



# wazuh.

## **Wazuh – SSH Brute Force Attack ACTIVE RESPONSE**

**Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY**

**Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)**

## Overview

Wazuh is an open-source security monitoring platform that offers intrusion detection, integrity monitoring, and vulnerability detection capabilities. One of its powerful features is Active Response, which allows Wazuh to automatically take action when certain security events are detected. In the context of an SSH brute force attack on a Linux system, Wazuh can be configured to detect and respond to such threats effectively.

## SSH Brute Force Attack

An SSH brute force attack is a method used by attackers to gain unauthorized access to a server by systematically trying different combinations of usernames and passwords. This type of attack can overwhelm a server with login attempts, potentially leading to successful breaches if weak credentials are used.

## Wazuh Active Response Mechanism

Wazuh Active Response can mitigate the risk of SSH brute force attacks by automatically taking predefined actions when it detects such attempts. The process involves the following steps:

### Detection:

Wazuh uses its intrusion detection capabilities to monitor SSH login attempts. This is done through analyzing logs from the SSH daemon (sshd), which records all login attempts. When Wazuh identifies a pattern indicative of a brute force attack (e.g., multiple failed login attempts from a single IP address within a short period), it triggers an alert.

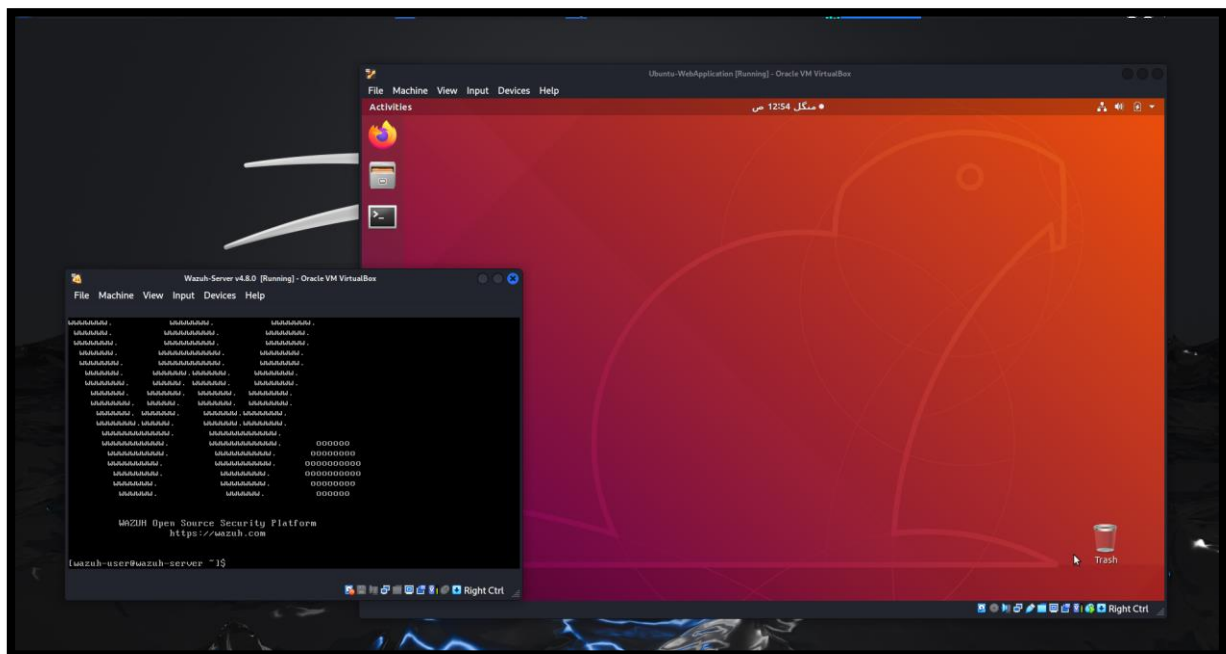
### Configuration:

Active Response rules are defined in the Wazuh configuration files. These rules specify the conditions under which responses should be executed and the type of response to be taken. For SSH brute force attacks, a common response is to block the attacking IP address using a firewall rule or to temporarily ban the IP using tools like Fail2ban.

