Capstone Project - Enhancing Linux Endpoint Security with Wazuh: Unauthorized Process Detection and Malicious IP Blocking

Tasks 1 and 2

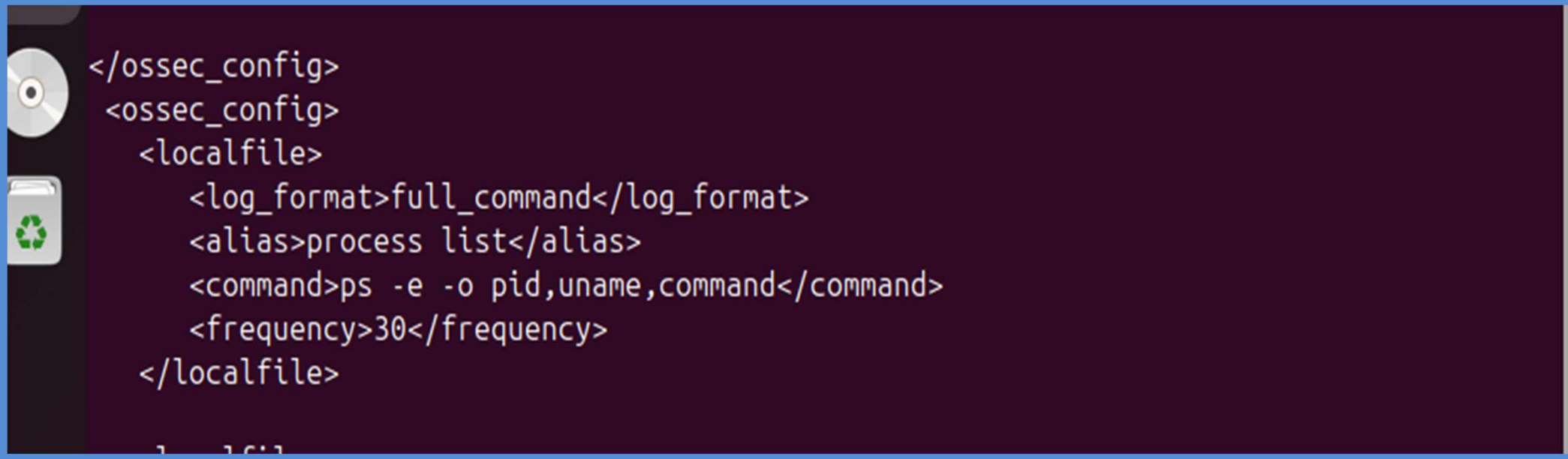
Presented by: Akpevweoghene Ememu

Task 1 Overview

Objective: Detect unauthorized Netcat usage
Approach: Wazuh command monitoring
Detection: Custom rules for Netcat process alerts

Wazuh Agent Configuration

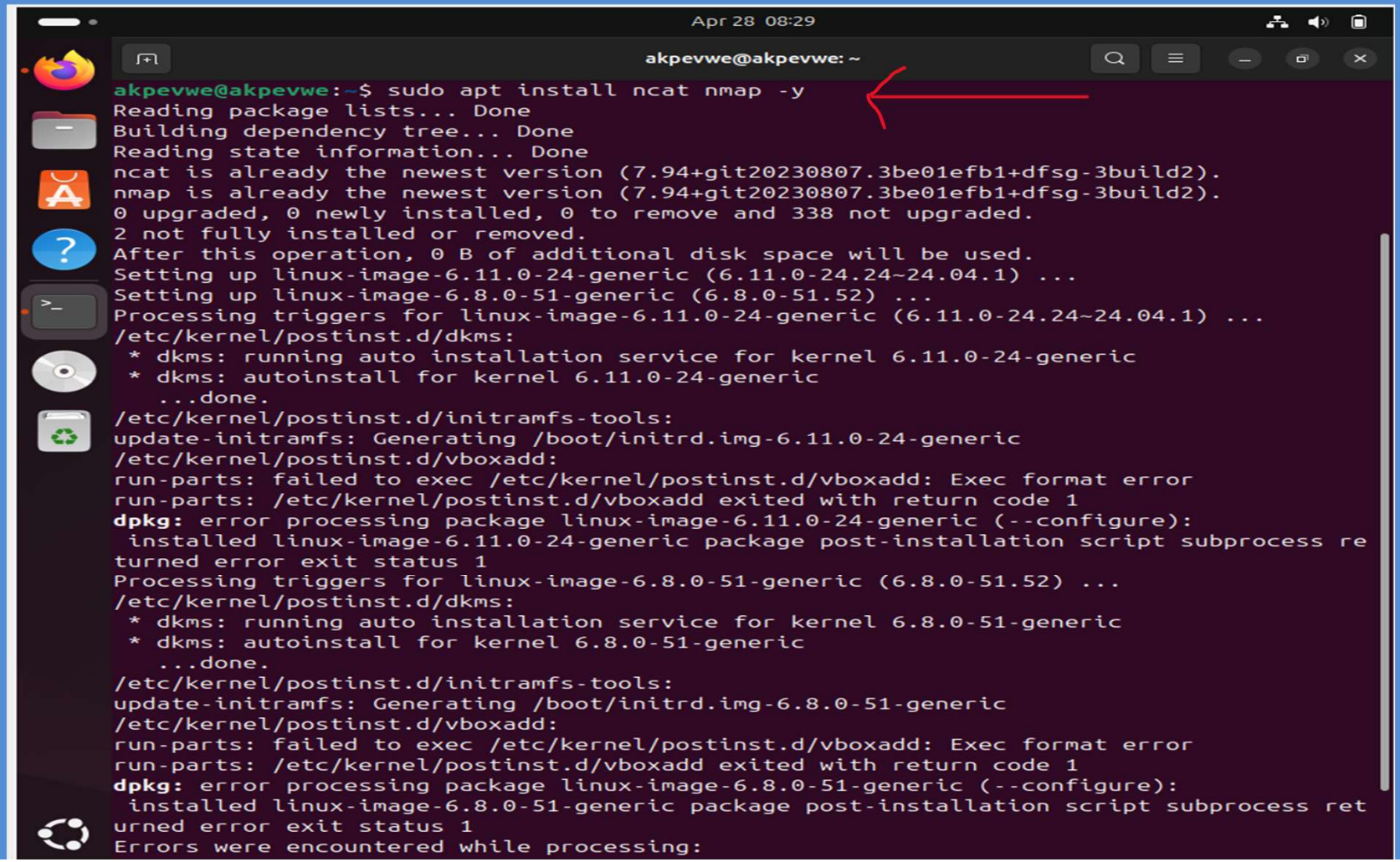
Added config to ossec.conf using /var/ossec/etc/ossec.conf file
Restarted Wazuh agent



