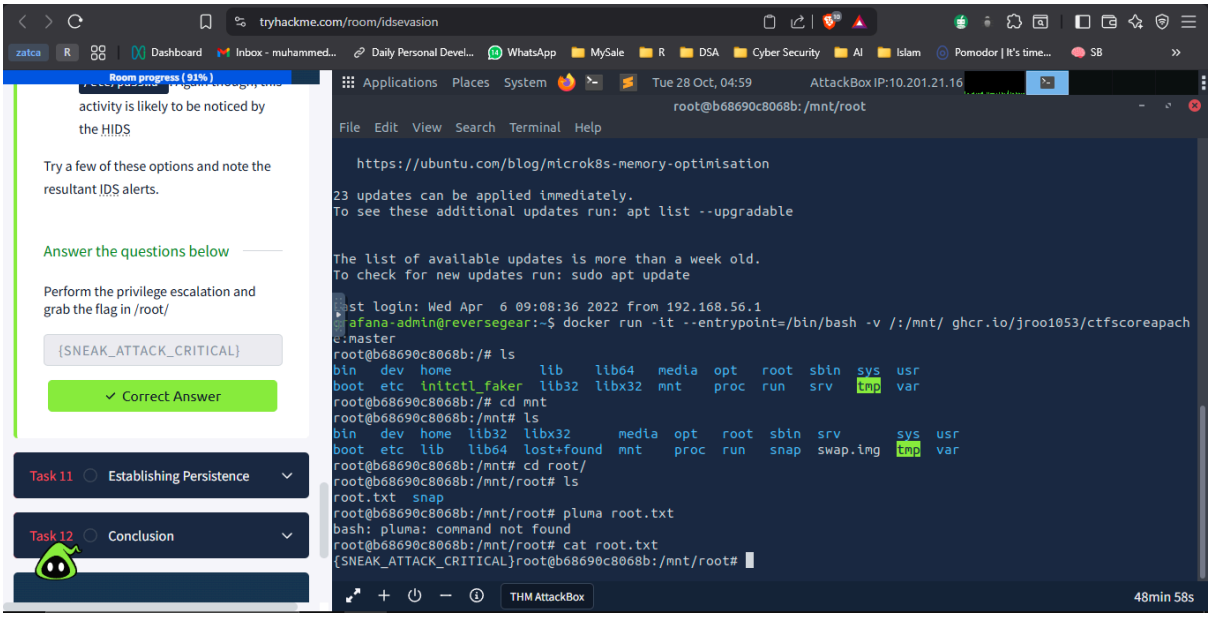
8. By going through the alert was able to find the alert category



