

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

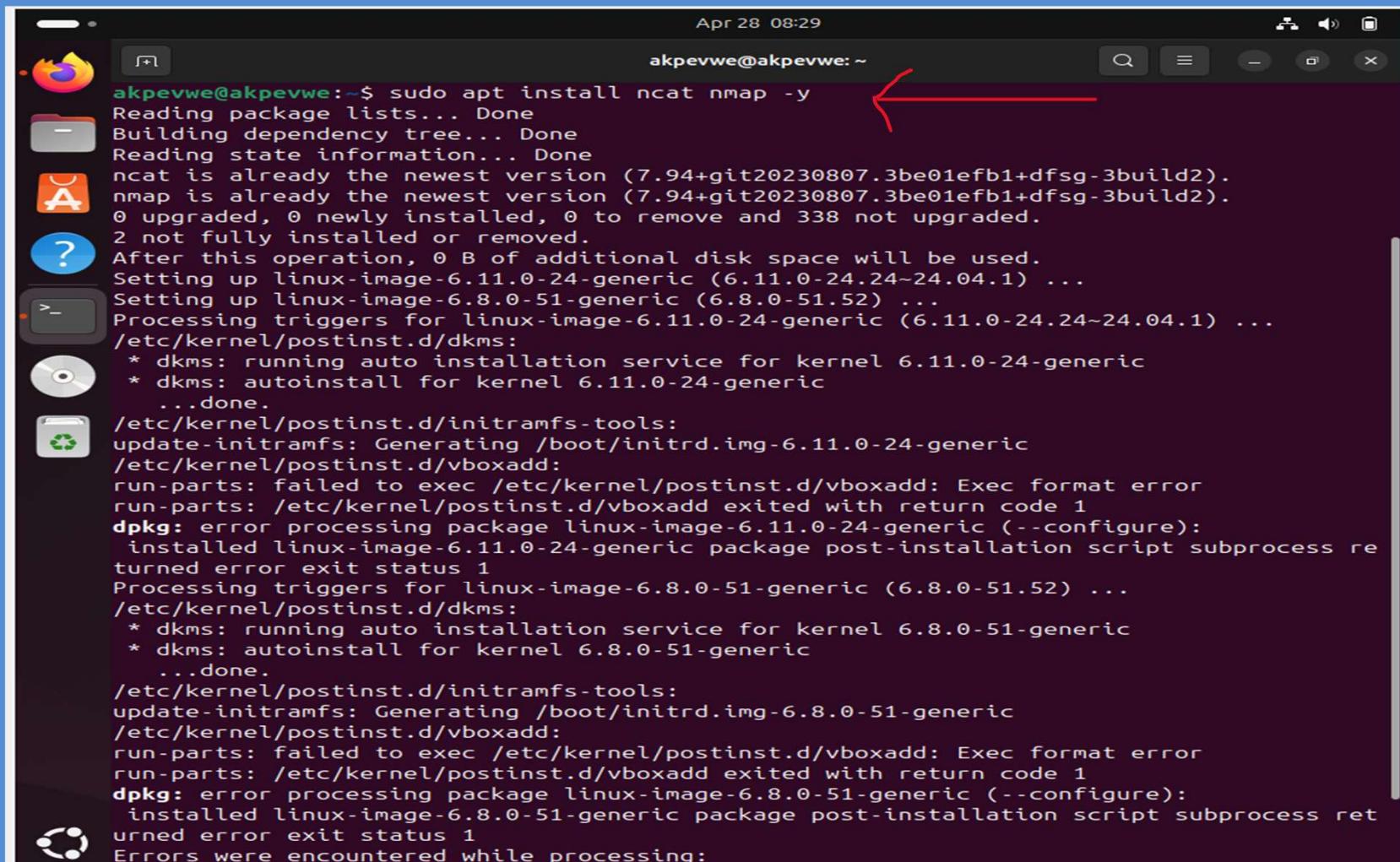
Added config to ossec.conf using /var/ossec/etc/ossec.conf file
Restarted Wazuh agent

```
</ossec_config>
<ossec_config>
  <localfile>
    <log_format>full_command</log_format>
    <alias>process list</alias>
    <command>ps -e -o pid,uname,command</command>
    <frequency>30</frequency>
  </localfile>
```