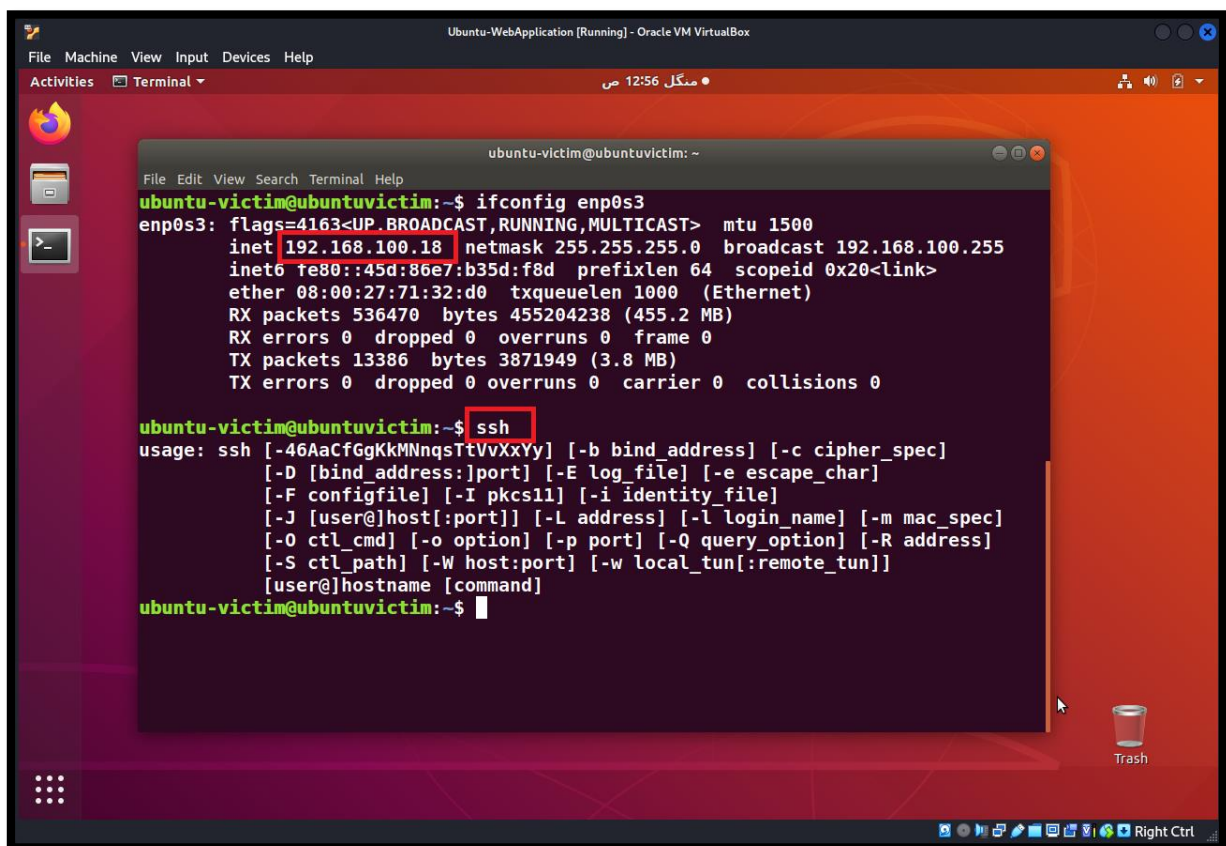
### Response:

Upon detecting an SSH brute force attack, Wazuh executes the predefined response. This could involve adding a rule to the iptables firewall to block traffic from the offending IP address or calling a script that integrates with Fail2ban to ban the IP for a certain period. The action taken is logged by Wazuh for auditing and review purposes.

Here is my Wazuh server running along with Ubuntu machine on virtualbox.



Ubuntu machine IP address "192.168.100.18" and SSH service is running.