Netcat Installation and Wazuh Rule

Installed ncat and nmap

Custom rules to detect nc –l



Netcat Installation and Wazuh Rule

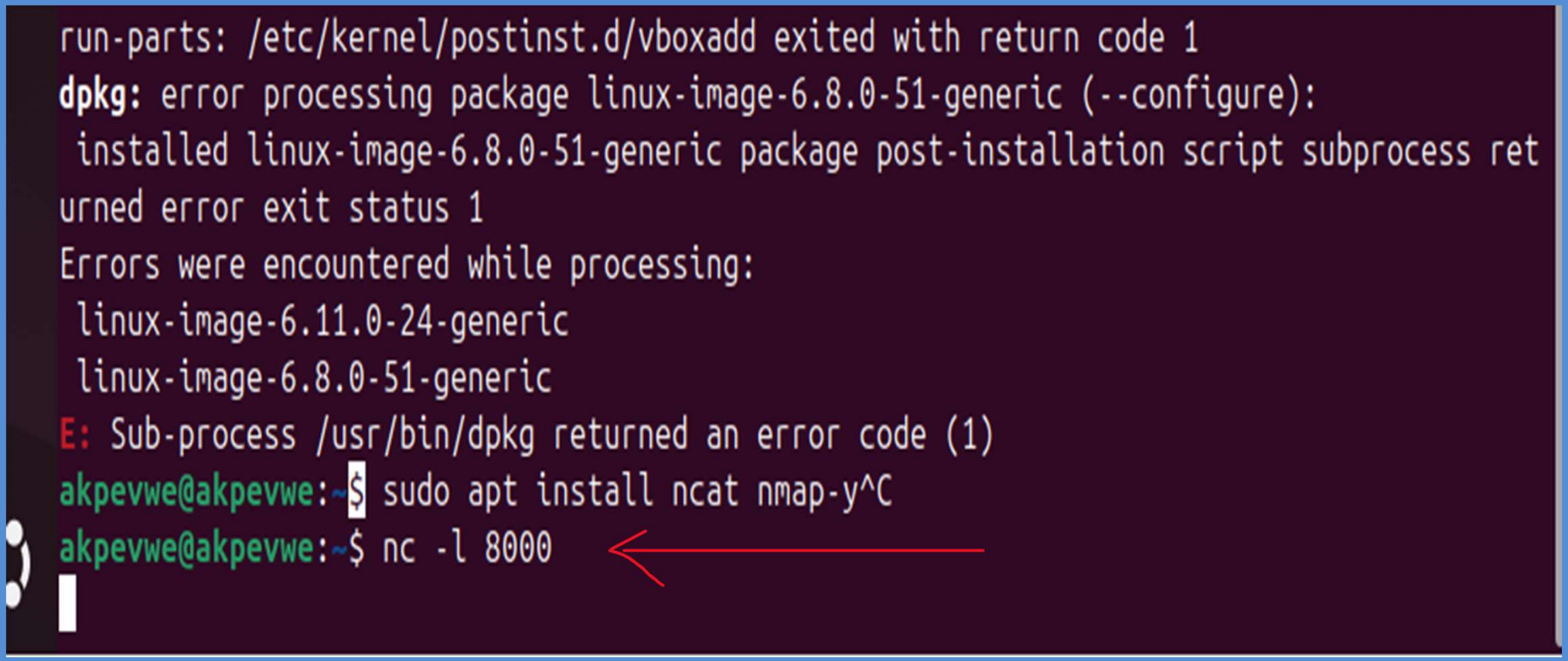
Inputted custom rules to detect nc –l

Added the following rules to the /var/ossec/etc/rules/local_rules.xml file on the Wazuh server

```
  GNU nano 2.9.8          /var/ossec/etc/rules/local_rules.xml


<group name="ossec,">
 <rule id="100050" level="0">
   <if_sid>530</if_sid>
   <match>^ossec: output: 'process list'</match>
   <description>List of running processes.</description>
   <group>process_monitor,</group>
  </rule>

<rule id="100051" level="7" ignore="900">
    <if_sid>100050</if_sid>
    <match>nc -l</match>
    <description>netcat listening for incoming connections.</description>
    <group>process_monitor,</group>
   </rule>
</group>
```

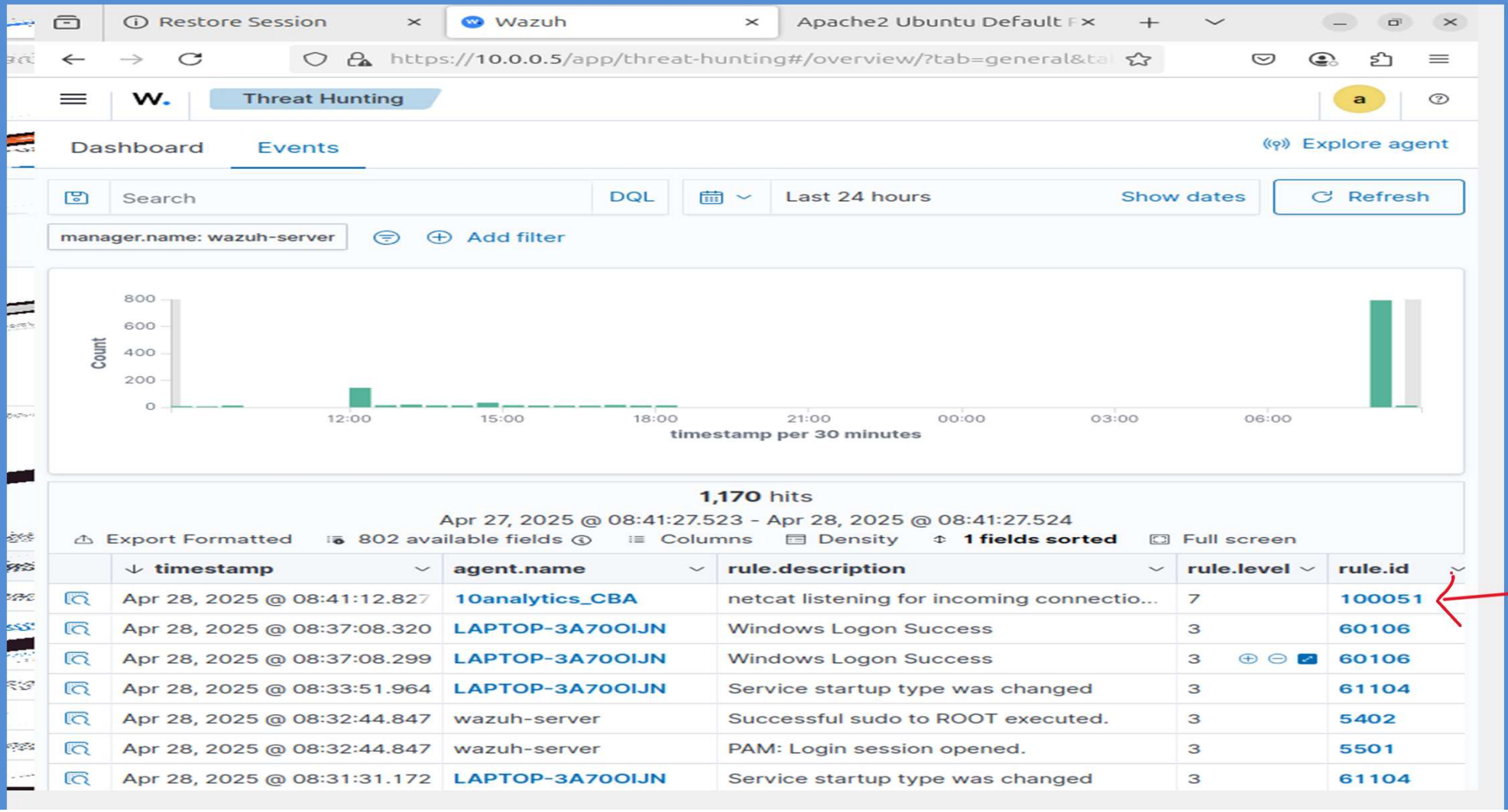
Attack Emulation

Ran nc -l 8000
Alerts triggered: rule.id (100051)



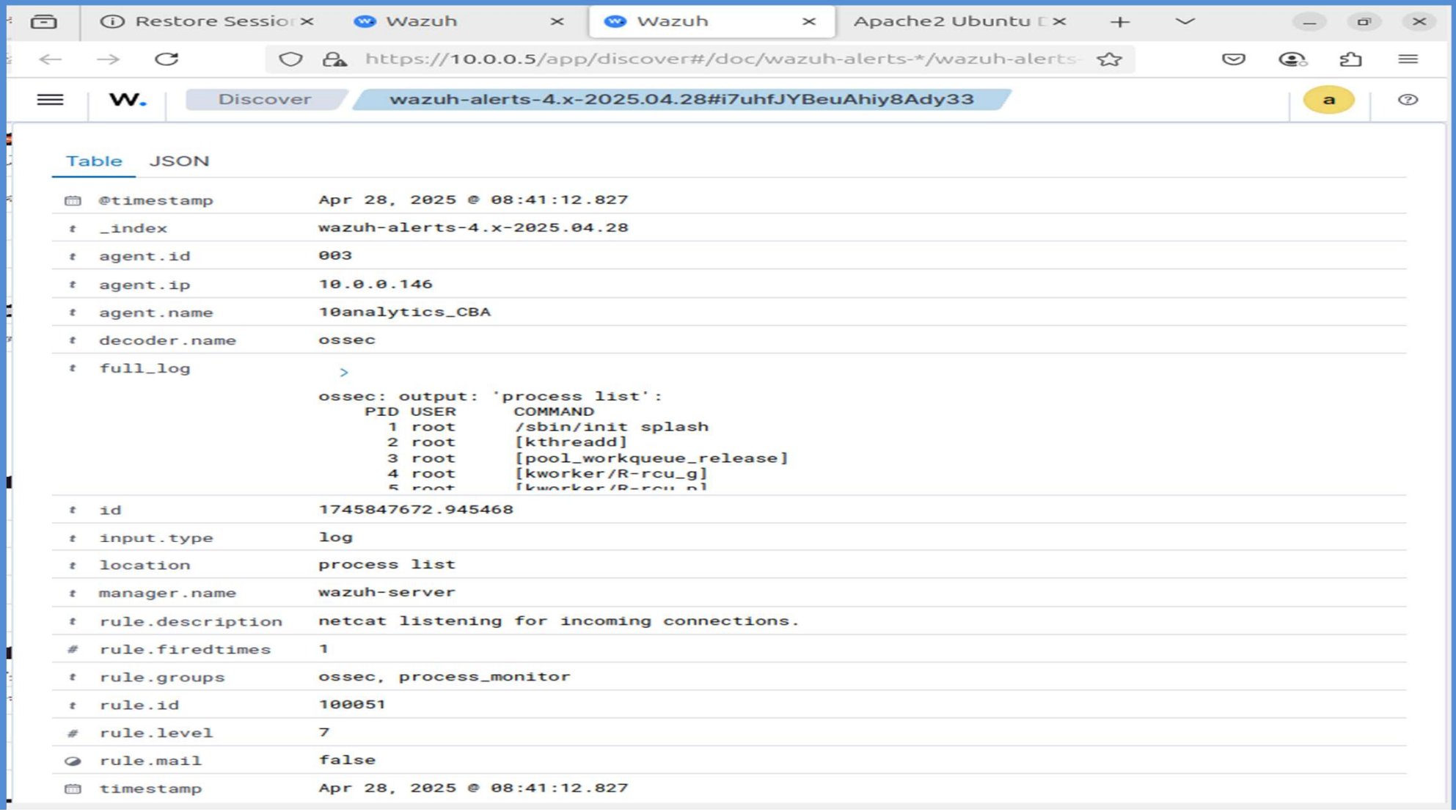
Visualisation of Alerts

I visualized the alert data in the Wazuh dashboard by going to the Threat Hunting module to obtain rule.id:(100051)