Netcat Installation and Wazuh Rule

Installed ncat and nmap

Custom rules to detect nc –l



```
Apr 28 08:29
akpevwe@akpevwe:~$ sudo apt install ncat nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ncat is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 338 not upgraded.
2 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Setting up linux-image-6.11.0-24-generic (6.11.0-24.24~24.04.1) ...
Setting up linux-image-6.8.0-51-generic (6.8.0-51.52) ...
Processing triggers for linux-image-6.11.0-24-generic (6.11.0-24.24~24.04.1) ...
/etc/kernel/postinst.d/dkms:
 * dkms: running auto installation service for kernel 6.11.0-24-generic
 * dkms: autoinstall for kernel 6.11.0-24-generic
 ...done.
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-6.11.0-24-generic
/etc/kernel/postinst.d/vboxadd:
run-parts: failed to exec /etc/kernel/postinst.d/vboxadd: Exec format error
run-parts: /etc/kernel/postinst.d/vboxadd exited with return code 1
dpkg: error processing package linux-image-6.11.0-24-generic (--configure):
 installed linux-image-6.11.0-24-generic package post-installation script subprocess returned error exit status 1
Processing triggers for linux-image-6.8.0-51-generic (6.8.0-51.52) ...
/etc/kernel/postinst.d/dkms:
 * dkms: running auto installation service for kernel 6.8.0-51-generic
 * dkms: autoinstall for kernel 6.8.0-51-generic
 ...done.
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-6.8.0-51-generic
/etc/kernel/postinst.d/vboxadd:
run-parts: failed to exec /etc/kernel/postinst.d/vboxadd: Exec format error
run-parts: /etc/kernel/postinst.d/vboxadd exited with return code 1
dpkg: error processing package linux-image-6.8.0-51-generic (--configure):
 installed linux-image-6.8.0-51-generic package post-installation script subprocess returned error exit status 1
Errors were encountered while processing:
```

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 "?" 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

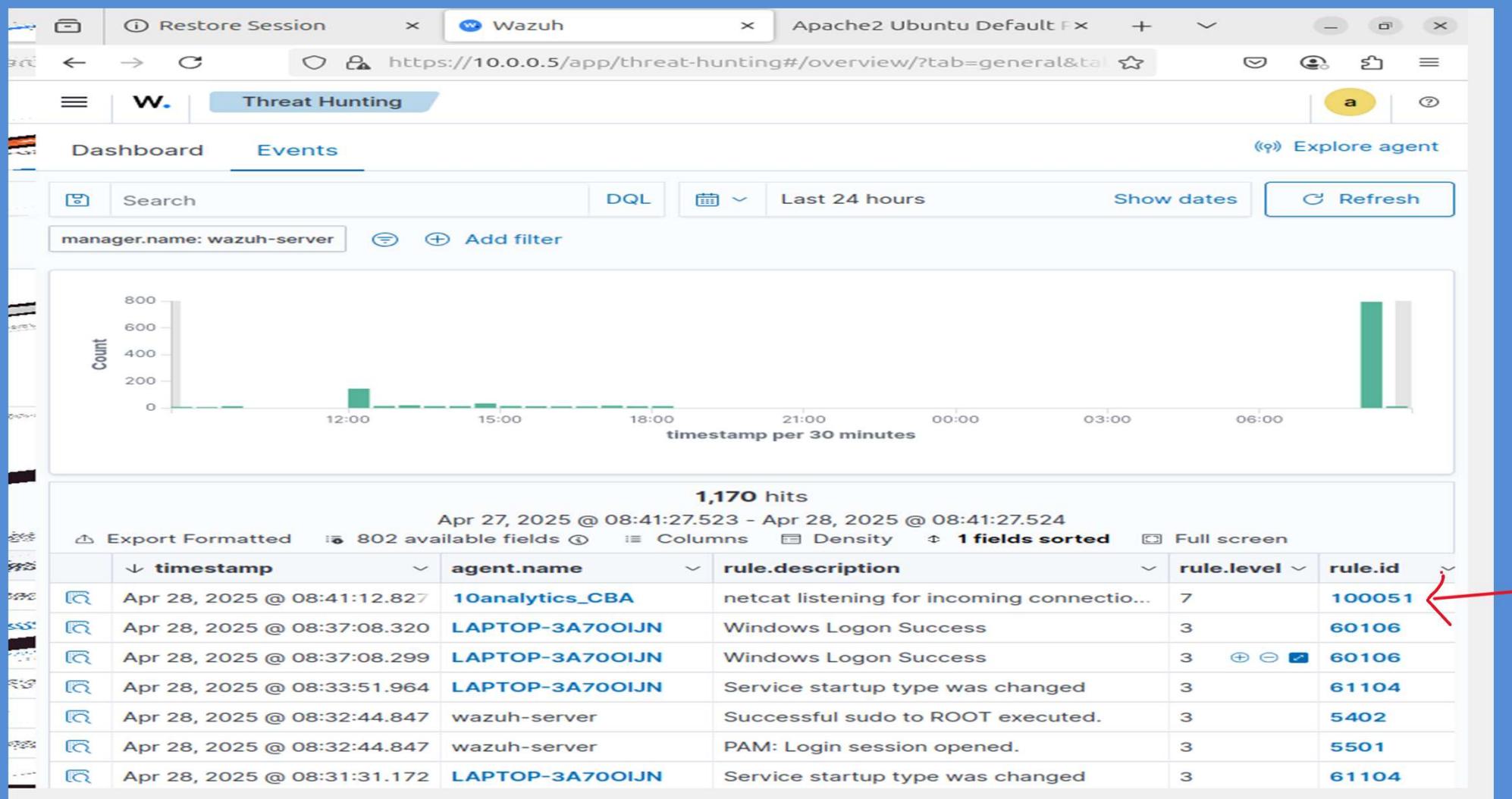
Alerts triggered: rule.id (100051)

```
run-parts: /etc/kernel/postinst.d/vboxadd exited with return code 1
dpkg: error processing package linux-image-6.8.0-51-generic (--configure):
        installed linux-image-6.8.0-51-generic package post-installation script subprocess returned error exit status 1
Errors were encountered while processing:
    linux-image-6.11.0-24-generic
    linux-image-6.8.0-51-generic
E: Sub-process /usr/bin/dpkg returned an error code (1)
akpevwe@akpevwe:~$ sudo apt install ncat nmap-y^C
akpevwe@akpevwe:~$ nc -l 8000
```