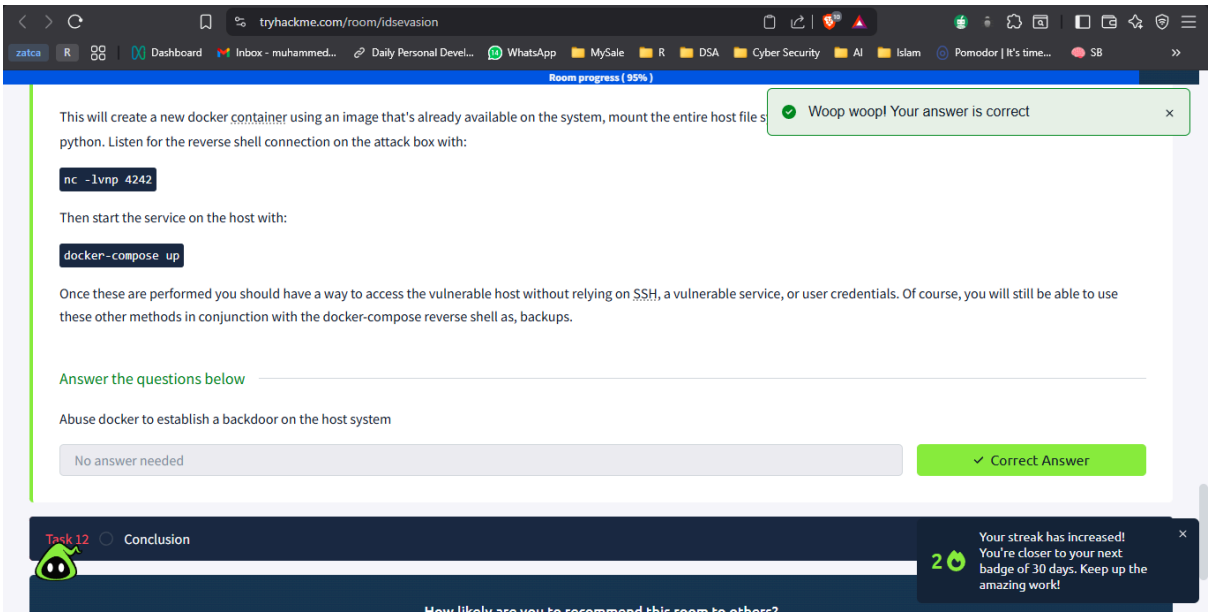
9. linPEAS detects docker tool



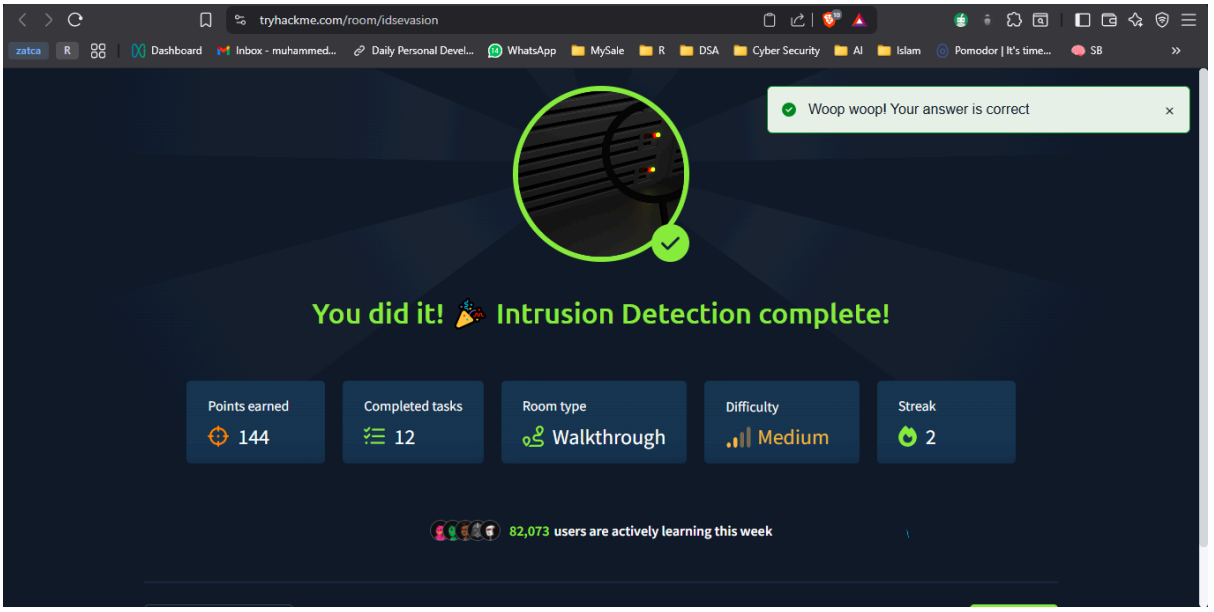
10. First **ssh grafana-admin@10.201.59.42** entered the password we got from previous step .Using the docker run command was able to gain root privileges and after going through every /root was able to grab the flag



11. Established a backdoor on the host system



12. Conclusion


tryhackme.com/room/idsevasion
Woop woop! Your answer is correct
You did it! Intrusion Detection complete!
Points earned
144
Completed tasks
12
Room type
Walkthrough
Difficulty
Medium
Streak
2
82,073 users are actively learning this week