Incident Response Team Exercise

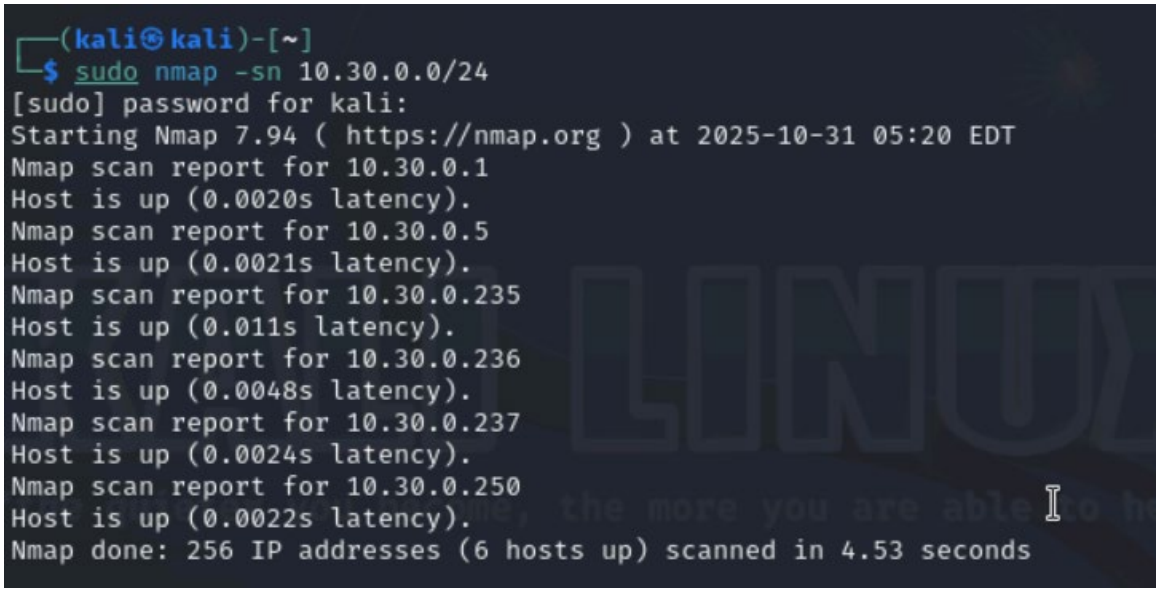
Contents

IRT Exercise Observation

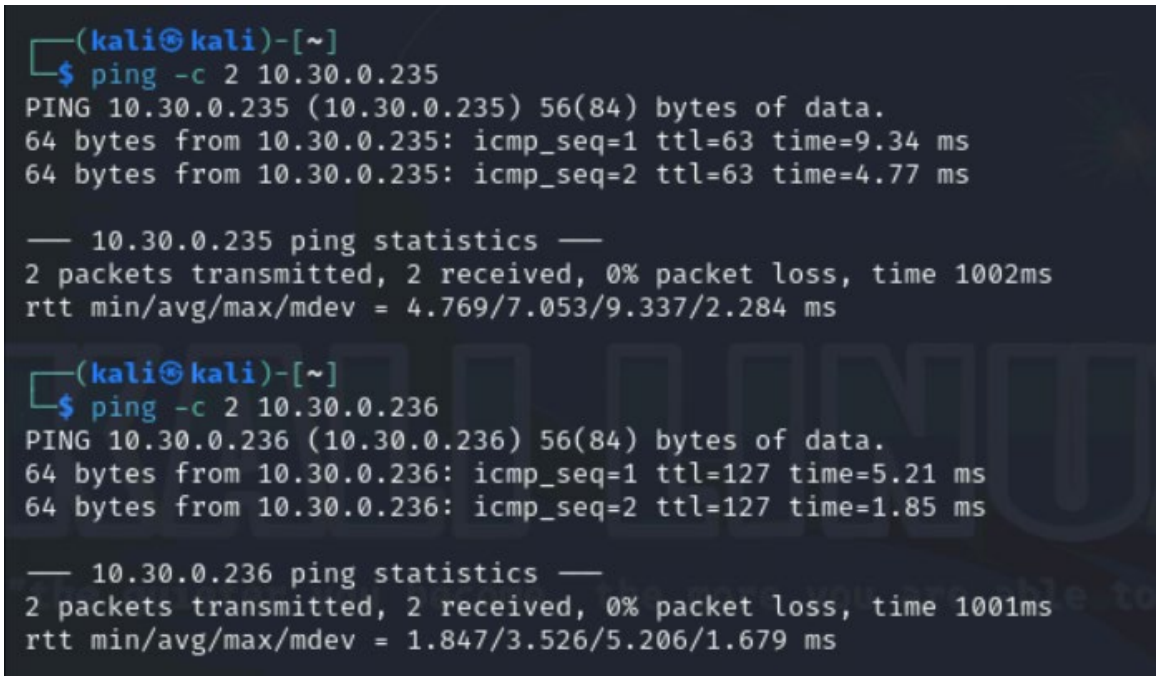
Red team: Andrew Negapatan, Md Salam
Observed by: Blue team – Md Salam, Andrew Negapatan, Nickolai Balida
Date: 06/11/2025

1. Screenshot(s) of ping results showing attempted connection(s) with the attack target(s)

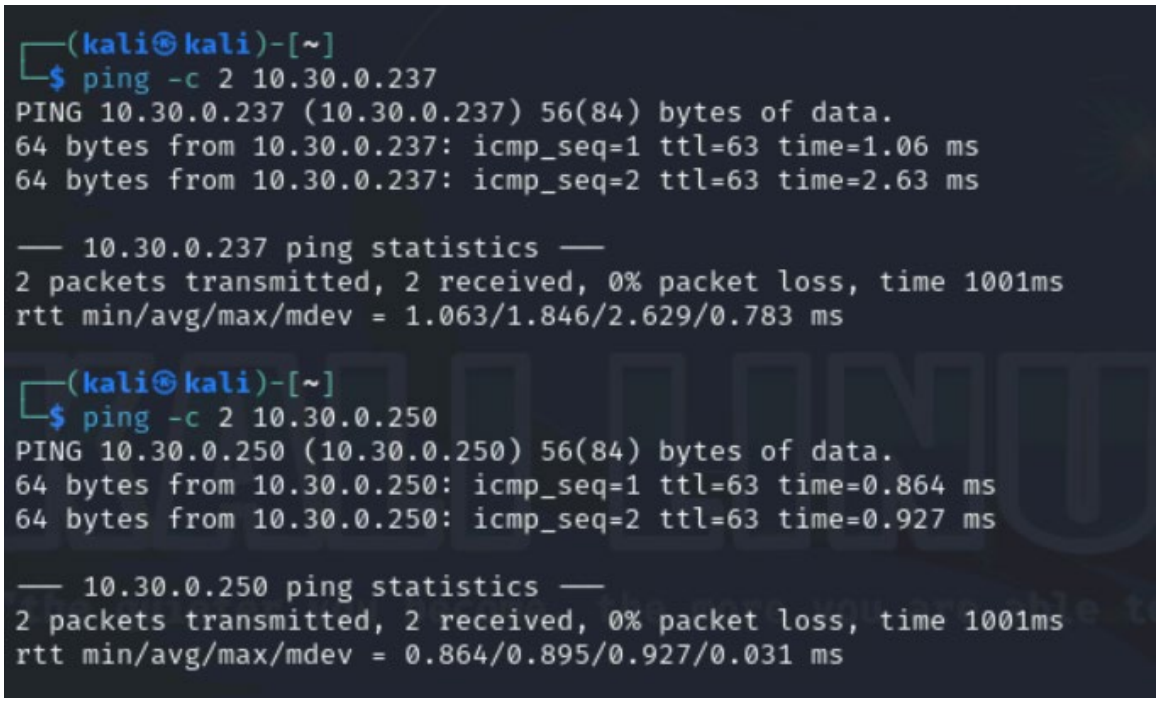
Nmap on network 10.30.0.0/24 to get IP address of Blackbox Host (10.30.0.250) and then Ping from Red Team Kali Host (192.168.1.27)



To Metasploitable (10.30.0.235) and Windows Server (10.30.0.236)



To Web Servers Farm (10.30.0.237) and Blackbox Host (10.30.0.250)



2. Notes and screenshots verifying attack attempts and types of incidents

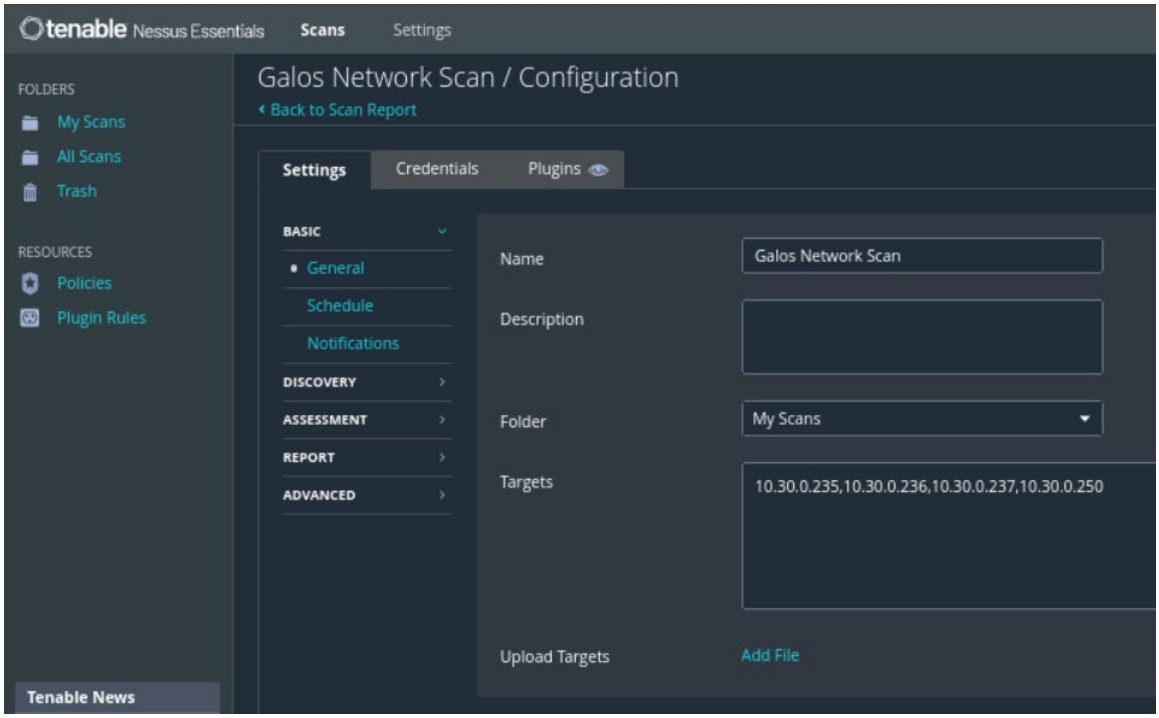
2.1 Nessus Vulnerability Scan

Red Team Activity:

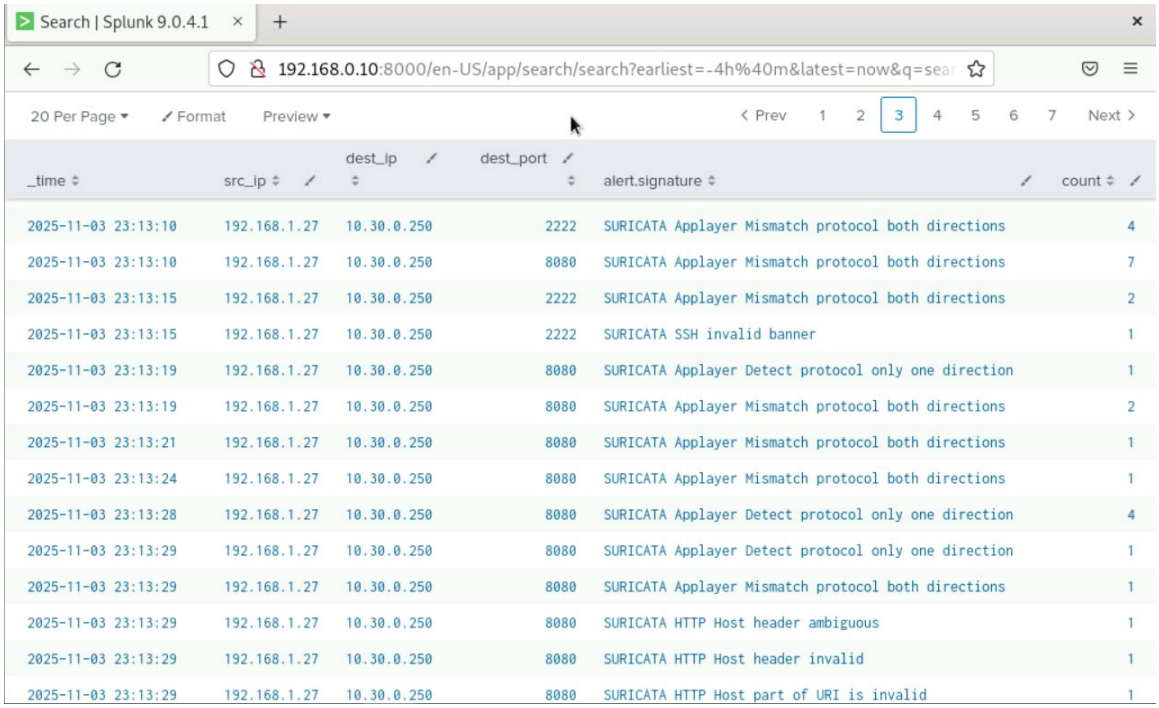
The red team conducted a vulnerability assessment across all target hosts within the DMZ using Nessus to systematically identify known security weaknesses that could be exploited by attackers. This process enabled the organisation to evaluate its current security posture and prioritise remediation efforts to address the identified vulnerabilities.

