Detecting Brute Force attack

SAMEER HASSAN

Wazuh lab

Github-link: GitHub - sameerhassancode/Wazuh-

Linkedin: https://www.linkedin.com/in/sameer-hassan-15a428255/

Overview

Wazuh is an open-source Security Information and Event Management (SIEM) tool that provides intrusion detection, log analysis, file integrity monitoring, and real-time threat detection across endpoints and servers.

SSH Brute Force attack

A **brute force attack** involves systematically guessing credentials (usernames/passwords) to gain unauthorized access to systems — especially common on SSH, RDP, and web login interfaces.

Response And Detection with wazuh

How Wazuh Detects Brute Force Attacks

1. **Log Collection**

   Wazuh collects logs from systems and services (e.g., SSH, RDP, FTP, Apache, etc.) using its **agent or agentless mode**.

2. **Decoding & Parsing**

   These logs are processed through **decoders** that extract useful fields such as:

   - Source IP
   - Username
   - Success/failure status

3. **Rules Engine**

   Wazuh uses a **rich rule set** to detect patterns that indicate brute force activity. For example:

   - Multiple failed logins from the same IP
   - Multiple login attempts with different usernames
   - High frequency of attempts over a short time

Example Rule:

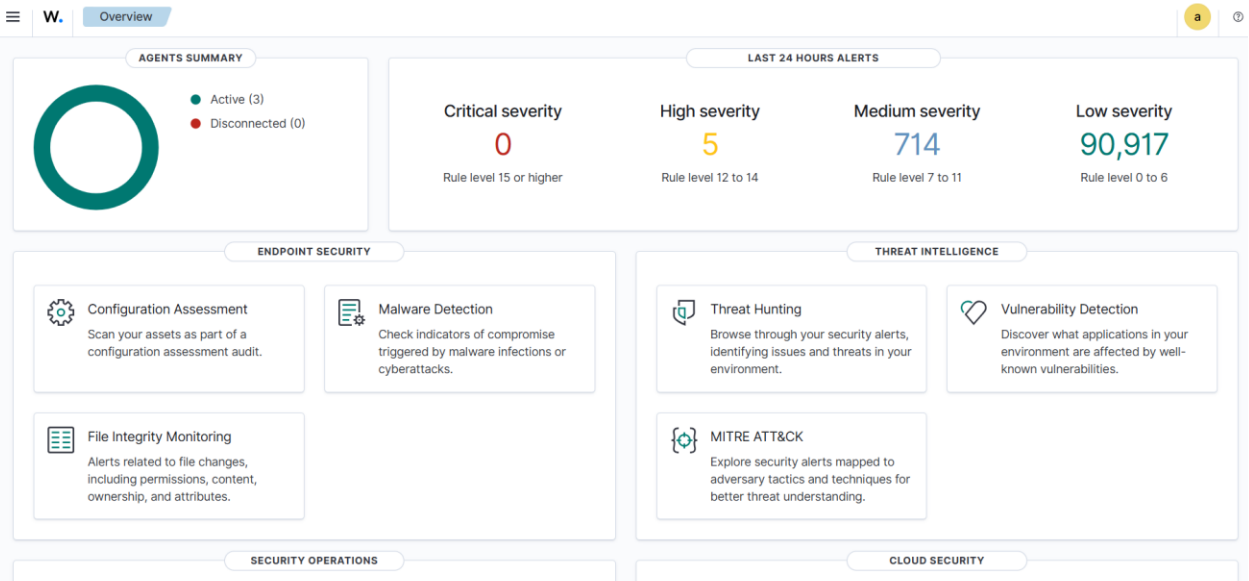
> Rule ID: 5710
> Description: Multiple SSH failed login attempts
> Level: 10

4. Active Response

Wazuh can trigger automatic responses, such as:

- Blocking IP addresses via firewall rules (iptables)
- Sending alerts (email, Slack, syslog)
- Executing custom scripts

Wazuh Dashboard:



AGENTS SUMMARY

● Active (3)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	5	714	90,917
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