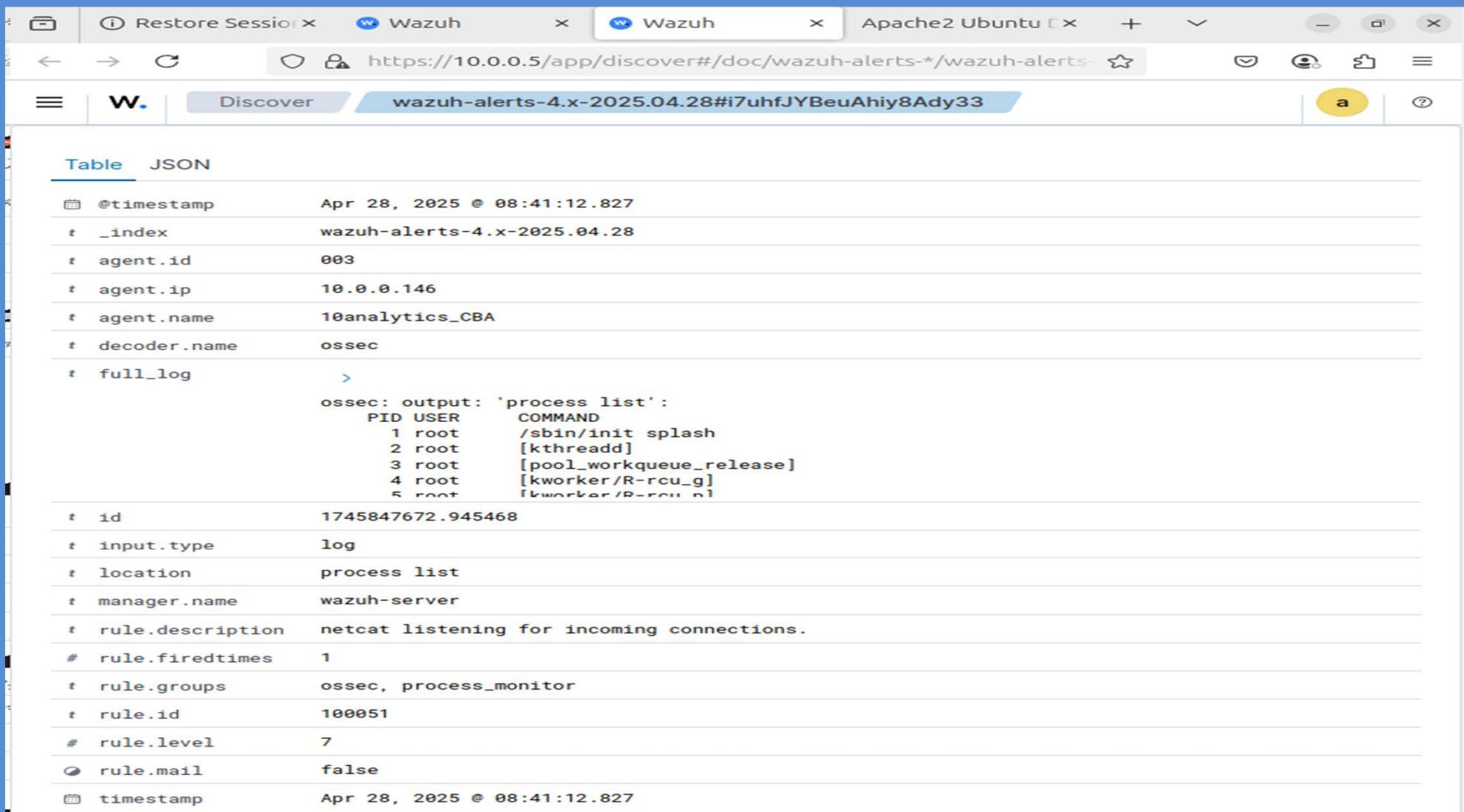
Visualisation of Alerts

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)



The screenshot shows a web browser window with three tabs open. The active tab is titled "Wazuh" and displays the URL https://10.0.0.5/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4.x-2025.04.28#i7uhfJYBeuAhiy8Ady33. The browser interface includes a header with "Restore Session", "Wazuh", "Apache2 Ubuntu", and a search bar. Below the header is a toolbar with icons for back, forward, search, and refresh. The main content area shows a table of alert details.