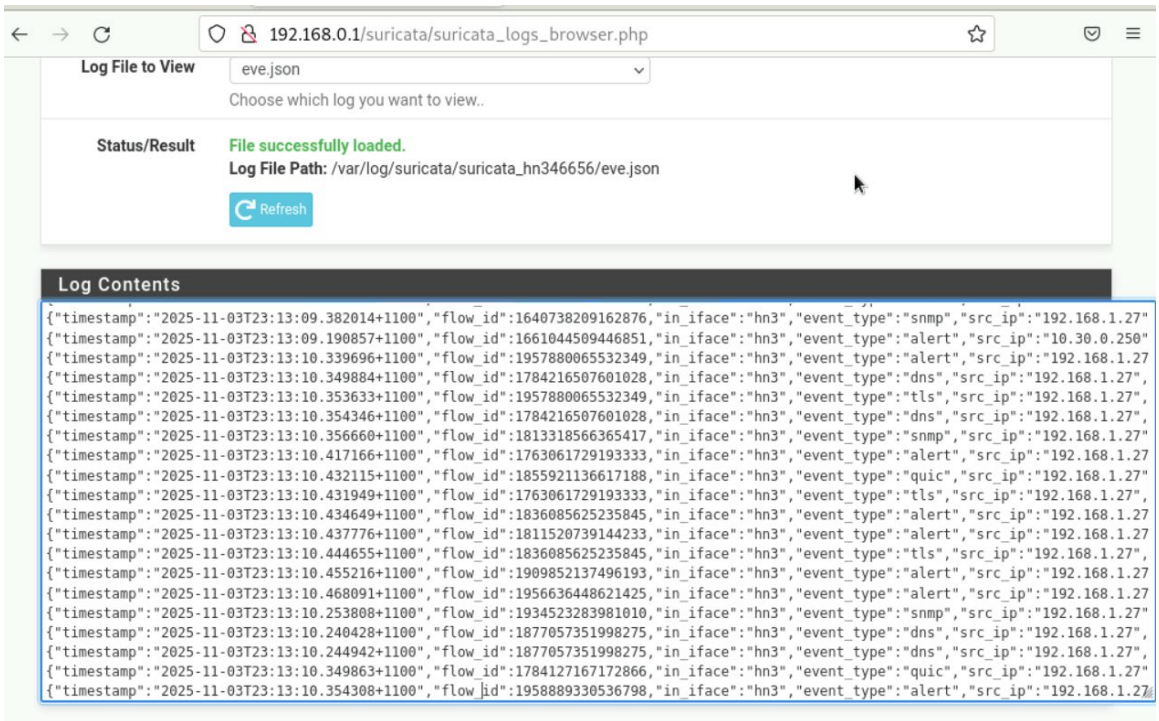
Target: 10.30.0.235 (Metaspoitable), 10.30.0.236 (Windows Server), 10.30.0.237 (Web Servers Farm), 10.30.0.250 (Black Box)

The scan report will be provided at the end of the project.



Blue Team Activity:





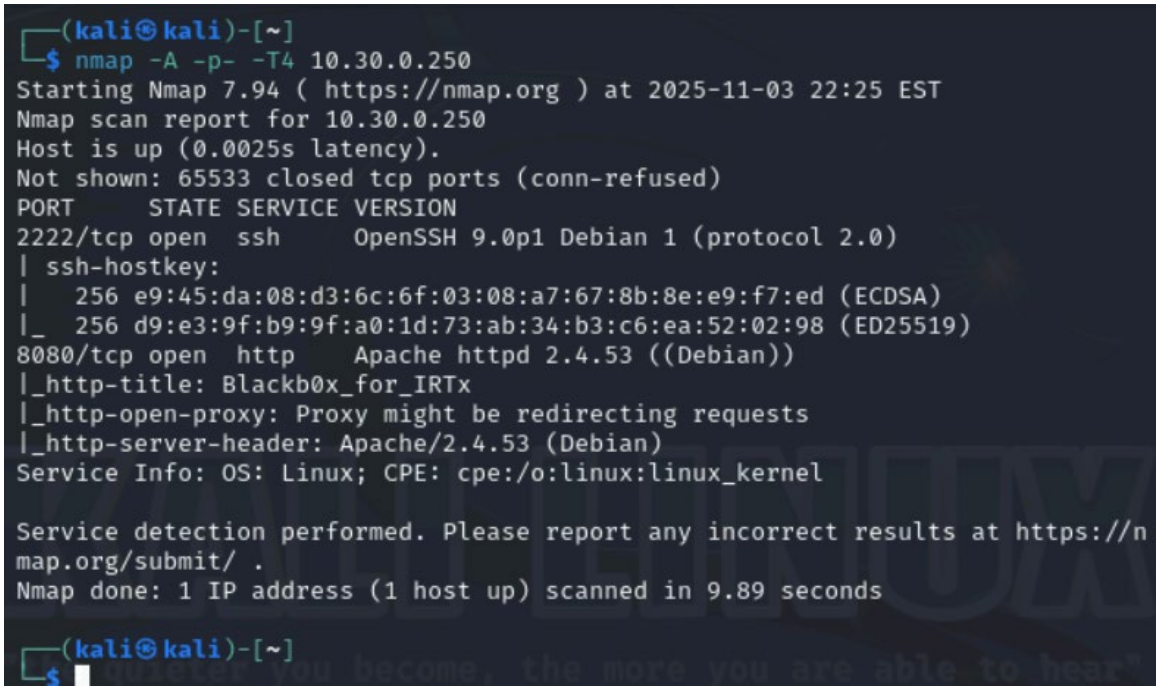
From Splunk and pfSense Suricata, we were able to monitor the Nessus vulnerability scanning activities as shown above.

2.2 Port Scanning

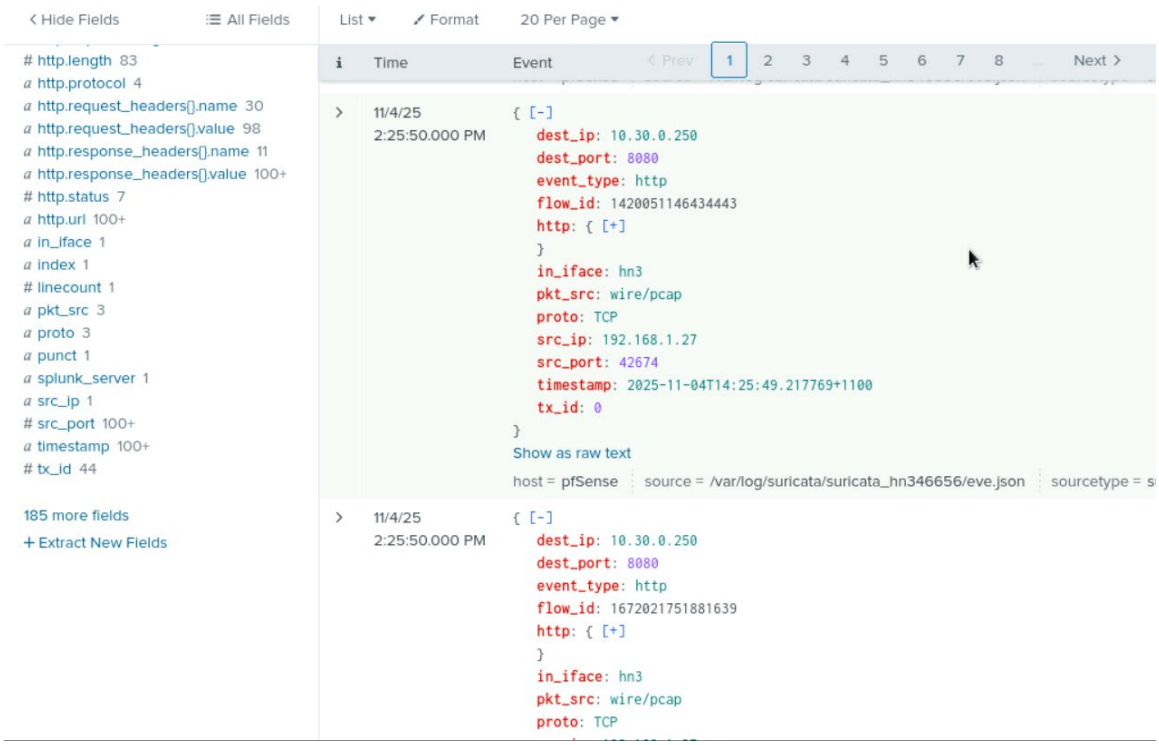
Red Team Activity:

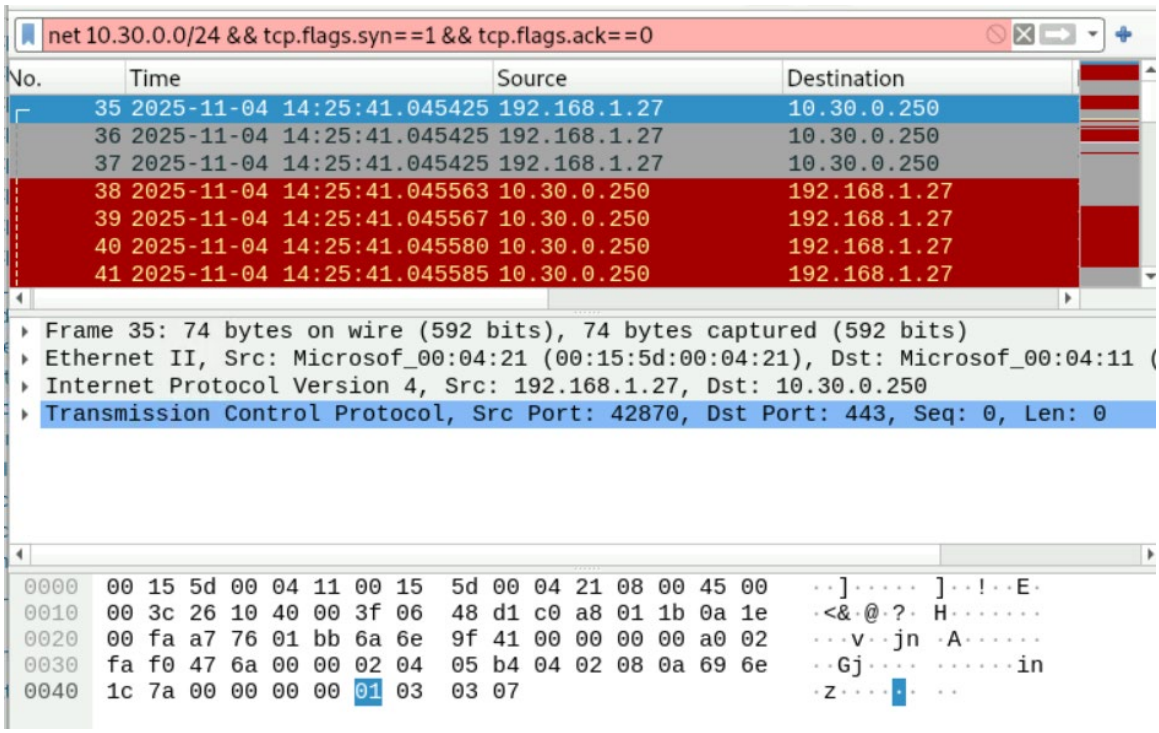
The red team performed Nmap port scanning on the Blackbox host to identify open ports, live hosts, and active services within the target network.

