Wazuh Proof-of-Concept Lab Report

Task 01: Wazuh POC Setup and Use Case Demonstration
Student Name: Sheeza Alam Khan

Date: 21 November 2025

1. Objective

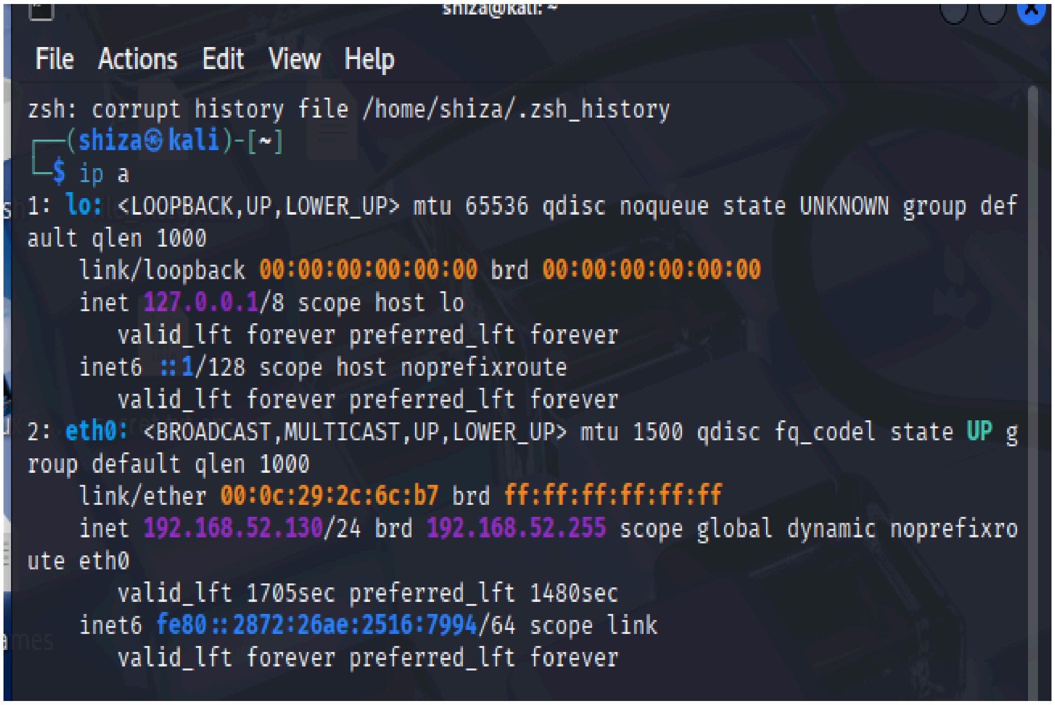
Successfully deploy a fully functional Wazuh environment and demonstrate its real-time detection capabilities using an SSH brute-force attack scenario.

2. Lab Environment Overview

Component	Name	IP Address	Role	Wazuh Version
Wazuh All-in-One	Wazuh-Server	192.168.52.134	Manager, Indexer, Dashboard	4.14.1
Endpoint 1	Kali Linux	192.168.52.130	Monitored agent	4.14.1
Endpoint 2 (Victim)	vm2	192.168.52.133	Monitored agent (target)	4.14.1
Attacker	Kali Linux	192.168.52.130	Wazuh agent + Hydra tool	4.14.1

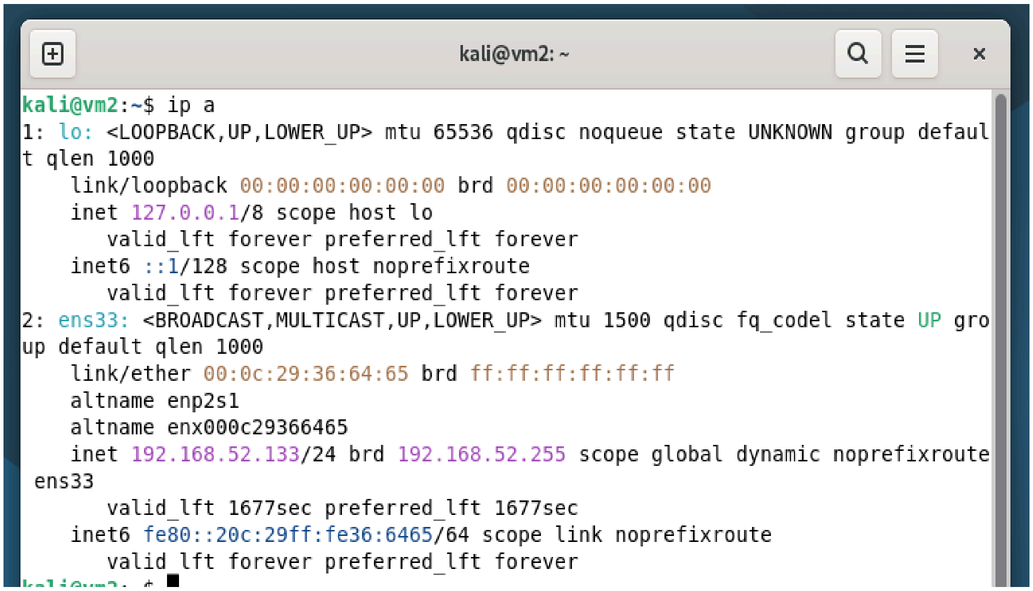
All components were deployed using the official Wazuh Proof-of-Concept OVA and additional VMs in VMware Workstation

Kali Linux:



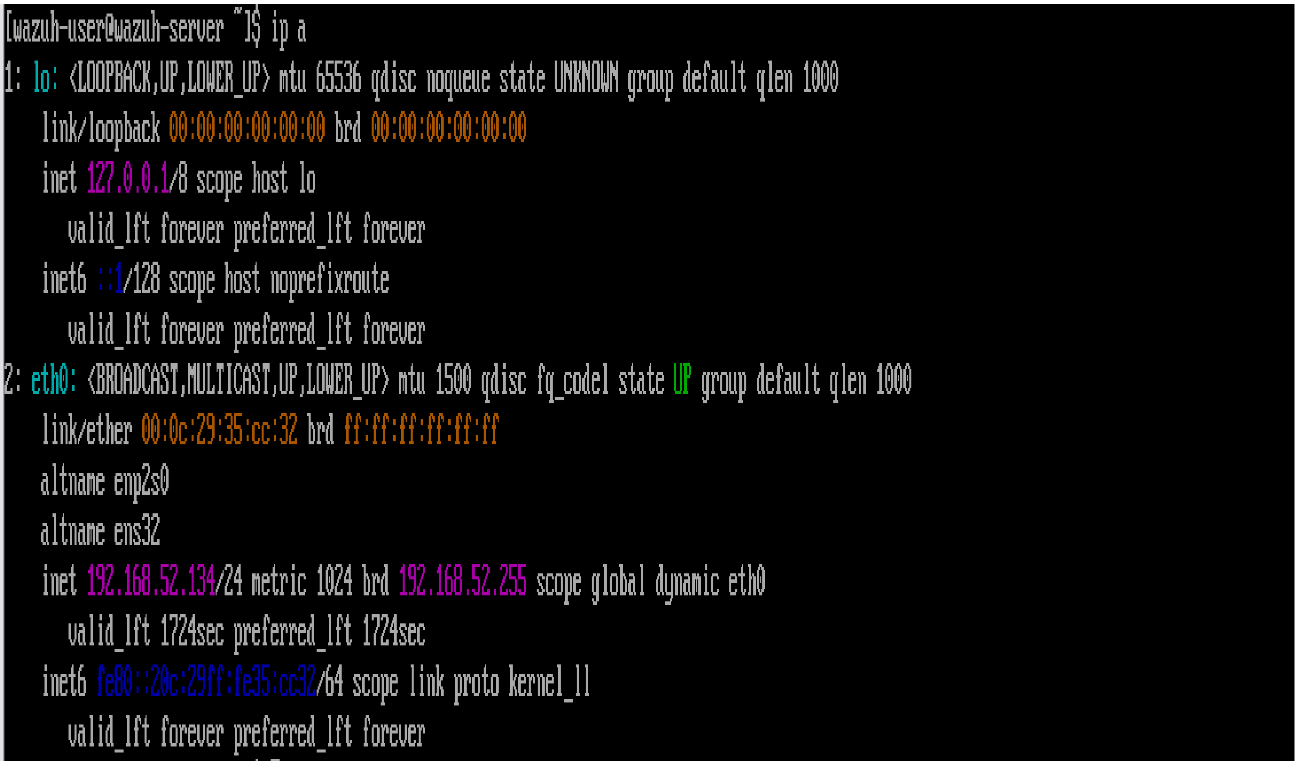
```
zsh: corrupt history file /home/shiza/.zsh_history
┌──(shiza㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft 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 g
roup default qlen 1000
    link/ether 00:0c:29:2c:6c:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.52.130/24 brd 192.168.52.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1705sec preferred_lft 1480sec
    inet6 fe80::2872:26ae:2516:7994/64 scope link
       valid_lft forever preferred_lft forever
```

Vm2:



```
kali@vm2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:36:64:65 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname enx000c29366465
    inet 192.168.52.133/24 brd 192.168.52.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1677sec preferred_lft 1677sec
    inet6 fe80::20c:29ff:fe36:6465/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@vm2:~$
```

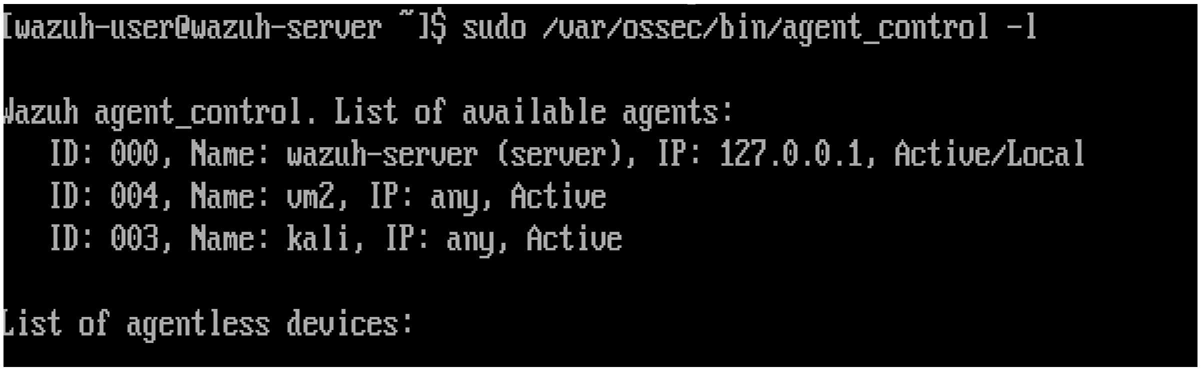
Wazuh-Server:



```
[wazuh-user@wazuh-server ~]$ 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 00:0c:29:35:cc:32 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname ens32
    inet 192.168.52.134/24 metric 1024 brd 192.168.52.255 scope global dynamic eth0
       valid_lft 1724sec preferred_lft 1724sec
    inet6 fe80::20c:29ff:fe35:cc32/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Deployment Steps (Evidence)

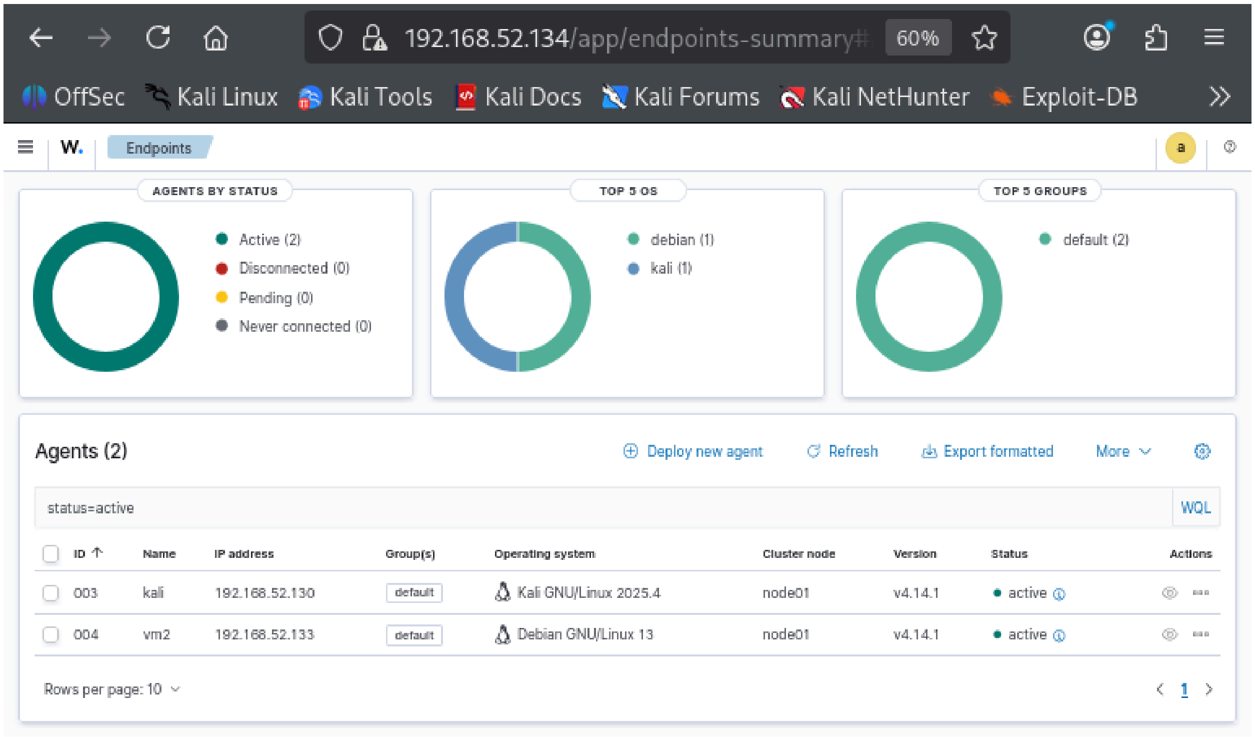
1. Imported and started the official Wazuh All-in-One OVA
2. Added and registered three agents (Wazuh-server, vm2, Kali) using /var/ossec/bin/manage_agents
3. Verified agent connectivity and status in the Wazuh dashboard
4. Confirmed all services (wazuh-manager, wazuh-indexer, wazuh-dashboard) are active