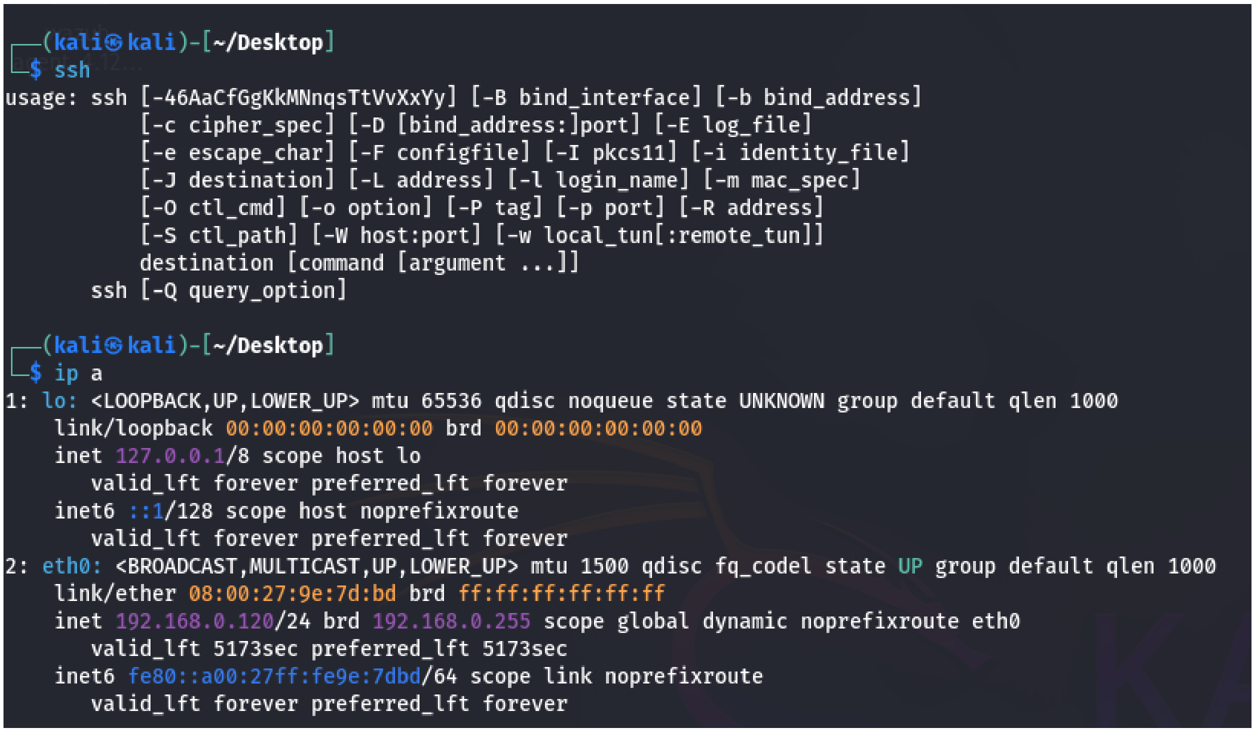
CLOUD SECURITY

Ubuntu:

Working Linux and Proper connected to Internet machine.

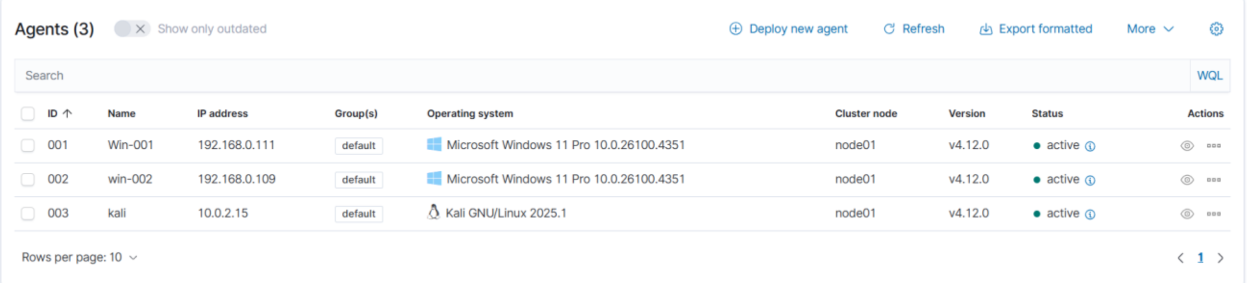
Attacker IP: 192.168.0.120

SSH: updated and working



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-P tag] [-p port] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           destination [command [argument ...]]
       ssh [-Q query_option]

┌──(kali㉿kali)-[~/Desktop]
└─$ 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9e:7d:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.120/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
       valid_lft 5173sec preferred_lft 5173sec
    inet6 fe80::a00:27ff:fe9e:7dbd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

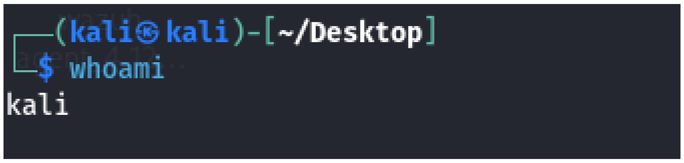
In my system 3 agent are working



ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Win-001	192.168.0.111	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	● active	
002	win-002	192.168.0.109	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	● active	
003	kali	10.0.2.15	default	Kali GNU/Linux 2025.1	node01	v4.12.0	● active	

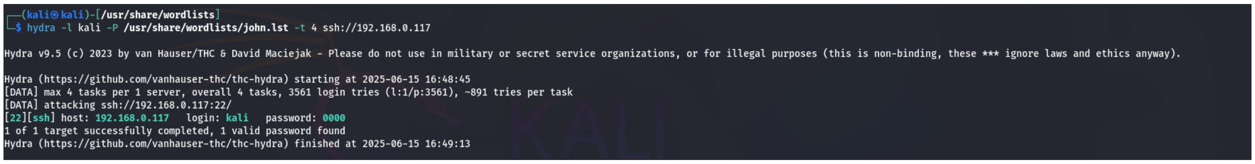
I will use kali as a attacker and perform Brute force attack on Another Kali machine

Victim Username: Kali



```
┌──(kali㉿kali)-[~/Desktop]
└─$ whoami
kali
```

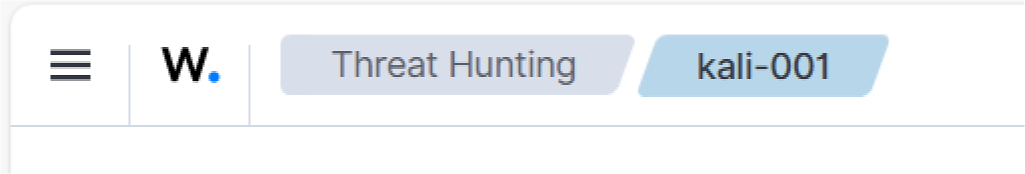
Ok now Start Brute Force attack on the user!



