# Wazuh – SSH Brute Force Attack

## ACTIVE RESPONSE

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

**Follow Me: 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.

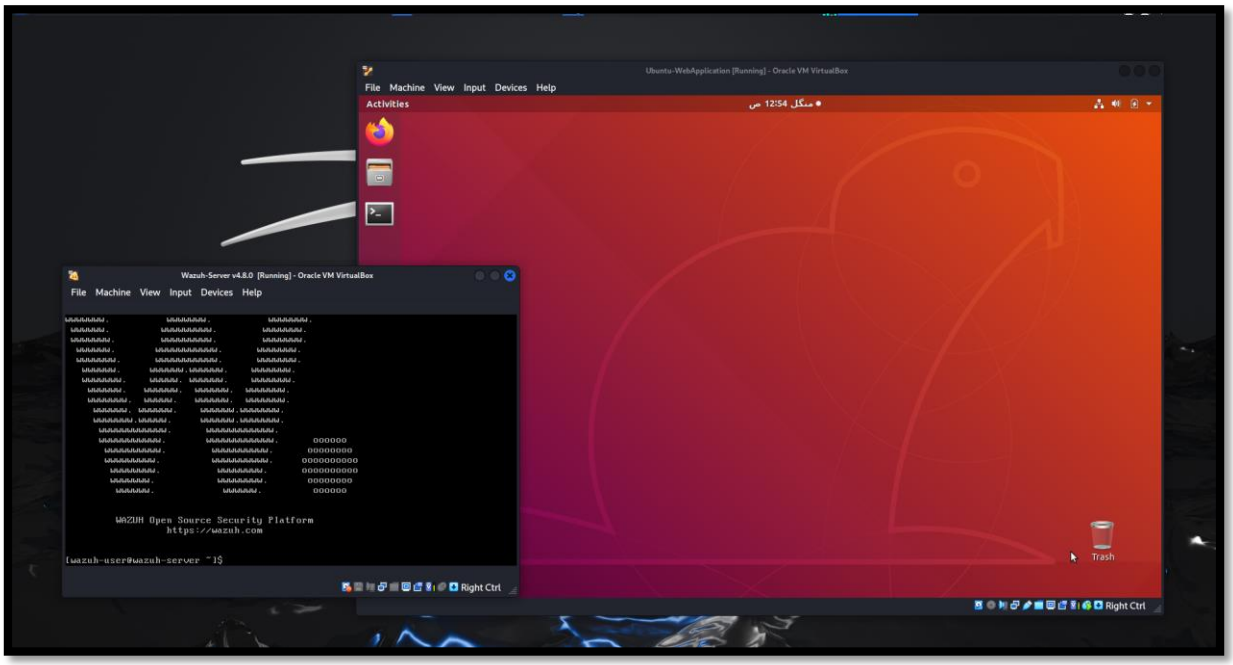
### Configuration:

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.

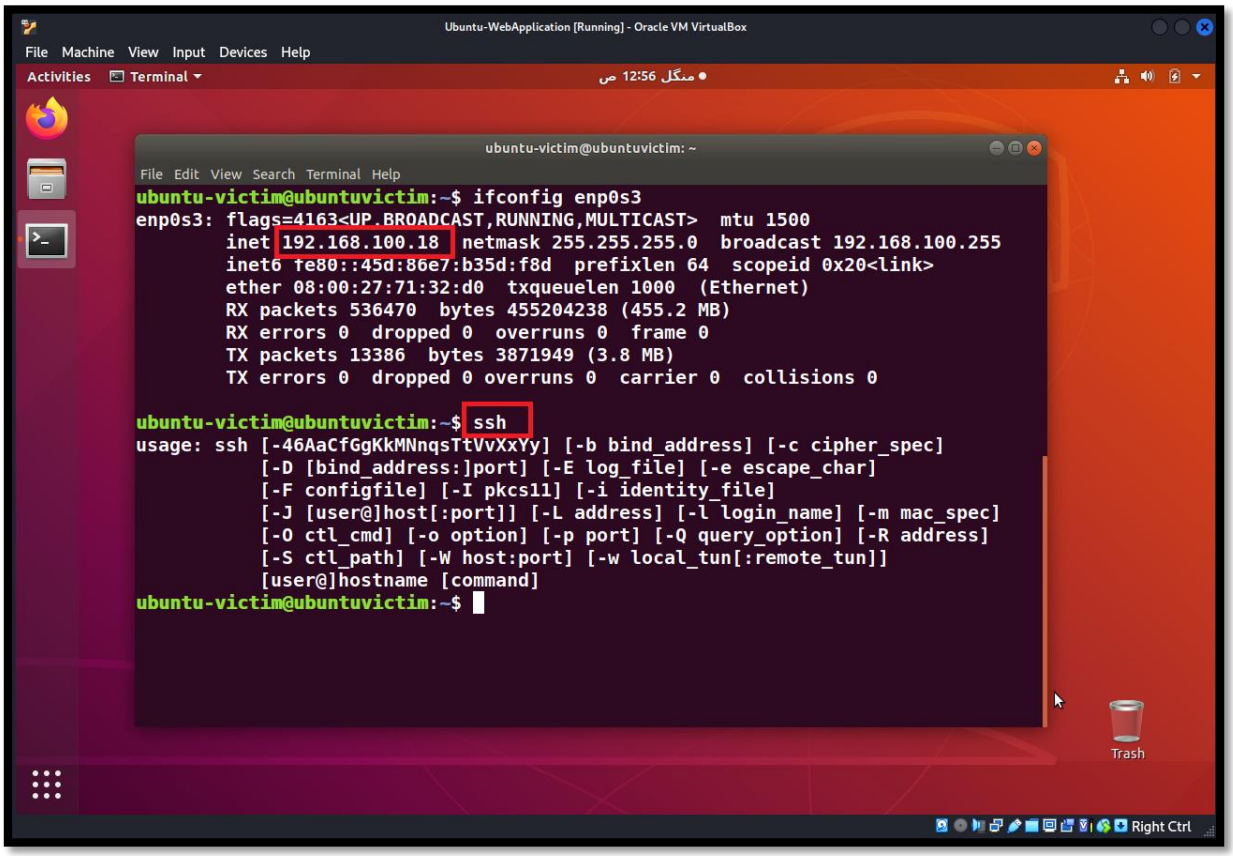
### Response:

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.

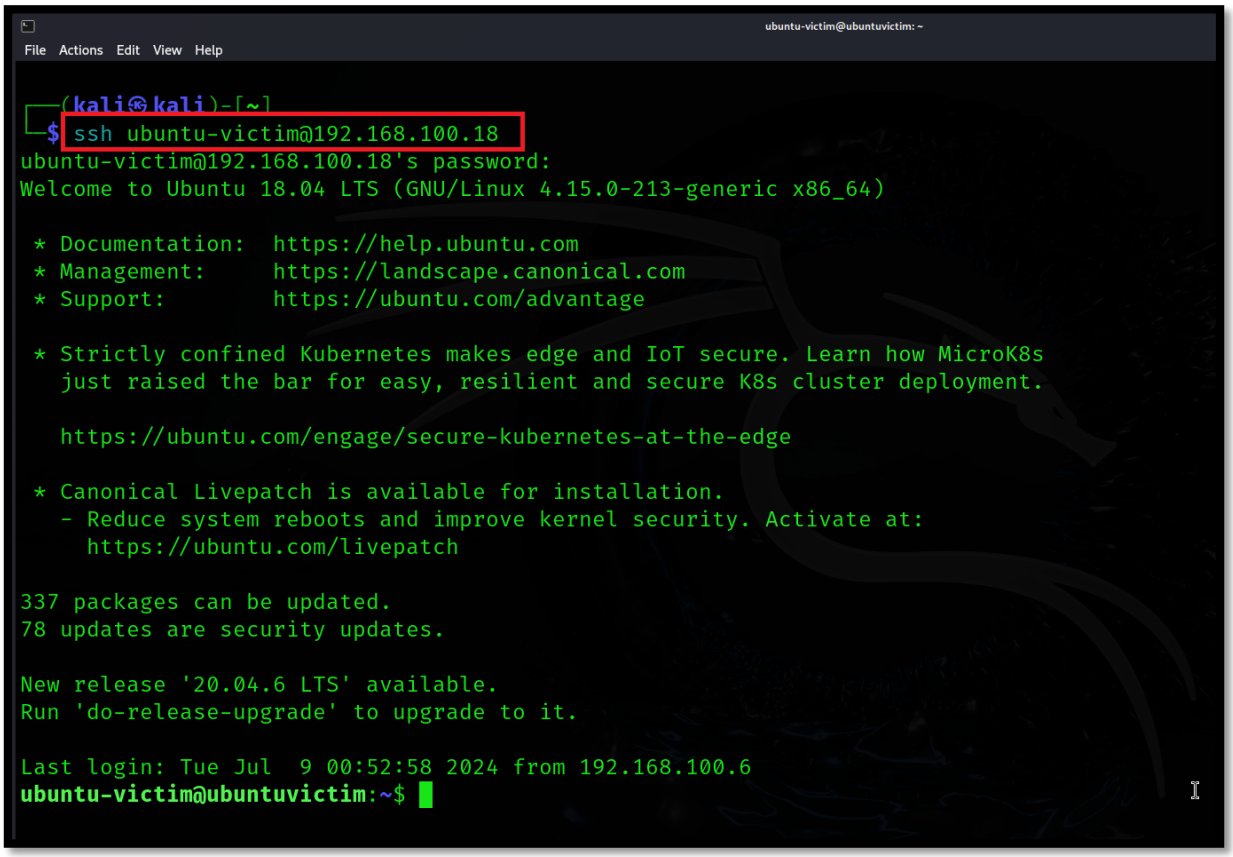
Here is my Wazuh server running along with Ubuntu machine on virtualbox.