SSH connection establish with Ubuntu machine.

```
File Actions Edit View Help
ubuntu-victim@ubuntu-victim: ~

(kali@kali)-[~]
$ ssh ubuntu-victim@192.168.100.18
ubuntu-victim@192.168.100.18's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

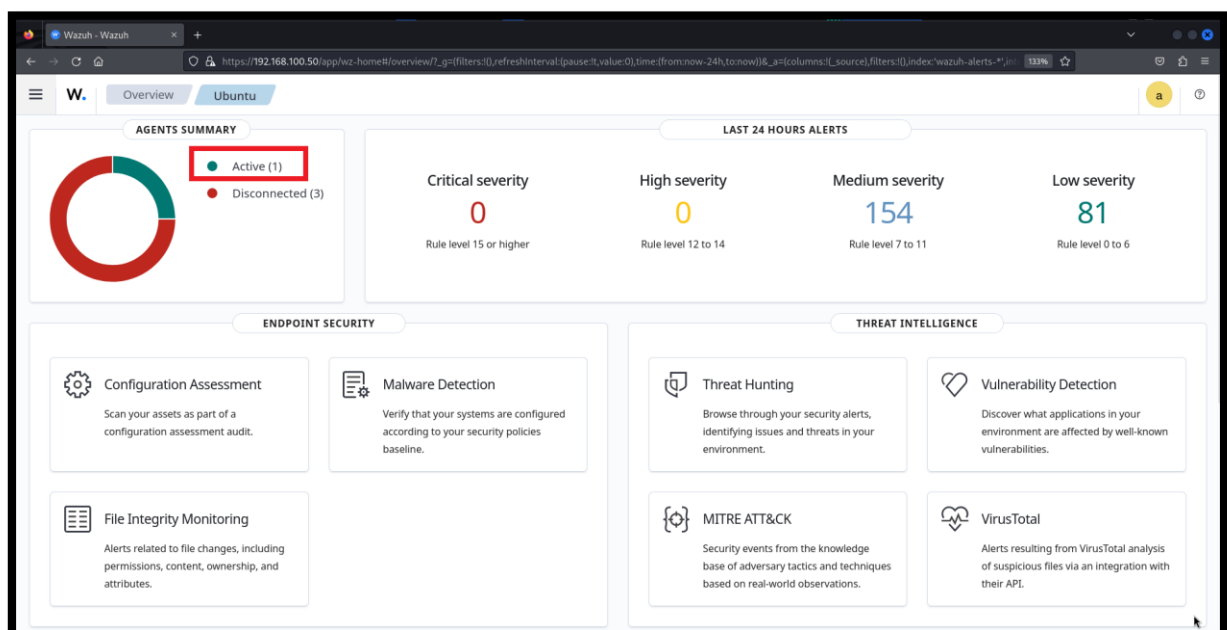
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

337 packages can be updated.
78 updates are security updates.

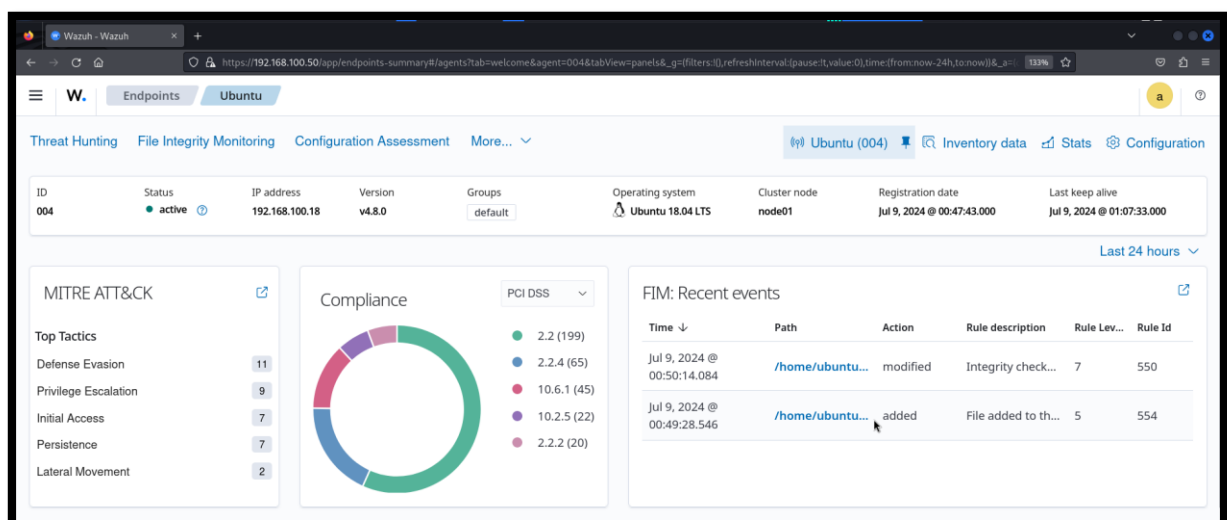
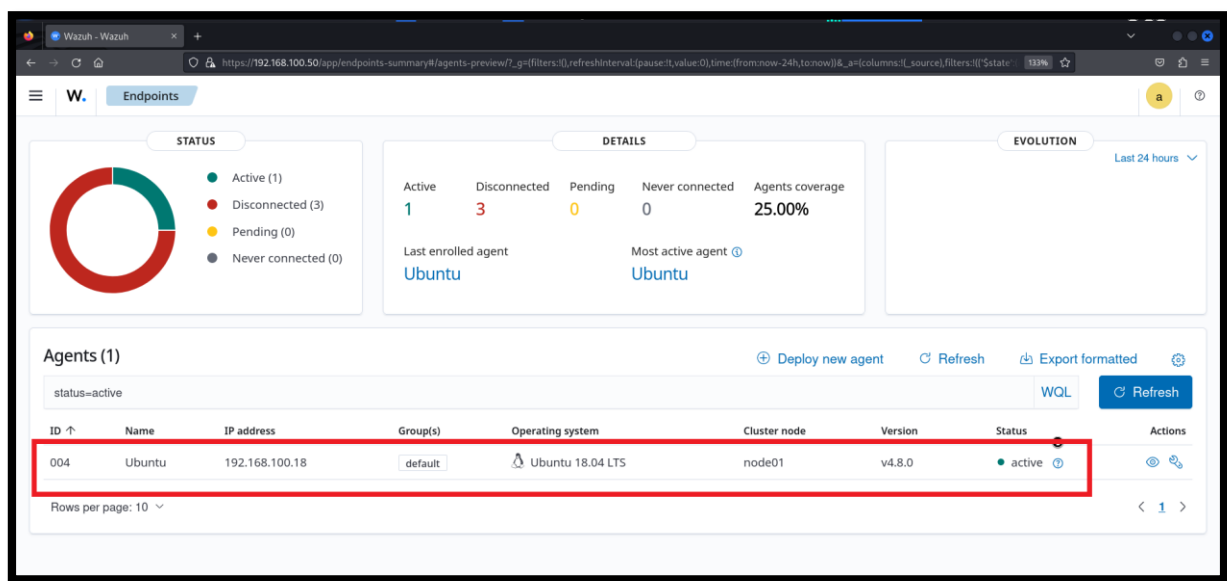
New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jul  9 00:52:58 2024 from 192.168.100.6
ubuntu-victim@ubuntu-victim:~$
```

In Wazuh dashboard here is an “Active” agent.



Ubuntu agent is active and running.