```
[wazuh-user@wazuh-server ~]$ sudo /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
   ID: 000, Name: wazuh-server (server), IP: 127.0.0.1, Active/Local
   ID: 004, Name: vm2, IP: any, Active
   ID: 003, Name: kali, IP: any, Active

List of agentless devices:
```



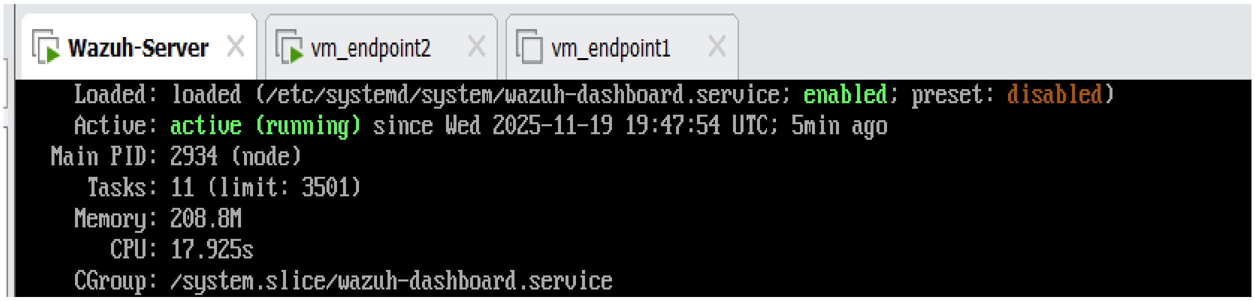
Agents (2)

status=active

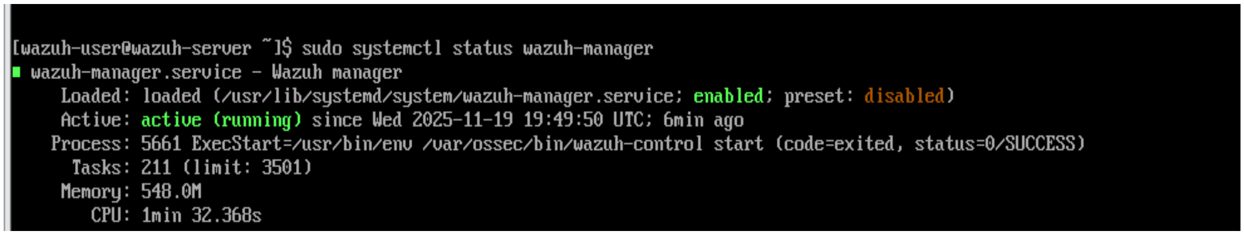
ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
003	kali	192.168.52.130	default	Kali GNU/Linux 2025.4	node01	v4.14.1	● active	
004	vm2	192.168.52.133	default	Debian GNU/Linux 13	node01	v4.14.1	● active	

Rows per page: 10

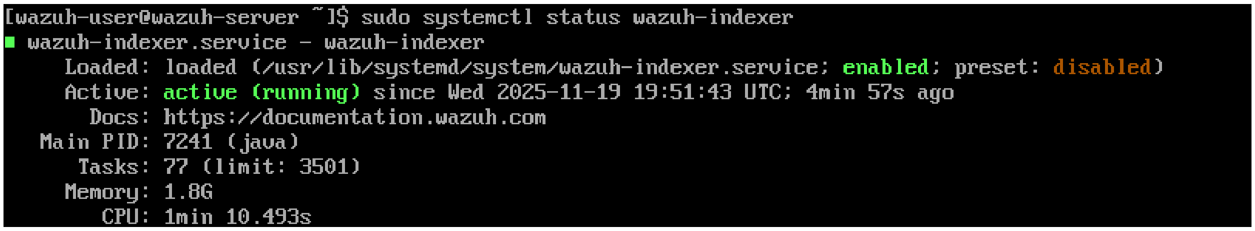
Wazuh-Server: services



```
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; preset: disabled)
   Active: active (running) since Wed 2025-11-19 19:47:54 UTC; 5min ago
 Main PID: 2934 (node)
    Tasks: 11 (limit: 3501)
   Memory: 208.8M
      CPU: 17.925s
   CGroup: /system.slice/wazuh-dashboard.service
```

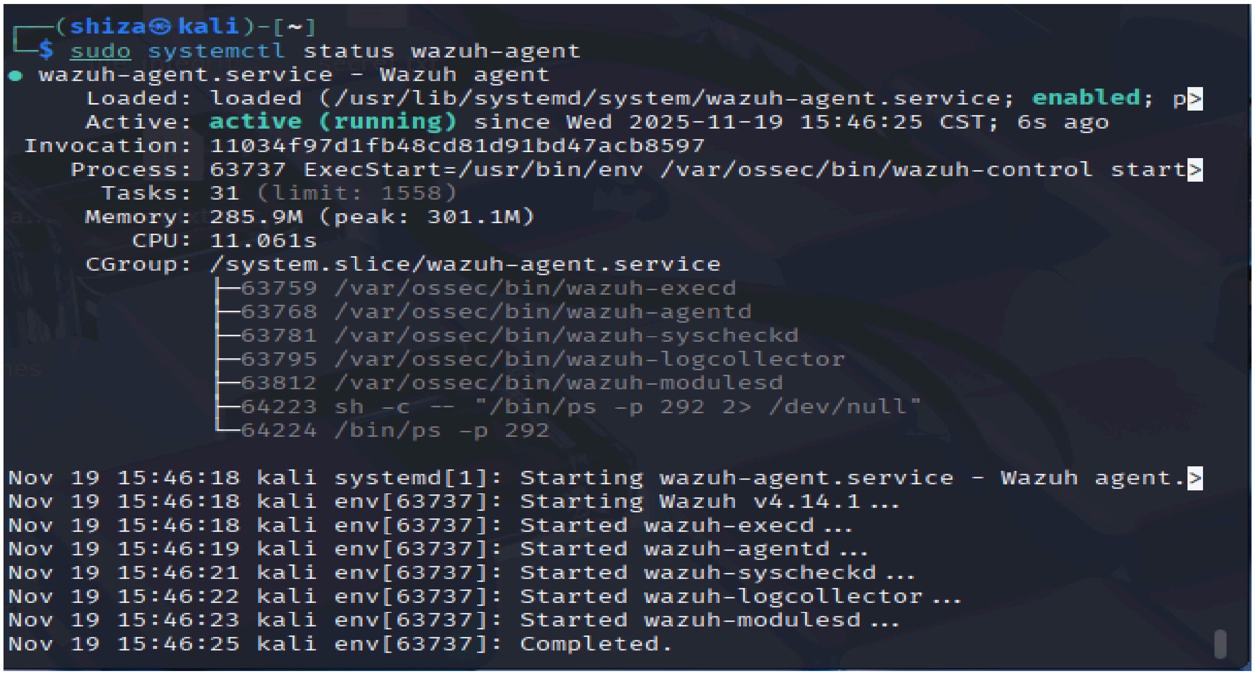