Visualisation of Alerts

Details of rule.id (100051)



Mitigation Strategies for Netcat

Usage rules for authorised persons
Limit installation
Detect behavior
Track commands
Network monitoring
Secure alternatives

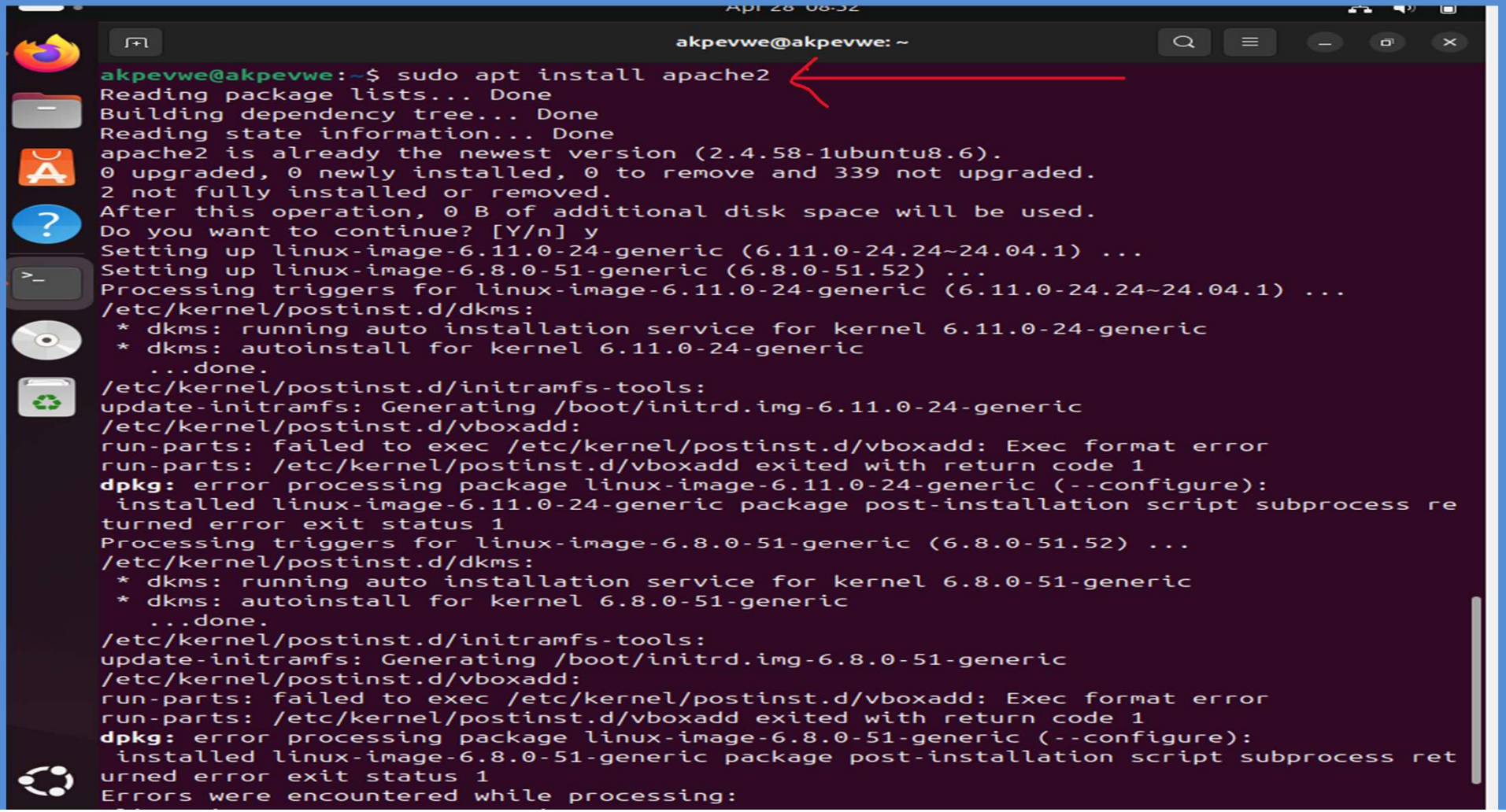
Task 2 Overview

Objective: Block malicious IPs
Environment: Wazuh, Ubuntu server & RHEL attacker(Kali)