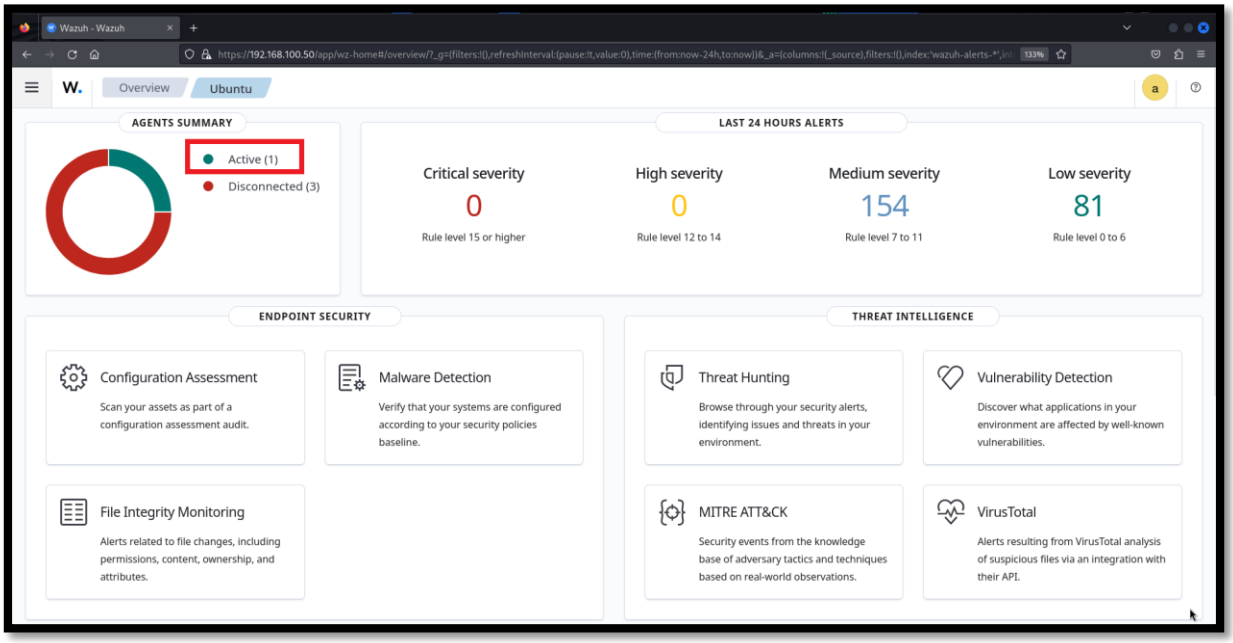

Ubuntu machine IP address “192.168.100.18” and SSH service is running.



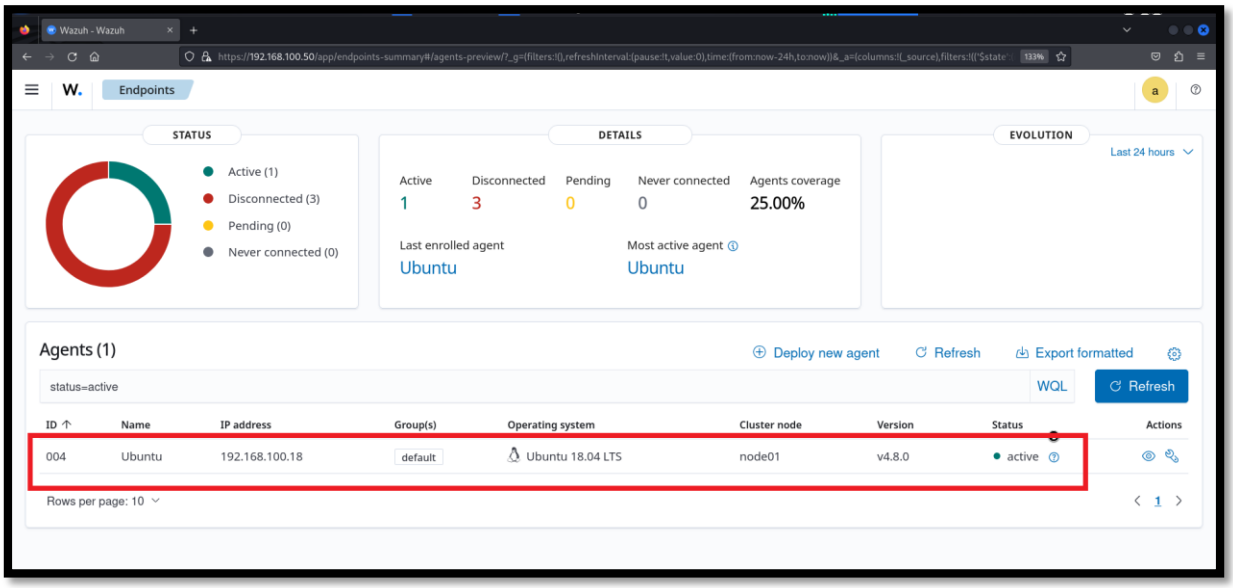
SSH connection establish with Ubuntu machine.