```
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-11-19 19:49:50 UTC; 6min ago
    Process: 5661 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 211 (limit: 3501)
     Memory: 548.0M
        CPU: 1min 32.368s
```



```
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - wazuh-indexer
     Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-11-19 19:51:43 UTC; 4min 57s ago
       Docs: https://documentation.wazuh.com
   Main PID: 7241 (java)
      Tasks: 77 (limit: 3501)
     Memory: 1.8G
        CPU: 1min 10.493s
```

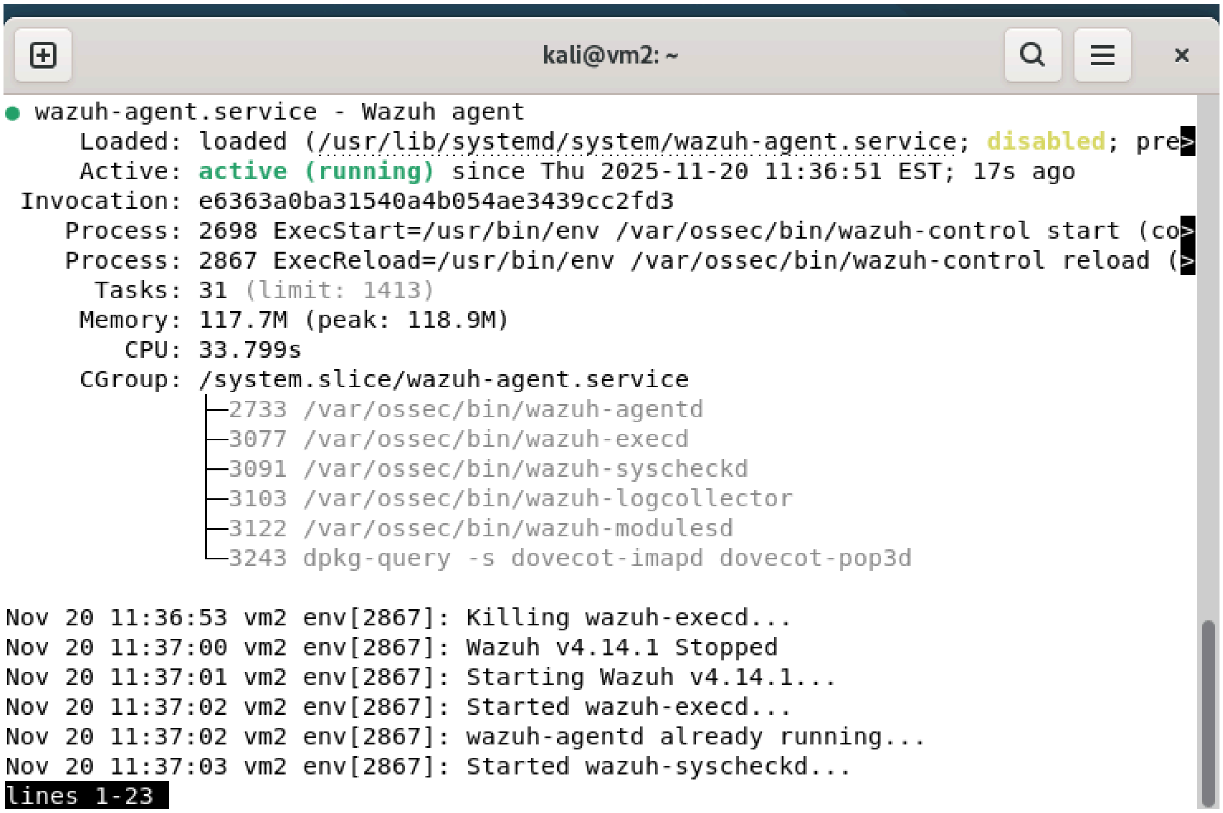
Kali:services



```
┌──(shiza㉿kali)-[~]
└─$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; p>
     Active: active (running) since Wed 2025-11-19 15:46:25 CST; 6s ago
 Invocation: 11034f97d1fb48cd81d91bd47acb8597
    Process: 63737 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start>
      Tasks: 31 (limit: 1558)
     Memory: 285.9M (peak: 301.1M)
        CPU: 11.061s
     CGroup: /system.slice/wazuh-agent.service
             ├─63759 /var/ossec/bin/wazuh-execd
             ├─63768 /var/ossec/bin/wazuh-agentd
             ├─63781 /var/ossec/bin/wazuh-syscheckd
             ├─63795 /var/ossec/bin/wazuh-logcollector
             ├─63812 /var/ossec/bin/wazuh-modulesd
             ├─64223 sh -c -- "/bin/ps -p 292 2> /dev/null"
             └─64224 /bin/ps -p 292