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l kali -P /usr/share/wordlists/john.lst -t 4 ssh://192.168.0.117

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 2025-06-15 16:48:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3561 login tries (l:1/p:3561), ~891 tries per task
[DATA] attacking ssh://192.168.0.117:22/
[22][ssh] host: 192.168.0.117   login: kali   password: 0000
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-15 16:49:13
```

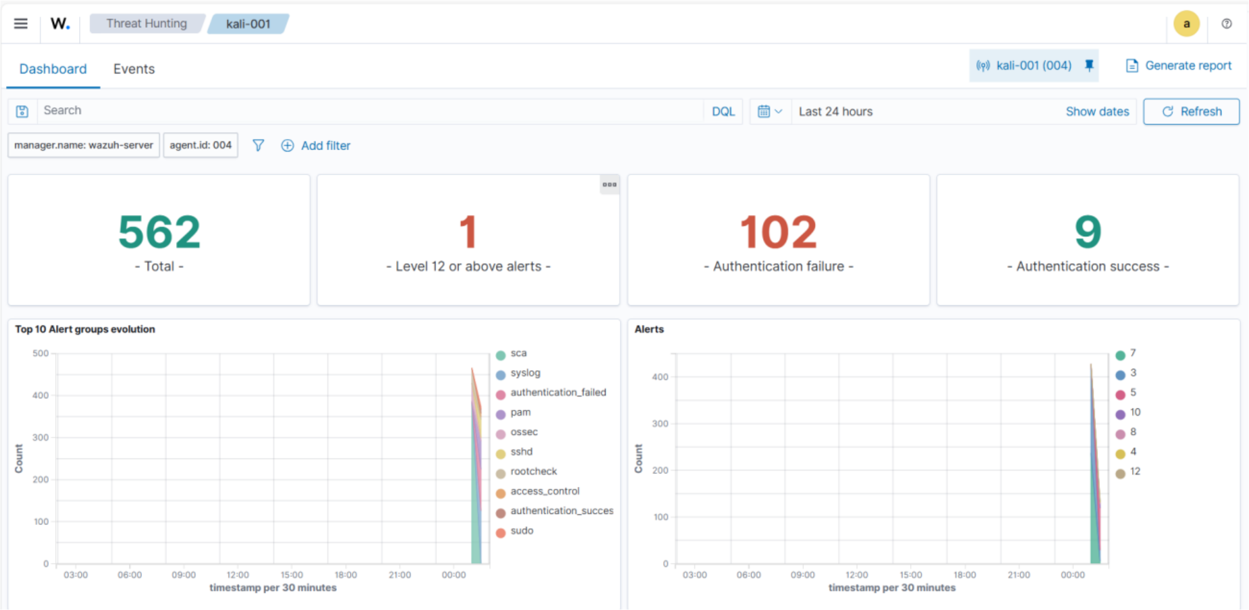
Done I password match and I connected using SSH.

Now open your Wazuh dashboard and go to

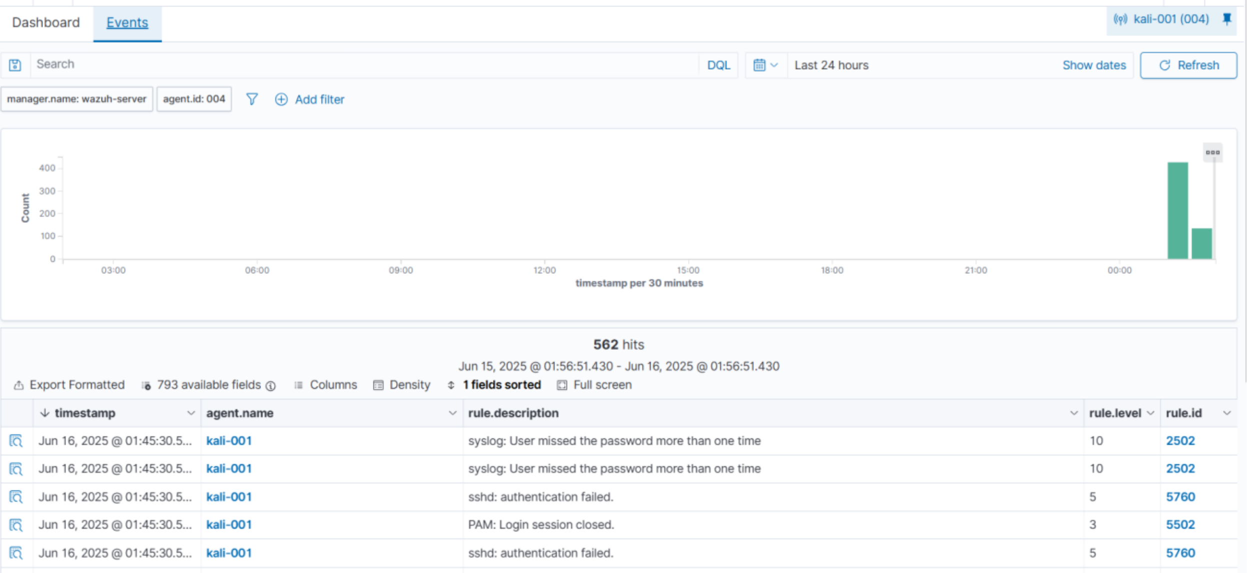


And under this you will see the alert.

102 authentication failure/attempts.



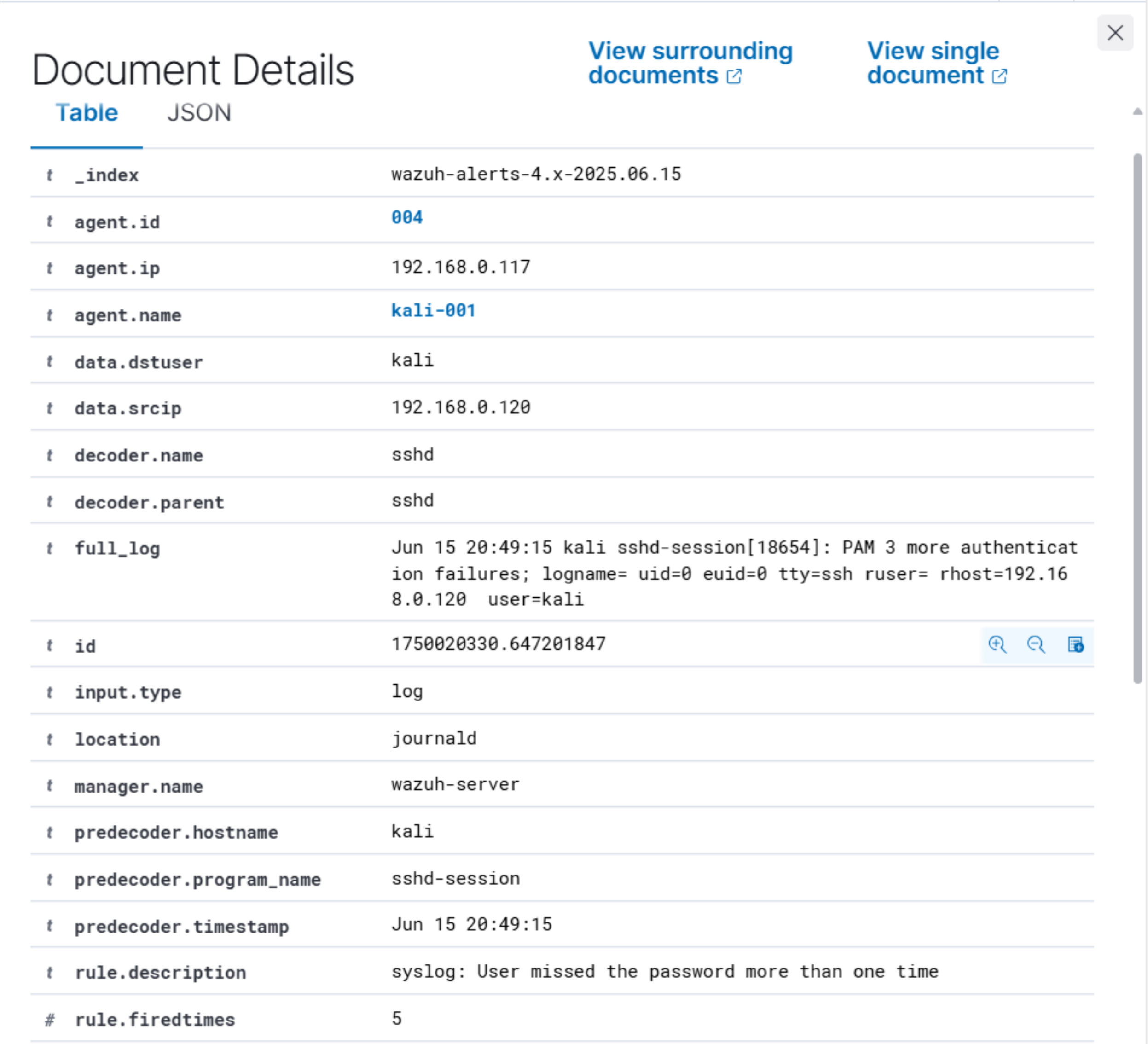
Click on the events button and analyze the logs.



562 hits

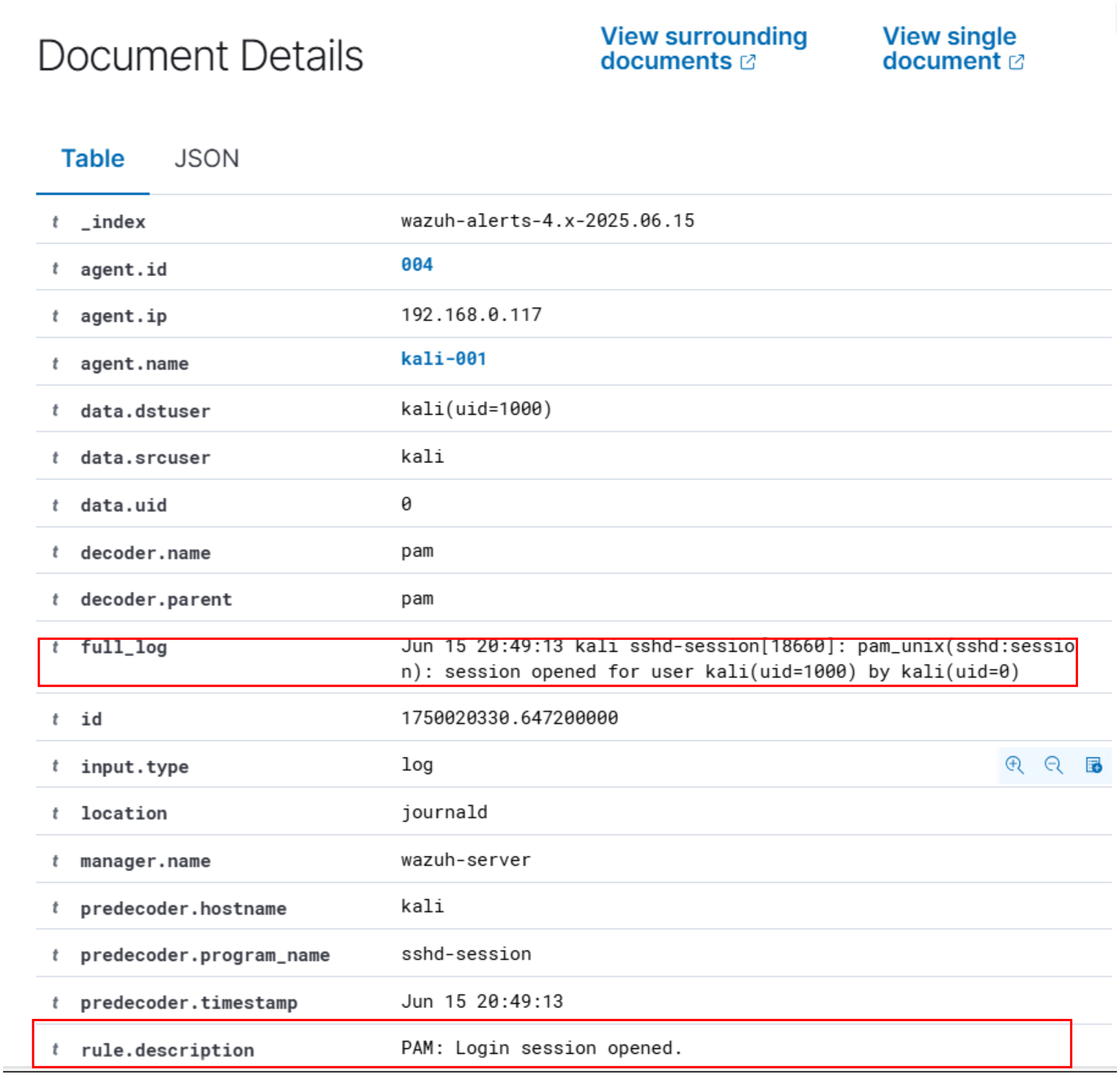
Jun 15, 2025 @ 01:56:51.430 - Jun 16, 2025 @ 01:56:51.430

timestamp	agent.name	rule.description	rule.level	rule.id
Jun 16, 2025 @ 01:45:30.5...	kali-001	syslog: User missed the password more than one time	10	2502
Jun 16, 2025 @ 01:45:30.5...	kali-001	syslog: User missed the password more than one time	10	2502
Jun 16, 2025 @ 01:45:30.5...	kali-001	sshd: authentication failed.	5	5760
Jun 16, 2025 @ 01:45:30.5...	kali-001	PAM: Login session closed.	3	5502
Jun 16, 2025 @ 01:45:30.5...	kali-001	sshd: authentication failed.	5	5760