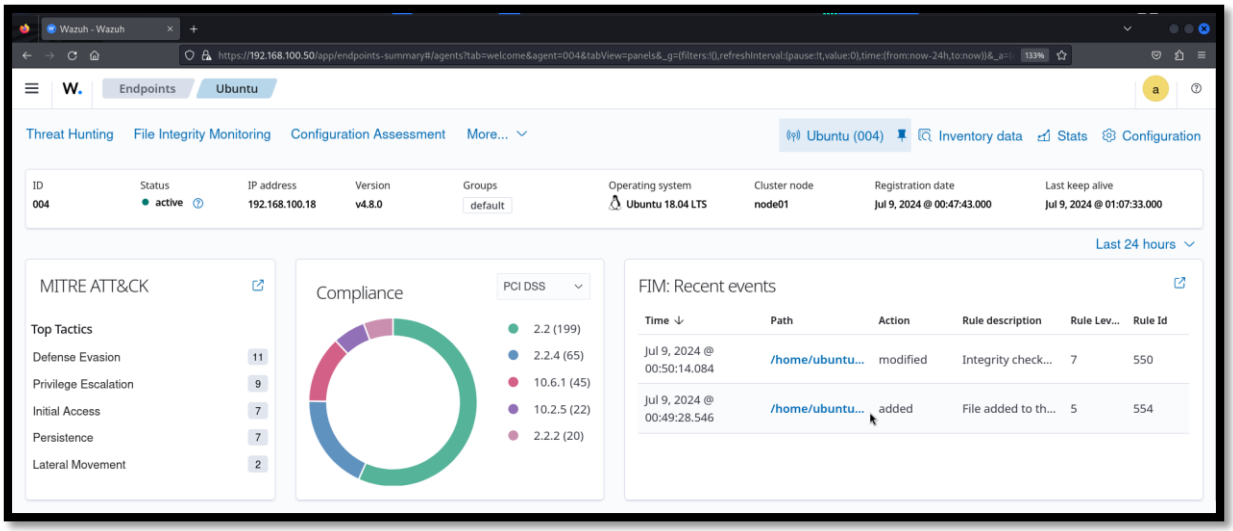



In Wazuh dashboard here is an “Active” agent.



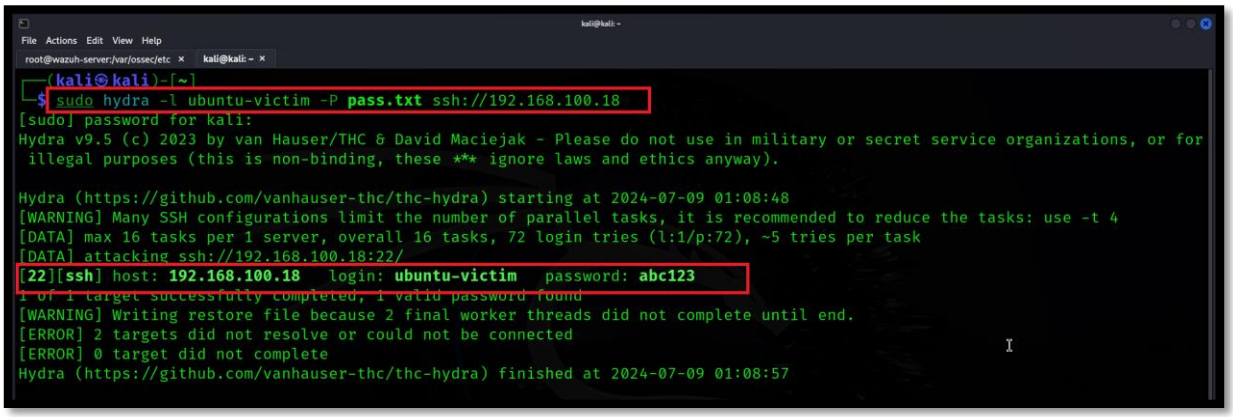
Ubuntu agent is active and running.