Table		JSON
t	@timestamp	Apr 28, 2025 @ 08:41:12.827
t	_index	wazuh-alerts-4.x-2025.04.28
t	agent.id	003
t	agent.ip	10.0.0.146
t	agent.name	10analytics_CBA
t	decoder.name	ossec
t	full_log	<pre>> ossec: output: 'process list': PID USER COMMAND 1 root /sbin/init splash 2 root [kthreadd] 3 root [pool_workqueue_release] 4 root [kworker/R-rcu_g] 5 root [kworker/R-rcu_n]</pre>
t	id	1745847672.945468
t	input.type	log
t	location	process list
t	manager.name	wazuh-server
t	rule.description	netcat listening for incoming connections.
#	rule.firedtimes	1
t	rule.groups	ossec, process_monitor
t	rule.id	100051
#	rule.level	7
⌚	rule.mail	false
⌚	timestamp	Apr 28, 2025 @ 08:41:12.827

Mitigation Strategies for Netcat

Usage rules for authorised persons

Limit installation

Detect behavior

Track commands

Network monitoring

Secure alternatives

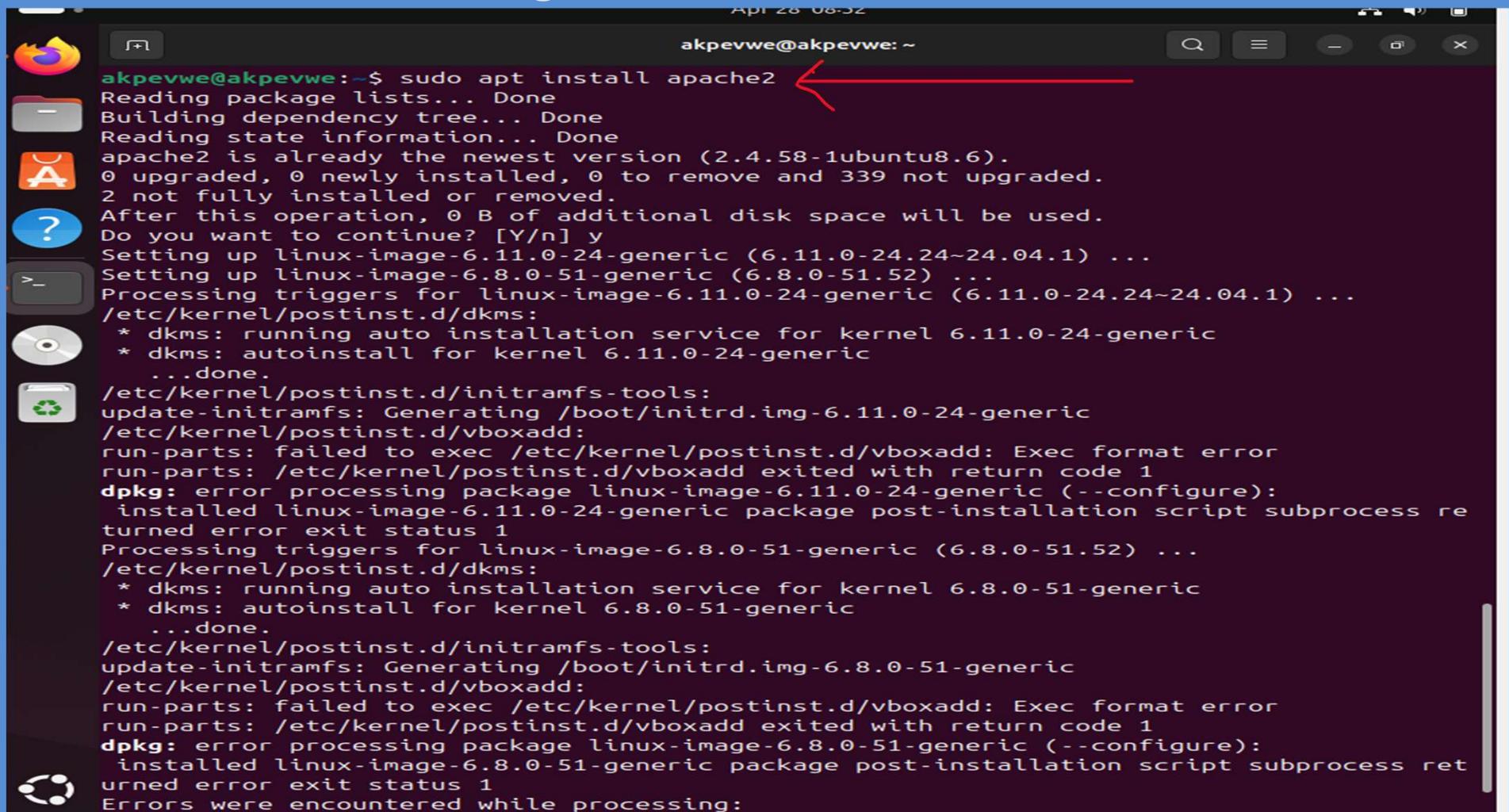
Task 2 Overview

Objective: Block malicious IPs

Environment: Wazuh, Ubuntu server & RHEL attacker(Kali)

