SSH Brute Force Attack Detection & Active Response using Wazuh

Introduction to Brute Force Attacks

A brute force attack is a type of cyberattack in which an attacker repeatedly tries different username and password combinations to gain unauthorized access to a system. These attacks commonly target services such as SSH, FTP, RDP, web login pages, and databases.

Brute force attacks rely on automation and speed rather than exploiting software vulnerabilities. If a system does not have proper monitoring and protection, an attacker can eventually guess valid credentials and gain access to the server.

Common signs of a brute force attack include multiple failed login attempts from the same IP address within a short time period. Early detection of such behavior is very important to prevent account compromise and full system takeover.

Purpose of Brute Force Detection using Wazuh

The purpose of implementing brute force attack detection in Wazuh is to:

- Detect repeated failed login attempts
- Identify malicious or suspicious IP addresses
- Generate real-time security alerts
- Automatically block attacker IPs using Active Response
- Protect servers from unauthorized access

Preconditions

Before implementing and testing this use case, the following conditions must be met:

Wazuh Manager is installed and running

Wazuh Agent is installed on the Ubuntu server

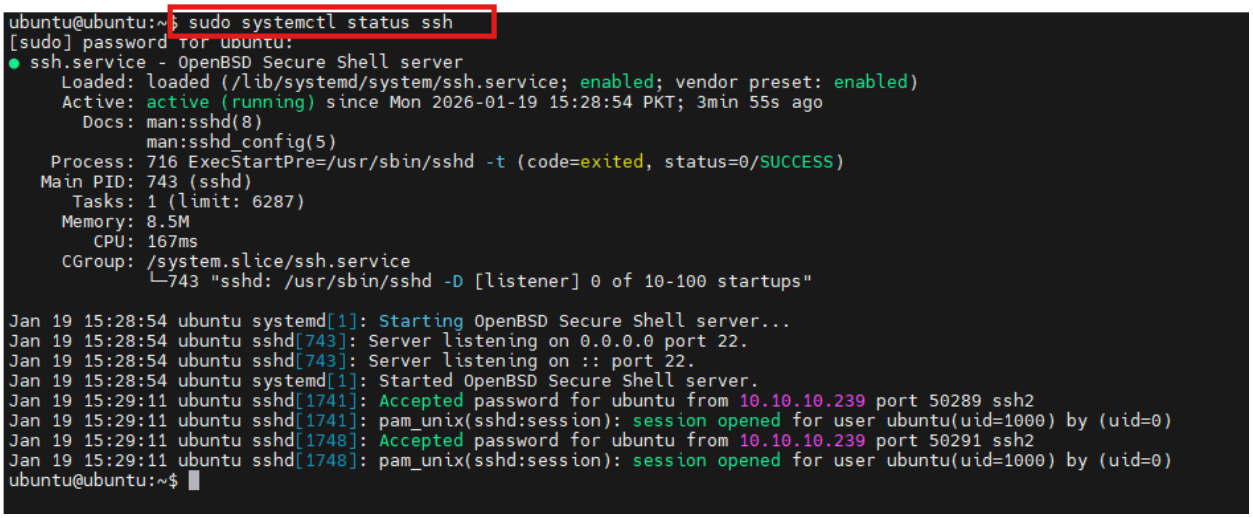
SSH service is enabled on the agent machine

Agent is properly connected to the Wazuh Manager

System time is synchronized

Before testing, verify that the SSH service is active on the victim machine (Ubuntu) using the following command:

sudo systemctl status ssh



Enable SSH Log Monitoring on Wazuh Agent

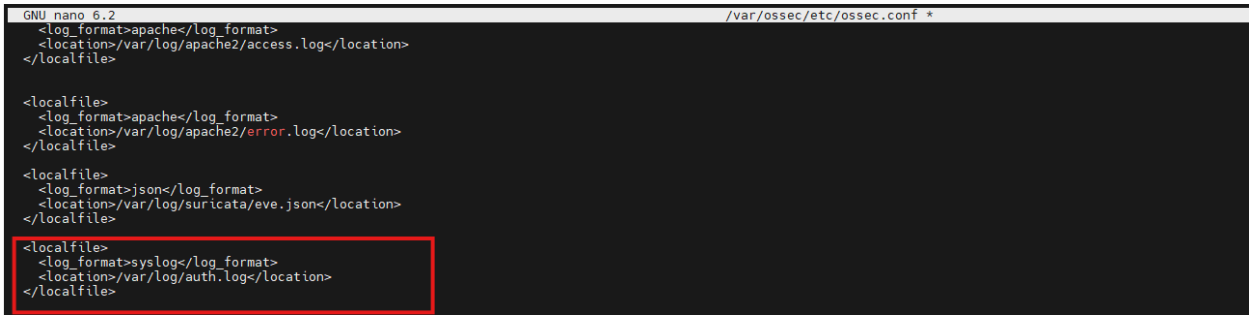
Edit the agent configuration file:

sudo nano /var/ossec/etc/ossec.conf

Add the following configuration to monitor SSH authentication logs:

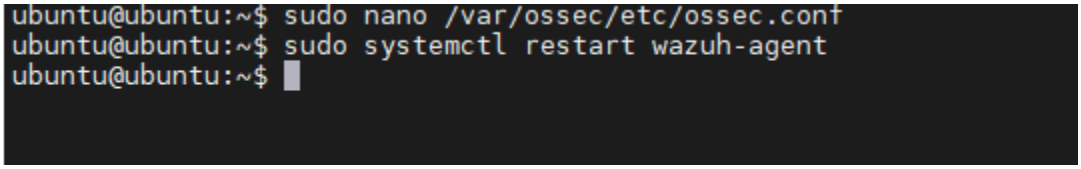
<localfile>

```
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```



Save the file and restart the Wazuh Agent:

```
sudo systemctl restart wazuh-agent
```



Default Brute Force Detection in Wazuh

Wazuh already includes built-in rules to detect brute force attacks, especially for SSH services. These rules are capable of detecting:

- Multiple failed SSH login attempts
- Authentication failures from the same IP address
- Suspicious authentication behavior

This allows Wazuh to identify brute force attacks without requiring custom rules.

Simulate a Brute Force Attack using Hydra

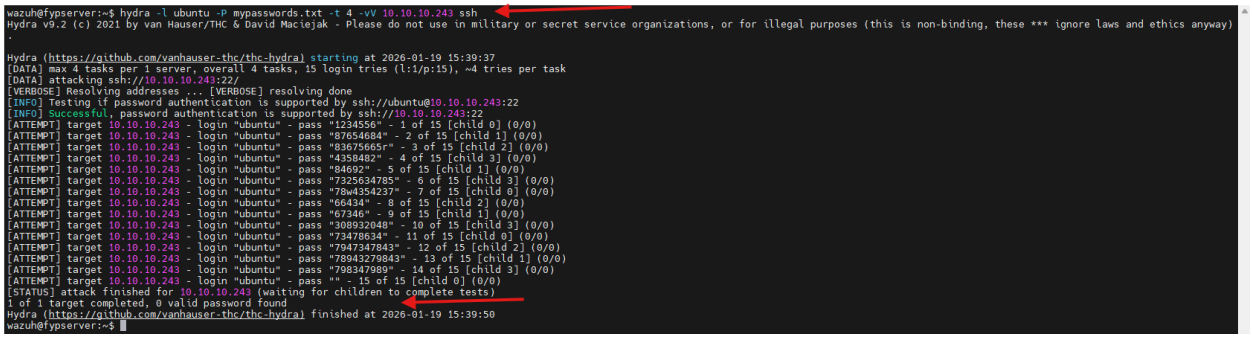
From the attacker machine (Ubuntu Server Desktop), Hydra is used to simulate a brute force attack against the victim's SSH service.

