Bootcamp Analista SOC Nivel 1 - 2025

Comunidad DOJO - WoSEC Panamá

Nombre y Apellido: Ingrid Kaufmann

Email: ingridkaufmannok@gmail.com

Agosto 2025

Implementación de Wazuh

Evidencia N.º 1:

Máquina virtual iniciada. Datos de acceso:

user **wazuh-user**

password **wazuh**

Evidencia N.º 2:

Validación de IP con **ip addr**.

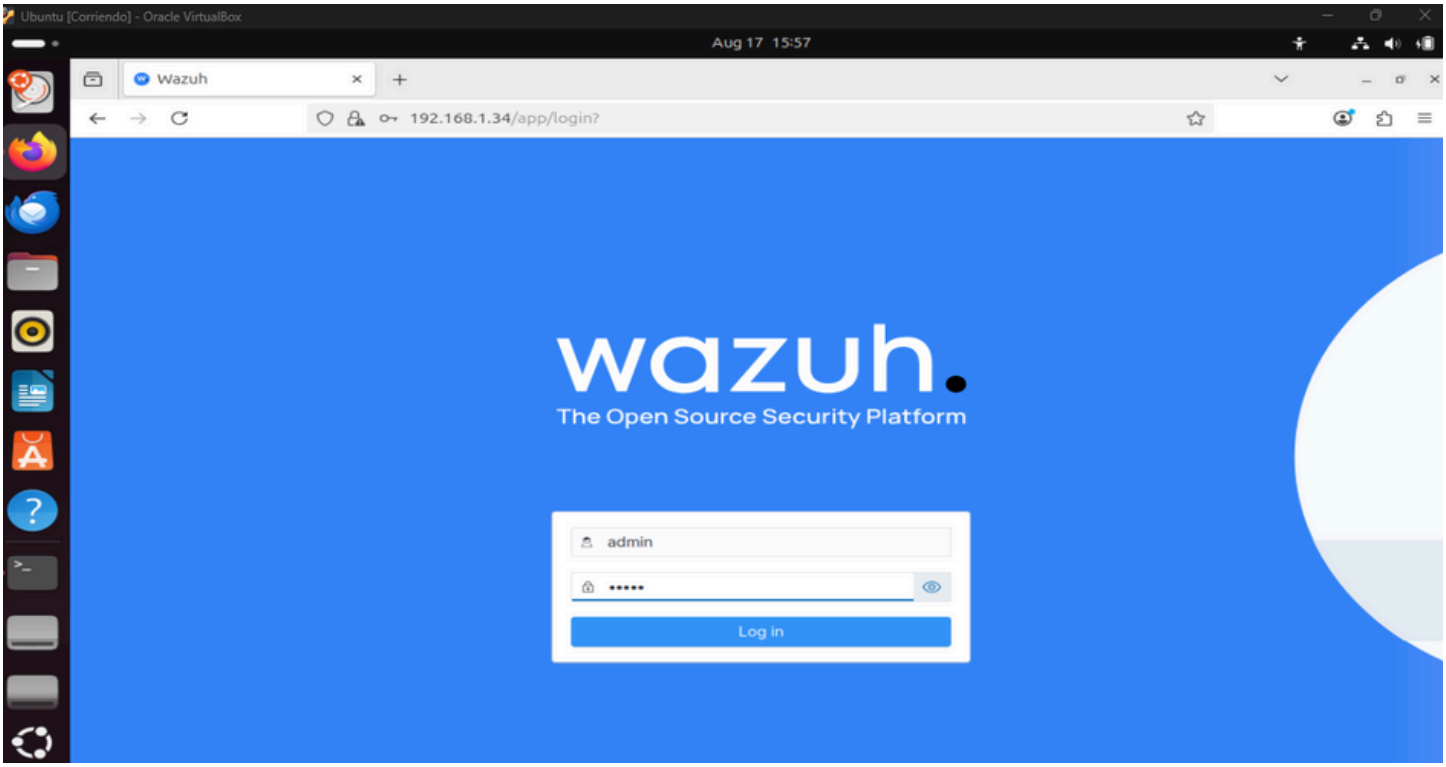
```
      wwwwwww. wwwwwww.     wwwwwww.wwwwwww.
     wwwwwwww.wwwww.      wwwwwww.wwwwwwww.
      wwwwwwwwwwwww.       wwwwwwwwwwwwww.
      wwwwwwwwwwww.        wwwwwwwwwwwwww.       ooooooo
       wwwwwwwwwww.         wwwwwwwwwwww.      oooooooo
       wwwwwwwwww.          wwwwwwwwwwww.     oooooooooo