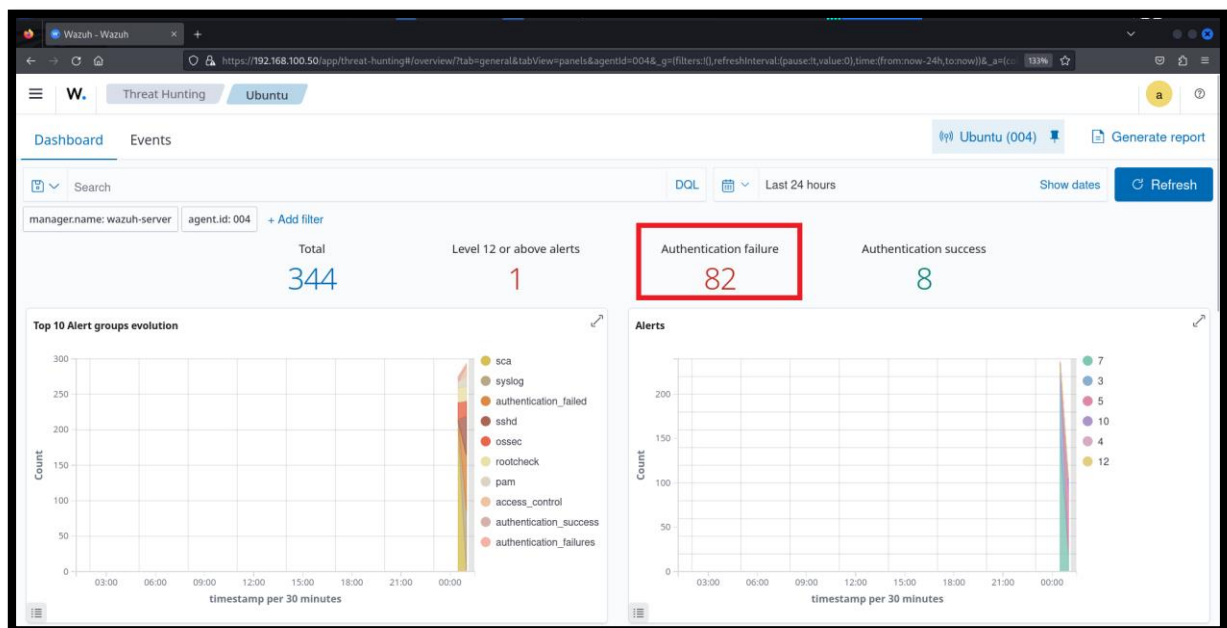
**Step 01:** Now trying to brute-force attack on Ubuntu machine.

Command: `sudo hydra -l ubuntu-victim -P pass.txt ssh://192.168.100.18`

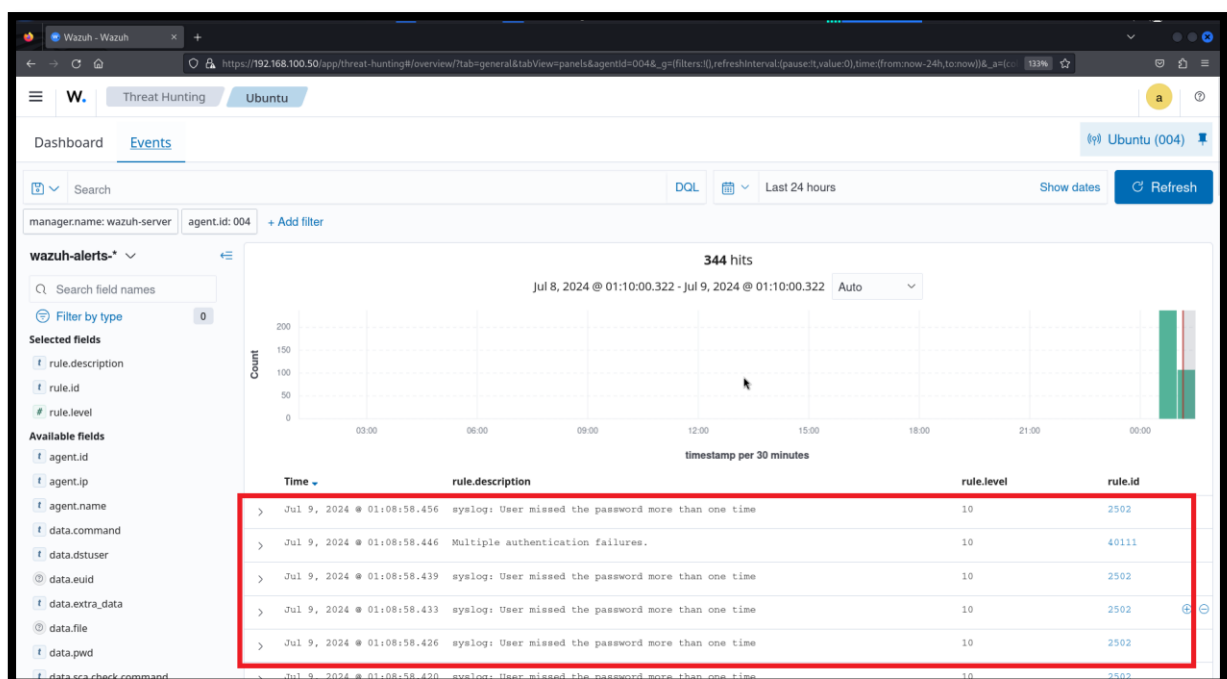
```
kali@kali: ~  
root@wazuh-server:~$ sudo hydra -l ubuntu-victim -P pass.txt ssh://192.168.100.18  
[sudo] password for kali:  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for  
illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-09 01:08:48  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 72 login tries (l:1/p:72), ~5 tries per task  
[DATA] attacking ssh://192.168.100.18:22/  
[22][ssh] host: 192.168.100.18 login: ubuntu-victim password: abc123  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 2 final worker threads did not complete until end.  
[ERROR] 2 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-09 01:08:57
```

We successfully able to brute-force attack on Ubuntu-victim machine.

Here you can see “Authentication failure”. This means brute-force attack.



Now go to “Events” tab and analyze logs.