Nov 19 15:46:18 kali systemd[1]: Starting wazuh-agent.service - Wazuh agent.>
Nov 19 15:46:18 kali env[63737]: Starting Wazuh v4.14.1 ...
Nov 19 15:46:18 kali env[63737]: Started wazuh-execd ...
Nov 19 15:46:19 kali env[63737]: Started wazuh-agentd ...
Nov 19 15:46:21 kali env[63737]: Started wazuh-syscheckd ...
Nov 19 15:46:22 kali env[63737]: Started wazuh-logcollector ...
Nov 19 15:46:23 kali env[63737]: Started wazuh-modulesd ...
Nov 19 15:46:25 kali env[63737]: Completed.
```

Vm2:services



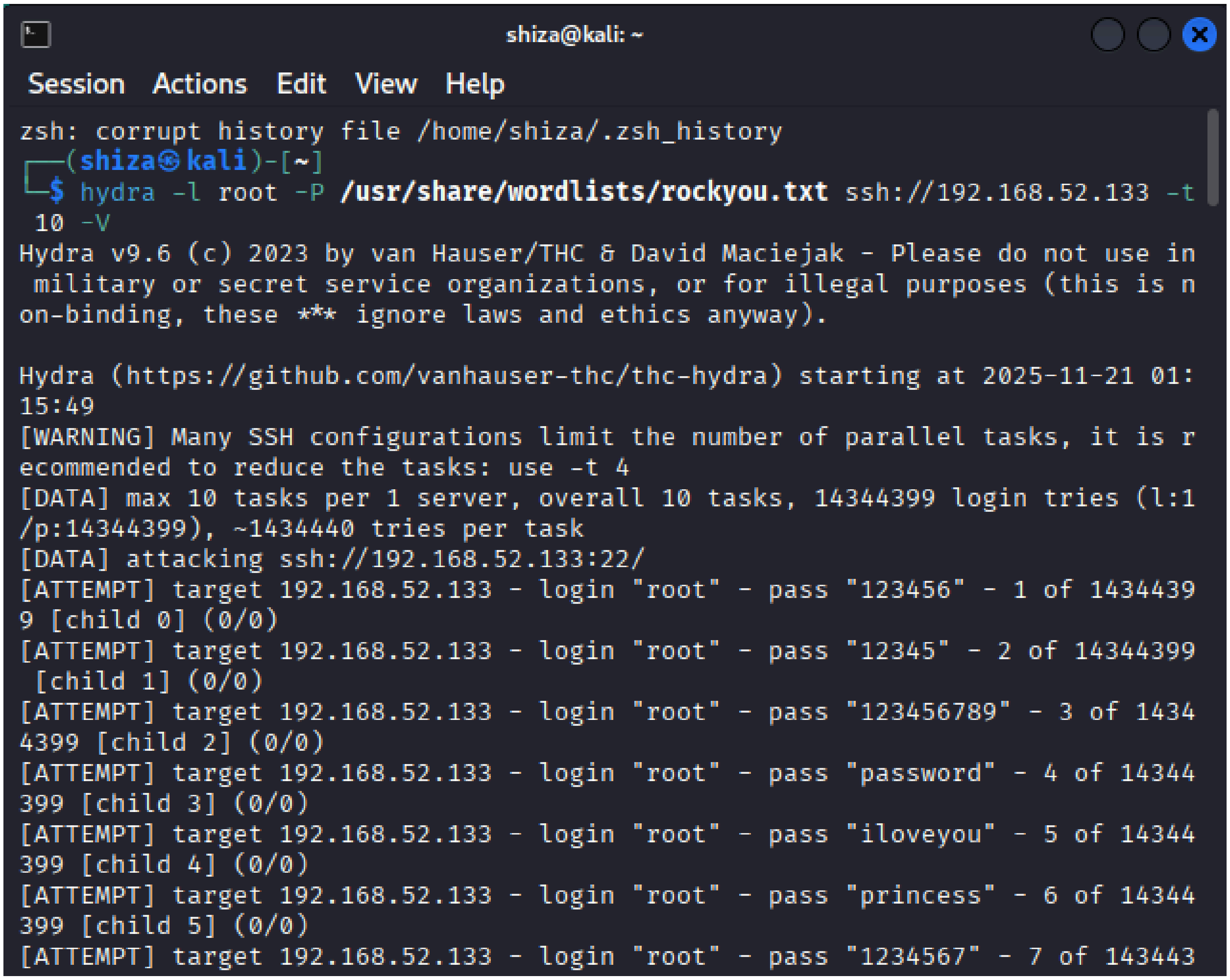
```
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; disabled; pre>
     Active: active (running) since Thu 2025-11-20 11:36:51 EST; 17s ago
 Invocation: e6363a0ba31540a4b054ae3439cc2fd3
    Process: 2698 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (co>
    Process: 2867 ExecReload=/usr/bin/env /var/ossec/bin/wazuh-control reload (>
      Tasks: 31 (limit: 1413)
     Memory: 117.7M (peak: 118.9M)
        CPU: 33.799s
     CGroup: /system.slice/wazuh-agent.service
             ├─2733 /var/ossec/bin/wazuh-agentd
             ├─3077 /var/ossec/bin/wazuh-execd
             ├─3091 /var/ossec/bin/wazuh-syscheckd
             ├─3103 /var/ossec/bin/wazuh-logcollector
             ├─3122 /var/ossec/bin/wazuh-modulesd
             └─3243 dpkg-query -s dovecot-imapd dovecot-pop3d

Nov 20 11:36:53 vm2 env[2867]: Killing wazuh-execd...
Nov 20 11:37:00 vm2 env[2867]: Wazuh v4.14.1 Stopped
Nov 20 11:37:01 vm2 env[2867]: Starting Wazuh v4.14.1...
Nov 20 11:37:02 vm2 env[2867]: Started wazuh-execd...
Nov 20 11:37:02 vm2 env[2867]: wazuh-agentd already running...
Nov 20 11:37:03 vm2 env[2867]: Started wazuh-syscheckd...
lines 1-23
```

4. Use Case: SSH Brute-Force Attack Detection

4.1 Attack Execution

- Attacker: Kali Linux (192.168.52.130)
- Target: vm_endpoint2 (192.168.52.133)
- Tool: Hydra 9.6 with rockyou.txt wordlist
- Command executed: hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.52.133