Apache Setup and Monitoring

Installed Apache

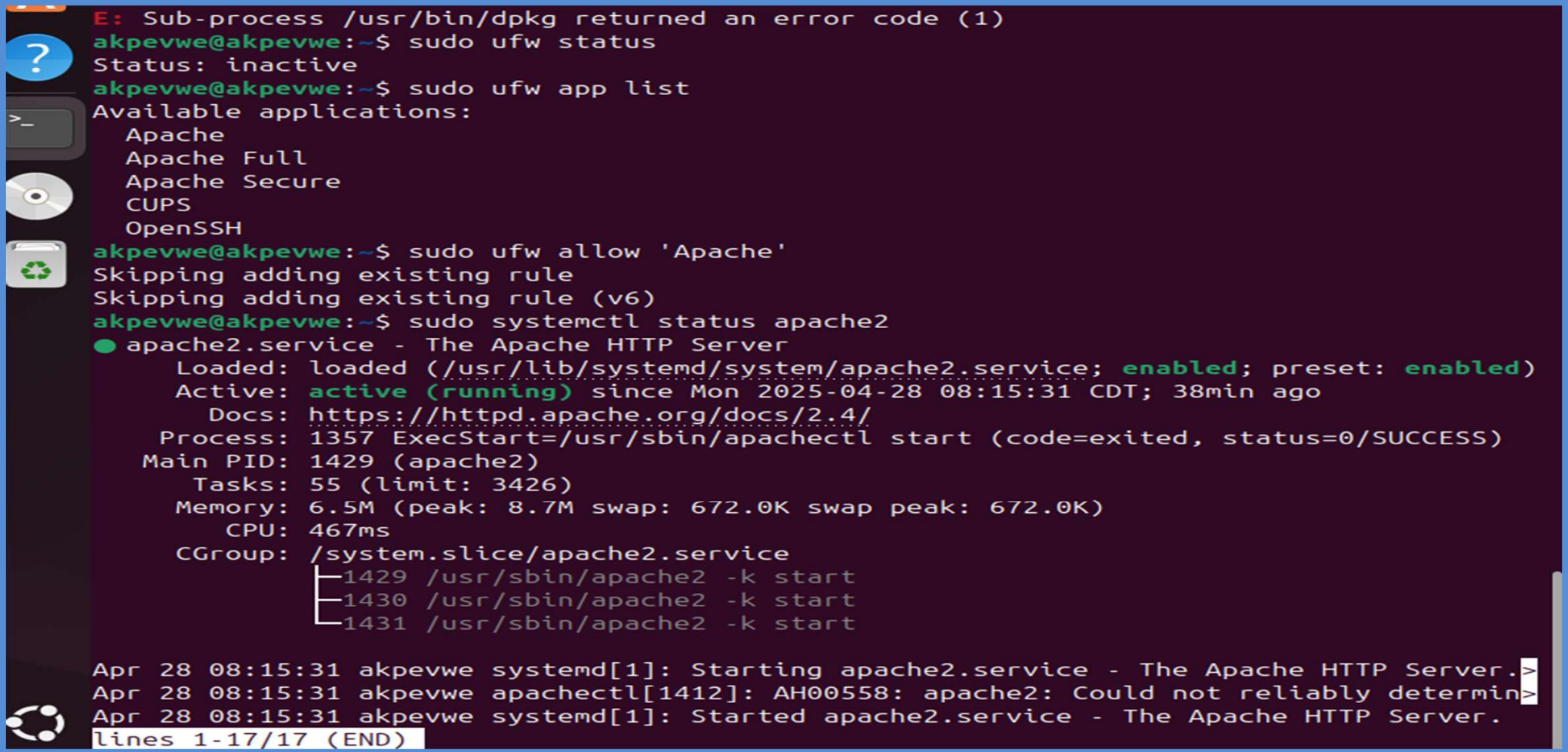
Monitored access.log with Wazuh



Apache Setup and Monitoring

Installed Apache

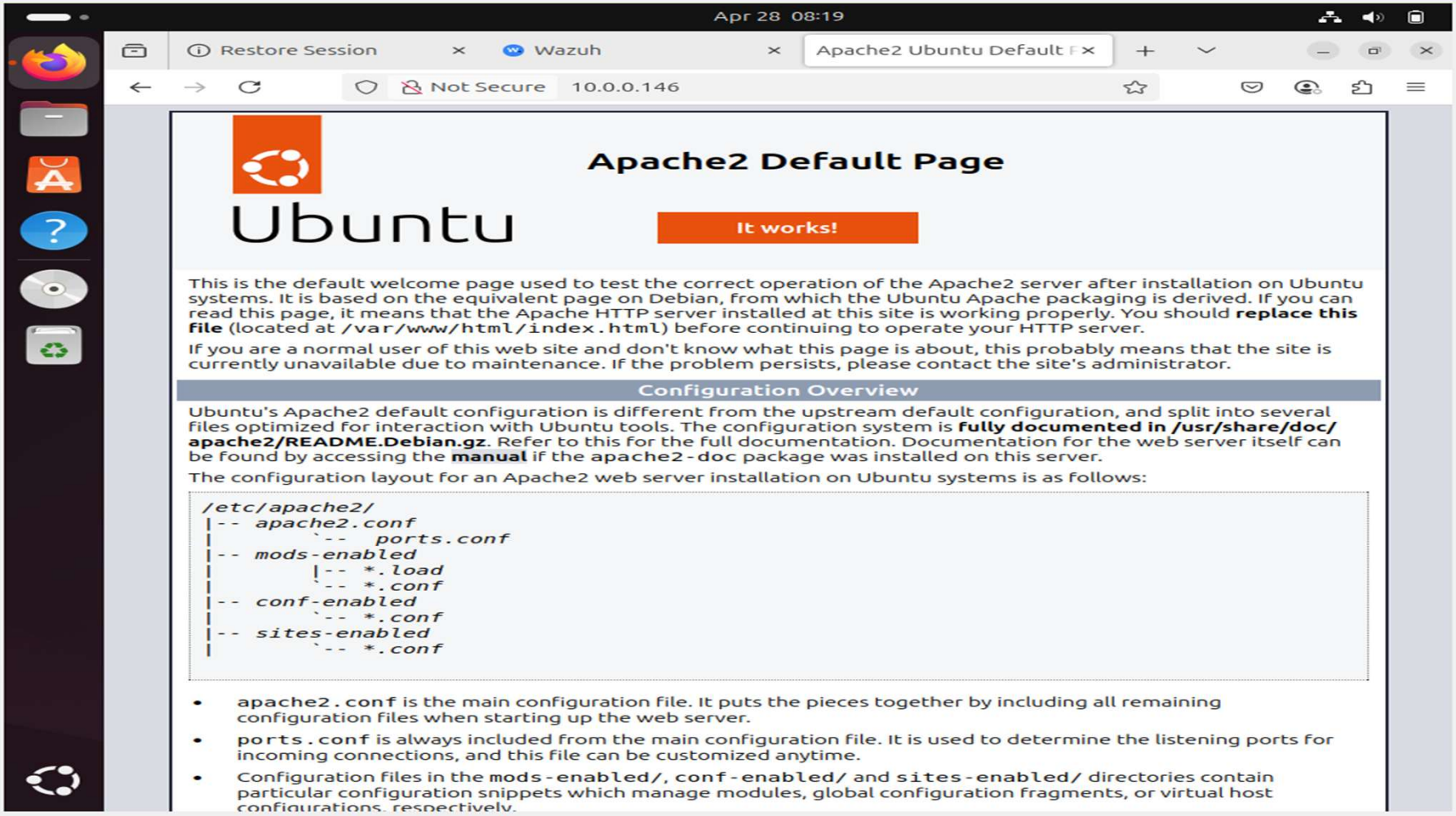
Monitored access.log with Wazuh



Apache Setup and Monitoring

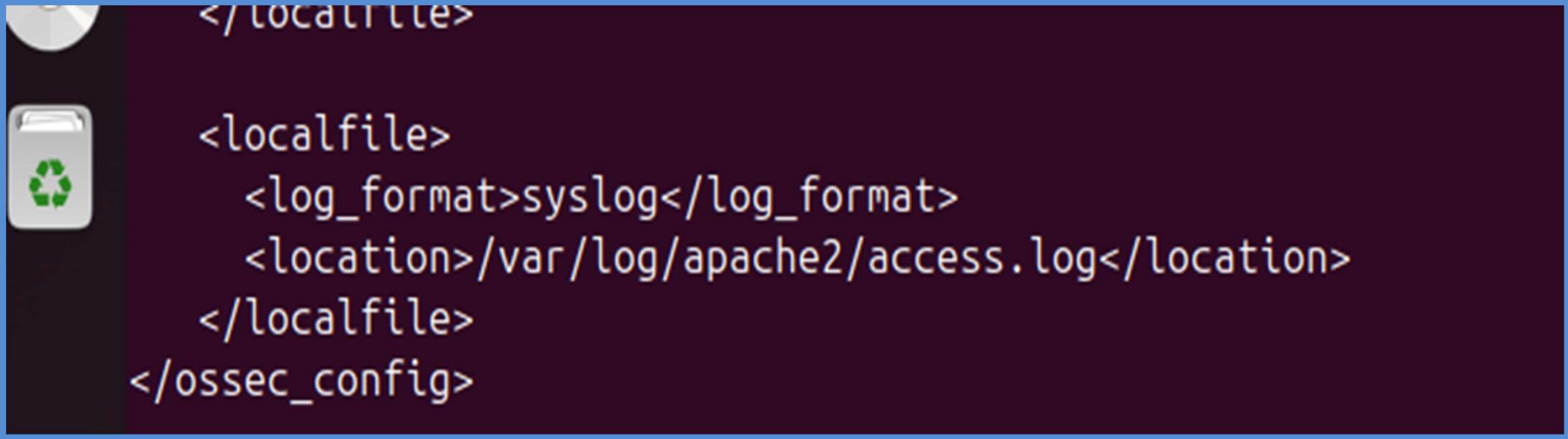
Use the curl command $ curl http://10.0.0.146

in a browser to view the Apache landing page and verify the installation:



Apache Setup and Monitoring

Add the following to /var/ossec/etc/ossec.conf file to configure the Wazuh



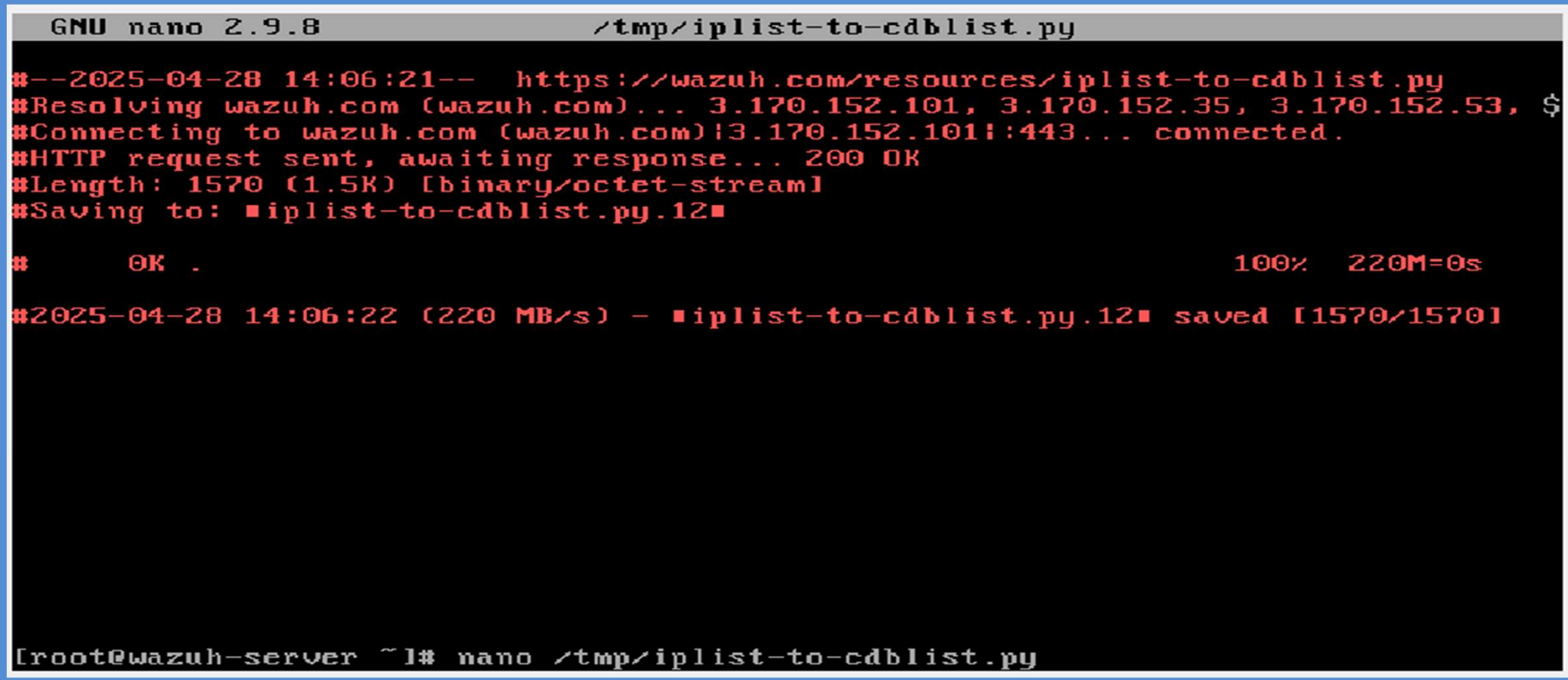
Wazuh Server Configuration

Downloaded IP list
Converted to .cdb
Updated permissions

```
[root@wazuh-server ~]# sudo yum update && sudo yum install -y wget
Loaded plugins: langpacks, priorities, update-motd
amzn2-core                                               | 3.6 kB     00:00
No packages marked for update
Loaded plugins: langpacks, priorities, update-motd
Package wget-1.14-18.amzn2.1.x86_64 already installed and latest version
Nothing to do
[root@wazuh-server ~]# sudo wget https://raw.githubusercontent.com/firehol/block
list-ipsets/master/alienvault_reputation.ipset -o /var/ossec/etc/lists/alienvaul
t_reputation.ipset
[root@wazuh-server ~]# sudo echo 10.0.0.75 >> /var/ossec/etc/lists/alienvault_re
putation.ipset
[root@wazuh-server ~]# $sudo wget https://wazuh.com/resources/iplist-to-cdblist.
py -o /tmp/iplist-to-cdblist.py
[root@wazuh-server ~]# sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-
to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/li
sts/blacklist-alienvault
  File "/tmp/iplist-to-cdblist.py", line 1
    --2025-04-28 14:06:21--  https://wazuh.com/resources/iplist-to-cdblist.py
          ^
SyntaxError: leading zeros in decimal integer literals are not permitted; use an
 0o prefix for octal integers
[root@wazuh-server ~]#
```

Wazuh Server Configuration

Downloaded IP list
Converted to .cdb
Updated permissions



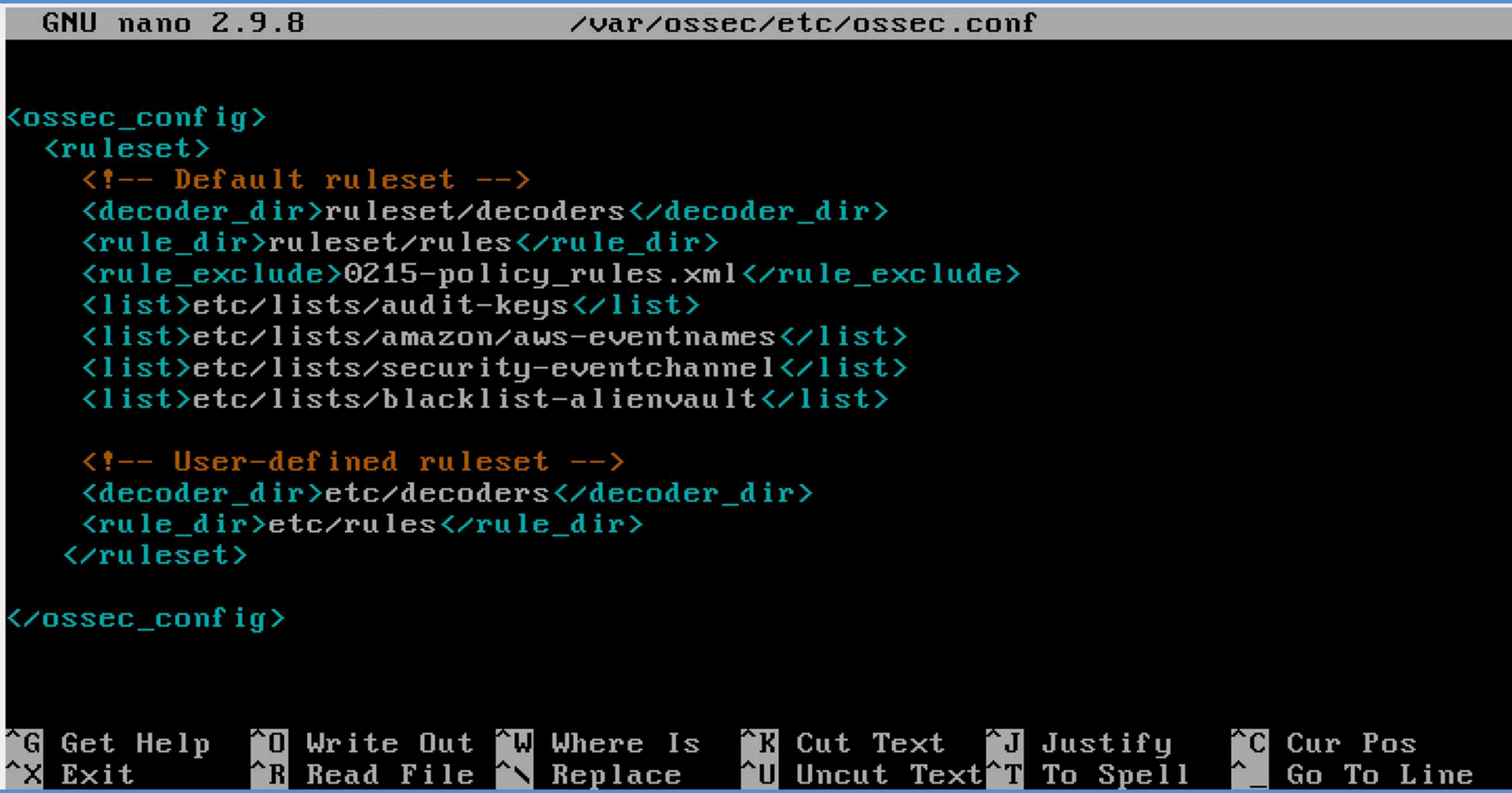
Wazuh Server Configuration

```
#HTTP request sent, awaiting response... 200 OK
#Length: 1570 (1.5K) [binary/octet-stream]
#Saving to: ▪iplist-to-cdblist.py.12▪

#     0K .                                                    100%  220M=0s

#2025-04-28 14:06:22 (220 MB/s) - ▪iplist-to-cdblist.py.12▪ saved [1570/1570]

[root@wazuh-server ~]# sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-
to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/li
sts/blacklist-alienvault
[root@wazuh-server ~]# sudo chown wazuh:wazuh /var/ossec/etc/lists/blacklist-ali
envault
[root@wazuh-server ~]#
```