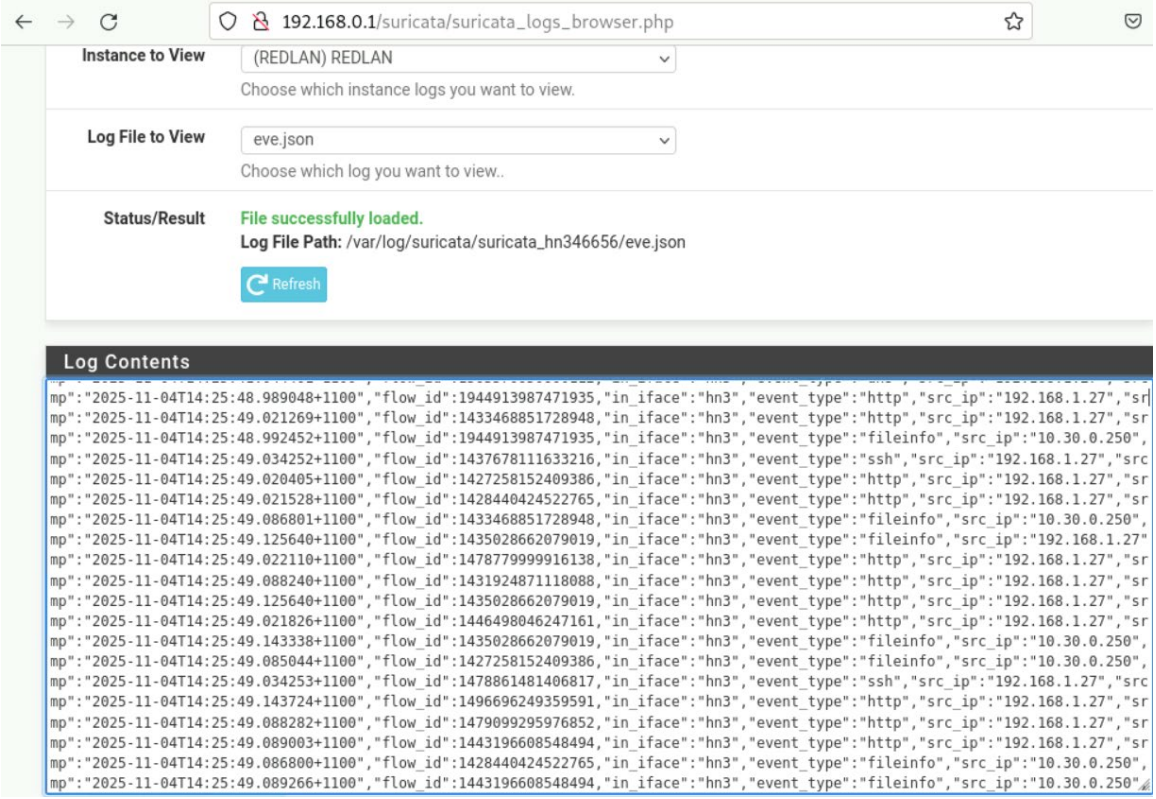
Target: 10.30.0.250



Blue Team Activity:


Hide Fields
All Fields
List
Format
20 Per Page
http.length 83
a http.protocol 4
a http.request_headers{}.name 30
a http.request_headers{}.value 98
a http.response_headers{}.name 11
a http.response_headers{}.value 100+
http.status 7
a http.url 100+
a in_iface 1
a index 1
linecount 1
a pkt_src 3
a proto 3
a punct 1
a splunk_server 1
a src_ip 1
src_port 100+
a timestamp 100+
tx_id 44
185 more fields
+ Extract New Fields
Time
Event
Prev
1
2
3
4
5
6
7
8
Next
11/4/25
2:25:50.000 PM
{ [-]
dest_ip: 10.30.0.250
dest_port: 8080
event_type: http
flow_id: 1420051146434443
http: { [+]
}
in_iface: hn3
pkt_src: wire/pcap
proto: TCP
src_ip: 192.168.1.27
src_port: 42674
timestamp: 2025-11-04T14:25:49.217769+1100
tx_id: 0
}
Show as raw text
host = pfSense
source = /var/log/suricata/suricata_hn346656/eve.json
11/4/25
2:25:50.000 PM
{ [-]
dest_ip: 10.30.0.250
dest_port: 8080
event_type: http
flow_id: 1672021751881639
http: { [+]
}
in_iface: hn3
pkt_src: wire/pcap
proto: TCP


net 10.30.0.0/24 && tcp.flags.syn==1 && tcp.flags.ack==0
No.
Time
Source
Destination
35 2025-11-04 14:25:41.045425 192.168.1.27 10.30.0.250
36 2025-11-04 14:25:41.045425 192.168.1.27 10.30.0.250
37 2025-11-04 14:25:41.045425 192.168.1.27 10.30.0.250
38 2025-11-04 14:25:41.045563 10.30.0.250 192.168.1.27
39 2025-11-04 14:25:41.045567 10.30.0.250 192.168.1.27
40 2025-11-04 14:25:41.045580 10.30.0.250 192.168.1.27
41 2025-11-04 14:25:41.045585 10.30.0.250 192.168.1.27
Frame 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Microsof_00:04:21 (00:15:5d:00:04:21), Dst: Microsof_00:04:11 (
Internet Protocol Version 4, Src: 192.168.1.27, Dst: 10.30.0.250
Transmission Control Protocol, Src Port: 42870, Dst Port: 443, Seq: 0, Len: 0
0000 00 15 5d 00 04 11 00 15 5d 00 04 21 08 00 45 00
0010 00 3c 26 10 40 00 3f 06 48 d1 c0 a8 01 1b 0a 1e
0020 00 fa a7 76 01 bb 6a 6e 9f 41 00 00 00 00 a0 02
0030 fa f0 47 6a 00 00 02 04 05 b4 04 02 08 0a 69 6e
0040 1c 7a 00 00 00 00 01 03 03 07



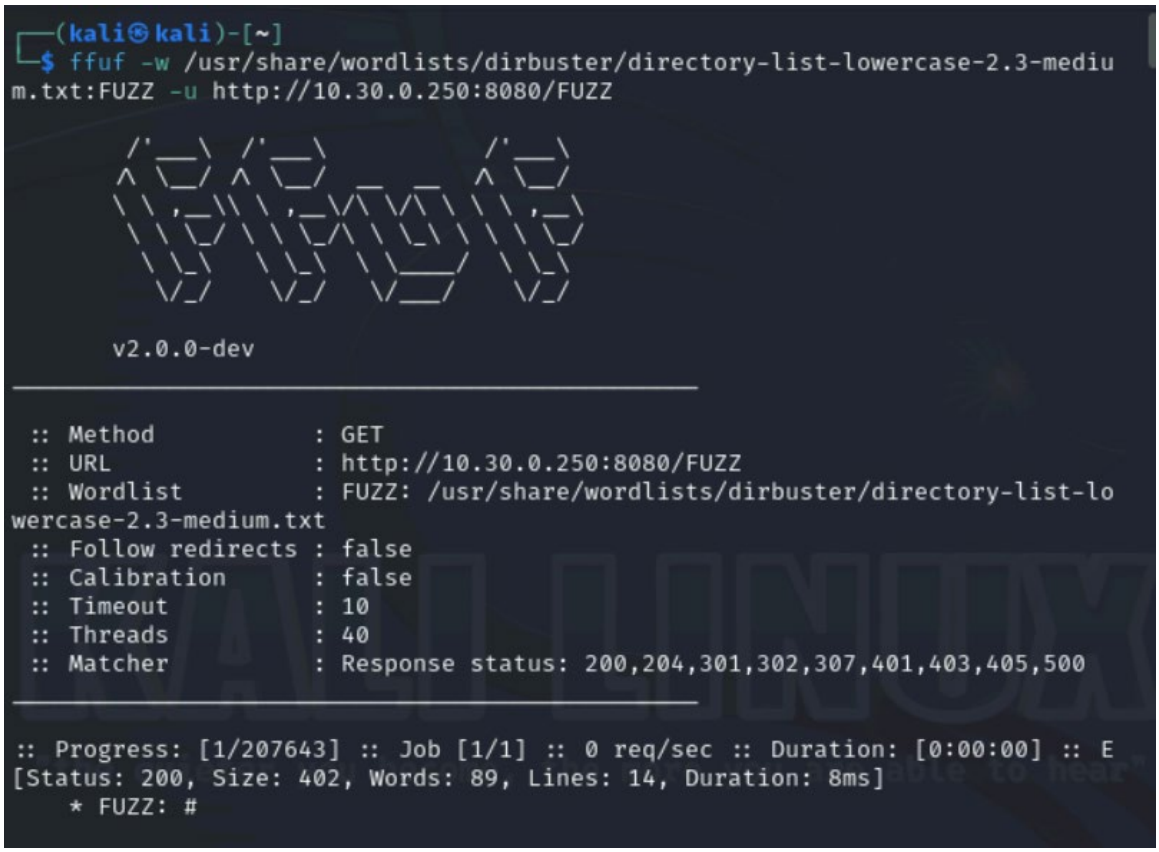
We detected port-scanning activity using Splunk, Wireshark and pfSense suricata indicating a potential hacking attempt.

2.3 Directory Busting

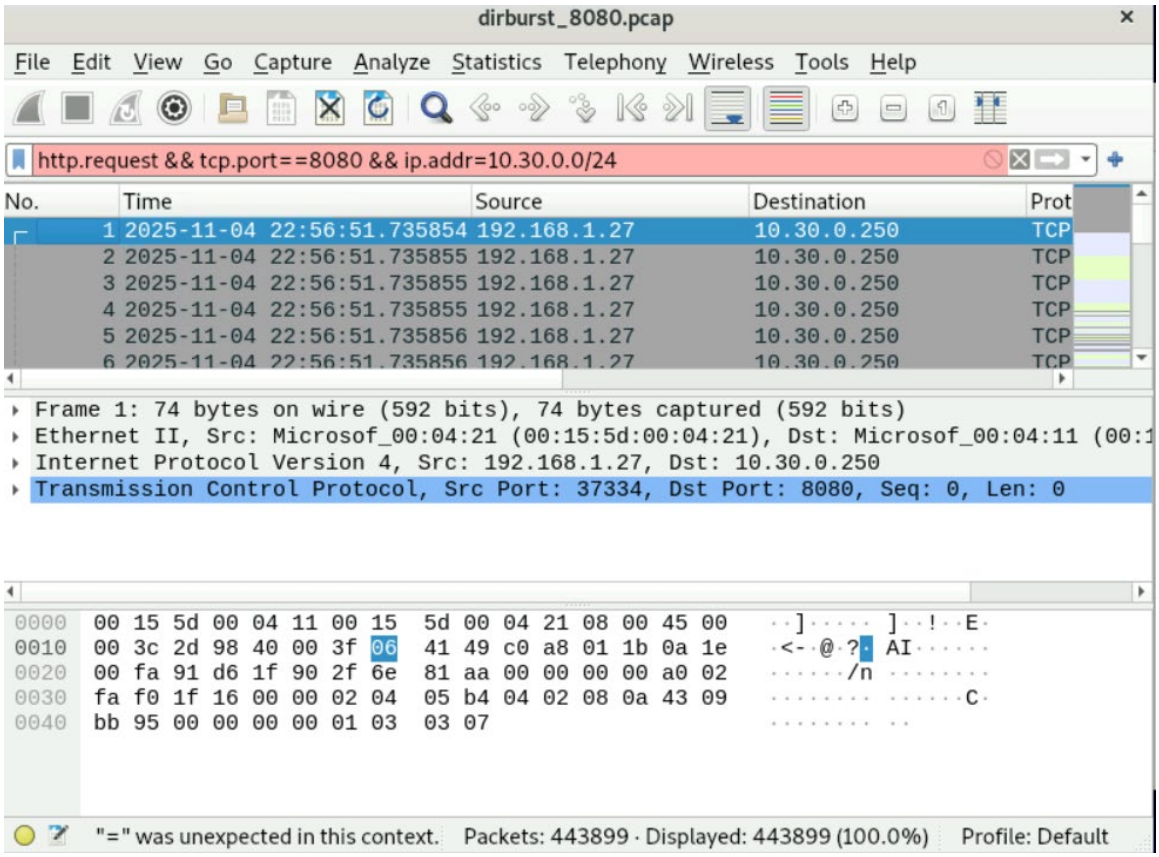
Red Team Activity:

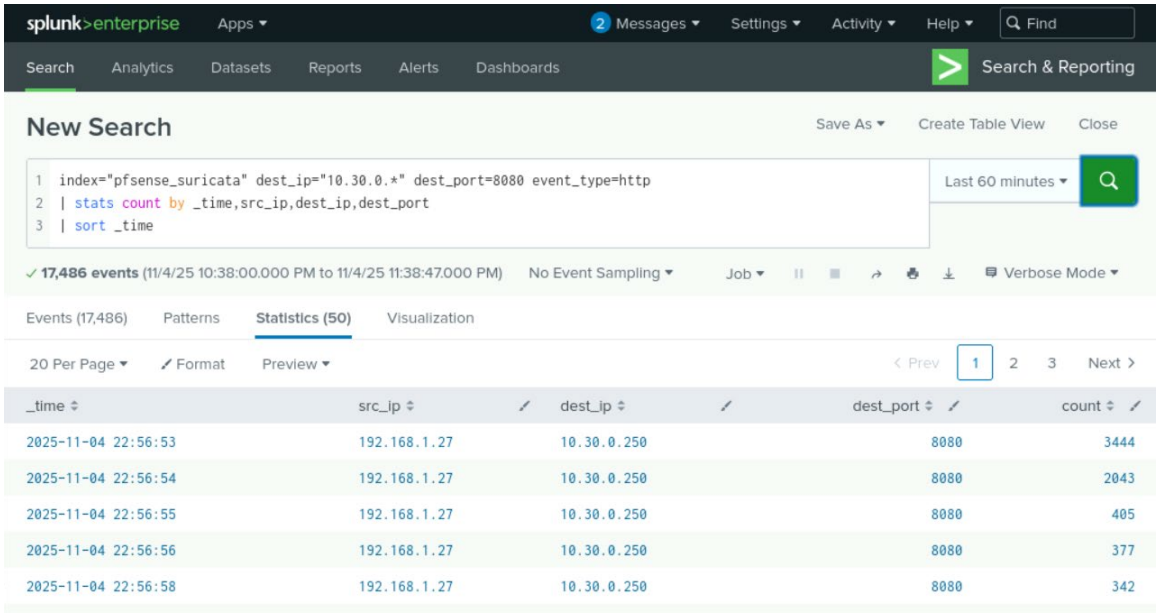
The red team launched web content scanning to identify hidden web content, directories, files, and potential vulnerabilities within the target web application.