t	_index	wazuh-alerts-4.x-2025.06.15
t	agent.id	004
t	agent.ip	192.168.0.117
t	agent.name	kali-001
t	data.dstuser	kali
t	data.srcip	192.168.0.120
t	decoder.name	sshd
t	decoder.parent	sshd
t	full_log	Jun 15 20:49:15 kali sshd-session[18654]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.0.120 user=kali
t	id	1750020330.647201847
t	input.type	log
t	location	journald
t	manager.name	wazuh-server
t	predecoder.hostname	kali
t	predecoder.program_name	sshd-session
t	predecoder.timestamp	Jun 15 20:49:15
t	rule.description	syslog: User missed the password more than one time
#	rule.firedtimes	5

SSH Success Log



t	_index	wazuh-alerts-4.x-2025.06.15
t	agent.id	004
t	agent.ip	192.168.0.117
t	agent.name	kali-001
t	data.dstuser	kali(uid=1000)
t	data.srcuser	kali
t	data.uid	0
t	decoder.name	pam
t	decoder.parent	pam
t	full_log	Jun 15 20:49:13 kali sshd-session[18660]: pam_unix(sshd:session): session opened for user kali(uid=1000) by kali(uid=0)
t	id	1750020330.647200000
t	input.type	log
t	location	journald
t	manager.name	wazuh-server
t	predecoder.hostname	kali
t	predecoder.program_name	sshd-session
t	predecoder.timestamp	Jun 15 20:49:13
t	rule.description	PAM: Login session opened.

Active Response:

Connect with the Wazuh server using SSH to configure active response

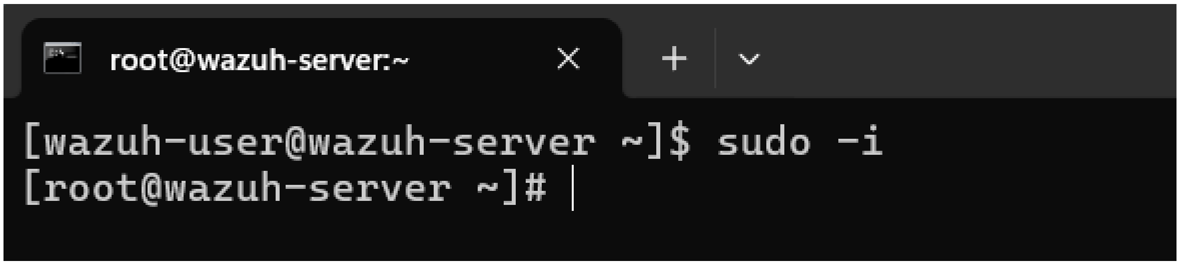
Command:

ssh Wazuh-ser@192.168.0.114