```
sudo nano mypasswords.txt
```

```
wazuh@fypserver:~$ sudo nano mypasswords.txt
[sudo] password for wazuh:
wazuh@fypserver:~$
```

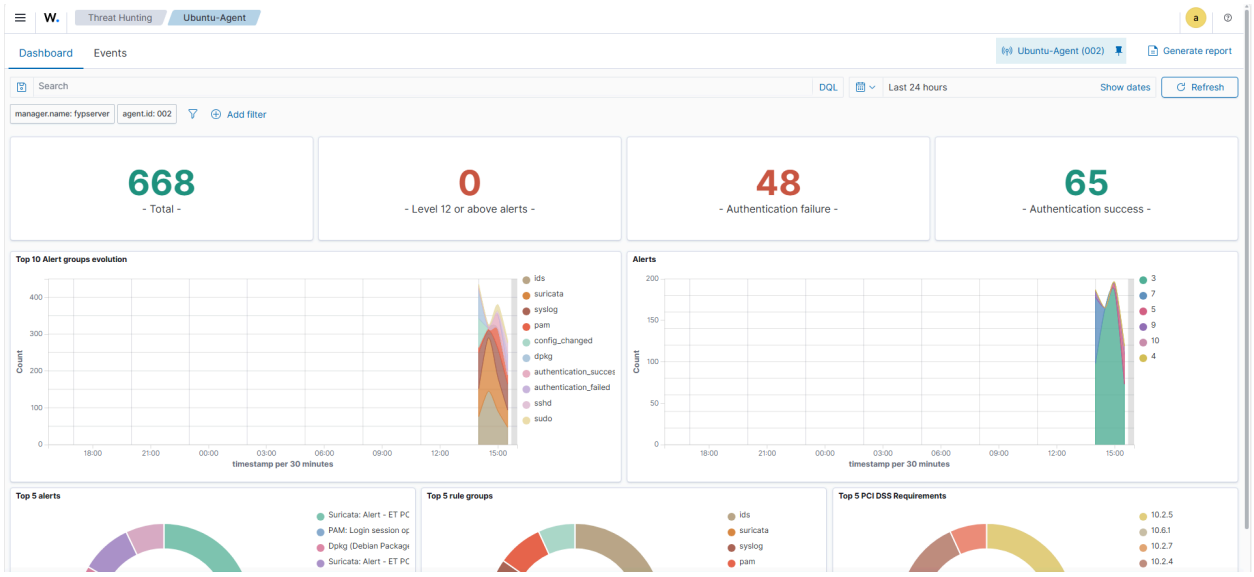
```
 GNU nano 6.2                                                    mypasswords.txt *
1234556
87654684
83675665r
4358482
84692
7325634785
78w4354237
66434
67346
308932048
73478634
7947347843
78943279843
798347989
```

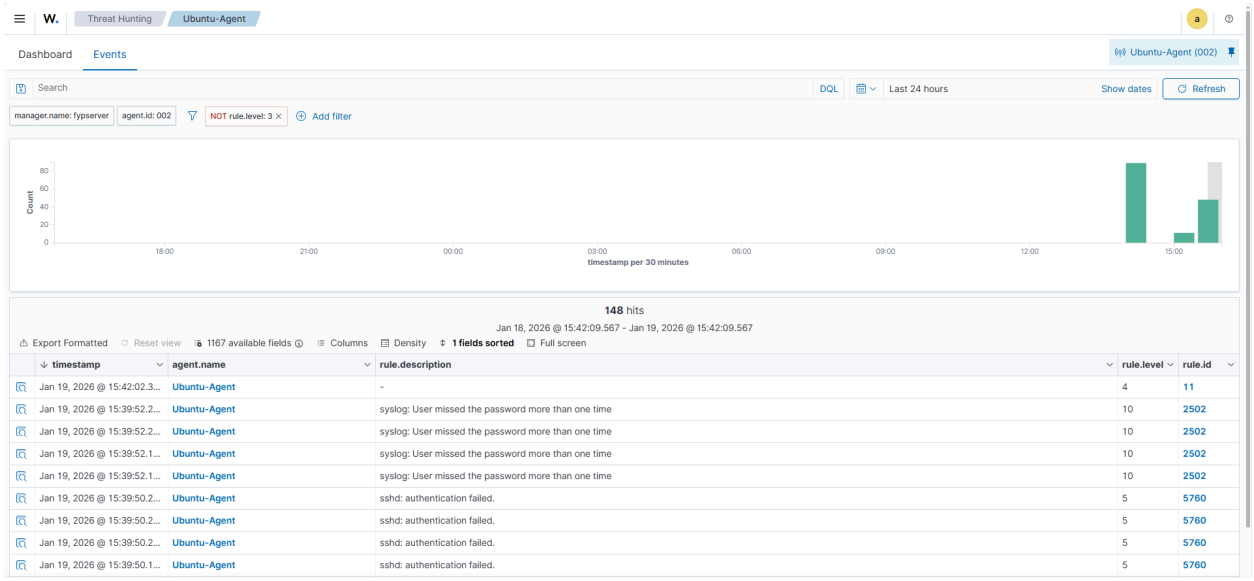
hydra -l ubuntu -P mypasswords.txt -t 4 -vV 10.10.10.243 ssh



After successfully obtaining the password using Hydra, the attacker is able to log in to the target machine using valid credentials.

In the **Wazuh Dashboard**, navigate to the **Threat Hunting** section. Under the **Events** tab, multiple authentication failure logs can be observed, confirming SSH brute force activity.





Details Alerts:

Table JSON

@timestamp	Jan 19, 2026 @ 15:39:52.198
_index	wazuh-alerts-4.x-2026.01.19
agent.id	002
agent.ip	10.10.10.243
agent.name	Ubuntu-Agent
data.dstuser	ubuntu
data.srcip	10.10.10.240
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 19 15:39:50 ubuntu sshd[6633]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.240 user=ubuntu
id	1768819192.940660
input.type	log
location	/var/log/auth.log
manager.name	fypserver
predecoder.hostname	ubuntu
predecoder.program_name	sshd
rule.description	syslog: User missed the password more than one time
rule.firedtimes	8
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.8
rule.groups	syslog, access_control, authentication_failed
rule.hipaa	164.312.b
rule.id	2502
rule.level	10
rule.mail	false
rule.mitre.id	T1110
rule.mitre.tactic	Credential Access
rule.mitre.technique	Brute Force
rule.nist_800_53	AU.14, AC.7
rule.pci_dss	10.2.4, 10.2.5
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Jan 19, 2026 @ 15:39:52.226

Table JSON

@timestamp	Jan 19, 2026 @ 15:39:50.228
_index	wazuh-alerts-4.x-2026.01.19
agent.id	002
agent.ip	10.10.10.243
agent.name	Ubuntu-Agent
data.dstuser	ubuntu
data.srcip	10.10.10.240
data.srcport	46054
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 19 10:39:49 ubuntu sshd[6633]: Failed password for ubuntu from 10.10.10.240 port 46054 ssh2
id	1768819190.938676
input.type	log
location	journald
manager.name	fypserver
predecoder.hostname	ubuntu
predecoder.program_name	sshd
rule.description	sshd: authentication failed.
rule.firedtimes	26
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.1
rule.groups	syslog, sshd, authentication_failed
rule.hipaa	164.312.b
rule.id	5760
rule.level	5
rule.mail	false
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH
rule.nist_800_53	AU.14, AC.7
rule.pci_dss	10.2.4, 10.2.5
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Jan 19, 2026 @ 15:39:50.228

When I put the original password in the the password file then with the help of brute force attack I successfully find the original password:

hydra -l ubuntu -P mypasswords.txt -t 4 -vV 10.10.10.243 ssh