Target: 10.30.0.250



Blue Team Activity:





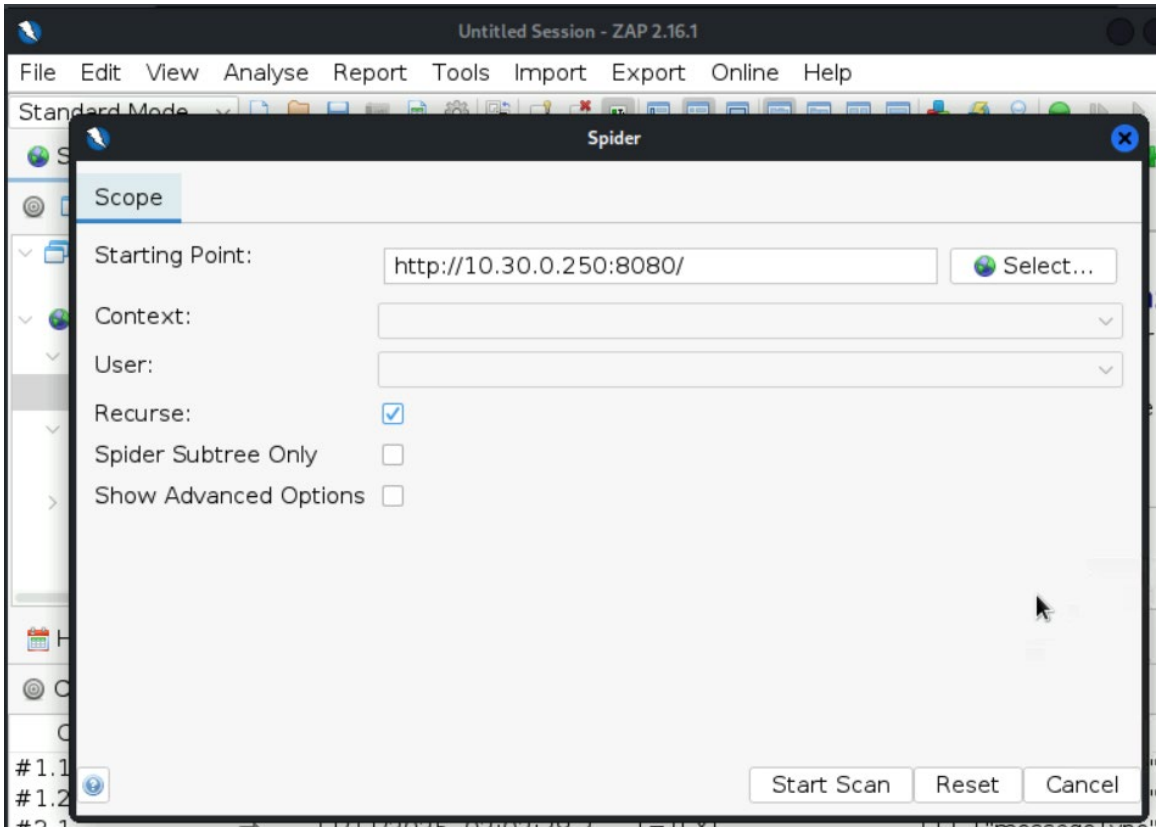
We were able to monitor this suspicious activity of web content scanning from Wireshark and Splunk. At this stage, we may have to report to a team supervisor on this potential hacking attempt.

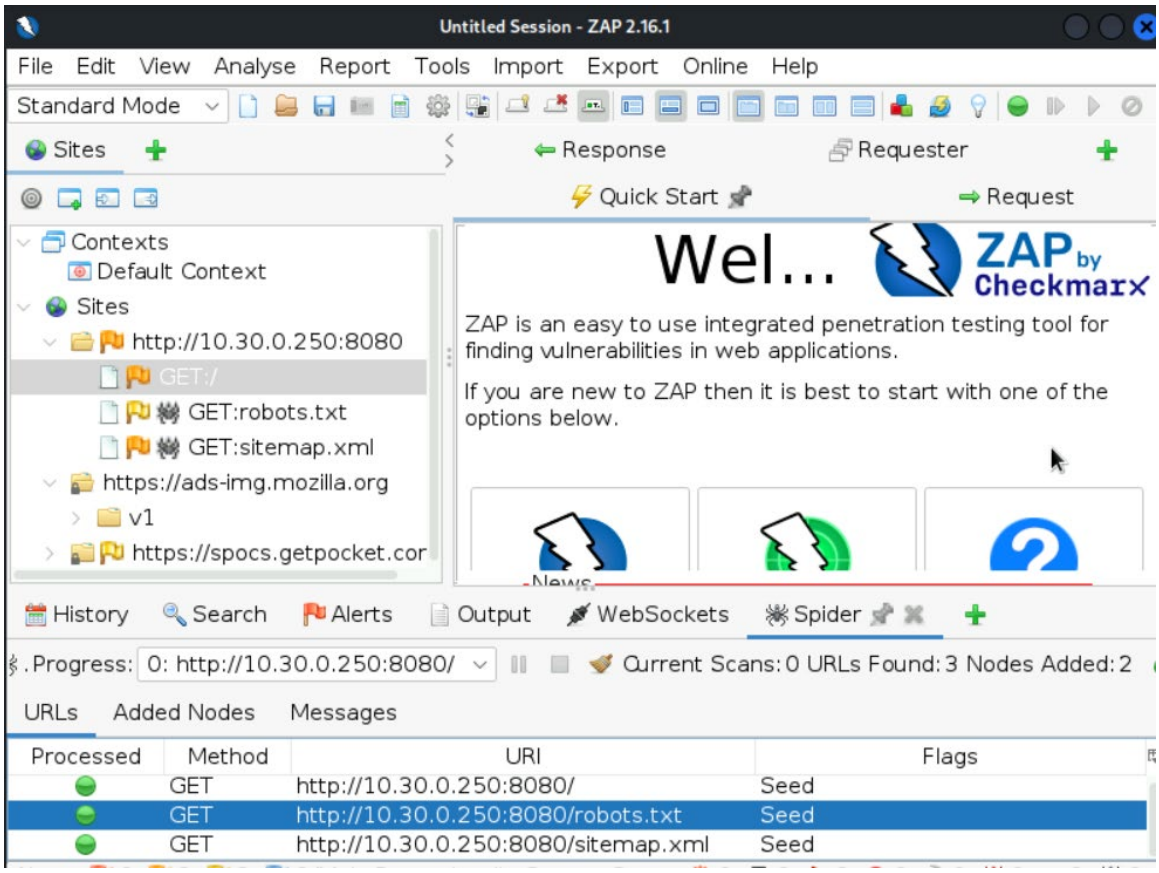
2.4 Spidering

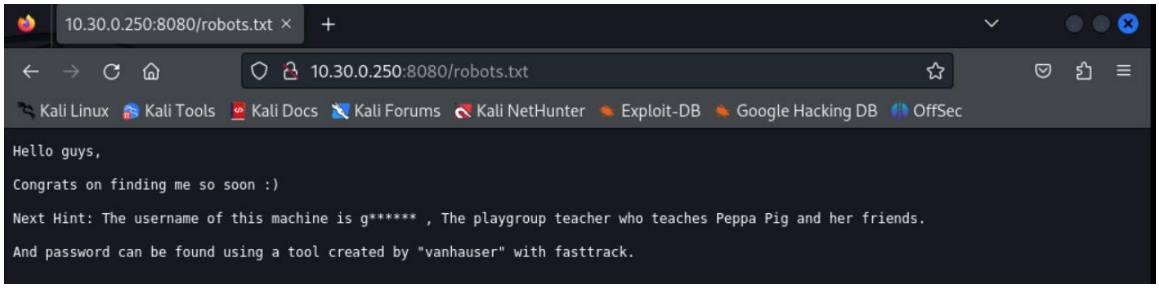
Red Team Activity:

The red team performed web spidering to map the structure of the target web application, uncover hidden or unlinked content, and identify potential vulnerabilities. The scan successfully located *robots.txt* file containing hints for a username and password.