```
[wazuh-user@wazuh-server ~]$
```

Get the root access

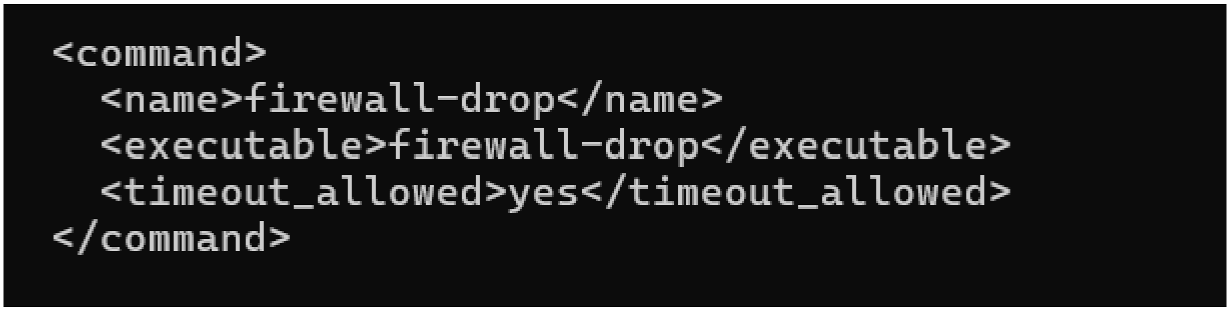
Sudo -i