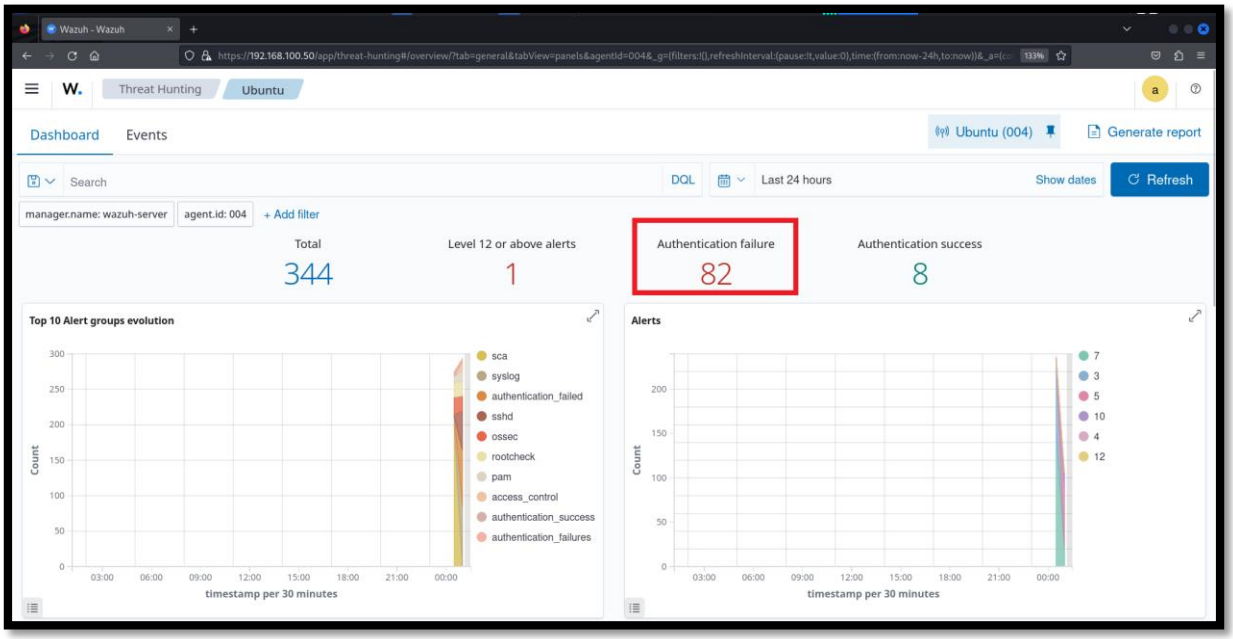

**Step 01:** Now trying to brute-force attack on Ubuntu machine.

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

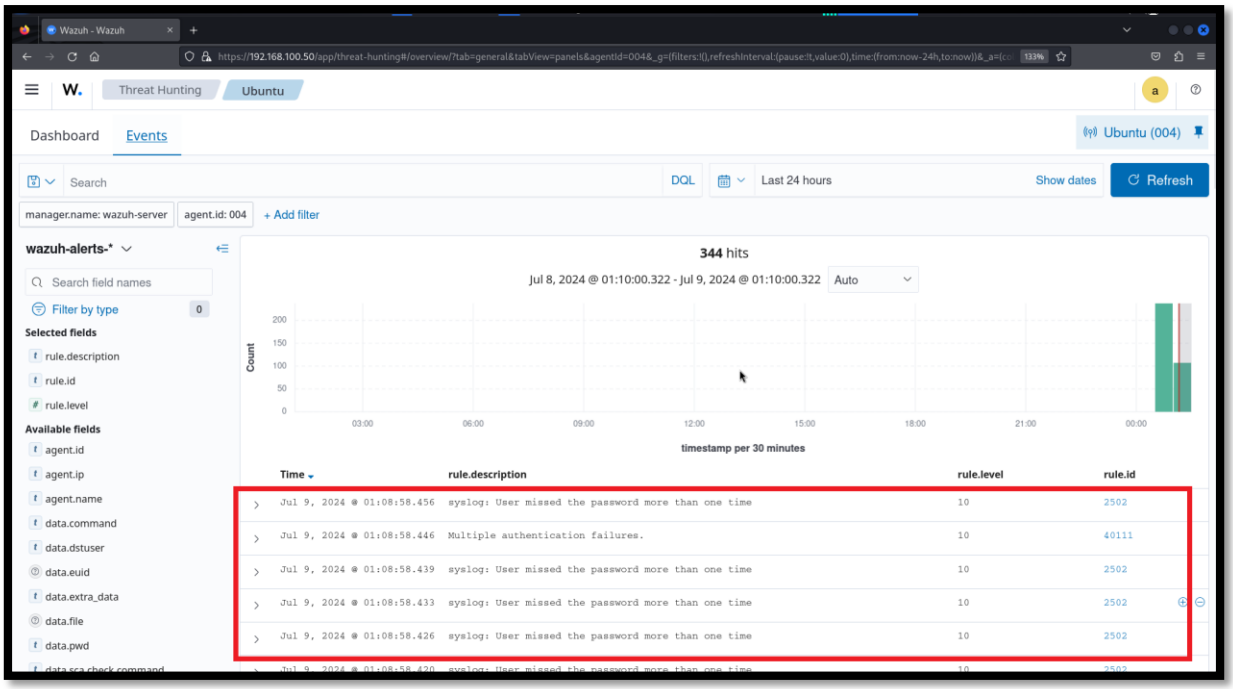