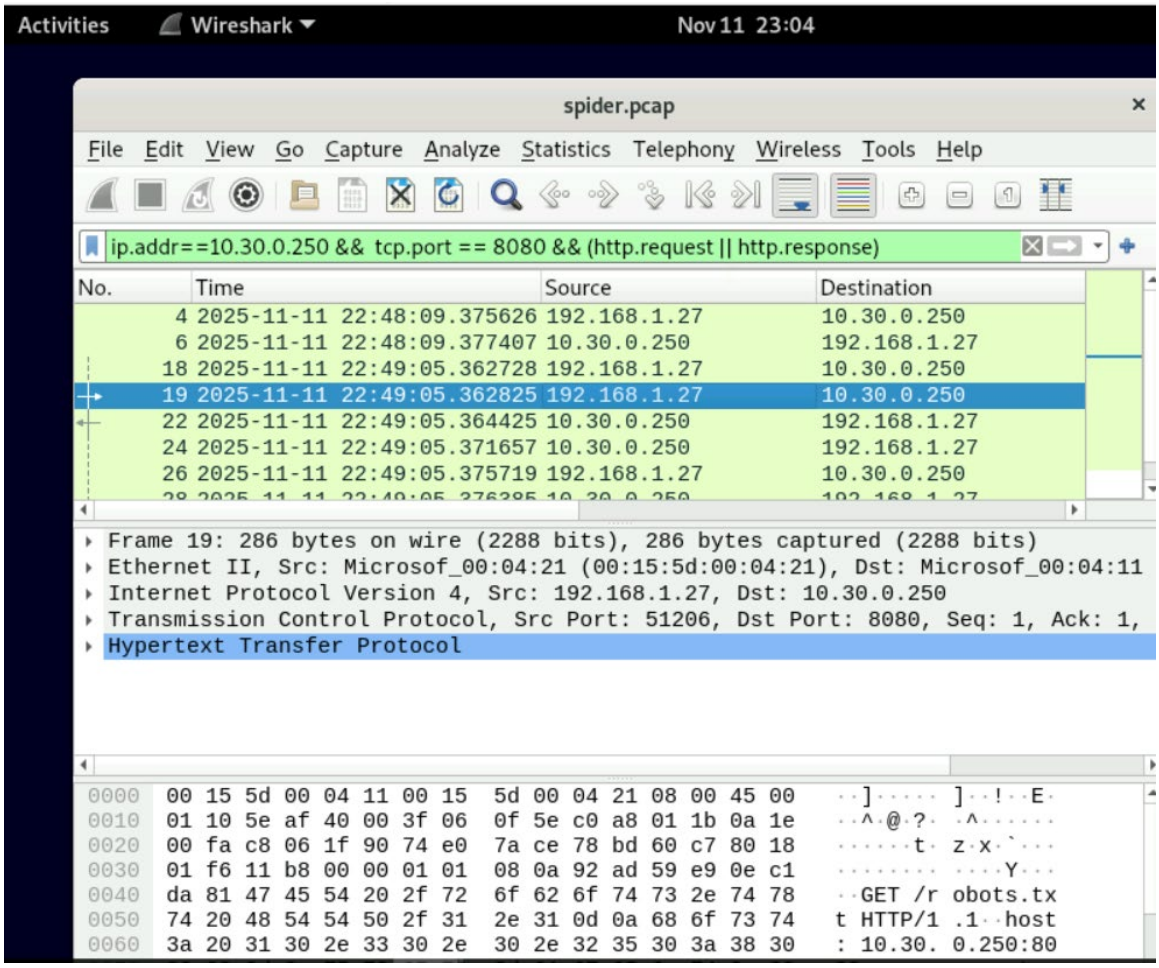
Target: 10.30.0.250

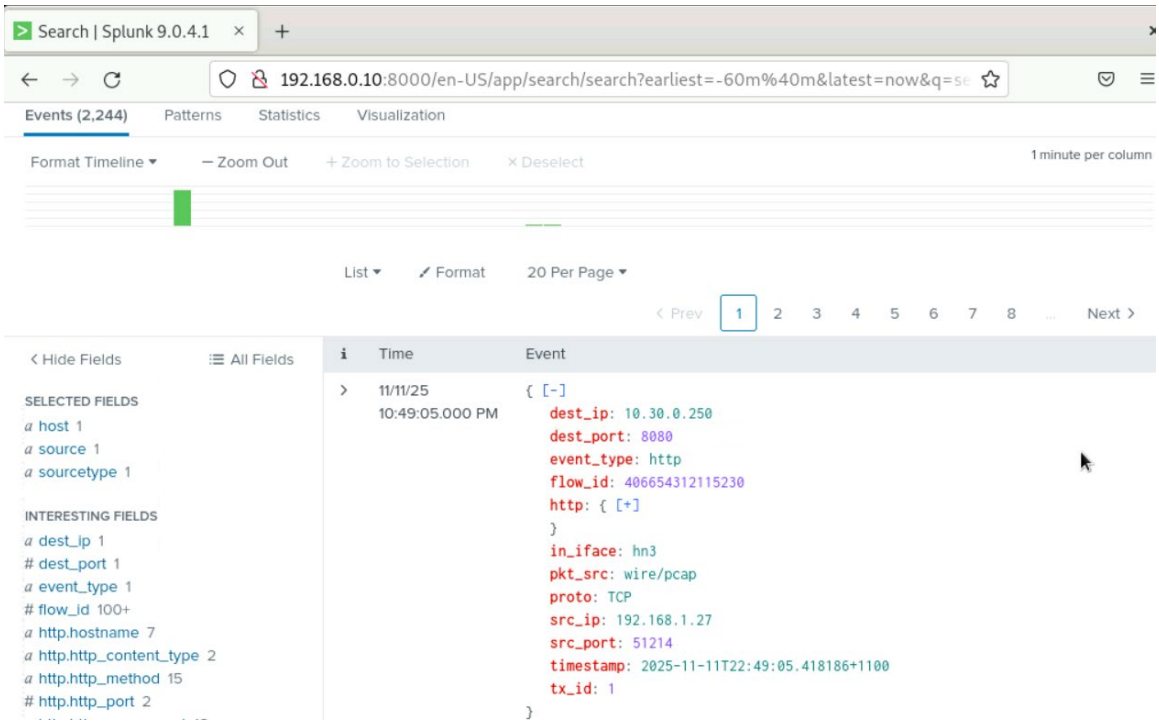


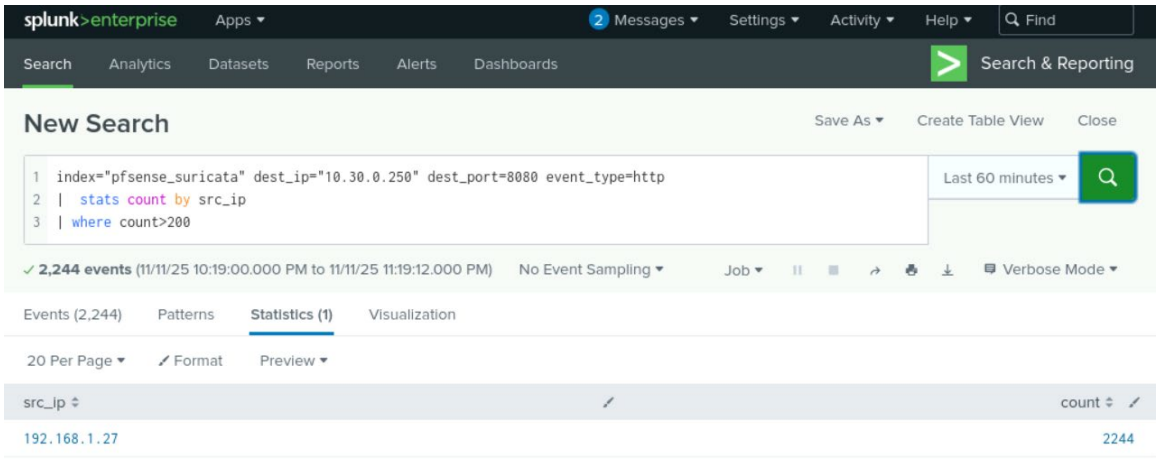




Blue Team Activity:


Activities
Wireshark
Nov 11 23:04
spider.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.30.0.250 && tcp.port == 8080 && (http.request || http.response)
No. Time Source Destination
4 2025-11-11 22:48:09.375626 192.168.1.27 10.30.0.250
6 2025-11-11 22:48:09.377407 10.30.0.250 192.168.1.27
18 2025-11-11 22:49:05.362728 192.168.1.27 10.30.0.250
19 2025-11-11 22:49:05.362825 192.168.1.27 10.30.0.250
22 2025-11-11 22:49:05.364425 10.30.0.250 192.168.1.27
24 2025-11-11 22:49:05.371657 10.30.0.250 192.168.1.27
26 2025-11-11 22:49:05.375719 192.168.1.27 10.30.0.250
Frame 19: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits)
Ethernet II, Src: Microsof_00:04:21 (00:15:5d:00:04:21), Dst: Microsof_00:04:11
Internet Protocol Version 4, Src: 192.168.1.27, Dst: 10.30.0.250
Transmission Control Protocol, Src Port: 51206, Dst Port: 8080, Seq: 1, Ack: 1,
Hypertext Transfer Protocol
0000 00 15 5d 00 04 11 00 15 5d 00 04 21 08 00 45 00
0010 01 10 5e af 40 00 3f 06 0f 5e c0 a8 01 1b 0a 1e
0020 00 fa c8 06 1f 90 74 e0 7a ce 78 bd 60 c7 80 18
0030 01 f6 11 b8 00 00 01 01 08 0a 92 ad 59 e9 0e c1
0040 da 81 47 45 54 20 2f 72 6f 62 6f 74 73 2e 74 78
0050 74 20 48 54 54 50 2f 31 2e 31 0d 0a 68 6f 73 74
0060 3a 20 31 30 2e 33 30 2e 30 2e 32 35 30 3a 38 30


Search | Splunk 9.0.4.1
192.168.0.10:8000/en-US/app/search/search?earliest=-60m%40m&latest=now&q=
Events (2,244) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
1 minute per column
List Format 20 Per Page
Prev 1 2 3 4 5 6 7 8 Next
Hide Fields All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a dest_ip 1
dest_port 1
a event_type 1
flow_id 100+
a http.hostname 7
a http.http_content_type 2
a http.http_method 15
http.http_port 2
Time Event
11/11/25 10:49:05.000 PM
{ [-]
dest_ip: 10.30.0.250
dest_port: 8080
event_type: http
flow_id: 406654312115230
http: { [+]
}
in_iface: hn3
pkt_src: wire/pcap
proto: TCP
src_ip: 192.168.1.27
src_port: 51214
timestamp: 2025-11-11T22:49:05.418186+1100
tx_id: 1
}



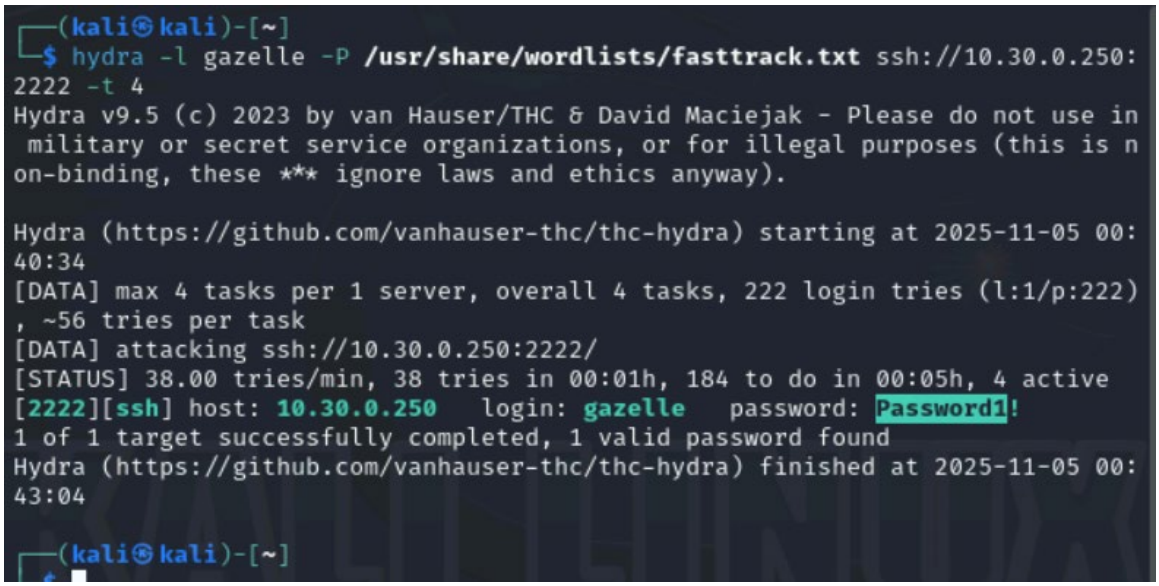
We were able to monitor this spidering activity via Wireshark and Splunk.

2.5 Brute Force Attack

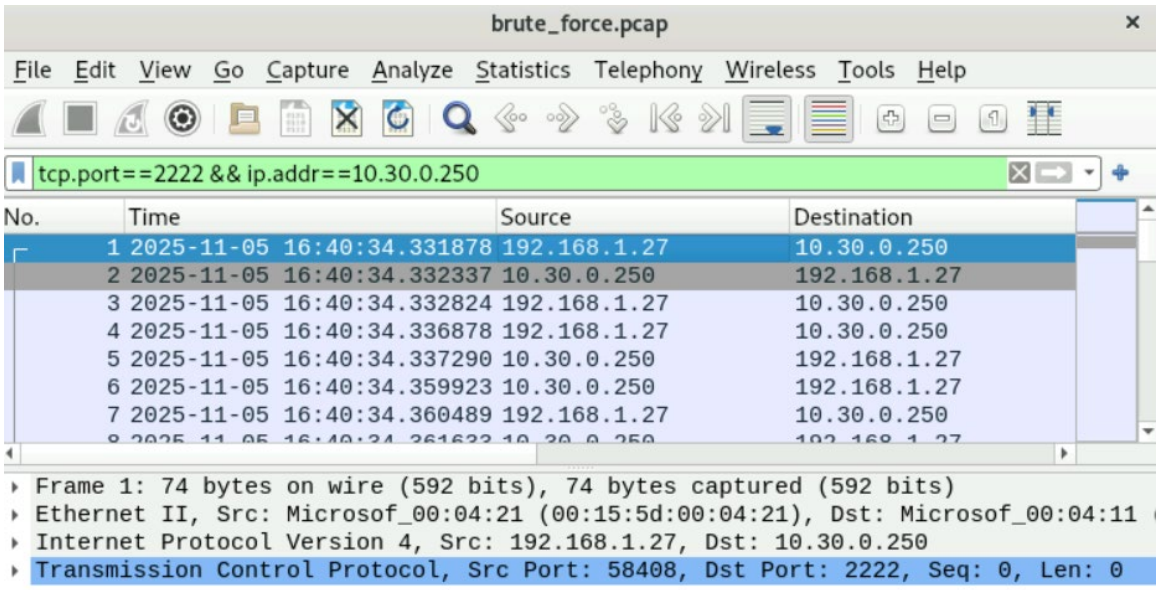
Red Team Activity:

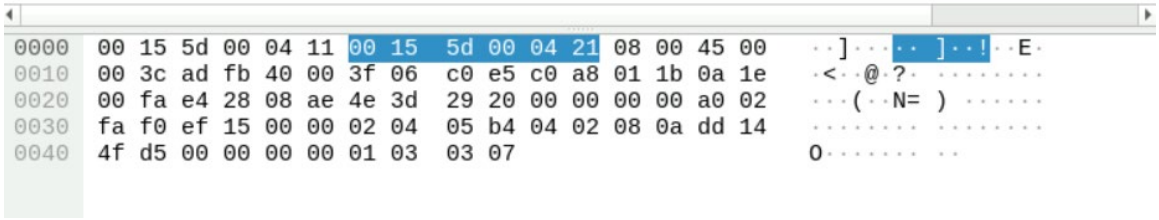
The red team conducted a brute force attack on the target system to gain unauthorised access by systematically attempting multiple password combinations until a valid one was found. The attack was successful, and the team obtained the correct password.