	Time	rule.description	rule.level	rule.id
>	Jul 9, 2024 @ 01:08:58.456	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.446	Multiple authentication failures.	10	40111
>	Jul 9, 2024 @ 01:08:58.439	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.433	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.426	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.420	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.414	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.407	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.400	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.397	syslog: User missed the password more than one time	10	2502
>	Jul 9, 2024 @ 01:08:58.392	sshd: authentication failed.	5	5760
>	Jul 9, 2024 @ 01:08:58.388	sshd: authentication failed.	5	5760
>	Jul 9, 2024 @ 01:08:58.383	sshd: authentication failed.	5	5760
>	Jul 9, 2024 @ 01:08:58.380	sshd: authentication failed.	5	5760
>	Jul 9, 2024 @ 01:08:58.371	sshd: authentication failed.	5	5760
>	Jul 9, 2024 @ 01:08:58.365	sshd: authentication failed.	5	5760

Jul 9, 2024 @ 01:08:58.392	sshd: authentication failed.	5	5760
----------------------------	------------------------------	---	------

Expanded document

View surrounding documents View single document

Table	JSON
f _index	wazuh-alerts-4.x-2024.07.08
f agent.id	004
f agent.ip	192.168.100.18
f agent.name	Ubuntu
f data.dstuser	ubuntu-victim
f data.srcip	192.168.100.6
f data.srcport	44052
f decoder.name	sshd
f decoder.parent	sshd
f full_log	Jul 9 01:08:56 mail sshd[8962]: Failed password for ubuntu-victim from 192.168.100.6 port 44052 ssh2
f id	1720469338.625277
f input.type	log
f location	/var/log/auth.log
f manager.name	wazuh-serves

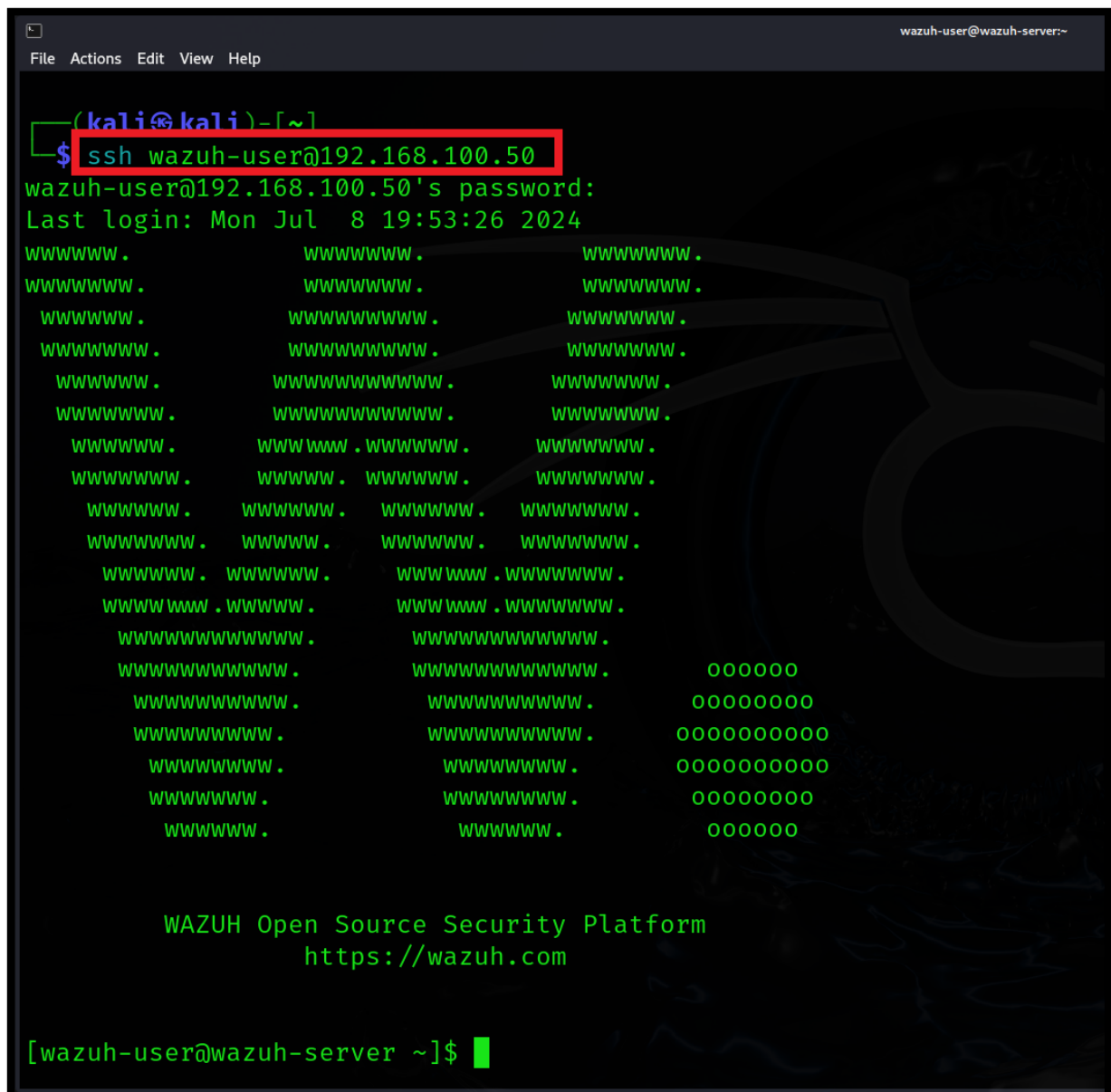
t	location	/var/log/auth.log
t	manager.name	wazuh-server
t	predecoder.hostname	mail
t	predecoder.program_name	sshd
t	predecoder.timestamp	Jul 9 01:08:56
t	rule.description	sshd: authentication failed.
#	rule.firedtimes	49
t	rule.gdpr	IV_35.7.d, IV_32.2
t	rule.gpg13	7.1
t	rule.groups	syslog, sshd, authentication_failed
t	rule.hipaa	164.312.b
t	rule.id	5760
#	rule.level	5
●	rule.mail	false
t	rule.mitre.id	T1110.001, T1021.004
t	rule.mitre.tactic	Credential Access, Lateral Movement
t	rule.mitre.technique	Password Guessing, SSH