```
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]#
```

Now open Ossec.conf file located at “/var/ossec/etc/ossec.conf”

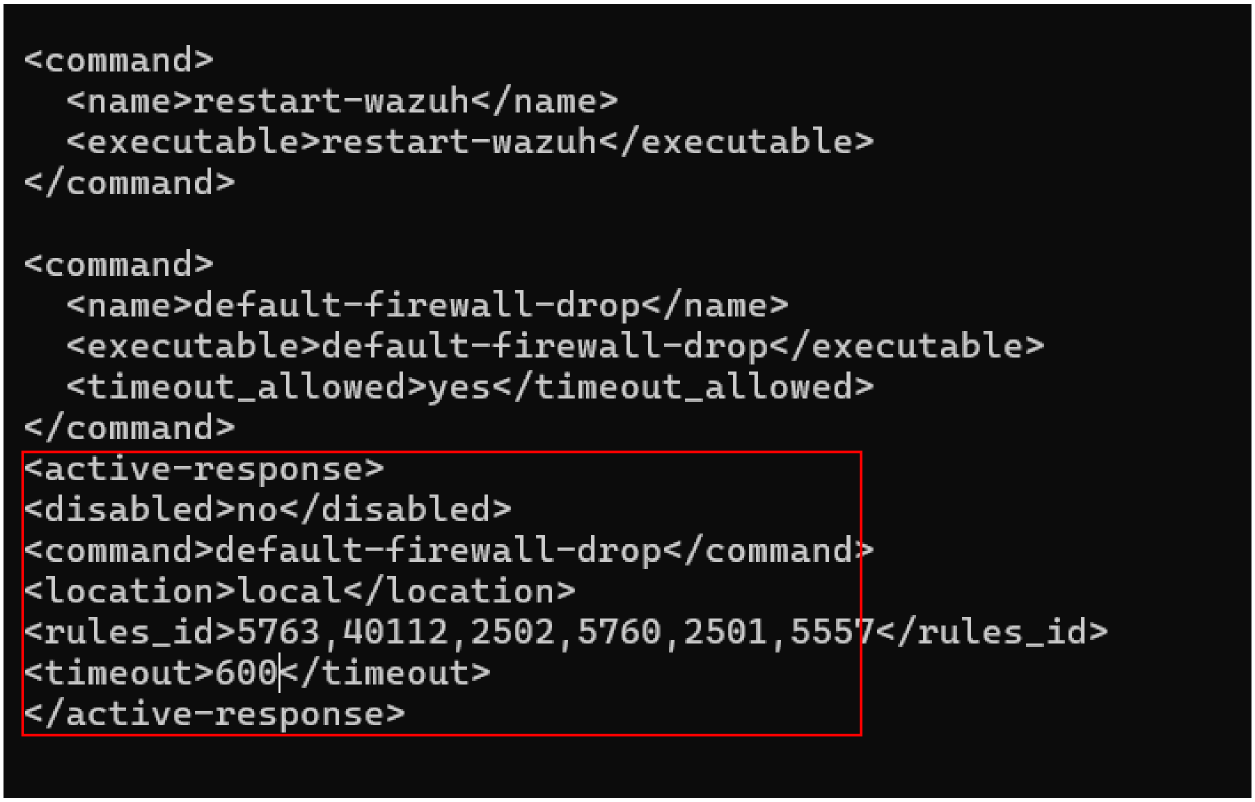
Open it using nano and **file path.** After opening the file go to active response section.



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

And add this commands

```
 <active-response>
<disabled>no</disabled>
<command>default-firewall-drop</command>
<location>local</location>
<rules_id>5763,40112,2502,5760,2501,5557</rules_id>
<timeout>600</timeout>
</active-response>
```



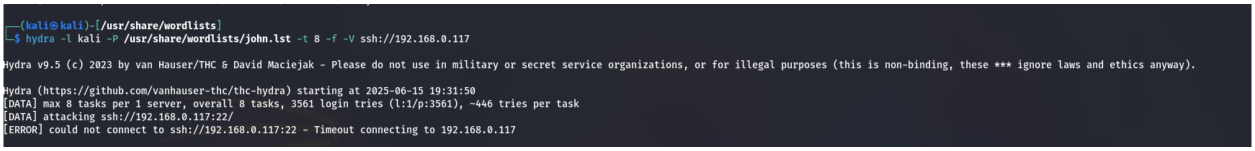
```
<command>
  <name>restart-wazuh</name>
  <executable>restart-wazuh</executable>
</command>