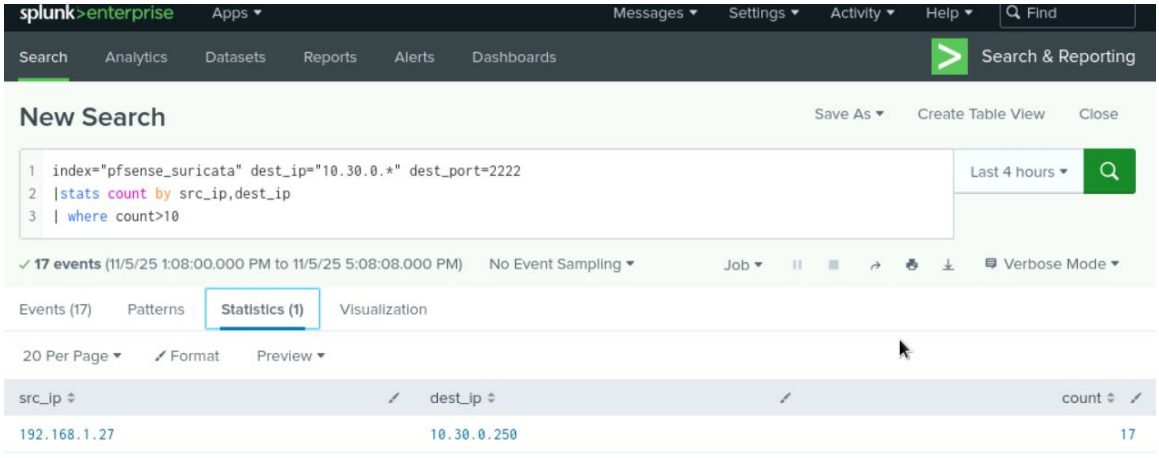
Target: 10.30.0.250

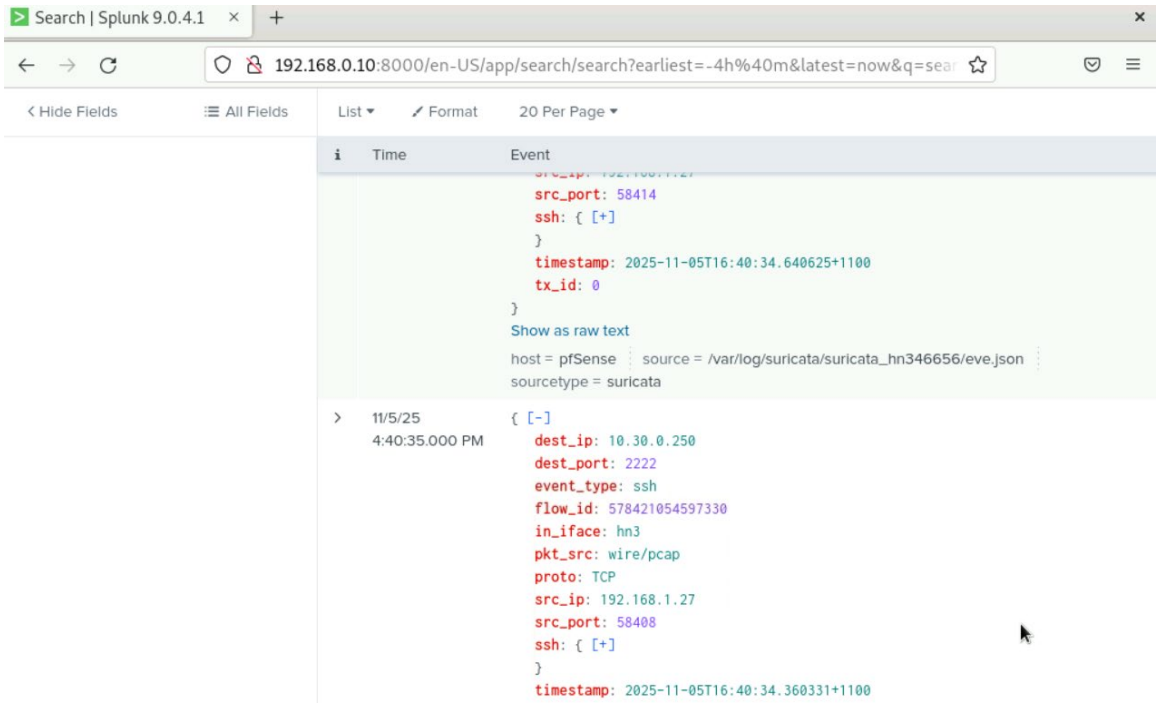


Blue Team Activity:


brute_force.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==2222 && ip.addr==10.30.0.250
No. Time Source Destination
1 2025-11-05 16:40:34.331878 192.168.1.27 10.30.0.250
2 2025-11-05 16:40:34.332337 10.30.0.250 192.168.1.27
3 2025-11-05 16:40:34.332824 192.168.1.27 10.30.0.250
4 2025-11-05 16:40:34.336878 192.168.1.27 10.30.0.250
5 2025-11-05 16:40:34.337290 10.30.0.250 192.168.1.27
6 2025-11-05 16:40:34.359923 10.30.0.250 192.168.1.27
7 2025-11-05 16:40:34.360489 192.168.1.27 10.30.0.250
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Microsof_00:04:21 (00:15:5d:00:04:21), Dst: Microsof_00:04:11
Internet Protocol Version 4, Src: 192.168.1.27, Dst: 10.30.0.250
Transmission Control Protocol, Src Port: 58408, Dst Port: 2222, Seq: 0, Len: 0


0000 00 15 5d 00 04 11 00 15 5d 00 04 21 08 00 45 00
0010 00 3c ad fb 40 00 3f 06 c0 e5 c0 a8 01 1b 0a 1e
0020 00 fa e4 28 08 ae 4e 3d 29 20 00 00 00 00 a0 02
0030 fa f0 ef 15 00 00 02 04 05 b4 04 02 08 0a dd 14
0040 4f d5 00 00 00 00 01 03 03 07


splunk>enterprise Apps Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Create Table View Close
1 index="pfsense_suricata" dest_ip="10.30.0.*" dest_port=2222
2 |stats count by src_ip,dest_ip
3 | where count>10
Last 4 hours
17 events (11/5/25 1:08:00.000 PM to 11/5/25 5:08:08.000 PM) No Event Sampling Job Verbose Mode
Events (17) Patterns Statistics (1) Visualization
20 Per Page Format Preview
src_ip dest_ip count
192.168.1.27 10.30.0.250 17



Using Wireshark and Splunk, we were able to monitor multiple login attempts to 10.30.0.250. It seems that the attacker finally logged into the system.

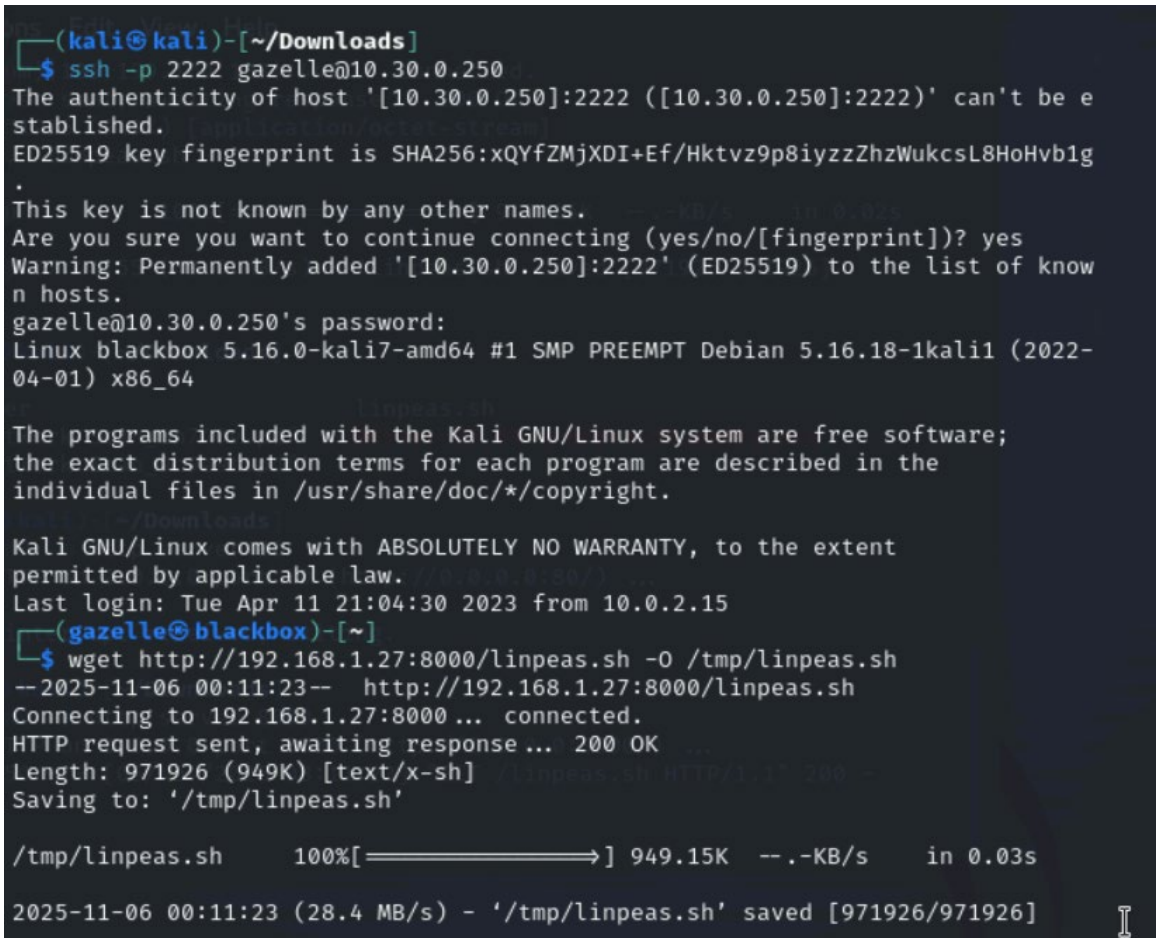
2.6 Post-Exploitation Enumeration

Red Team Activity:

The red team deployed *linpeas.sh* on the target Linux machine to assess its security posture and identify vulnerabilities or misconfigurations that could enable privilege escalation or system compromise.

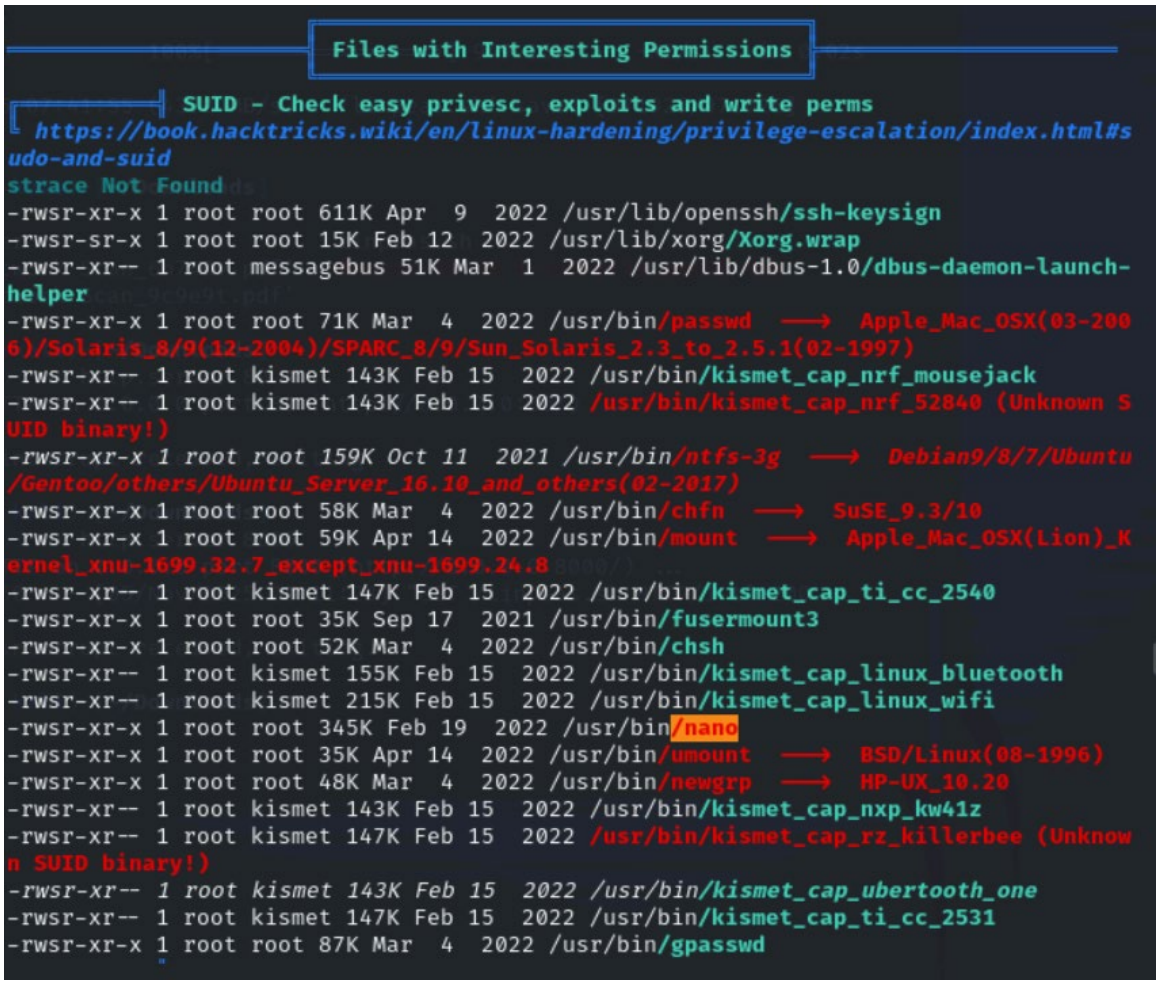
Target: 10.30.0.250

Red team used a simple http server and uploaded linpeas.sh to the target machine as shown below.