```
zsh: corrupt history file /home/shiza/.zsh_history
┌──(shiza㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.52.133 -t
 10 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-21 01:
15:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (l:1
/p:14344399), ~1434440 tries per task
[DATA] attacking ssh://192.168.52.133:22/
[ATTEMPT] target 192.168.52.133 - login "root" - pass "123456" - 1 of 1434439
9 [child 0] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "12345" - 2 of 14344399
 [child 1] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "123456789" - 3 of 1434
4399 [child 2] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "password" - 4 of 14344
399 [child 3] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "iloveyou" - 5 of 14344
399 [child 4] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "princess" - 6 of 14344
399 [child 5] (0/0)
[ATTEMPT] target 192.168.52.133 - login "root" - pass "1234567" - 7 of 143443
```

4.2 Detection Results

Wazuh instantly detected and classified the attack:

Metric	Value	Description
Total alerts generated	1,065	During the attack window
Authentication failures	580	Direct result of Hydra attempts
Highest alert level	12	Multiple level 10–12 alerts triggered
MITRE ATTACK Mapping	T1110 Brute Force T1110.001 Password Guessing T1078 Valid Accounts	Correctly mapped to Credential Access tactics
Affected agent	vm2 (192.168.52.133)	Clear victim identification

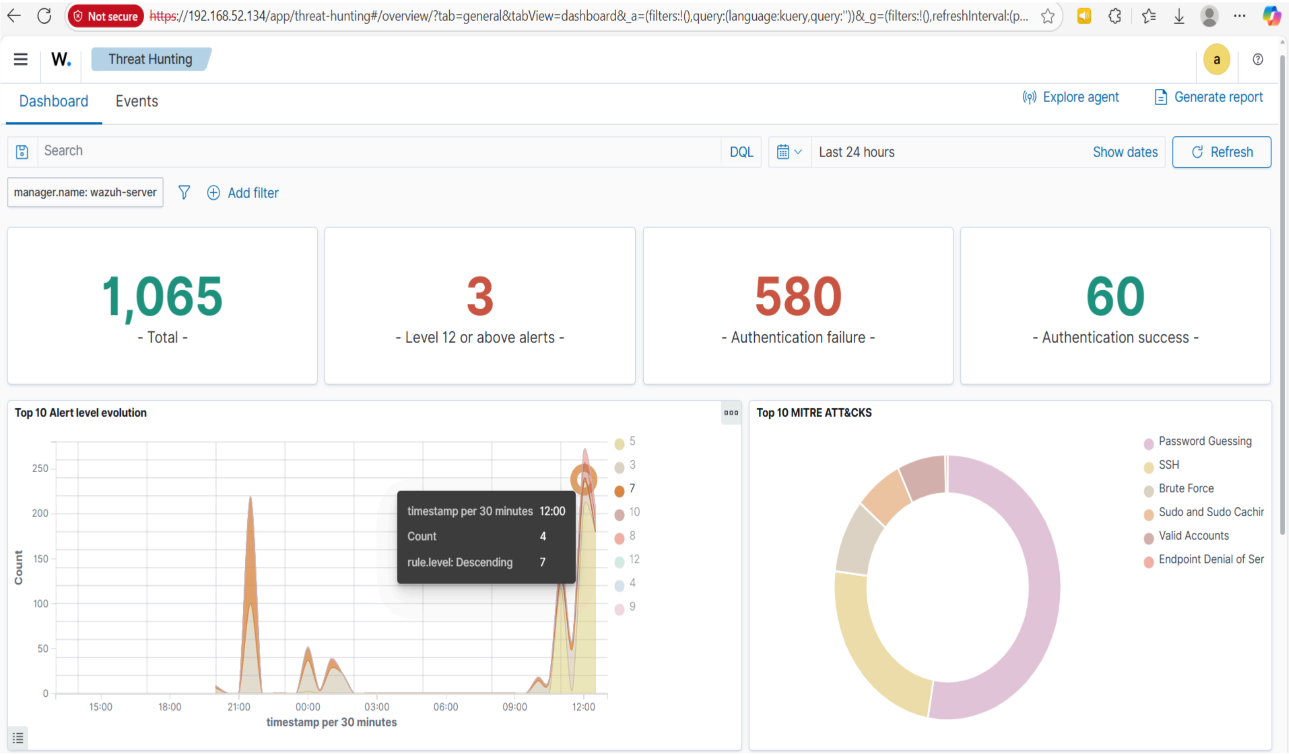
Key rules triggered:

- 40111 – Multiple authentication failures (Level 10)
- 5758 – Maximum authentication attempts exceeded (Level 8)
- 5760 – sshd: authentication failed (Level 5)

4.3 Key Evidence Screenshots