```
wazuh@fypserver:~$ hydra -l ubuntu -P mypasswords.txt -t 4 -vV 10.10.10.243 ssh
Hydra v9.2 (c) 2021 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 2026-01-19 15:50:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:1/p:16), ~4 tries per task
[DATA] attacking ssh://10.10.10.243:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://ubuntu@10.10.10.243:22
[INFO] Successful, password authentication is supported by ssh://10.10.10.243:22
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "1234556" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "87654684" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "83675665r" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "4358482" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "84692" - 5 of 16 [child 2] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "7325634785" - 6 of 16 [child 0] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "78w4354237" - 7 of 16 [child 3] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "66434" - 8 of 16 [child 1] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "67346" - 9 of 16 [child 2] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "308932048" - 10 of 16 [child 0] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "73478634" - 11 of 16 [child 3] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "7947347843" - 12 of 16 [child 1] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "78943279843" - 13 of 16 [child 2] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "798347989" - 14 of 16 [child 3] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "123@akistan" - 15 of 16 [child 0] (0/0)
[ATTEMPT] target 10.10.10.243 - login "ubuntu" - pass "" - 16 of 16 [child 1] (0/0)
[STATUS] attack finished for 10.10.10.243 (waiting for children to complete tests)
[22][ssh] host: 10.10.10.243   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-19 15:51:03
wazuh@fypserver:~$
```

Now see the alerts related to successful login on Wazuh Dashboard

194 hits

Jan 18, 2026 @ 15:58:41.522 - Jan 19, 2026 @ 15:58:41.522

Export Formatted | Reset view | 1167 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Jan 19, 2026 @ 15:51:04.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:04.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:02.9...	Ubuntu-Agent	sshd: authentication failed.	5	5760
Jan 19, 2026 @ 15:51:02.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:02.9...	Ubuntu-Agent	sshd: authentication failed.	5	5760
Jan 19, 2026 @ 15:51:02.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:01.0...	Ubuntu-Agent	sshd: authentication failed.	5	5760
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	Multiple authentication failures followed by a success.	12	40112
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	sshd: authentication failed.	5	5760
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	sshd: authentication failed.	5	5760
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	Multiple authentication failures followed by a success.	12	40112
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	syslog: User missed the password more than one time	10	2502
Jan 19, 2026 @ 15:51:00.9...	Ubuntu-Agent	sshd: authentication failed.	5	5760

Table | JSON

t _index	wazuh-alerts-4.x-2026.01.19
t agent.id	002
t agent.ip	10.10.10.243
t agent.name	Ubuntu-Agent
t data.dstuser	ubuntu
t data.srcip	10.10.10.240
t data.srcport	32774
t decoder.name	sshd
t decoder.parent	sshd
t full_log	Jan 19 10:50:59 ubuntu sshd[7001]: Accepted password for ubuntu from 10.10.10.240 port 32774 ssh2
t id	1768819860.1040782
t input.type	log
t location	journald
t manager.name	fypserver
t predecoder.hostname	ubuntu
t predecoder.program_name	sshd
t predecoder.timestamp	Jan 19 10:50:59
t rule.description	Multiple authentication failures followed by a success.

Enable Active Response for Brute Force Attacks

Active Response allows Wazuh to automatically block attacker IP addresses once a brute force attack is detected.

Add this in the agent configuration file:

sudo nano /var/ossec/etc/ossec.conf

<active-response>

<location>/var/ossec/logs/active-responses.log</location>

</active-response>