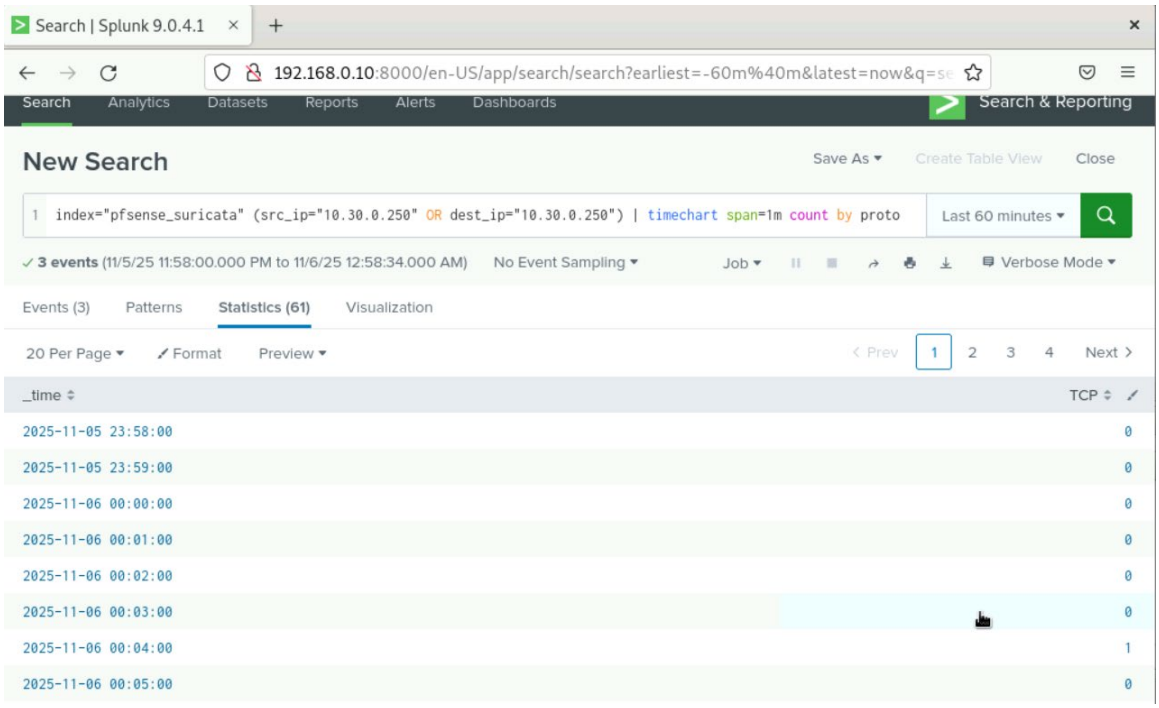


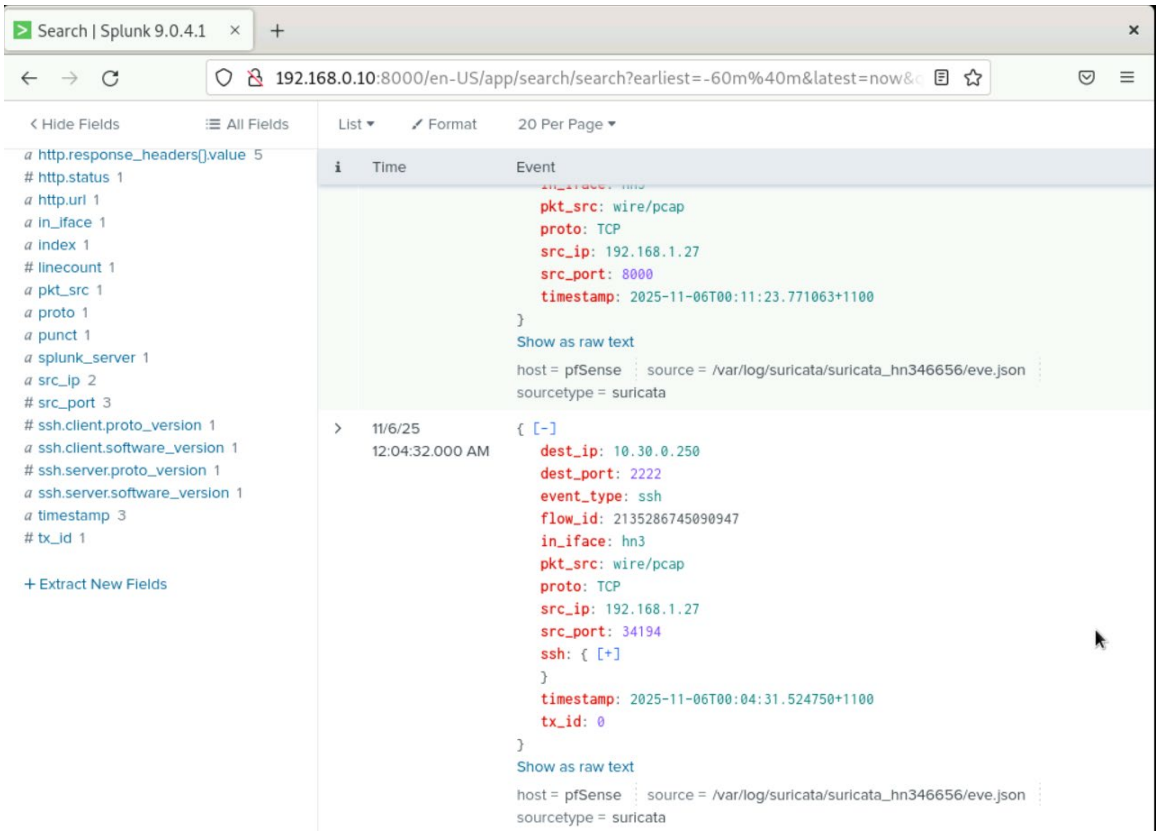
Then they run linpeas.sh

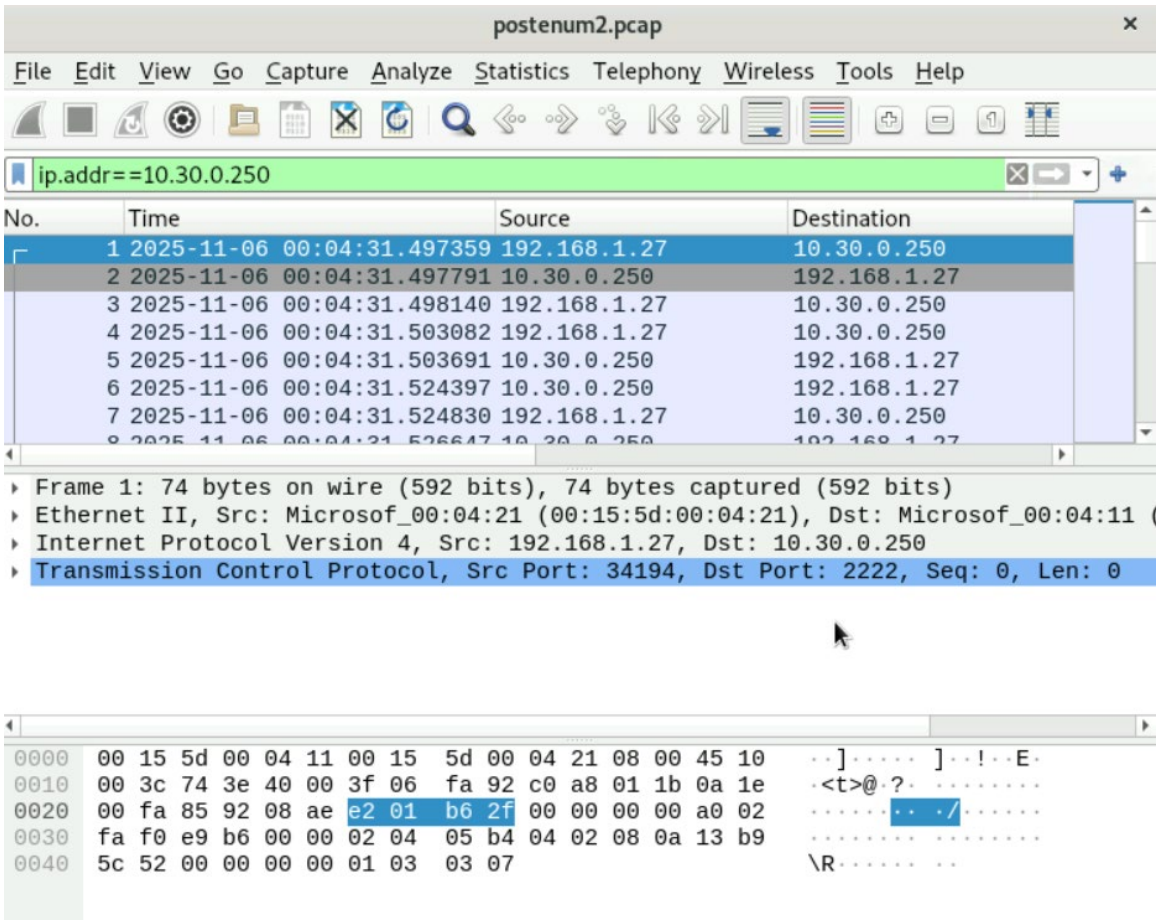
From the scanning result of linpeas.sh, the red team found that SUID was set on nano editor

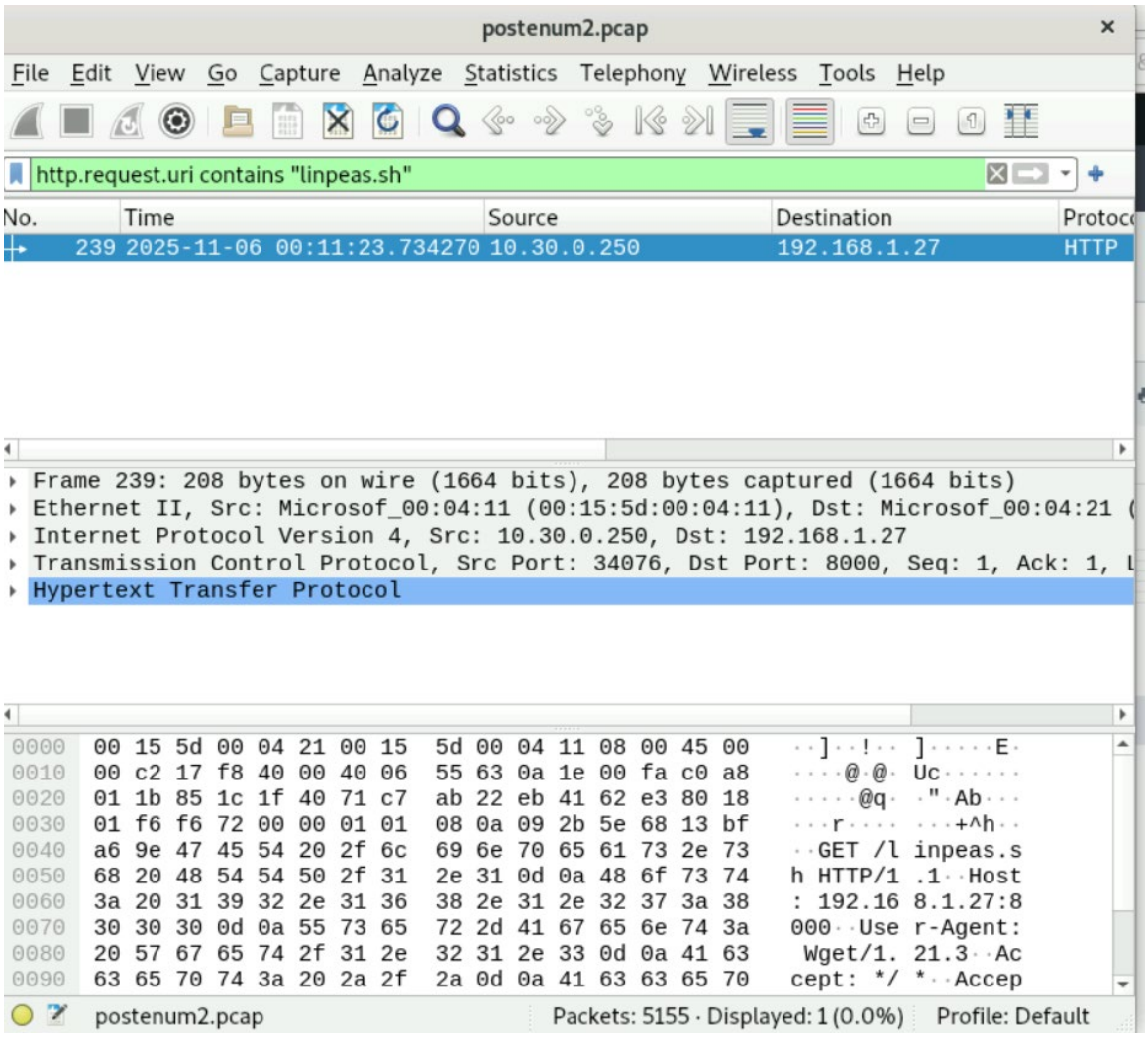


Blue Team Activity:


Search | Splunk 9.0.4.1
192.168.0.10:8000/en-US/app/search/search?earliest=-60m%40m&latest=now&q=se
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
1 index="pfsense_suricata" (src_ip="10.30.0.250" OR dest_ip="10.30.0.250") | timechart span=1m count by proto
Last 60 minutes
3 events (11/5/25 11:58:00.000 PM to 11/6/25 12:58:34.000 AM)
No Event Sampling
Job
Verbose Mode
Events (3)
Patterns
Statistics (61)
Visualization
20 Per Page
Format
Preview
Prev
1
2
3
4
Next
_time
TCP
2025-11-05 23:58:00 0
2025-11-05 23:59:00 0
2025-11-06 00:00:00 0
2025-11-06 00:01:00 0
2025-11-06 00:02:00 0
2025-11-06 00:03:00 0
2025-11-06 00:04:00 1
2025-11-06 00:05:00 0


Search | Splunk 9.0.4.1
192.168.0.10:8000/en-US/app/search/search?earliest=-60m%40m&latest=now&
Hide Fields
All Fields
List
Format
20 Per Page
a http.response_headers{}.value 5
http.status 1
a http.url 1
a in_iface 1
a index 1
linecount 1
a pkt_src 1
a proto 1
a punct 1
a splunk_server 1
a src_ip 2
src_port 3
ssh.client.proto_version 1
a ssh.client.software_version 1
ssh.server.proto_version 1
a ssh.server.software_version 1
a timestamp 3
tx_id 1
+ Extract New Fields
Time
Event
pkt_src: wire/pcap
proto: TCP
src_ip: 192.168.1.27
src_port: 8000
timestamp: 2025-11-06T00:11:23.771063+1100
}
Show as raw text
host = pfSense source = /var/log/suricata/suricata_hn346656/eve.json
sourcetype = suricata
11/6/25
12:04:32.000 AM
{ [-]
dest_ip: 10.30.0.250
dest_port: 2222
event_type: ssh
flow_id: 2135286745090947
in_iface: hn3
pkt_src: wire/pcap
proto: TCP
src_ip: 192.168.1.27
src_port: 34194
ssh: { [+]
}
timestamp: 2025-11-06T00:04:31.524750+1100
tx_id: 0
}
Show as raw text
host = pfSense source = /var/log/suricata/suricata_hn346656/eve.json
sourcetype = suricata


postenum2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.30.0.250
No. Time Source Destination
1 2025-11-06 00:04:31.497359 192.168.1.27 10.30.0.250
2 2025-11-06 00:04:31.497791 10.30.0.250 192.168.1.27
3 2025-11-06 00:04:31.498140 192.168.1.27 10.30.0.250
4 2025-11-06 00:04:31.503082 192.168.1.27 10.30.0.250
5 2025-11-06 00:04:31.503691 10.30.0.250 192.168.1.27
6 2025-11-06 00:04:31.524397 10.30.0.250 192.168.1.27
7 2025-11-06 00:04:31.524830 192.168.1.27 10.30.0.250
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Microsof_00:04:21 (00:15:5d:00:04:21), Dst: Microsof_00:04:11
Internet Protocol Version 4, Src: 192.168.1.27, Dst: 10.30.0.250
Transmission Control Protocol, Src Port: 34194, Dst Port: 2222, Seq: 0, Len: 0
0000 00 15 5d 00 04 11 00 15 5d 00 04 21 08 00 45 10
0010 00 3c 74 3e 40 00 3f 06 fa 92 c0 a8 01 1b 0a 1e
0020 00 fa 85 92 08 ae e2 01 b6 2f 00 00 00 00 a0 02
0030 fa f0 e9 b6 00 00 02 04 05 b4 04 02 08 0a 13 b9
0040 5c 52 00 00 00 00 01 03 03 07



Using Splunk and Wireshark, we were able to monitor the incident and capture both Wget traffic and linpeas.sh enumeration.

2.7 Privilege Escalation

Red Team Activity:

Target: 10.30.0.250

Red team used SUID-enabled /bin/nano to edit /etc/passwd, created user 'demo' with password '123', and gained root access.

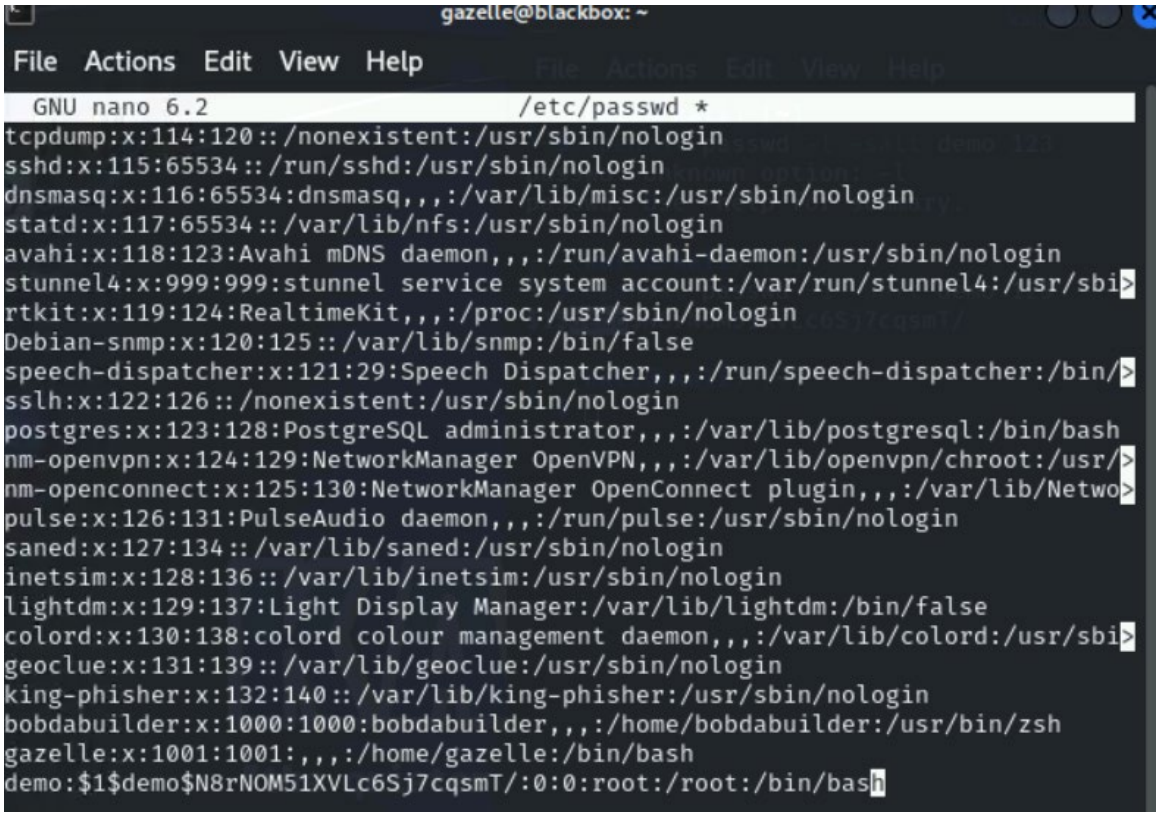
Generate a password hash as shown below:

```
┌──(kali㉿kali)-[~]
└─$ openssl passwd -1 -salt demo 123
$1$demo$N8rNOM51XVLc6Sj7cqsmT/
```

Edit /etc/passwd using nano.

```
┌──(gazelle㉿blackbox)-[~]
└─$ nano /etc/passwd
```

Add user 'demo' and password hash at the end. Save the file and exit.



Switch the use from ‘gazelle’ to ‘demo’.

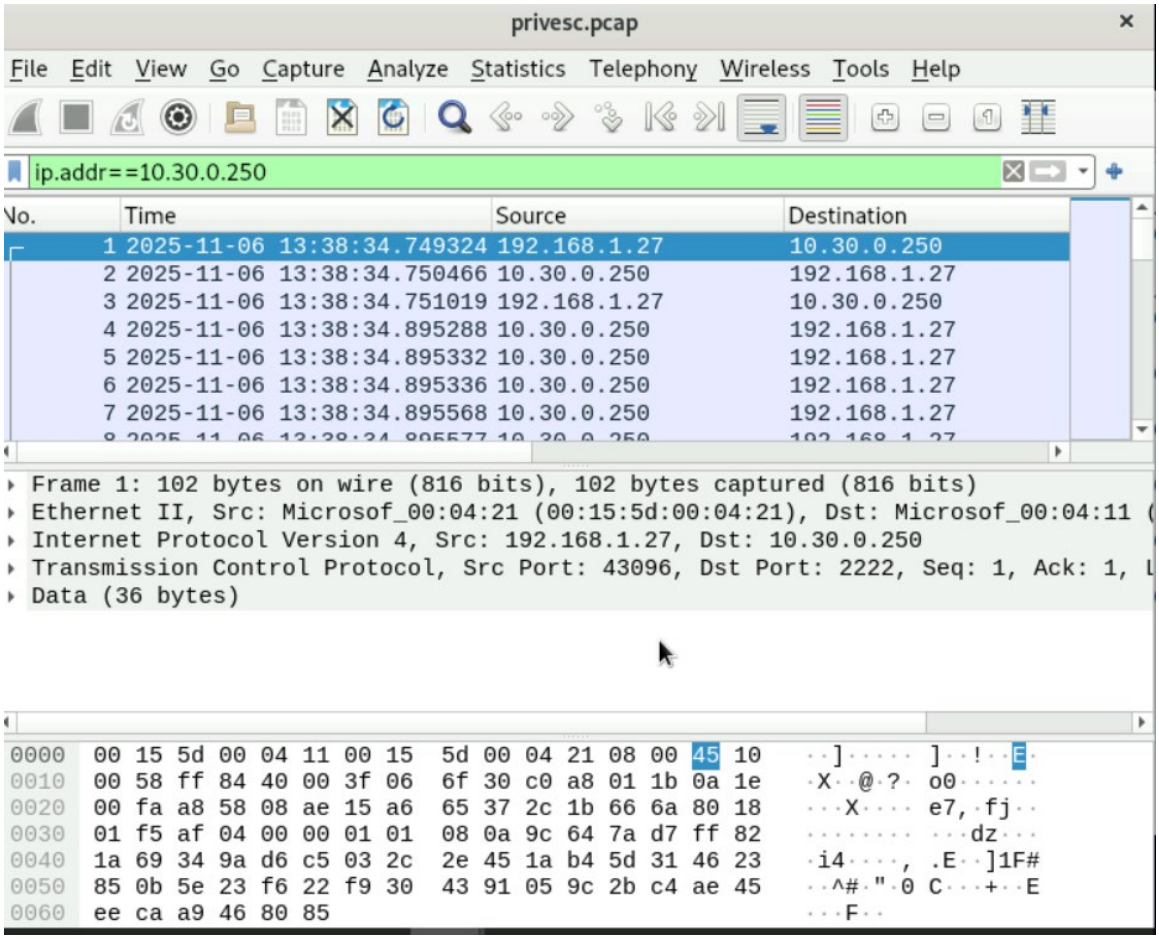
```
┌──(gazelle㉿blackbox)-[~]
└─$ su demo
Password:
┌──(root㉿blackbox)-[/home/gazelle]
└─# id
uid=0(root) gid=0(root) groups=0(root)

┌──(root㉿blackbox)-[/home/gazelle]
└─# whoami
root

┌──(root㉿blackbox)-[/home/gazelle]
└─#
```

Now the red team gets root access to this Blackbox machine.

Blue Team Activity:



Using Wireshark, we could see attacker's IP address at that time. Unfortunately, we failed to monitor this privilege escalation activity.

2.8 Blue Team Observation Checklist

Table 1 – Blue team observation checklist

Time	Attack detected	Victim IP	Source IP	Description	Response
03/11/2025 23:13:10	Vulnerability Scanning	10.30.0.235, 10.30.0.236, 10.30.0.237, 10.30.0.250	192.168.1.27	Vulnerability Scanning to identify any know vulnerabilities on target hosts	Setting up IDS or WAF to monitor and block suspicious scanning.
04/11/2025 14:25:41	Port scanning	10.30.0.250	192.168.1.27	Port scanning to discover open ports on the target	Setting up IDS or WAF to monitor and block suspicious scanning.
04/11/2025 22:56:51	Directory Busting	10.30.0.250	192.168.1.27	Web content scanning to discover hidden web content	Setting up IDS or WAF to monitor and block directory requests.
11/11/2025 22:49:05	Spidering	10.30.0.250	192.168.1.27	Web spidering to map web application's structure and find hidden items	Setting up IDS or WAF to monitor and block suspicious activities.
05/11/2025 16:40:34	Brute Force Attack	10.30.0.250	192.168.1.27	To gain unauthorized access to the target system by trying a large	Setting up IDS or WAF to monitor for excessive

				number of possible passwords in the dictionary	failed login attempts and block suspicious IP addresses.
06/11/2025 00:04:31	Post-exploitation enumeration	10.30.0.250	192.168.1.27	To identify potential vulnerabilities or misconfigurations that could lead to privilege escalation or compromise	Treat the presence of linpeas.sh as a potential security incident. Initiate an incident response process.
06/11/2025 13:38:34	Privilege Escalation	10.30.0.250	192.168.1.27	To gain full access to the system	Blue team failed to monitor the activity