Apache Setup and Monitoring

Installed Apache
Monitored access.log with Wazuh



```
akpevwe@akpevwe:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.6).
0 upgraded, 0 newly installed, 0 to remove and 339 not upgraded.
2 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Setting up linux-image-6.11.0-24-generic (6.11.0-24.24~24.04.1) ...
Setting up linux-image-6.8.0-51-generic (6.8.0-51.52) ...
Processing triggers for linux-image-6.11.0-24-generic (6.11.0-24.24~24.04.1) ...
/etc/kernel/postinst.d/dkms:
 * dkms: running auto installation service for kernel 6.11.0-24-generic
 * dkms: autoinstall for kernel 6.11.0-24-generic
 ...done.
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-6.11.0-24-generic
/etc/kernel/postinst.d/vboxadd:
run-parts: failed to exec /etc/kernel/postinst.d/vboxadd: Exec format error
run-parts: /etc/kernel/postinst.d/vboxadd exited with return code 1
dpkg: error processing package linux-image-6.11.0-24-generic (--configure):
 installed linux-image-6.11.0-24-generic package post-installation script subprocess re
turned error exit status 1
Processing triggers for linux-image-6.8.0-51-generic (6.8.0-51.52) ...
/etc/kernel/postinst.d/dkms:
 * dkms: running auto installation service for kernel 6.8.0-51-generic
 * dkms: autoinstall for kernel 6.8.0-51-generic
 ...done.
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-6.8.0-51-generic
/etc/kernel/postinst.d/vboxadd:
run-parts: failed to exec /etc/kernel/postinst.d/vboxadd: Exec format error
run-parts: /etc/kernel/postinst.d/vboxadd exited with return code 1
dpkg: error processing package linux-image-6.8.0-51-generic (--configure):
 installed linux-image-6.8.0-51-generic package post-installation script subprocess ret
urned error exit status 1
Errors were encountered while processing:
```

Apache Setup and Monitoring

Installed Apache Monitored access.log with Wazuh

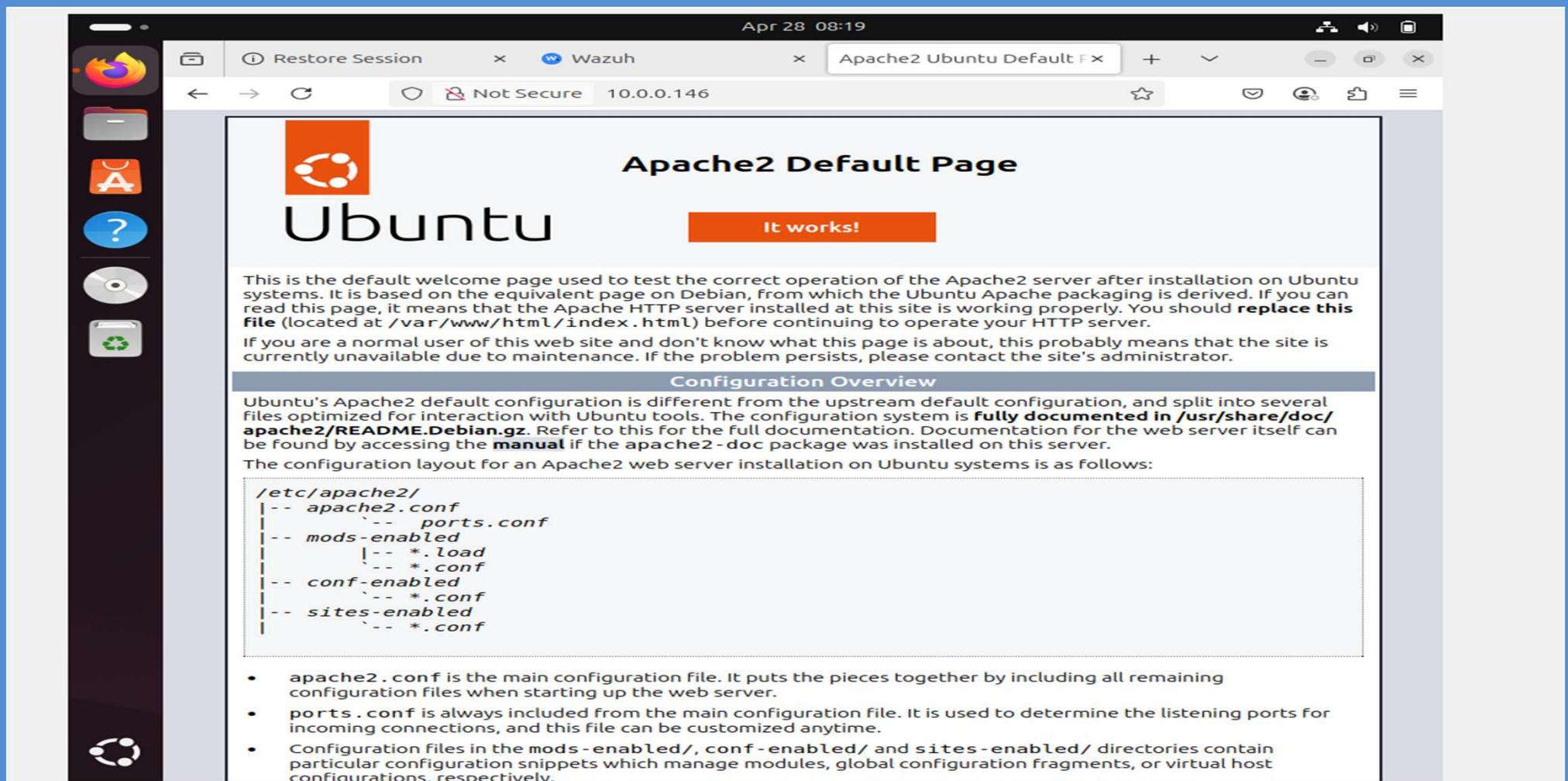
```
E: Sub-process /usr/bin/dpkg returned an error code (1)
akpevwe@akpevwe:~$ sudo ufw status
Status: inactive
akpevwe@akpevwe:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
  OpenSSH
akpevwe@akpevwe:~$ sudo ufw allow 'Apache'
Skipping adding existing rule
Skipping adding existing rule (v6)
akpevwe@akpevwe:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-04-28 08:15:31 CDT; 38min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1357 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1429 (apache2)
    Tasks: 55 (limit: 3426)
   Memory: 6.5M (peak: 8.7M swap: 672.0K swap peak: 672.0K)
      CPU: 467ms
     CGrou: /system.slice/apache2.service
             └─1429 /usr/sbin/apache2 -k start
                 ├─1430 /usr/sbin/apache2 -k start
                 └─1431 /usr/sbin/apache2 -k start

Apr 28 08:15:31 akpevwe systemd[1]: Starting apache2.service - The Apache HTTP Server.>
Apr 28 08:15:31 akpevwe apachectl[1412]: AH00558: apache2: Could not reliably determin>
Apr 28 08:15:31 akpevwe systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-17/17 (END)
```