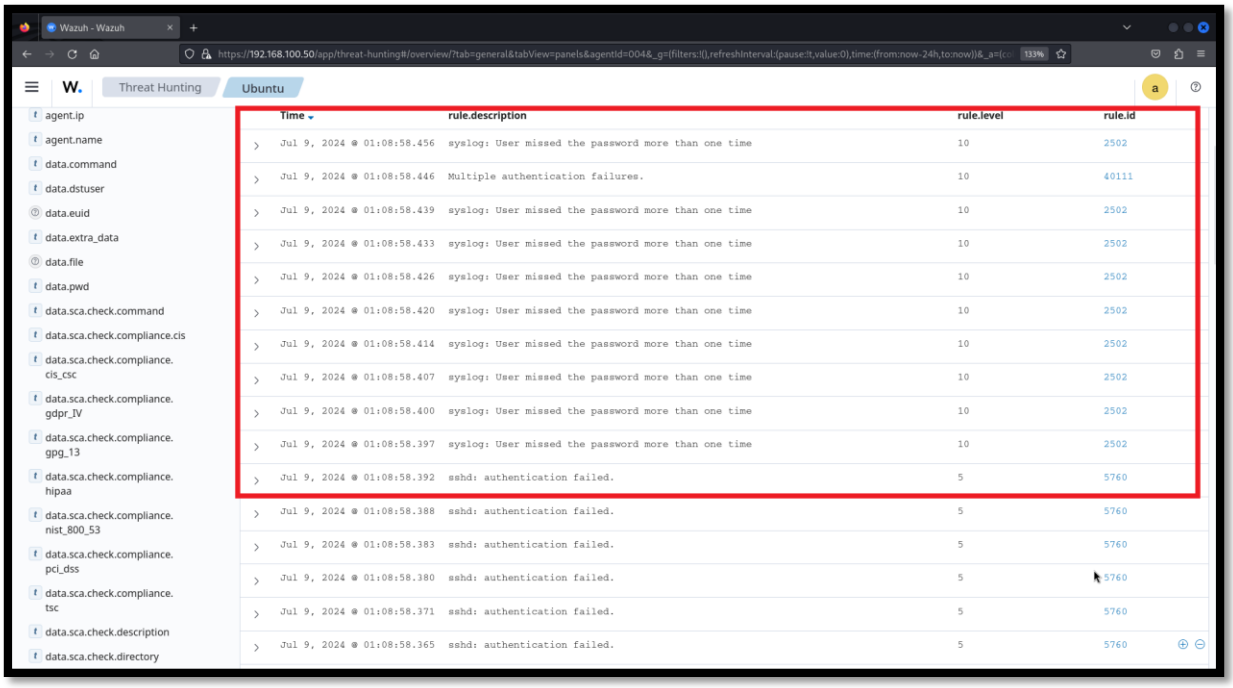
We successfully able to brute-force attack on Ubuntu-victim machine.

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




Now go to “Events” tab and analyze logs.