```
<active-response>
  <location>/var/ossec/logs/active-responses.log</location>
</active-response>
```

Edit the Wazuh Manager configuration file:

sudo nano /var/ossec/etc/ossec.conf

Add or ensure the following Active Response configuration exists:

<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>5760</rules_id>
<timeout>3600</timeout>
</active-response>

```
GNU nano 6.2                                                    /var/ossec/etc/ossec.conf *
    <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>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>5760</rules_id>
    <timeout>180</timeout>
  </active-response>
```

sudo nano /var/ossec/etc/rules/local_rules.xml

<group name="active_response,firewall,block",>

<rule id="100400" level="10">
  <if_matched_sid>5760</if_matched_sid>
  <description>Active Response executed: Attacker IP blocked by firewall-drop</description>
  <group>active_response,firewall,block</group>
  <mitre>
    <id>T1110</id>
  </mitre>
</rule>
</group>

```
<group name="active_response,firewall,block,">

  <rule id="100400" level="10">
    <if_matched_sid>5760</if_matched_sid>
    <description>Active Response executed: Attacker IP blocked by firewall-drop</description>
    <group>active_response,firewall,block</group>
    <mitre>
      <id>T1110</id>
    </mitre>
  </rule>
</group>
```

Restart Wazuh Services

Restart the Wazuh Manager:

sudo systemctl restart wazuh-manager

```
wazuh@fypserver:~$ sudo nano /var/ossec/etc/ossec.conf
wazuh@fypserver:~$ sudo systemctl restart wazuh-manager
wazuh@fypserver:~$
```

Restart the Wazuh Agent:

sudo systemctl restart wazuh-agent

```
ubuntu@ubuntu:~$ sudo systemctl restart wazuh-agent
[sudo] password for ubuntu:
ubuntu@ubuntu:~$
```

This ensures that all recent configuration changes are applied successfully.

Re-run the Brute Force Attack