<command>
  <name>default-firewall-drop</name>
  <executable>default-firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
<active-response>
<disabled>no</disabled>
<command>default-firewall-drop</command>
<location>local</location>
<rules_id>5763,40112,2502,5760,2501,5557</rules_id>
<timeout>600</timeout>
</active-response>
```

After that save the file by pressing CTRL + O then enter and lastly CTRL X

Now restart the Wazuh manger using command:

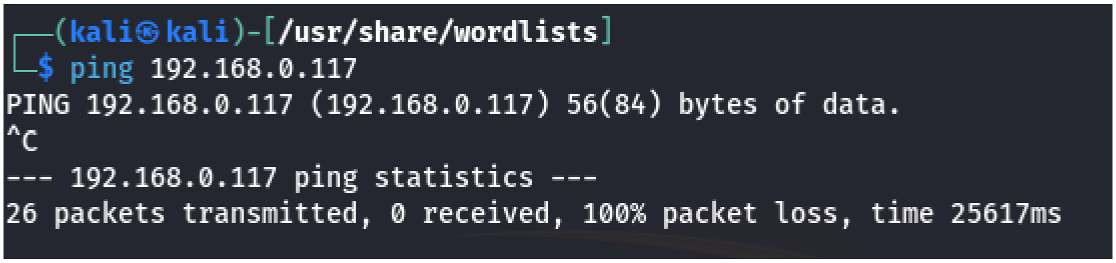
Systemctl restart Wazuh-manager

Perform SSH attack again



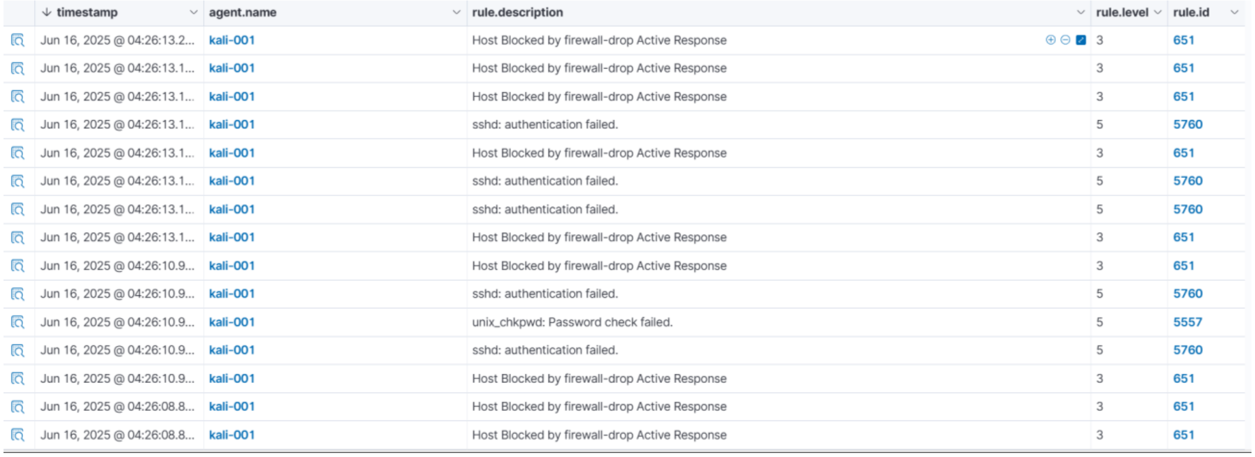
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l kali -P /usr/share/wordlists/john.lst -t 8 -f -V ssh://192.168.0.117

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 2025-06-15 19:31:50
[DATA] max 8 tasks per 1 server, overall 8 tasks, 3561 login tries (l:1/p:3561), ~446 tries per task
[DATA] attacking ssh://192.168.0.117:22/
[ERROR] could not connect to ssh://192.168.0.117:22 - Timeout connecting to 192.168.0.117
```

Ping the victim from attacker machine. The attacker machine is blocked for next 10 minutes