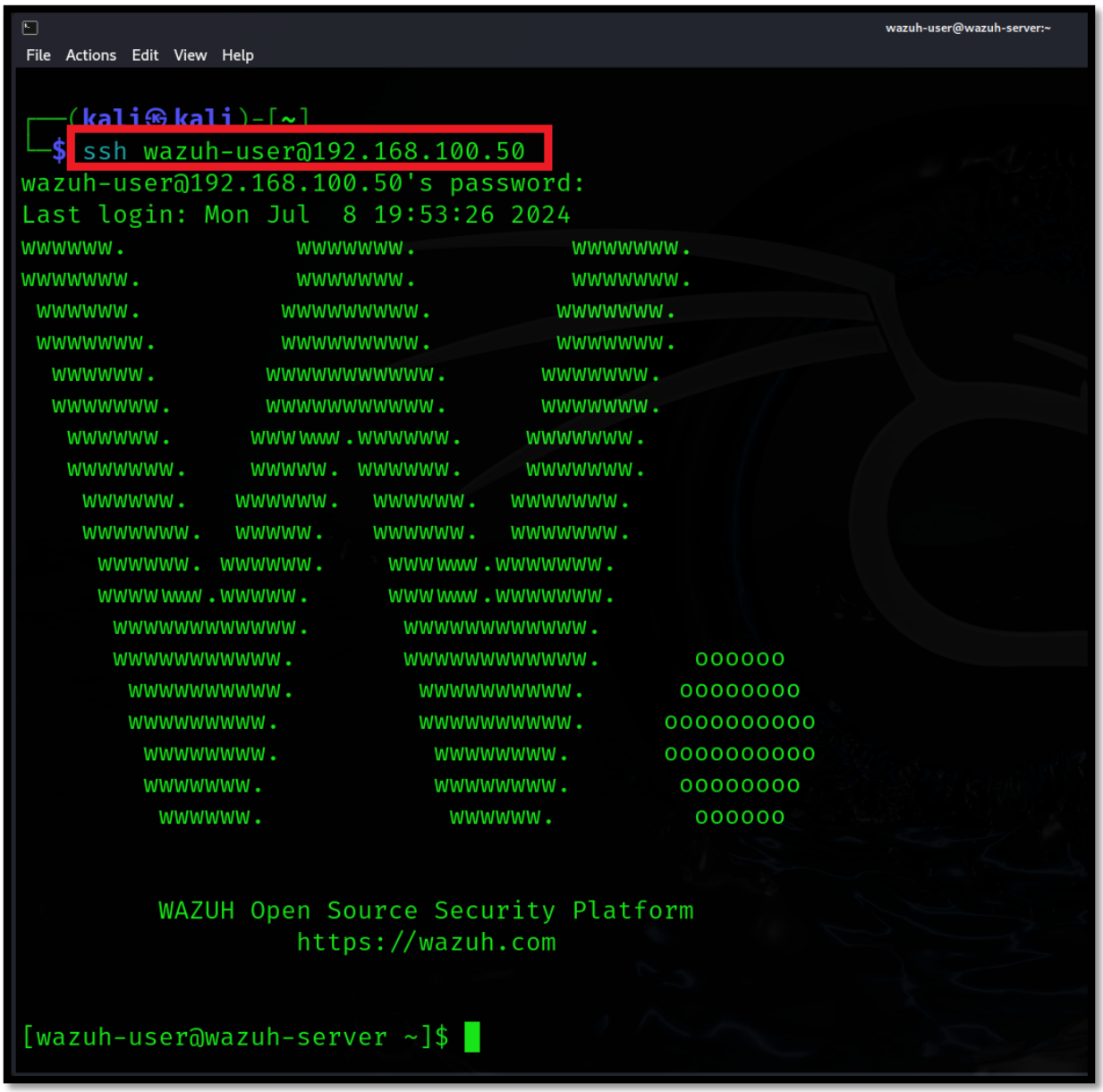



Wazuh - Wazuh
Threat Hunting
Ubuntu
agent.ip
agent.name
data.command
data.dstuser
data.euid
data.extra_data
data.file
data.pwd
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc
data.sca.check.compliance.gdpr_IV
data.sca.check.compliance.gpg_13
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.tsc
data.sca.check.description
data.sca.check.directory
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
_index wazuh-alerts-4.x-2024.07.08
agent.id 004
agent.ip 192.168.100.18
agent.name Ubuntu
data.dstuser ubuntu-victim
data.srcip 192.168.100.6
data.srcport 44052
decoder.name sshd
decoder.parent sshd
full_log Jul 9 01:08:56 mail sshd[8962]: Failed password for ubuntu-victim from 192.168.100.6 port 44052 ssh2
id 1720469338.625277
input.type log
location /var/log/auth.log
manager.name wazuh-server

| | | |
|---|---|---|
| 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




Now edit the “ossec.conf” file.

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

```
root@wazuh-server:/var/ossec/etc
File  Actions  Edit  View  Help
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]#
```

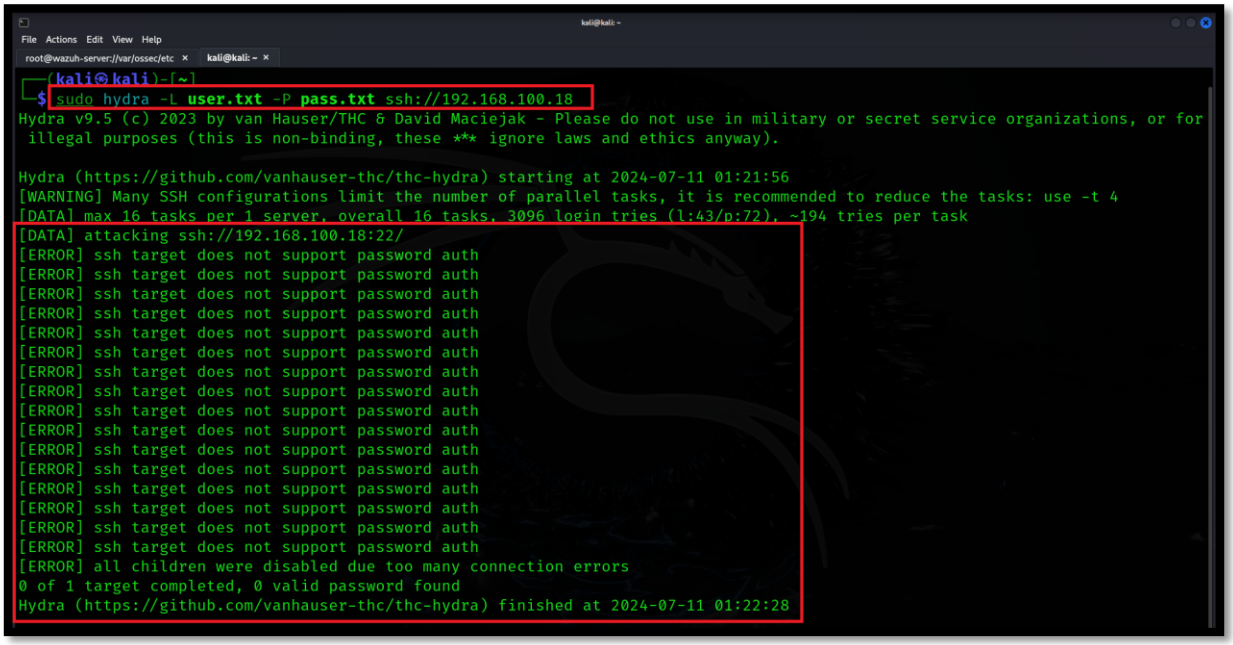
After restart wazuh manager we have to restart wazuh agent.