```
wazuh@fypserver:~$ sudo nano user.txt
wazuh@fypserver:~$ sudo nano pass.txt
wazuh@fypserver:~$
```

sudo nano user.txt

```
 GNU nano 6.2                                                    user.txt *
amir
ali
aslam
akram
amjad
bilal
basit
saif
akram
adnan
tanveer
faheem
ubuntu
kali
user
kashif
```

sudo nano pass.txt

```
 GNU nano 6.2                                                    pass.txt *
12344556
1234566787990
9478656473
43843
34784
4348734
47743897439
678234
62346234
77834
7747967
7892378
7843778
4787894789
74734
77347843
7789344378
7423789789432
789789432
272347
844
84327734
832475
i8324765
83247348
2863464
382366
382378
2383462754
2362345
```

Run the brute force attack again using Hydra:

sudo hydra -L user.txt -P pass.txt ssh://10.10.10.243

```
wazuh@fypserver:~$ sudo nano pass.txt
wazuh@fypserver:~$ sudo hydra -L user.txt -P pass.txt ssh://10.10.10.243
Hydra v9.2 (c) 2021 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 2026-01-26 09:24:36
[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, 88 login tries (l:4/p:22), ~6 tries per task
[DATA] attacking ssh://10.10.10.243:22/
1 of 1 target completed, 0 valid password found
```

This time, Wazuh detects the brute force attack and automatically blocks the attacker's IP address using Active Response. This confirms that Wazuh successfully detected and responded to the attack.

Confirm Active Response in Wazuh Logs

To verify the active response:

Open the Wazuh Dashboard

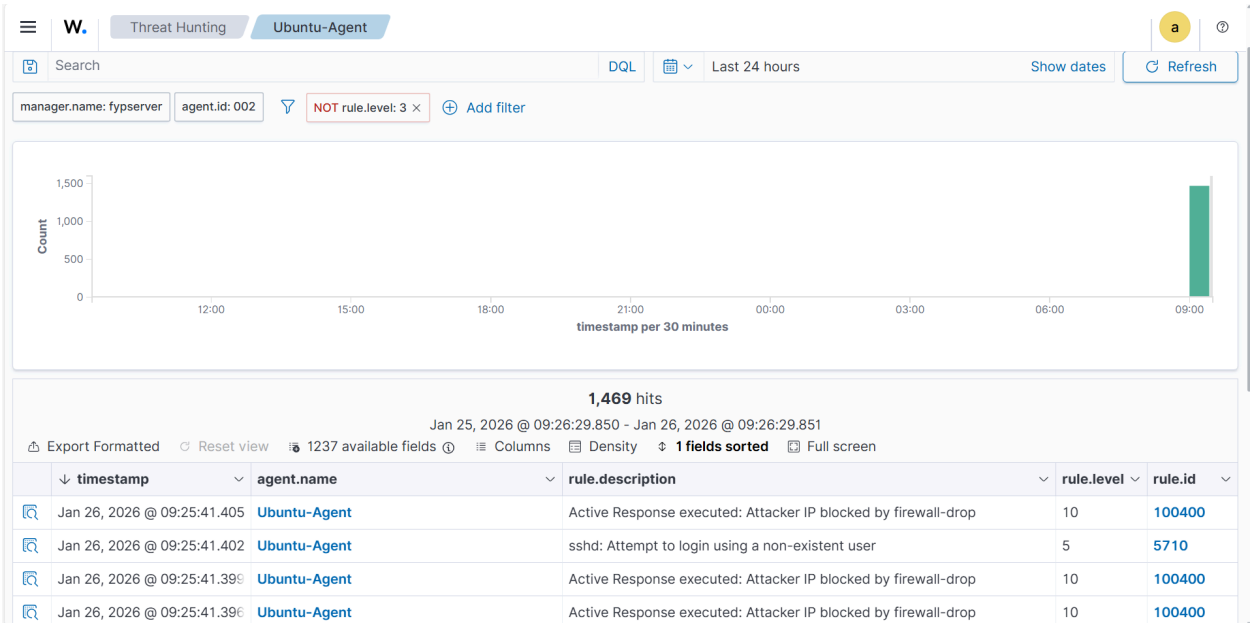
Go to Threat Hunting → Events

Search for logs indicating firewall blocking

You will see an event similar to:

"Active Response executed: Attacker IP blocked by firewall-drop"

This confirms that the attacker's IP was blocked automatically after brute force detection.



Details of Alerts:

Table JSON

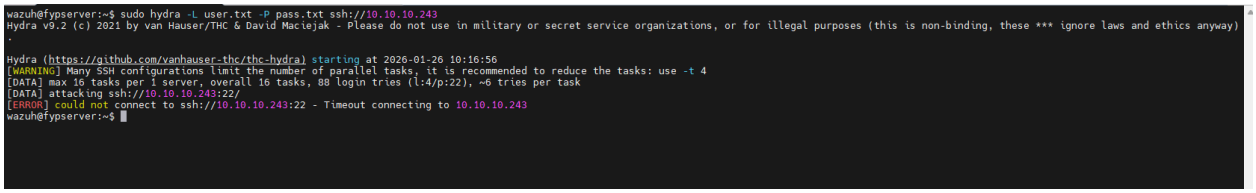
@timestamp	Jan 26, 2026 @ 09:25:41.402
_index	wazuh-alerts-4.x-2026.01.26
agent.id	002
agent.ip	10.10.10.243
agent.name	Ubuntu-Agent
data.srcip	10.10.10.240
data.srcuser	amir
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 22 14:18:35 ubuntu sshd[66970]: Failed password for invalid user amir from 10.10.10.240 port 35582 ssh2
id	1769401541.955249
input.type	log
location	journald
manager.name	fypserver
predecoder.hostname	ubuntu
predecoder.program_name	sshd
predecoder.timestamp	Jan 22 14:18:35
rule.description	sshd: Attempt to login using a non-existent user

Table JSON

@timestamp	Jan 26, 2026 @ 09:25:41.399