**Step 02:** Now we have to configure “Active-Response”

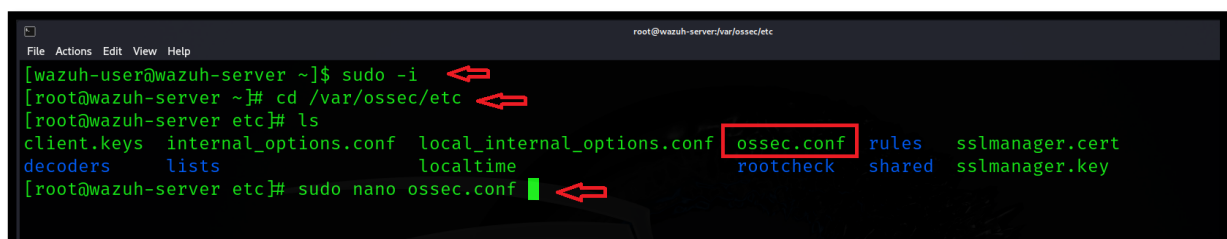
Login into Wazuh server via ssh

Command: `ssh wazuh-user@192.168.100.50`



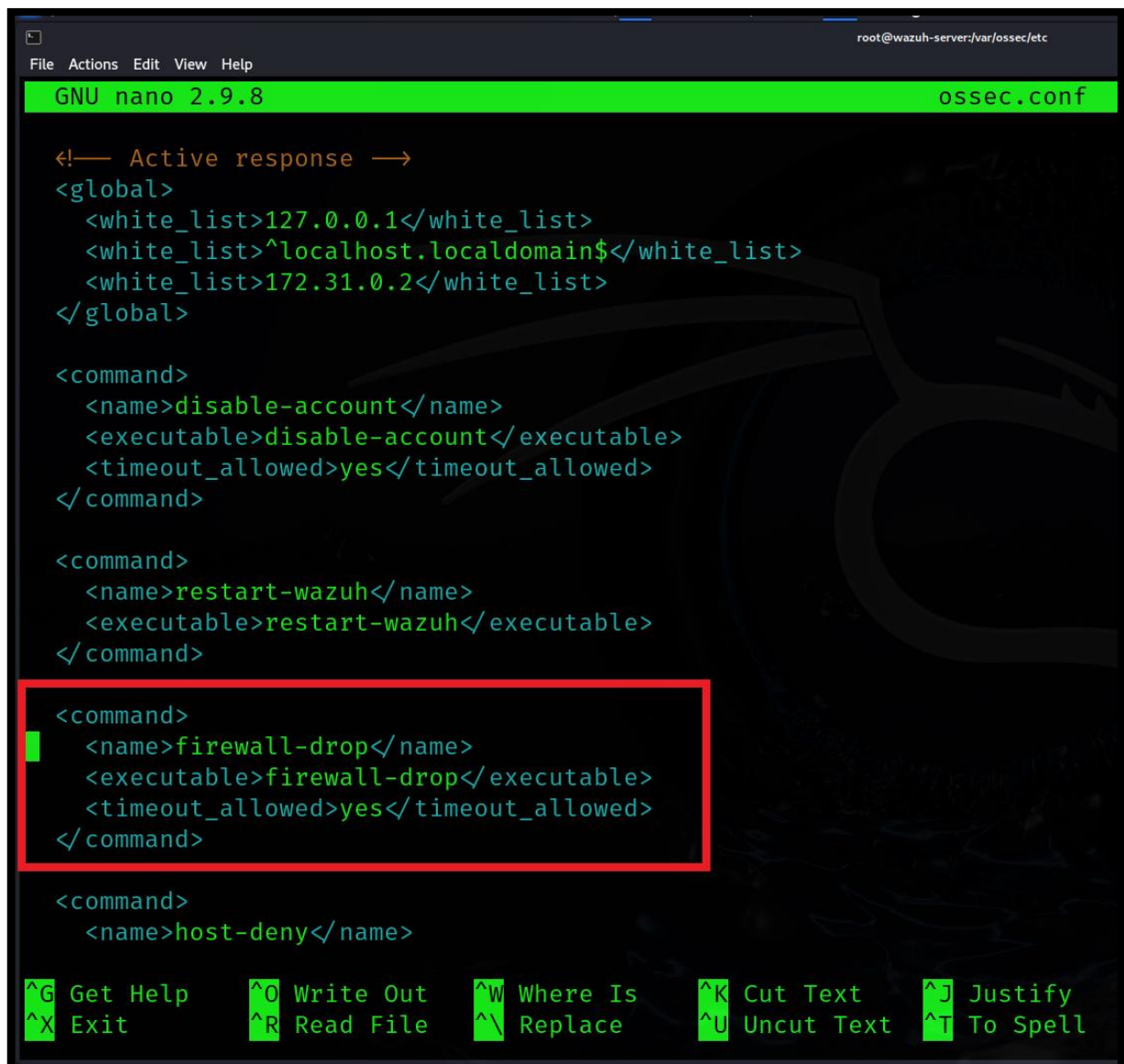
A terminal window showing an SSH session from a Kali machine to a Wazuh server. The command `ssh wazuh-user@192.168.100.50` is highlighted with a red box. The terminal displays the password prompt, the last login time (Mon Jul 8 19:53:26 2024), and a large ASCII art logo of a cat. Below the logo, it says "WAZUH Open Source Security Platform" and "https://wazuh.com". The prompt at the bottom is `[wazuh-user@wazuh-server ~]$`.