1. **Hydra brute-force attack in progress** (Kali terminal) → Shows real attempts with passwords such as “123456”, “password”, “princess”, etc.
2. **Threat Hunting** → **Overview** → 1,065 total alerts, 580 authentication failures, clear spike during attack time, MITRE ATT&CK showing Brute Force & Password Guessing as top tactics.
3. **Threat Hunting** → **Events list (1,065 hits)** → Detailed list of high-severity alerts on agent “vm2” with descriptions: “Multiple authentication failures.” “Maximum authentication attempts exceeded.” “sshd: authentication failed.”
4. **MITRE ATT&CK Dashboard** → Visual confirmation of attack classification under Credential Access → Brute Force.

Threat Hunting:



https://192.168.52.134/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(p...

Threat Hunting

Dashboard Events

Explore agent Generate report

Search DQL Last 24 hours Show dates Refresh

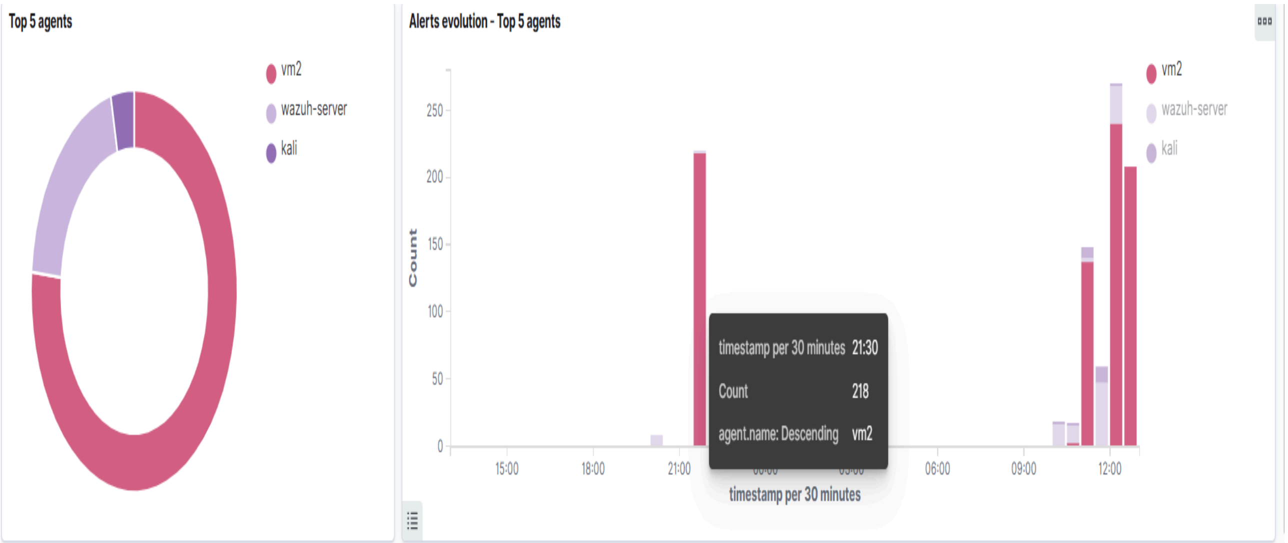
manager.name: wazuh-server Add filter

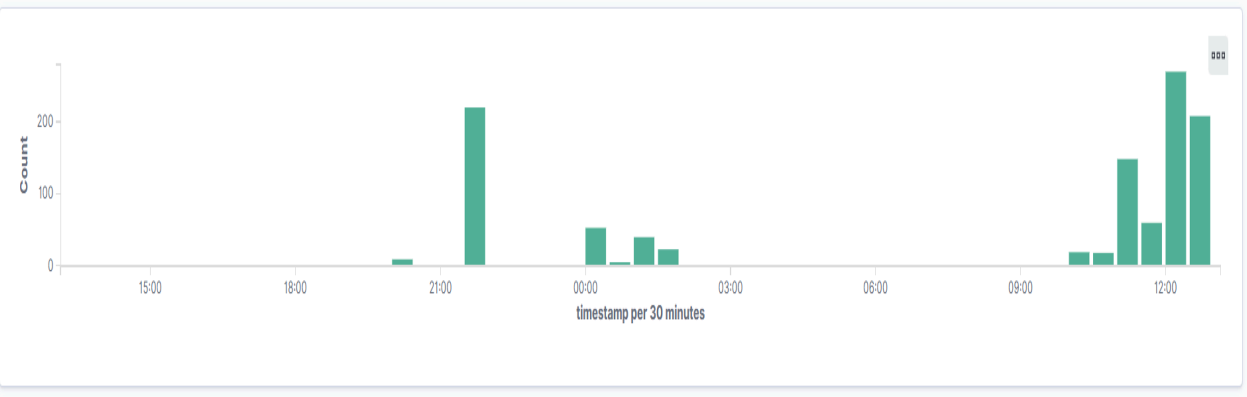
1,065 - Total -

3 - Level 12 or above alerts -

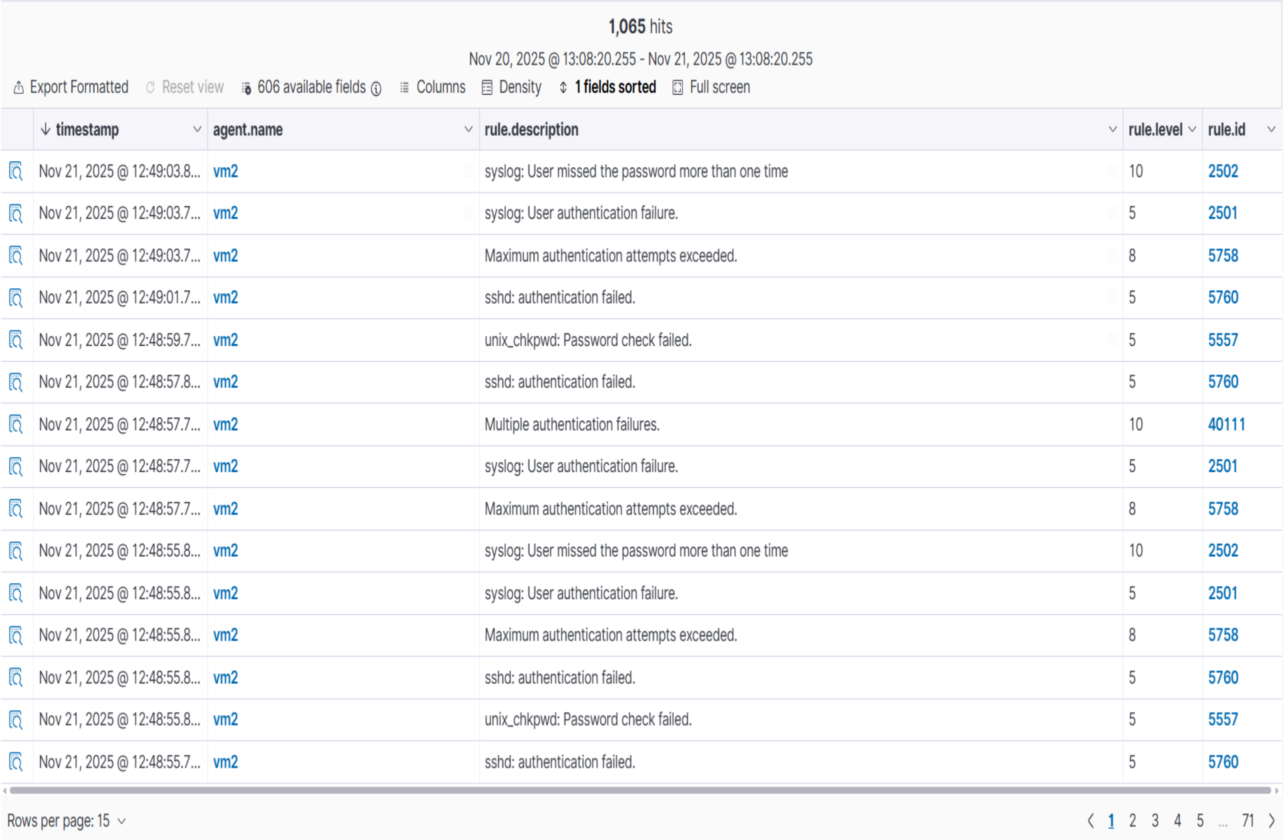
580 - Authentication failure -

60 - Authentication success -





Events:



1,065 hits

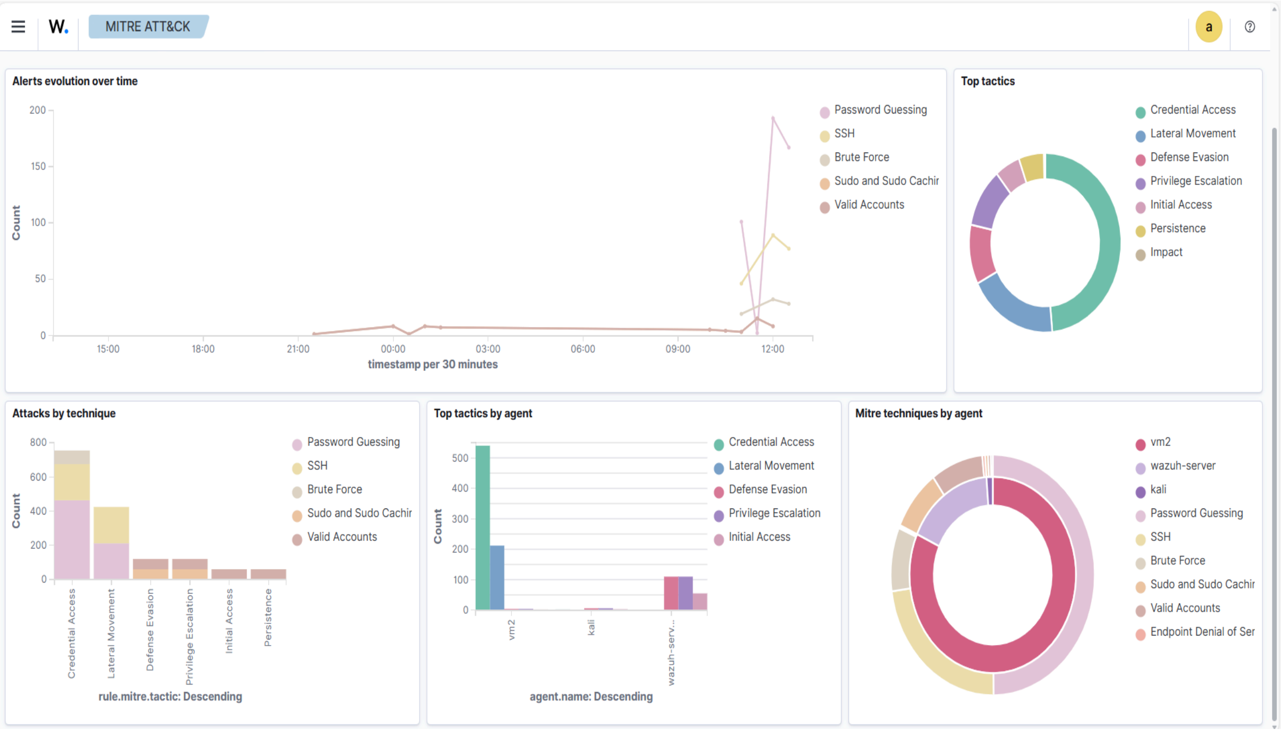
Nov 20, 2025 @ 13:08:20.255 - Nov 21, 2025 @ 13:08:20.255

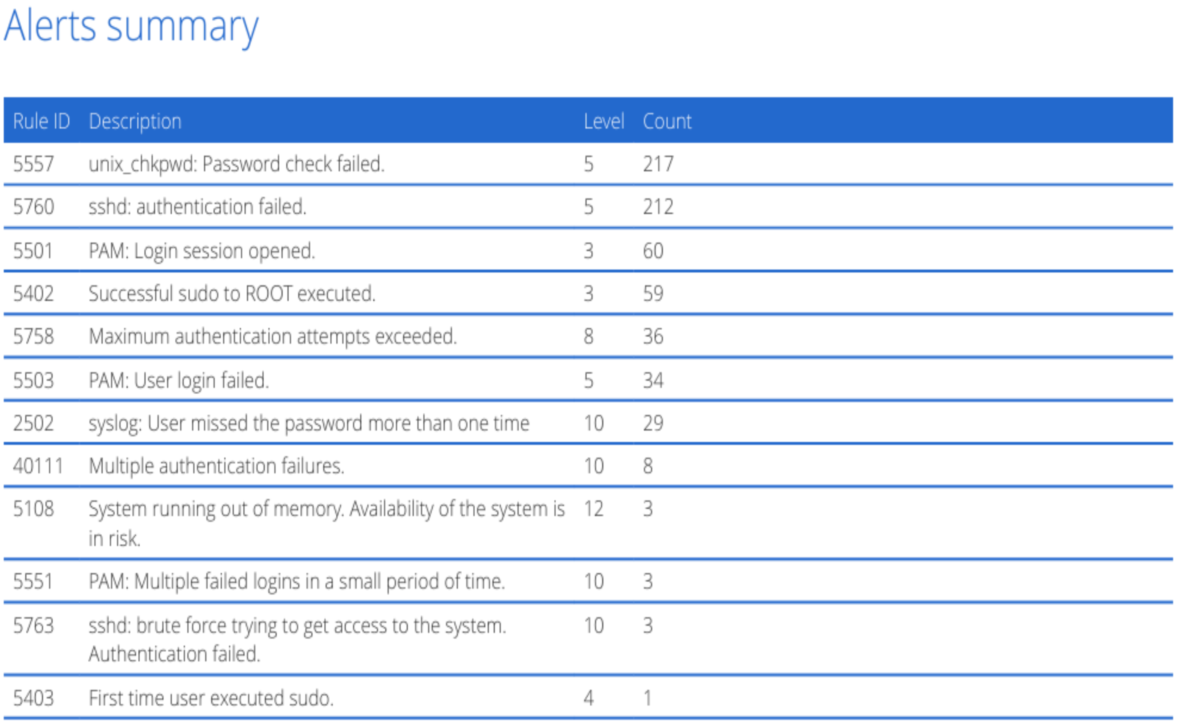
Export Formatted   Reset view   606 available fields   Columns   Density   **1 fields sorted**   Full screen

↓ timestamp	agent.name	rule.description	rule.level	rule.id
Nov 21, 2025 @ 12:49:03.8...	vm2	syslog: User missed the password more than one time	10	2502
Nov 21, 2025 @ 12:49:03.7...	vm2	syslog: User authentication failure.	5	2501