_index	wazuh-alerts-4.x-2026.01.26
agent.id	002
agent.ip	10.10.10.243
agent.name	Ubuntu-Agent
data.dstuser	ubuntu
data.srcip	10.10.10.240
data.srcport	35576
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 22 14:18:35 ubuntu sshd[66967]: Failed password for ubuntu from 10.10.10.240 port 35576 ssh2
id	1769401541.954770
input.type	log
location	journald
manager.name	fypserver
predecoder.hostname	ubuntu
predecoder.program_name	sshd

t	predecoder.timestamp	Jan 22 14:18:35
t	rule.description	Active Response executed: Attacker IP blocked by firewall-drop
#	rule.firedtimes	128
#	rule.frequency	2
t	rule.groups	active_response, firewall, block, active_response, firewall, block
t	rule.id	100400
#	rule.level	10
◕	rule.mail	false
t	rule.mitre.id	T1110
t	rule.mitre.tactic	Credential Access
t	rule.mitre.technique	Brute Force
🗓	timestamp	Jan 26, 2026 @ 09:25:41.399

Now if we try again to attack from the attacker machine to target then it shows the error as the ip is blocked.



Final Conclusion

In this project, I implemented SSH brute force attack detection and prevention using Wazuh and Active Response. When an attacker tries many wrong usernames and passwords on the SSH service, these failed login attempts are recorded in the system log file on the victim machine. The Wazuh agent reads these logs and sends them to the Wazuh manager.

The Wazuh manager analyzes the logs using its built-in rules. When the number of failed login attempts crosses a defined limit, Wazuh detects it as an SSH brute force attack. At this stage, an alert is generated on the Wazuh dashboard showing that a brute force attack has been detected.

After detection, the Active Response feature is triggered. The Wazuh manager sends a command to the Wazuh agent running on the victim system. The agent then executes the firewall-drop command locally. This command adds a firewall rule that blocks the attacker’s IP address using iptables or UFW.

Once the IP address is blocked, the attacker is no longer able to connect to the victim machine. Any further SSH attempts from the same IP fail immediately. After the IP is blocked, a confirmation alert is shown on the Wazuh dashboard indicating that the attacker’s IP has been successfully blocked.

This project shows that Wazuh can automatically detect SSH brute force attacks and stop them without manual action. By using log monitoring, rule-based detection, and Active Response, the system improves server security and protects it from unauthorized access.