Command: sudo systemctl restart wazuh-agent

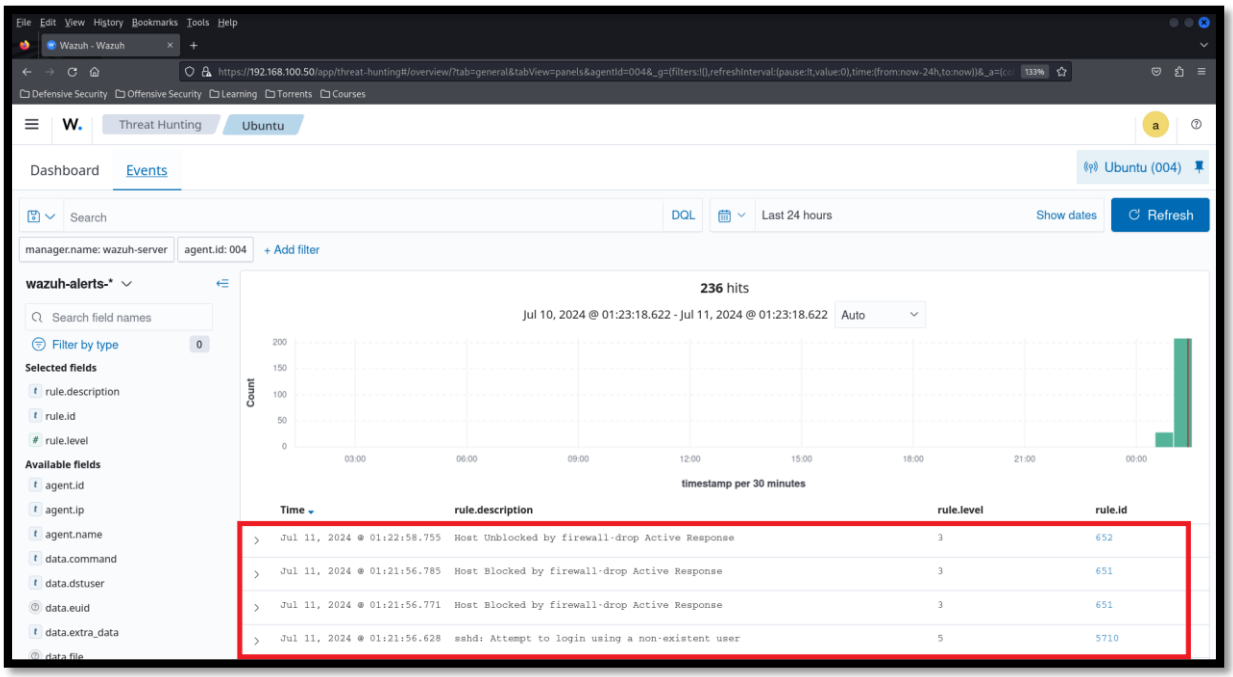
```
root@ubuntuvictim: ~
File  Edit  View  Search  Terminal  Help
root@ubuntuvictim:~# sudo systemctl restart wazuh-agent
root@ubuntuvictim:~#
```

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.




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



Ubuntu

| 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

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 |

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

| | |
|---|---|
| data.parameters.alert.rule.hipaa | 164.312.b |
| data.parameters.alert.rule.id | 5710 |
| 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, AU.6 |
| data.parameters.alert.rule.pci_dss | 10.2.4, 10.2.5, 10.6.1 |
| data.parameters.alert.rule.tsc | CC6.1, CC6.8, CC7.2, CC7.3 |
| data.parameters.alert.timestamp | 2024-07-10T20:21:56.628+0000 |
| data.parameters.extra_args | |
| data.parameters.program | active-response/bin/firewall-drop |
| data.srcip | 192.168.100.6 |
| data.version | 1 |
| decoder.name | ar_log_json |

| | |
|---|---|
| t decoder.name | ar_log_json |
| t decoder.parent | ar_log_json |
| t full_log | 2024/07/11 01:21:55 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2024-07-10T20:21:56.628+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"],"technique":["Password Guessing","SSH"]},"firedtimes":2,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7",[redacted] |
| 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
LinkedIn: www.linkedin.com/in/moizuddinrafay