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

```
</localfile>

<localfile>
    <log_format>syslog</log_format>
    <location>/var/log/apache2/access.log</location>
</localfile>
</ossec_config>
```

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
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/blocklist-ipsets/master/alienvault_reputation.ipset -o /var/ossec/etc/lists/alienvault_reputation.ipset
[root@wazuh-server ~]# sudo echo 10.0.0.75 >> /var/ossec/etc/lists/alienvault_reputation.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/lists/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

```
GNU nano 2.9.8                               /tmp/iplist-to-cdblist.py

--2025-04-28 14:06:21-- https://wazuh.com/resources/iplist-to-cdblist.py
Resolving wazuh.com (wazuh.com)... 3.170.152.101, 3.170.152.35, 3.170.152.53, ...
Connecting to wazuh.com (wazuh.com)|3.170.152.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1570 (1.5K) [binary/octet-stream]
Saving to: ■iplist-to-cdblist.py.12■

#      OK .                                         100%  220M=0s

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

[roo@wazuh-server ~]# nano /tmp/iplist-to-cdblist.py
```

Wazuh Server Configuration

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

#      OK .                                         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

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

<match>nc -l</match>
<description>netcat listening for incoming connections.</description>
<group>process_monitor,</group>
</rule>
</group>

<group name="attack,">
<rule id="100100" level="10">
<if_group>webiattackattacks</if_group>
<list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvaul$</list>
<description>IP address found in AlienVault reputation database.</description>
</rule>
</group>
```



^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

[Smooth scrolling enabled]

Custom Rules and Active Response

GNU nano 2.9.8

/var/ossec/etc/ossec.conf

```
<ossec_config>
  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>
    <list>etc/lists/blacklist-alienVault</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

</ossec_config>
```

^G Get Help **^O** Write Out **^W** Where Is **^K** Cut Text **^J** Justify **^C** Cur Pos
^X Exit **^R** Read File **^N** Replace **^U** Uncut Text **^T** To Spell **^L** Go To Line

Custom Rules and Active Response

Active response: firewall-drop