Now edit the “ossec.conf” file.



A terminal window showing the steps to edit the `ossec.conf` file. The user runs `sudo -i` to become root, then `cd /var/ossec/etc` to navigate to the configuration directory. The `ls` command shows the contents of the directory, with `ossec.conf` highlighted by a red box. Finally, the user runs `sudo nano ossec.conf` to open the file for editing. Red arrows point to the `sudo -i`, `cd /var/ossec/etc`, and `sudo nano ossec.conf` commands.

Here you can see under “Active Response”, the command indicates firewall-drop script. This command will execute when we have to do active response.



```
GNU nano 2.9.8 ossec.conf

<!-- Active response -->
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>172.31.0.2</white_list>
</global>

<command>
  <name>disable-account</name>
  <executable>disable-account</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>restart-wazuh</name>
  <executable>restart-wazuh</executable>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>host-deny</name>

^G Get Help    ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify
^X Exit        ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell
```

Now we have to add “Active Response” configuration.

```
<active-response>
<command>firewall-drop</command>
<location>local</local>
<rules_id>5710</rules_id>
<timeout>60</timeout>
</active-response>
```

```
GNU nano 2.9.8 ossec.conf

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
<active-response>
<command>firewall-drop</command>
<location>local</location>
<rules_id>5710</rules_id>
<timeout>60</timeout>
</active-response>
```

Save the “ossec.conf” file and restart wazuh manger

Command: systemctl restart wazuh-manager

```
root@wazuh-server/var/ossec/etc
File Actions Edit View Help
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc
[root@wazuh-server etc]# ls
client.keys  internal_options.conf  local_internal_options.conf  ossec.conf  rules  sslmanager.cert
decoders    lists                  localtime                  rootcheck   shared  sslmanager.key
[root@wazuh-server etc]# sudo nano ossec.conf
[root@wazuh-server etc]# systemctl restart wazuh-manager
[root@wazuh-server etc]#
```

After restart wazuh manager we have to restart wazuh agent.

Command: sudo systemctl restart wazuh-agent

```
root@ubuntuvictim: ~
File Edit View Search Terminal Help
root@ubuntuvictim:~# sudo systemctl restart wazuh-agent
root@ubuntuvictim:~#
```

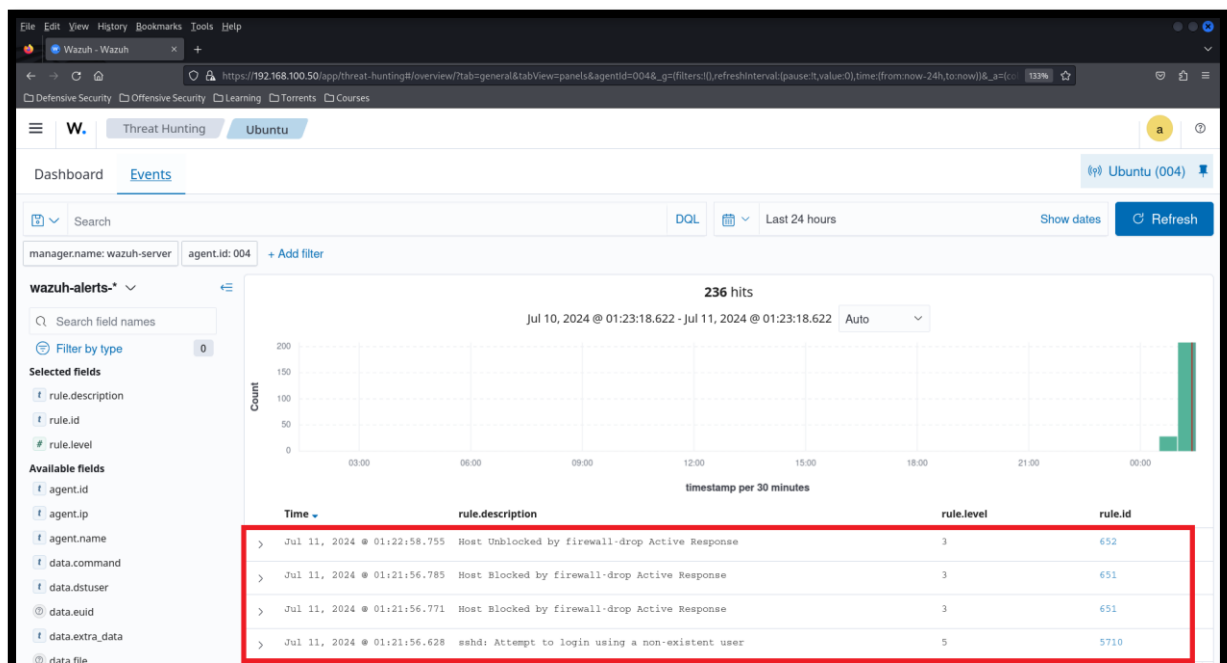
Step 03: Now again perform brute-force attack on Ubuntu machine.