Nov 21, 2025 @ 12:49:03.7...	vm2	Maximum authentication attempts exceeded.	8	5758
Nov 21, 2025 @ 12:49:01.7...	vm2	sshd: authentication failed.	5	5760
Nov 21, 2025 @ 12:48:59.7...	vm2	unix_chkpwd: Password check failed.	5	5557
Nov 21, 2025 @ 12:48:57.8...	vm2	sshd: authentication failed.	5	5760
Nov 21, 2025 @ 12:48:57.7...	vm2	Multiple authentication failures.	10	40111
Nov 21, 2025 @ 12:48:57.7...	vm2	syslog: User authentication failure.	5	2501
Nov 21, 2025 @ 12:48:57.7...	vm2	Maximum authentication attempts exceeded.	8	5758
Nov 21, 2025 @ 12:48:55.8...	vm2	syslog: User missed the password more than one time	10	2502
Nov 21, 2025 @ 12:48:55.8...	vm2	syslog: User authentication failure.	5	2501
Nov 21, 2025 @ 12:48:55.8...	vm2	Maximum authentication attempts exceeded.	8	5758
Nov 21, 2025 @ 12:48:55.8...	vm2	sshd: authentication failed.	5	5760
Nov 21, 2025 @ 12:48:55.8...	vm2	unix_chkpwd: Password check failed.	5	5557
Nov 21, 2025 @ 12:48:55.7...	vm2	sshd: authentication failed.	5	5760

Rows per page: 15   ‹ 1 2 3 4 5 ... 71 ›

MITRE ATTACK Dashboard





Alerts summary

Rule ID	Description	Level	Count
5557	unix_chkpwd: Password check failed.	5	217
5760	sshd: authentication failed.	5	212
5501	PAM: Login session opened.	3	60
5402	Successful sudo to ROOT executed.	3	59
5758	Maximum authentication attempts exceeded.	8	36
5503	PAM: User login failed.	5	34
2502	syslog: User missed the password more than one time	10	29
40111	Multiple authentication failures.	10	8
5108	System running out of memory. Availability of the system is in risk.	12	3
5551	PAM: Multiple failed logins in a small period of time.	10	3
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	3
5403	First time user executed sudo.	4	1