```
<ossec_config>
  <active-response>
    <disabled>no</disabled>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
</ossec_config>
```



^G Help
^X Exit

^O Write Out
^R Read File

^W Where Is
^\\ Replace

^K Cut
^U Paste

^T Execute
^J Justify

^C Location
^/ Go To Line

Custom Rules and Active Response

Active response: firewall-drop

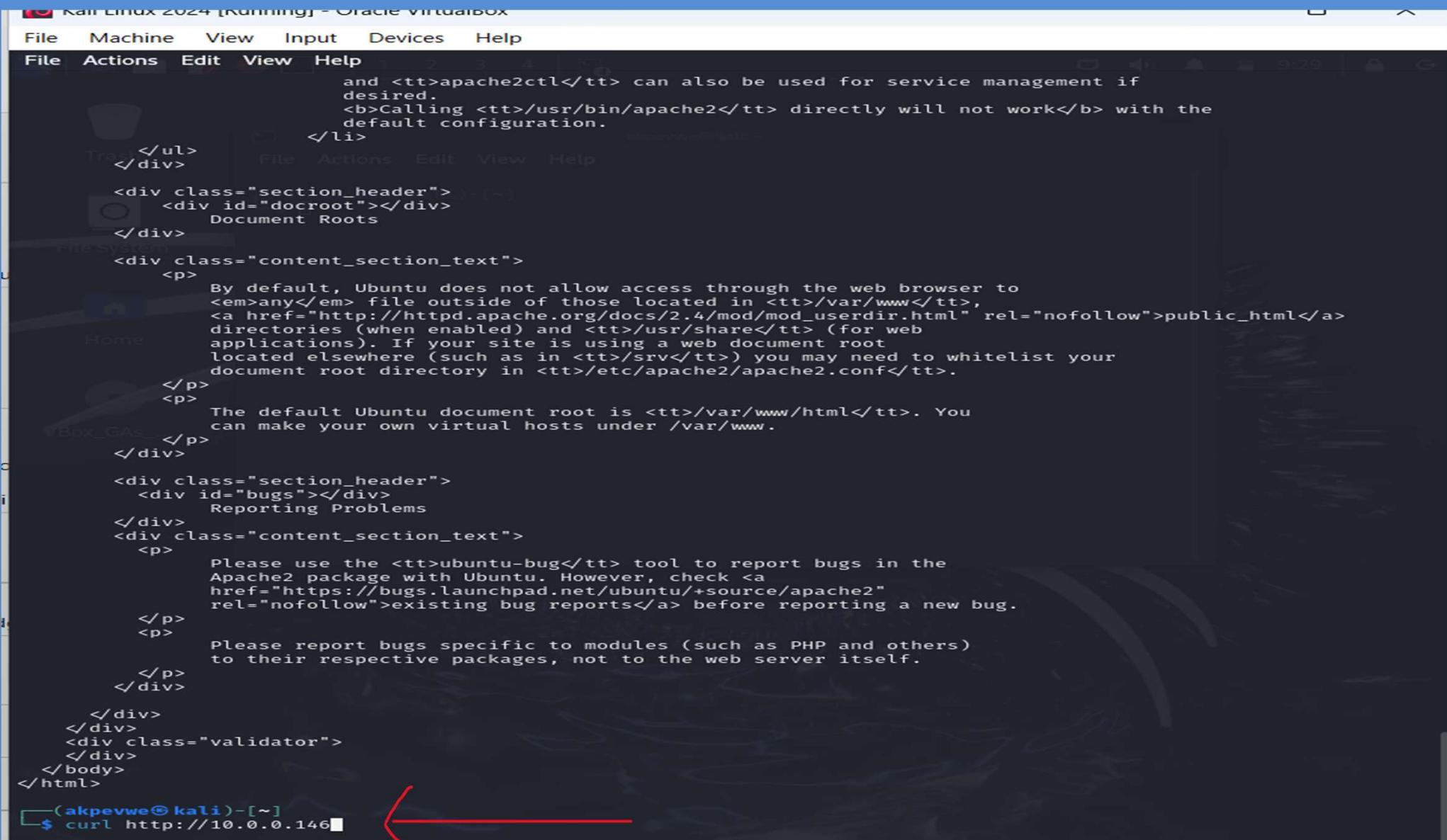
The screenshot shows a Firefox browser window with multiple tabs open. The active tab is titled "Wazuh" and displays the URL <https://10.0.0.5/app/dashboards-settings#/manager/?tab=config>. The page content is titled "Manager configuration" and shows the "Edit ossec.conf of Manager" section. The XML code includes several command definitions and one active-response definition at the end:

```
214  </command>
215
216  <command>
217      <name>route-null</name>
218      <executable>route-null</executable>
219      <timeout_allowed>yes</timeout_allowed>
220  </command>
221
222  <command>
223      <name>win_route-null</name>
224      <executable>route-null.exe</executable>
225      <timeout_allowed>yes</timeout_allowed>
226  </command>
227
228  <command>
229      <name>netsh</name>
230      <executable>netsh.exe</executable>
231      <timeout_allowed>yes</timeout_allowed>
232  </command>
233
234  <active-response>
235      <disabled>no</disabled>
236      <command>firewall-drop</command>
237      <location>local</location>
238      <rules_id>100100</rules_id>
239      <timeout>60</timeout>
240  </active-response>
241
```

A red arrow points from the bottom right towards the final line of the XML code, which defines the active-response rule.

Attack Emulation

Ran command \$ curl <http://10.0.0.146> on kali



```
Kali Linux 2024 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
and <tt>apache2ctl</tt> can also be used for service management if
desired.
<b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
    Document Roots
</div>
<div class="content_section_text">
<p>
        By default, Ubuntu does not allow access through the web browser to
        <em>any</em> file outside of those located in <tt>/var/www</tt>,
        <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
        directories (when enabled) and <tt>/usr/share</tt> (for web
        applications). If your site is using a web document root
        located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
        document root directory in <tt>/etc/apache2/apache2.conf</tt>.
    </p>
<p>
        The default Ubuntu document root is <tt>/var/www/html</tt>. You
        can make your own virtual hosts under /var/www.
    </p>
</div>