Custom Rules and Active Response

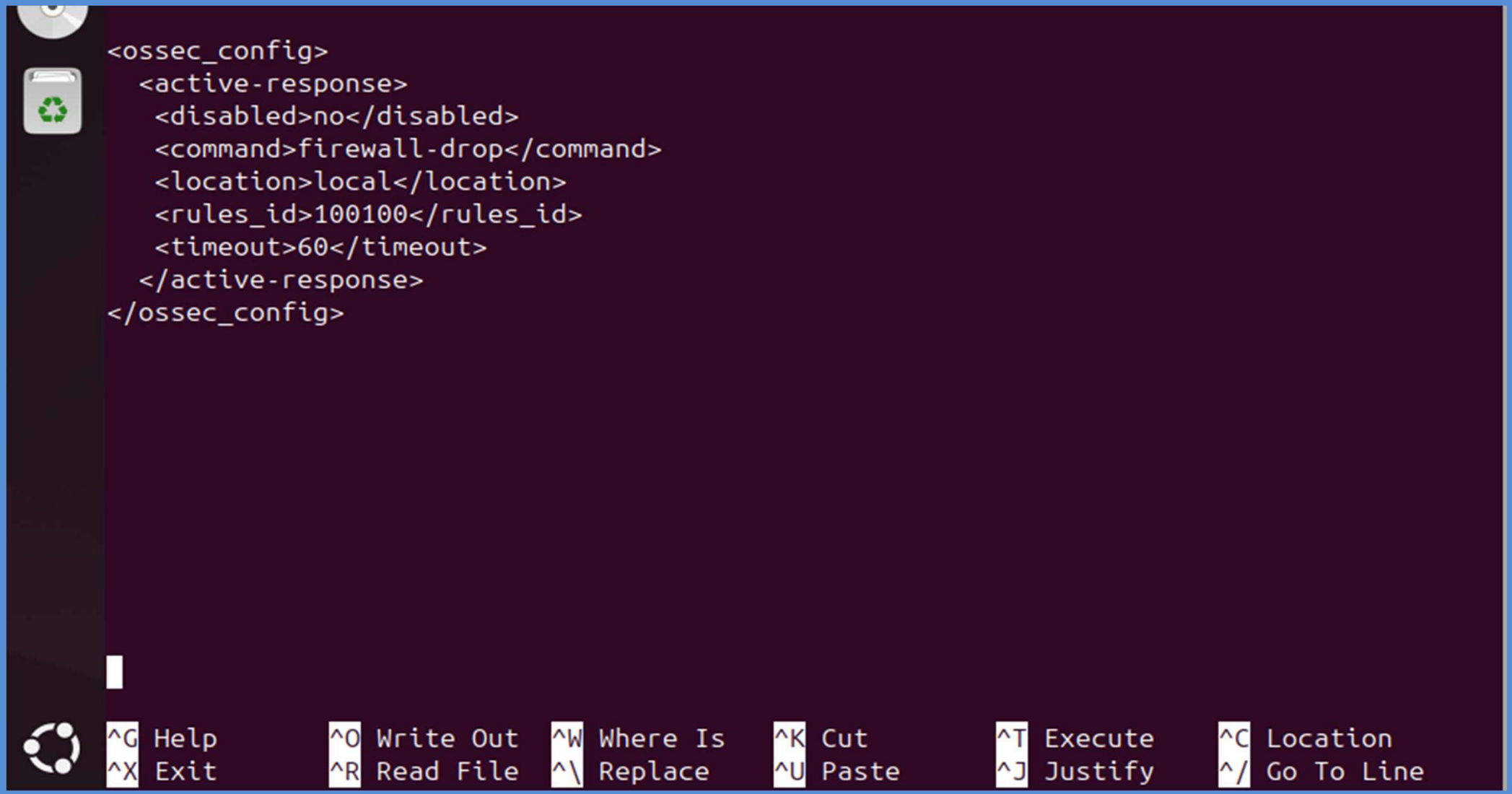
Match IPs
Active response: firewall-drop
Restarted manager