Command: `sudo hydra -L user.txt -P pass.txt ssh://192.168.100.18`

You can see in the figure SSH brute-force attack failed this time because Wazuh actively responding to brute-force attack.

```
kali@kali: ~  
$ sudo hydra -L user.txt -P pass.txt ssh://192.168.100.18  
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 2024-07-11 01:21:56  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3096 login tries (l:43/p:72), ~194 tries per task  
[DATA] attacking ssh://192.168.100.18:22/  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] ssh target does not support password auth  
[ERROR] all children were disabled due too many connection errors  
0 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-11 01:22:28
```

Now do log analysis, in the “Events” you can see “Host Blocked by firewall-drop Active Response”



Ubuntu				a	?
Time	rule.description	rule.level	rule.id		
> Jul 11, 2024 @ 01:22:58.755	Host Unblocked by firewall-drop Active Response	3	652		
> Jul 11, 2024 @ 01:21:56.785	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:21:56.771	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:21:56.628	sshd: Attempt to login using a non-existent user	5	5710		
> Jul 11, 2024 @ 01:21:56.625	sshd: Attempt to login using a non-existent user	5	5710		
> Jul 11, 2024 @ 01:14:52.244	Host Unblocked by firewall-drop Active Response	3	652		
> Jul 11, 2024 @ 01:13:52.249	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:52.216	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:52.201	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:52.183	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:52.156	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:52.143	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:50.383	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:50.369	Host Blocked by firewall-drop Active Response	3	651		
> Jul 11, 2024 @ 01:13:50.356	Host Blocked by firewall-drop Active Response	3	651		

Ubuntu				a	?
Jul 11, 2024 @ 01:21:56.785	Host Blocked by firewall-drop Active Response	3	651		
Expanded document					
View surrounding documents View single document					
Table JSON					
t _index	wazuh-alerts-4.x-2024.07.10				
t agent.id	004				
t agent.ip	192.168.100.18				
t agent.name	Ubuntu				
t data.command	add				
data.origin.module	wazuh-execd				
data.origin.name	node01				
data.parameters.alert.agent.id	004				
data.parameters.alert.agent.ip	192.168.100.18				
data.parameters.alert.agent.name	Ubuntu				
data.parameters.alert.data.srcip	192.168.100.6				
data.parameters.alert.data.srcport	49650				
data.parameters.alert.data.srcuser	msfadmin				

⑦	data.parameters.alert.data.srcuser	msfadmin
⑦	data.parameters.alert.decoder.name	sshd
⑦	data.parameters.alert.decoder.parent	sshd
⑦	data.parameters.alert.full_log	Jul 11 01:21:54 mail sshd[9212]: Disconnected from invalid user msfadmin 192.168.100.6 port 49650 [preauth]
⑦	data.parameters.alert.id	1720642916.215315
⑦	data.parameters.alert.location	/var/log/auth.log
⑦	data.parameters.alert.manager.name	wazuh-server
⑦	data.parameters.alert.predecoder.hostname	mail
⑦	data.parameters.alert.predecoder.program_name	sshd
⑦	data.parameters.alert.predecoder.timestamp	Jul 11 01:21:54
⑦	data.parameters.alert.rule.description	sshd: Attempt to login using a non-existent user
⑦	data.parameters.alert.rule.firedtimes	2
⑦	data.parameters.alert.rule.gdpr	IV_35.7.d, IV_32.2
⑦	data.parameters.alert.rule.gpg13	7.1
⑦	data.parameters.alert.rule.groups	syslog, sshd, authentication_failed, invalid_login

⑦	data.parameters.alert.rule.hipaa	164.312.b
⑦	data.parameters.alert.rule.id	5710
⑦	data.parameters.alert.rule.level	5
⑦	data.parameters.alert.rule.mail	false
⑦	data.parameters.alert.rule.mitre.id	T1110.001, T1021.004
⑦	data.parameters.alert.rule.mitre.tactic	Credential Access, Lateral Movement
⑦	data.parameters.alert.rule.mitre.technique	Password Guessing, SSH
⑦	data.parameters.alert.rule.nist_800_53	AU.14, AC.7, AU.6
⑦	data.parameters.alert.rule.pci_dss	10.2.4, 10.2.5, 10.6.1
⑦	data.parameters.alert.rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
⑦	data.parameters.alert.timestamp	2024-07-10T20:21:56.628+0000
f	data.parameters.extra_args	
⑦	data.parameters.program	active-response/bin/firewall-drop
f	data.srcip	192.168.100.6
⑦	data.version	1
f	decoder.name	ar_log_json

t decoder.name	ar_log_json
t decoder.parent	ar_log_json
t full_log	>
t id	1720642916.219132
t input.type	log
t location	/var/ossec/logs/active-responses.log
t manager.name	wazuh-server
t rule.description	Host Blocked by firewall-drop Active Response
# rule.firedtimes	2
t rule.gdpr	IV_35.7.d
t rule.gpg13	4.13
t rule.groups	ossec, active_response
t rule.id	651

t manager.name	wazuh-server
t rule.description	Host Blocked by firewall-drop Active Response
# rule.firedtimes	2
t rule.gdpr	IV_35.7.d
t rule.gpg13	4.13
t rule.groups	ossec, active_response
t rule.id	651
# rule.level	3
rule.mail	false
t rule.nist_800_53	SI.4
t rule.pci_dss	11.4
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3, CC7.4
timestamp	Jul 11, 2024 @ 01:21:56.785

## SUMMARY:

By leveraging Wazuh's Active Response feature, organizations can enhance their security posture by automating the mitigation of SSH brute force attacks. This not only helps in preventing unauthorized access but also reduces the administrative burden of manually handling such incidents. Proper configuration and testing of these responses ensure that they act effectively and as intended during an actual attack.

## Regards

**MUHAMMAD MOIZ UD DIN RAFAY**

Ethical Hacker | Cyber Security Analyst

## Need Training on Wazuh..?

Contact: +92-3004962168

Email: [muhammadmoizuddinrafay@gmail.com](mailto:muhammadmoizuddinrafay@gmail.com)

LinkedIn: [www.linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)