<div class="section_header">
<div id="bugs"></div>
    Reporting Problems
</div>
<div class="content_section_text">
<p>
        Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
        Apache2 package with Ubuntu. However, check <a
        href="https://bugs.launchpad.net/ubuntu/+source/apache2"
        rel="nofollow">existing bug reports</a> before reporting a new bug.
    </p>
<p>
        Please report bugs specific to modules (such as PHP and others)
        to their respective packages, not to the web server itself.
    </p>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
(akpevwe㉿kali)-[~]
```

\$ curl http://10.0.0.146

Attack Emulation

First SQL attack: success



```
akpevwe@kali: ~
File Actions Edit View Help
<p>
</p>
</div>
</div>
<div class="validator">
</div>
</body>
</html>

[(akpevwe㉿kali)-[~]
$ curl -XGET "http://10.0.0.146/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/2.4.58 (Ubuntu) Server at 10.0.0.146 Port 80</address>
</body></html>

[(akpevwe㉿kali)-[~]
$
```

Attack Emulation

First attack: success

1,949 hits				
Apr 24, 2025 @ 18:18:21.417 - Apr 25, 2025 @ 18:18:21.417		786 available fields	Columns	Density
Export Formatted	1 fields sorted	Full screen		
↓ timestamp	agent.name	rule.description	rule.level	rule.id
Apr 25, 2025 @ 18:16:45.447	10analytics_CBA	SQL injection a...	7	31103
Apr 25, 2025 @ 18:16:41.338	LAPTOP-3A700IJN	Windows Logo...	3	60106
Apr 25, 2025 @ 18:16:13.844	wazuh-server	Wazuh server s...	3	502
Apr 25, 2025 @ 18:16:05.896	wazuh-server	Listened ports ...	7	533
Apr 25, 2025 @ 18:13:55.500	wazuh-server	Listened ports ...	7	533
Apr 25, 2025 @ 18:10:36.504	10analytics_CBA	SQL injection a...	7	31103
Apr 25, 2025 @ 18:08:14.651	LAPTOP-3A700IJN	Windows Logo...	3	60106

Attack Emulation

- Inserted 31103 in my active response on wazuh server

The screenshot shows a web browser window with multiple tabs open, all labeled "Wazuh". The active tab is titled "Manager configuration" and displays the "Edit ossec.conf of Manager" page. The configuration file content is as follows:

```
226 </command>
227
228 <command>
229 |   <name>netsh</name>
230 |   <executable>netsh.exe</executable>
231 |   <timeout_allowed>yes</timeout_allowed>
232 </command>
233
234 <active-response>
235 |   <disabled>no</disabled>
236 |   <command>firewall-drop</command>
237 |   <location>local</location>
238 |   <rules_id>100100</rules_id>
239 |   <timeout>60</timeout>
240 </active-response>
241
242 <active-response>
243 |   <disabled>no</disabled>
244 |   <command>firewall-drop</command>
245 |   <location>local</location>
246 |   <rules_id>31103</rules_id>
247 |   <timeout>60</timeout>
248 </active-response>
249
```

A red arrow points from the bottom of the slide towards the second active-response block starting at line 242, specifically highlighting the line containing "<rules_id>31103</rules_id>".

Attack Emulation

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

Apr 28 09:44

Restore Sess Wazuh Wazuh Apache2 Ubuntu Detecting ar + - ×

https://10.0.0.5/app/threat-hunting

W Threat Hunting

1,217 hits

Apr 27, 2025 @ 09:39:46.765 – Apr 28, 2025 @ 09:39:46.765

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 28, 2025 @ 09:39:43.199	10analytics_CBA	Listened ports ...	7	533
Apr 28, 2025 @ 09:39:33.121	10analytics_CBA	Host Unblock...	3	652
Apr 28, 2025 @ 09:38:32.484	10analytics_CBA	Host Blocked b...	3	651
Apr 28, 2025 @ 09:38:31.512	10analytics_CBA	SQL injection a...	7	31103
Apr 28, 2025 @ 09:37:43.099	LAPTOP-3A700IJN	Service startu...	3	61104
Apr 28, 2025 @ 09:37:01.212	LAPTOP-3A700IJN	Software prote...	3	60642
Apr 28, 2025 @ 09:36:31.228	LAPTOP-3A700IJN	Windows Logo...	3	60106
Apr 28, 2025 @ 09:34:50.431	LAPTOP-3A700IJN	Service startu...	3	61104
Apr 28, 2025 @ 09:34:50.296	LAPTOP-3A700IJN	Windows Logo...	3	60106
Apr 28, 2025 @ 09:34:50.289	LAPTOP-3A700IJN	Windows Logo...	3	60106
Apr 28, 2025 @ 09:34:31.848	LAPTOP-3A700IJN	Summary even...	4	60608
Apr 28, 2025 @ 09:34:31.805	LAPTOP-3A700IJN	Summary even...	4	60608
Apr 28, 2025 @ 09:33:49.201	LAPTOP-3A700IJN	Windows Logo...	3	60106
Apr 28, 2025 @ 09:33:43.337	10analytics_CBA	Listened ports ...	7	533
Apr 28, 2025 @ 09:22:41.021	LAPTOP-3A700IJN	Windows Logo...	3	60106

Rows per page: 15 < 1 2 3 4 5 ... 82 >

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!