Custom Rules and Active Response



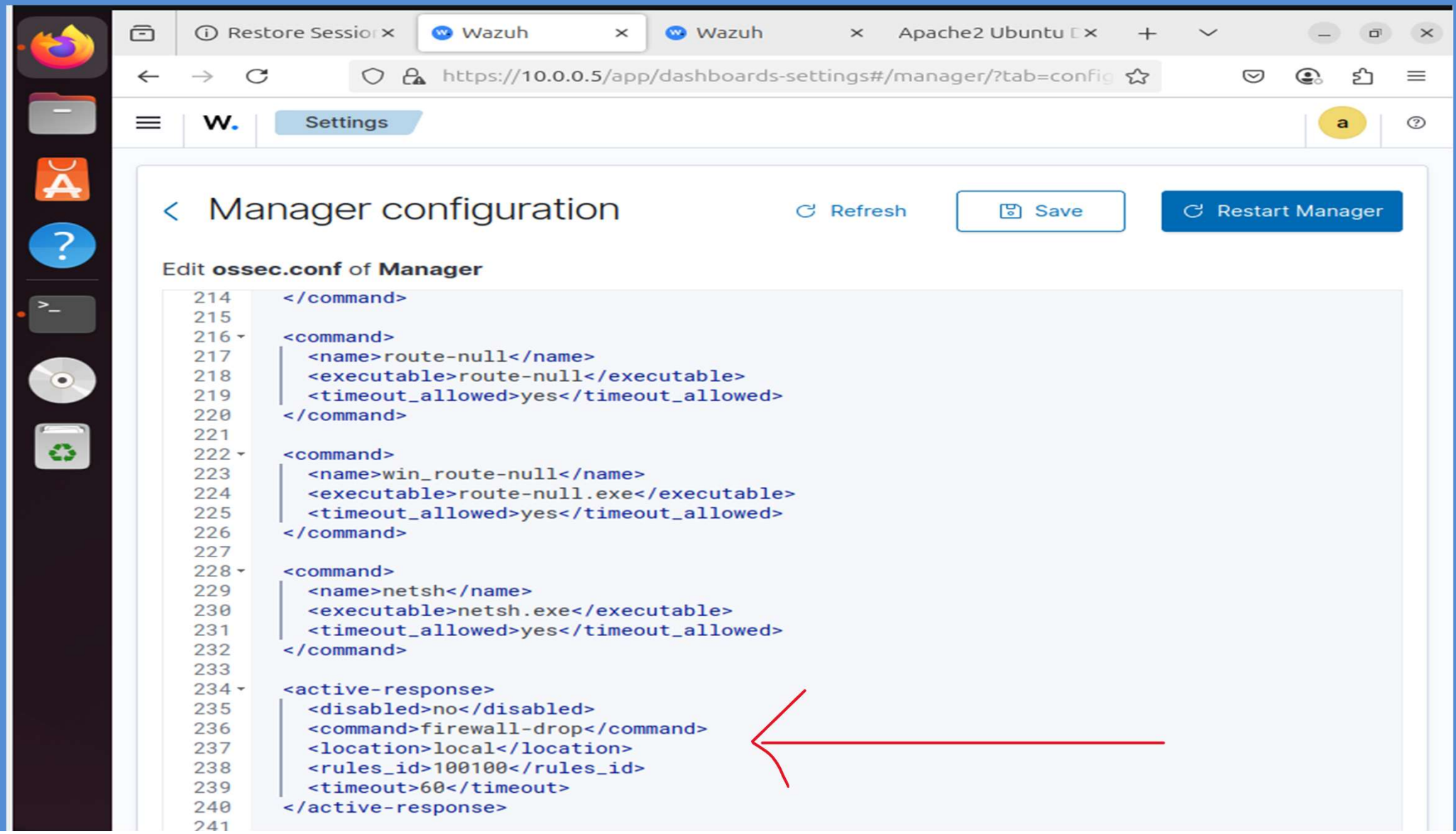
Custom Rules and Active Response

Active response: firewall-drop



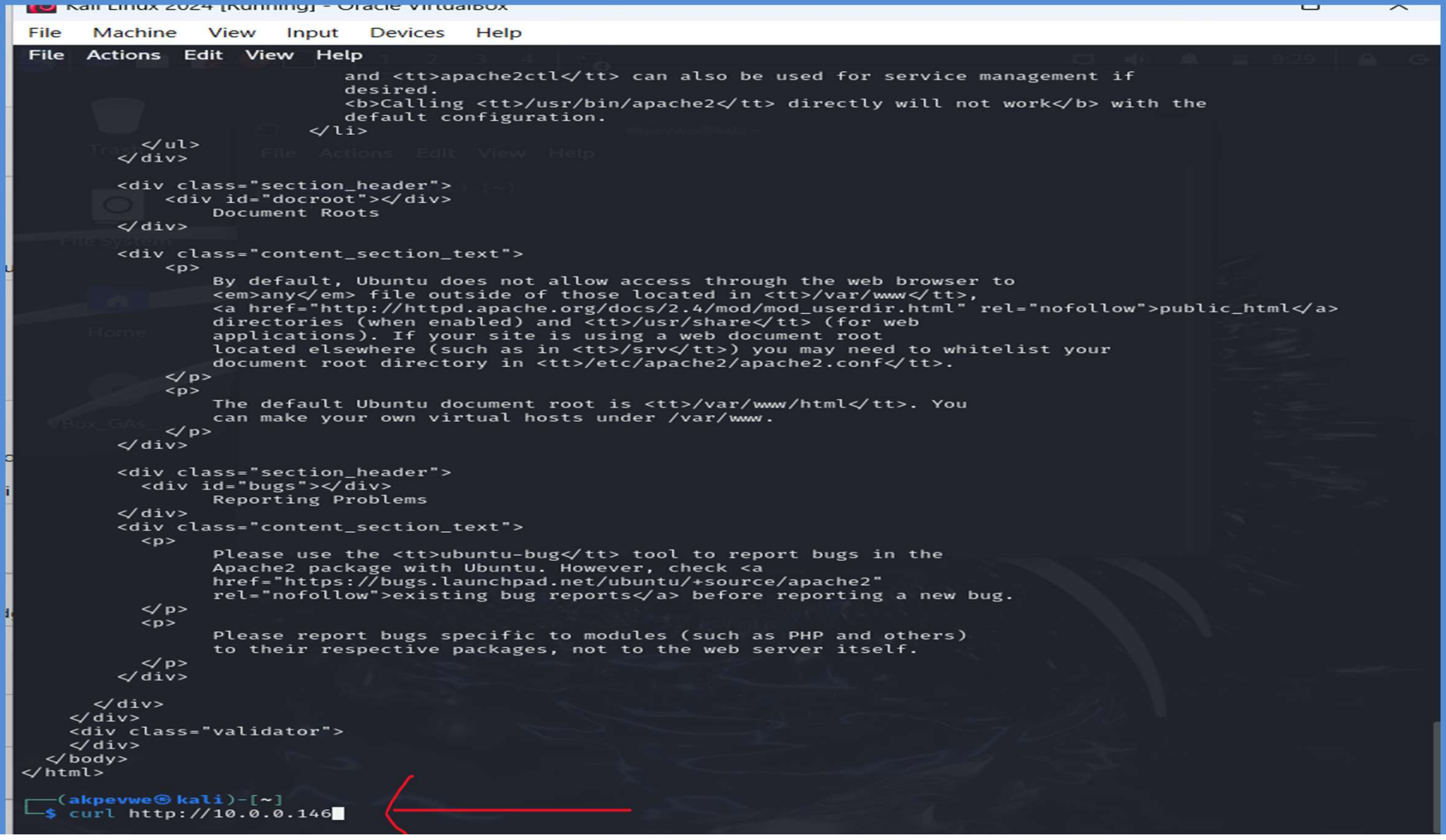
Custom Rules and Active Response

Active response: firewall-drop



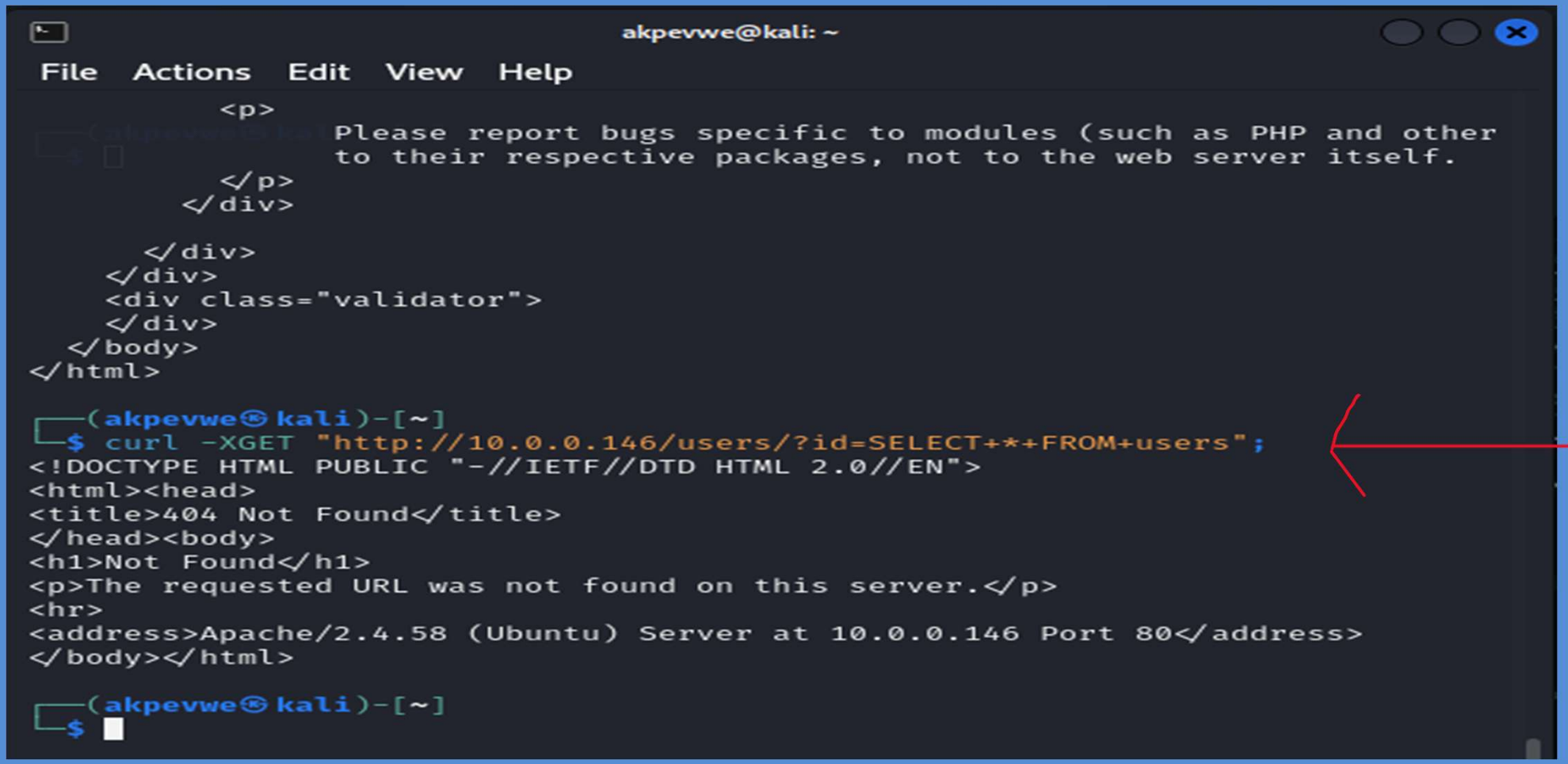
Attack Emulation

Ran command $ curl http://10.0.0.146 on kali



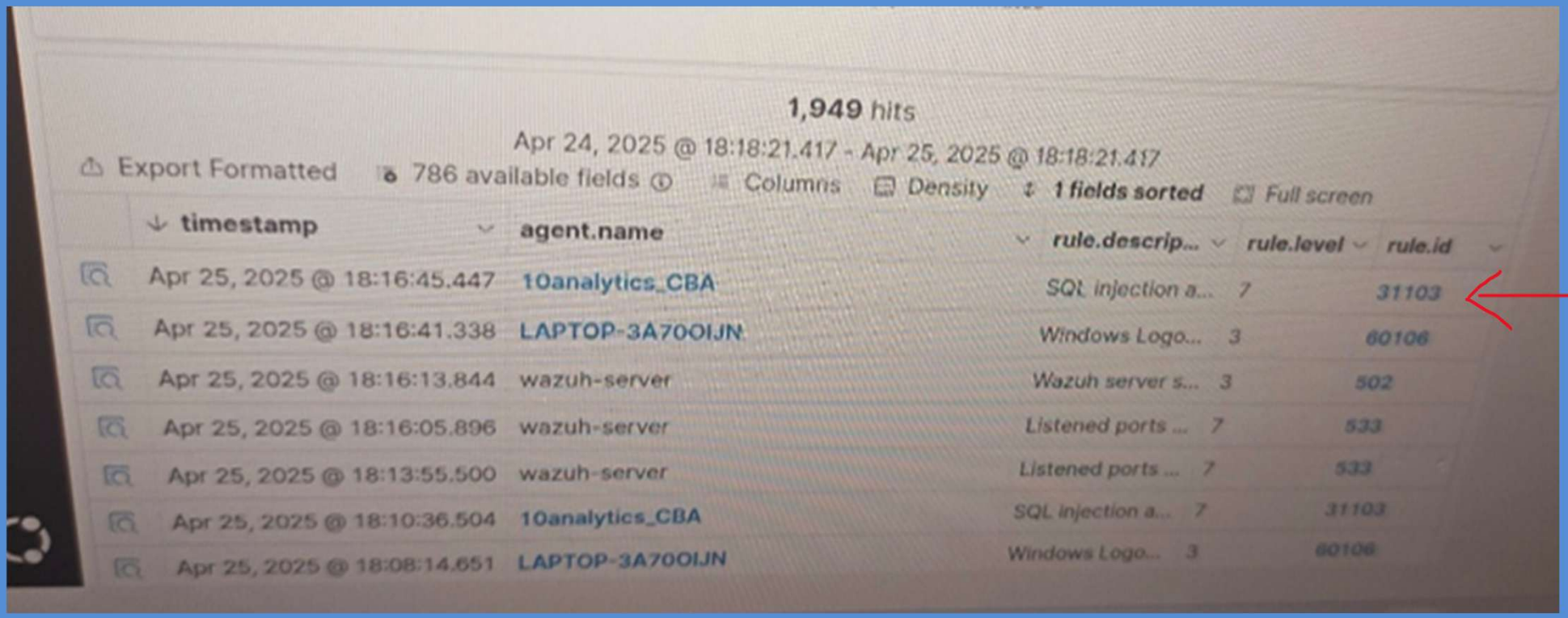
Attack Emulation

First SQL attack: success



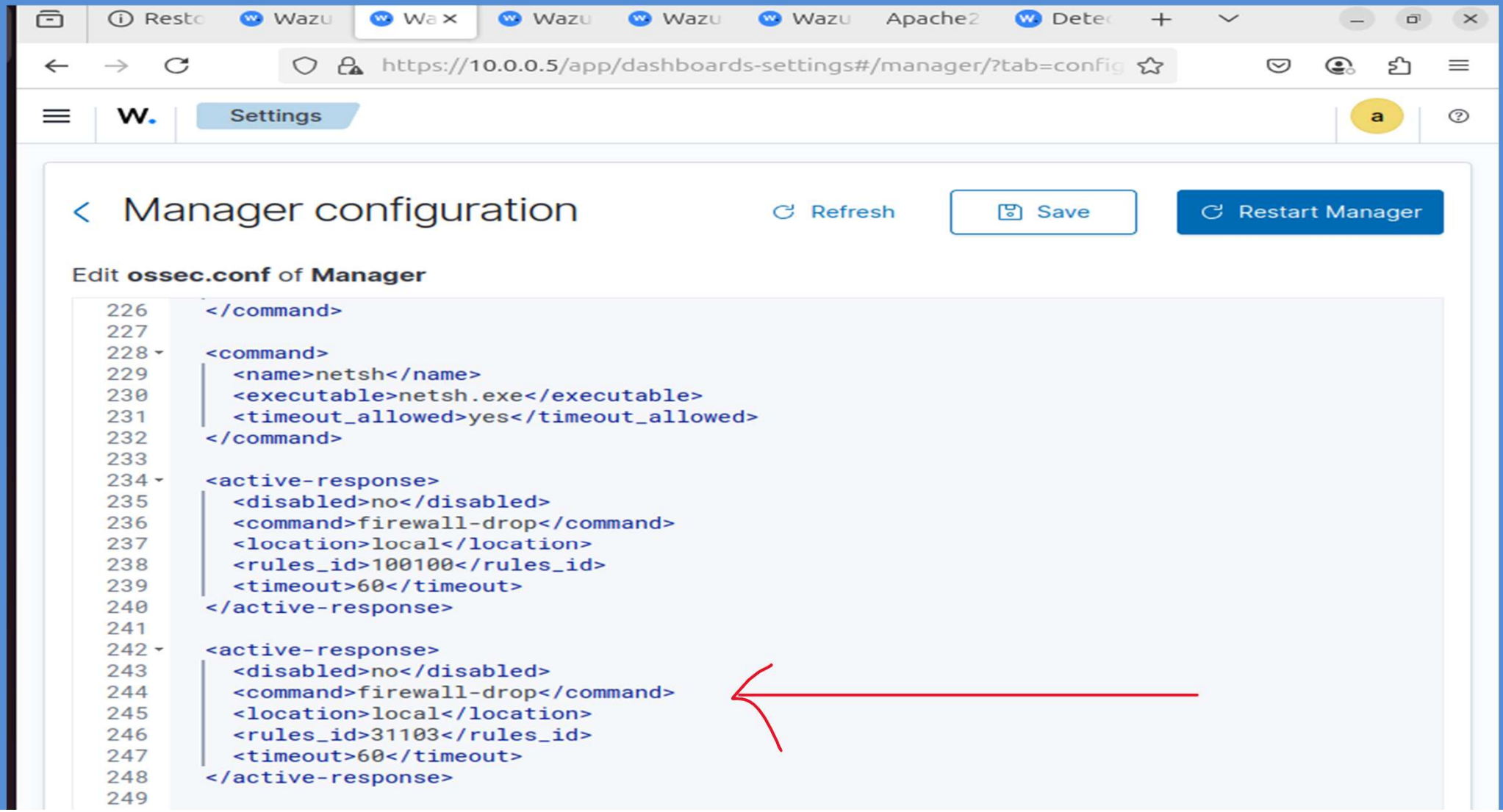
Attack Emulation

First attack: success



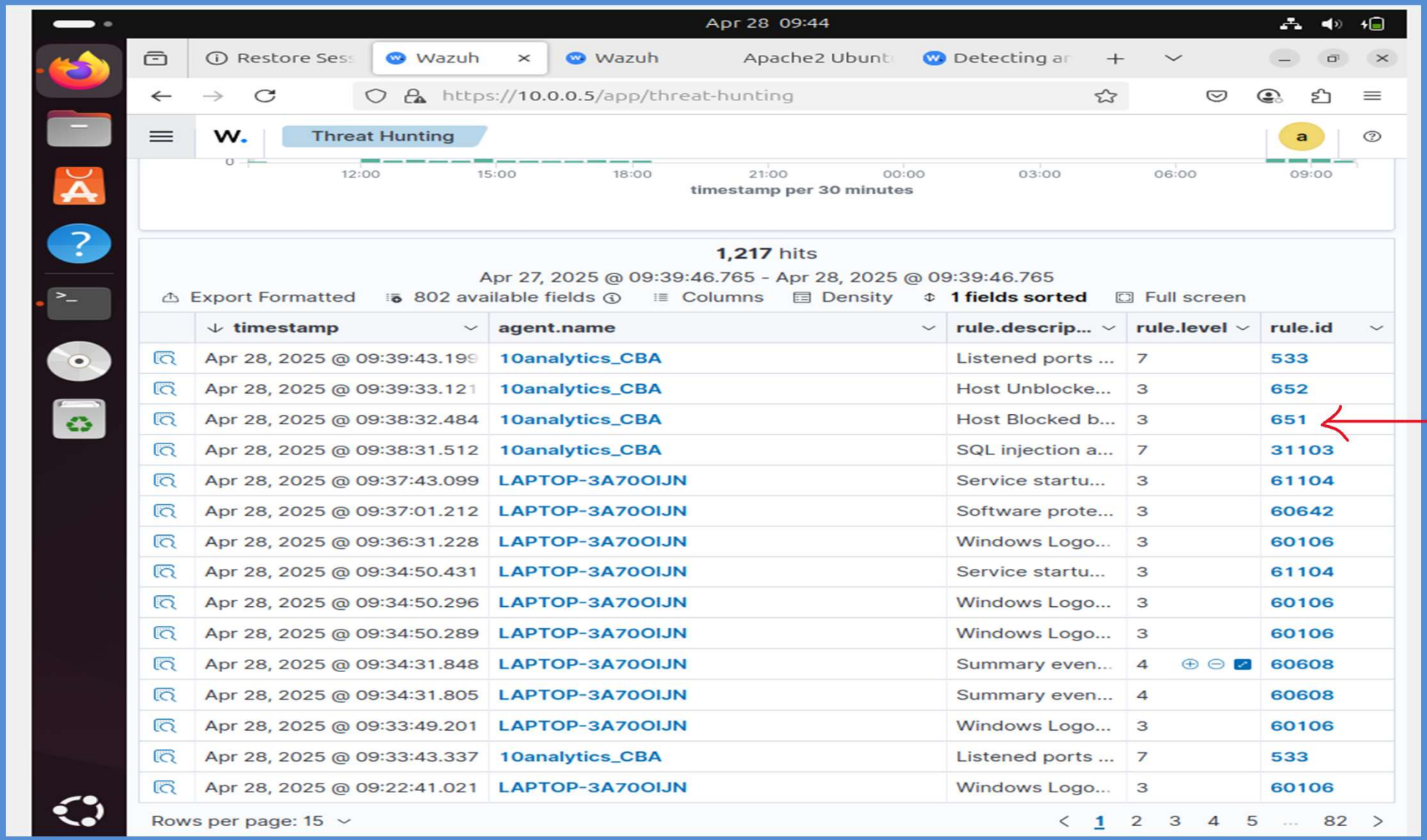
Attack Emulation

- Inserted 31103 in my active response on wazuh server



Attack Emulation

Second Attack: SQL injection detected and blocked with rule id:651



Active Response Actions

- Detection and logging of suspicious web requests.
- Temporary blocking of malicious IP via firewall rules.
- Validation through Threat Hunting module in Wazuh dashboard.
- Confirmed effectiveness by observing blocked access post-attack.

Recommendations

•Expand Detection Coverage: Add monitoring for additional high-risk utilities besides Netcat.

•Increase Automation: Shorten the response time by implementing faster Active Response triggers.

•User Training: Regular awareness campaigns to train staff on tool misuse and incident reporting.

•Red Team Exercises: Simulate real-world attacks to test and refine security posture. Log Retention and Analysis

•Maintain detailed logs for forensic investigations and legal compliance.

Conclusion

These investigations confirmed that proactive monitoring and automated responses using Wazuh effectively detect and block security threats. Unauthorized Netcat usage was successfully identified, and malicious IPs executing attacks were automatically blocked.

Strengthening detection rules, automating responses, and enhancing user training are recommended to further improve security. Overall, the measures implemented will enhance 10ALYTICS-DC ability in threat detection and response capabilities thereby reducing the risk of unauthorized access and potential data breaches.

Thank You!