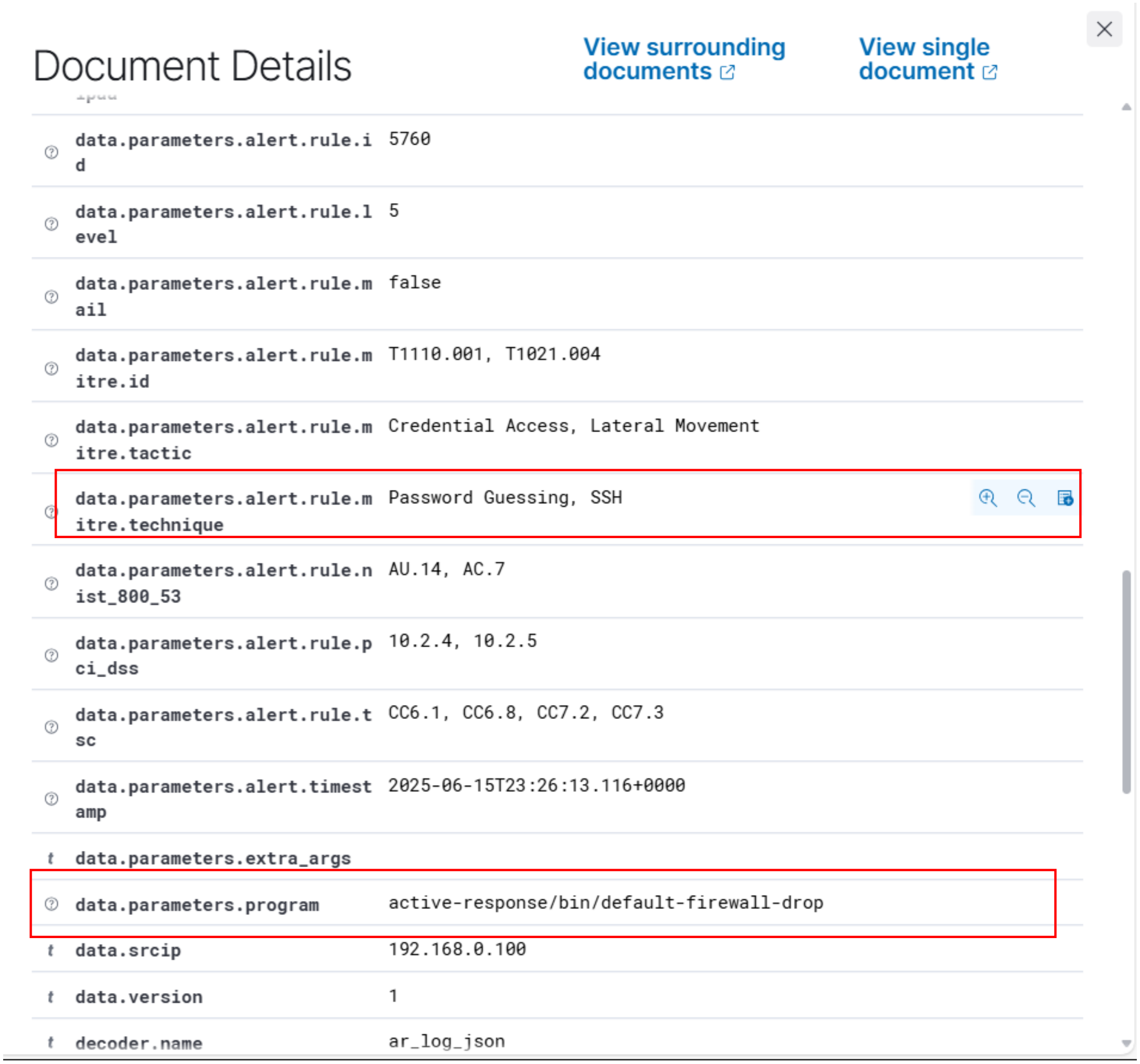


```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ping 192.168.0.117
PING 192.168.0.117 (192.168.0.117) 56(84) bytes of data.
^C
--- 192.168.0.117 ping statistics ---
26 packets transmitted, 0 received, 100% packet loss, time 25617ms
```

Now Wazuh is generating the logs from firewall saying blocking the Host



	↓ timestamp	agent.name	rule.description	rule.level	rule.id
	Jun 16, 2025 @ 04:26:13.2...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:13.1...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:13.1...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:13.1...	kali-001	sshd: authentication failed.	5	5760
	Jun 16, 2025 @ 04:26:13.1...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:13.1...	kali-001	sshd: authentication failed.	5	5760
	Jun 16, 2025 @ 04:26:13.1...	kali-001	sshd: authentication failed.	5	5760
	Jun 16, 2025 @ 04:26:13.1...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:10.9...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:10.9...	kali-001	sshd: authentication failed.	5	5760
	Jun 16, 2025 @ 04:26:10.9...	kali-001	unix_chkpwd: Password check failed.	5	5557
	Jun 16, 2025 @ 04:26:10.9...	kali-001	sshd: authentication failed.	5	5760
	Jun 16, 2025 @ 04:26:10.9...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:08.8...	kali-001	Host Blocked by firewall-drop Active Response	3	651
	Jun 16, 2025 @ 04:26:08.8...	kali-001	Host Blocked by firewall-drop Active Response	3	651



data.parameters.alert.rule.id	5760
data.parameters.alert.rule.level	5
data.parameters.alert.rule.mail	false
data.parameters.alert.rule.mitre.id	T1110.001, T1021.004
data.parameters.alert.rule.mitre.tactic	Credential Access, Lateral Movement
data.parameters.alert.rule.mitre.technique	Password Guessing, SSH
data.parameters.alert.rule.nist_800_53	AU.14, AC.7
data.parameters.alert.rule.pci_dss	10.2.4, 10.2.5
data.parameters.alert.rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
data.parameters.alert.timestamp	2025-06-15T23:26:13.116+0000
data.parameters.extra_args	
data.parameters.program	active-response/bin/default-firewall-drop
data.srcip	192.168.0.100
data.version	1
decoder.name	ar_log_json

Check your rules using this path.

/var/ossec/ruleset/rules

Rule ID	Description
5763	sshd: brute force trying to get access
40112	Multiple auth failures followed by success
2502, 2501, 5503	Multiple login failures
5557, 5760	Password/authentication failures
651, 652	Host blocked/unblocked by active response

Summary:

Using **Wazuh**, it's easy to detect and block SSH brute-force attacks in real-time. First, tools like **Hydra** can be used to simulate brute-force attempts against an SSH service. Wazuh, with its default ruleset, detects these attempts using rules such as `5763`, `40112`, and others that identify multiple failed login attempts or suspicious login patterns.

To actively block these attacks, Wazuh can trigger **active response scripts** like `default-firewall-drop`. By configuring the `ossec.conf` file with the appropriate `<command>` and `<active-response>` blocks linked to the relevant rule IDs, Wazuh will automatically add the attacker's IP to the firewall (e.g., via `iptables` or `firewalld`) and block it for a specified timeout period (like 10 minutes).

This setup allows Wazuh not only to monitor and alert on brute-force attempts but also to **automatically defend** your system by blocking the source IP. Logs can be reviewed in real-time using Kibana or via log files like `/var/ossec/logs/alerts/alerts.json`, making it a powerful and proactive intrusion detection and prevention system.

Need training on Wazuh ?

Contact number: +923355345678

Email: sameeerishassan@gmail.com

Linkedin: https://pk.linkedin.com/in/sameer-hassan-15a428255

Other SIEM

1. IBM Qradar
2. Splunk
3. Azure Sentinel