        wwwwwwwww.           wwwwwwwwww.      oooooooooo
        wwwwwwww.            wwwwwwwwww.      oooooooo
         wwwwwww.             wwwwwww.        ooooooo


         WAZUH Open Source Security Platform
                   https://wazuh.com
[wazuh-user@wazuh-server ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
p default qlen 1000
    link/ether 08:00:27:24:f2:e1 brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 192.168.1.34/24 metric 1024 brd 192.168.1.255 scope global dynamic
       valid_lft 86298sec preferred_lft 86298sec
    inet6 fe80::a00:27ff:fe24:f2e1/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

Evidencia N.º 3:

Acceso desde el navegador de Mozilla Firefox al servidor de Wazuh. Credenciales de acceso:

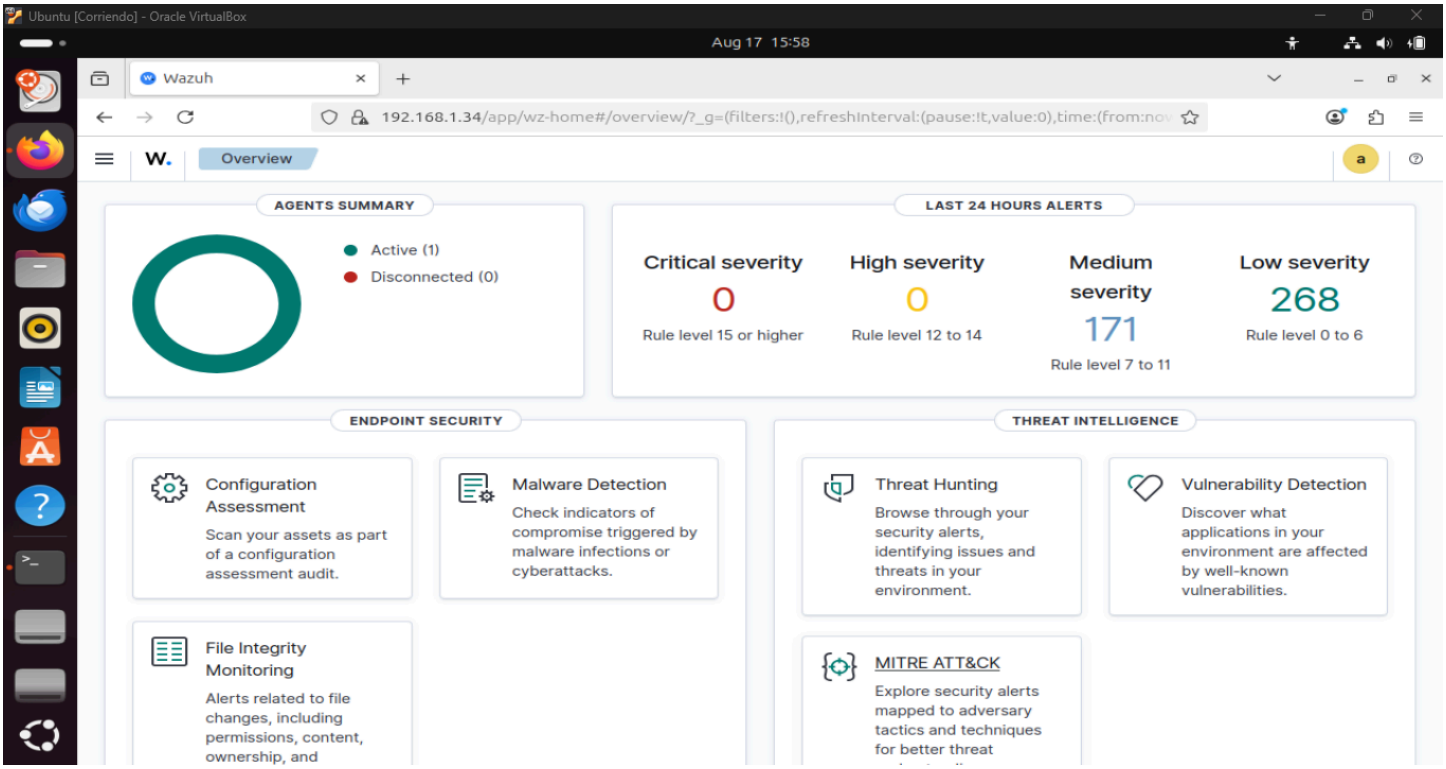
user **admin**

password **admin**



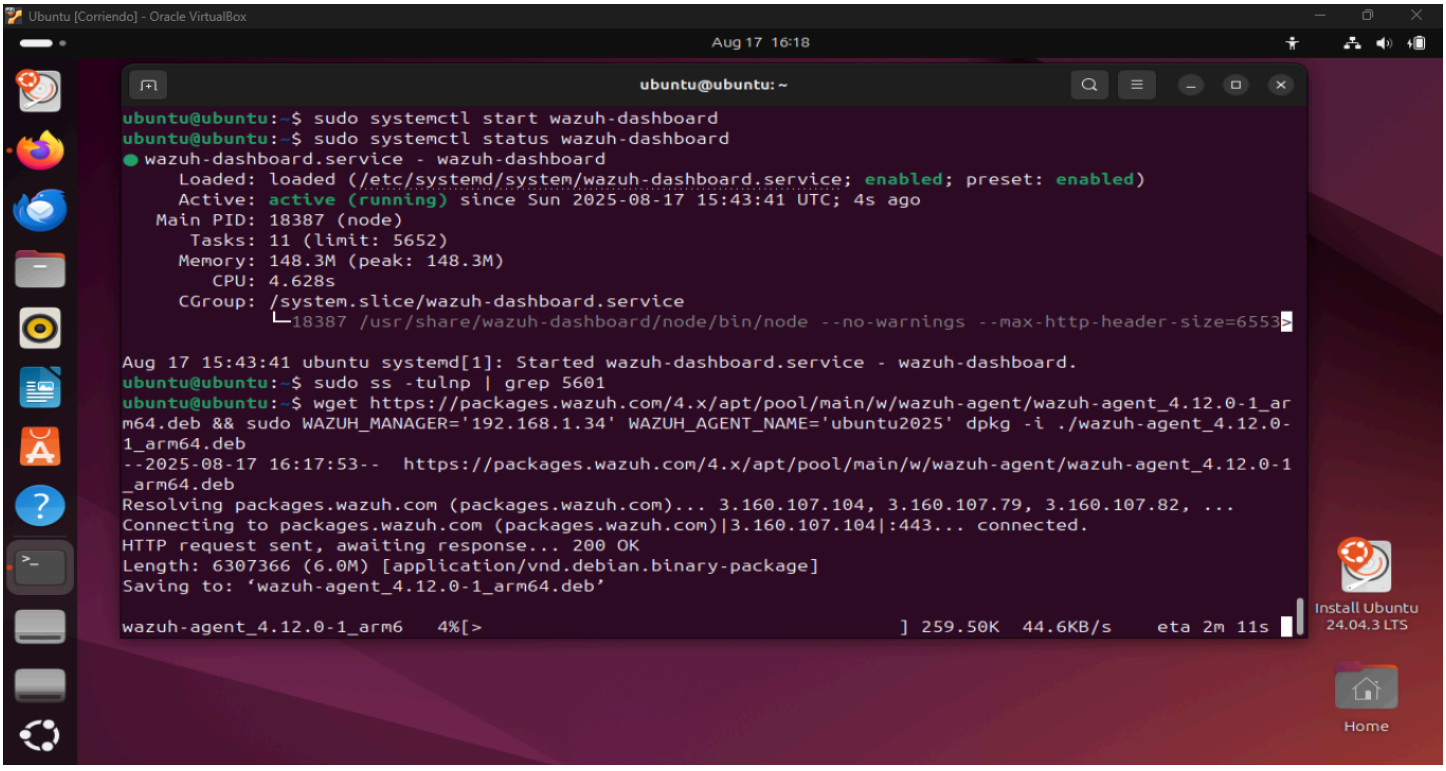
Evidencia N.º 4:

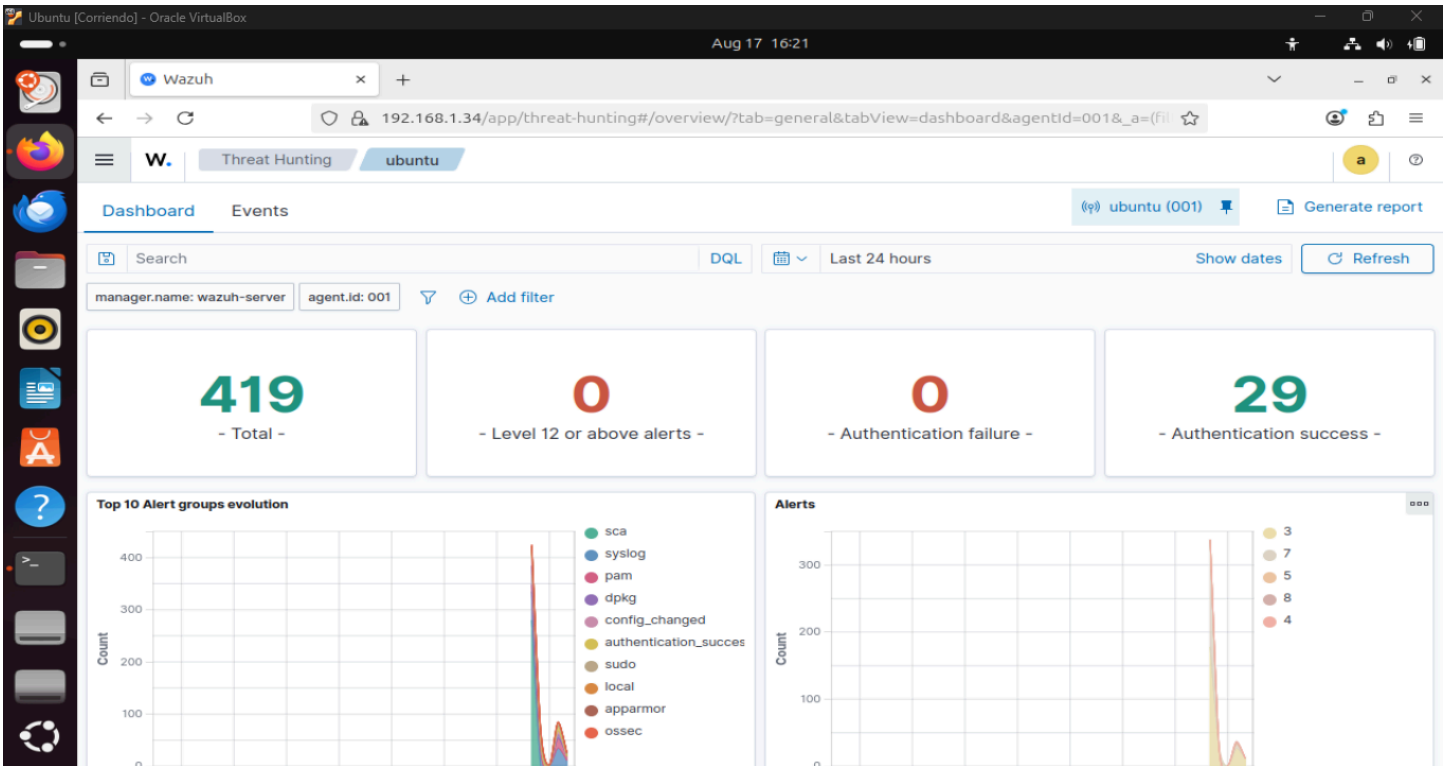
Panel inicial (overview) de Wazuh.

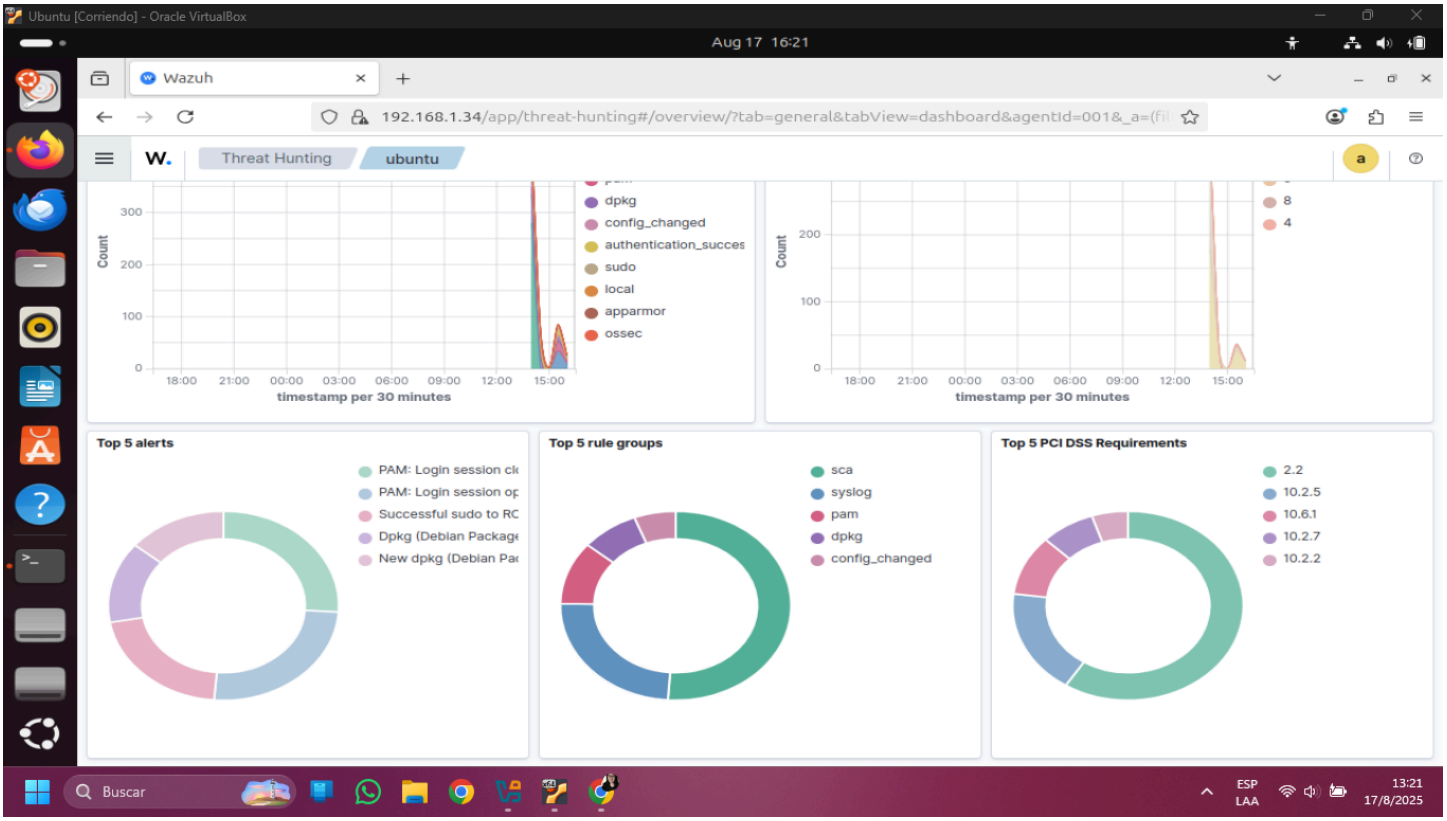


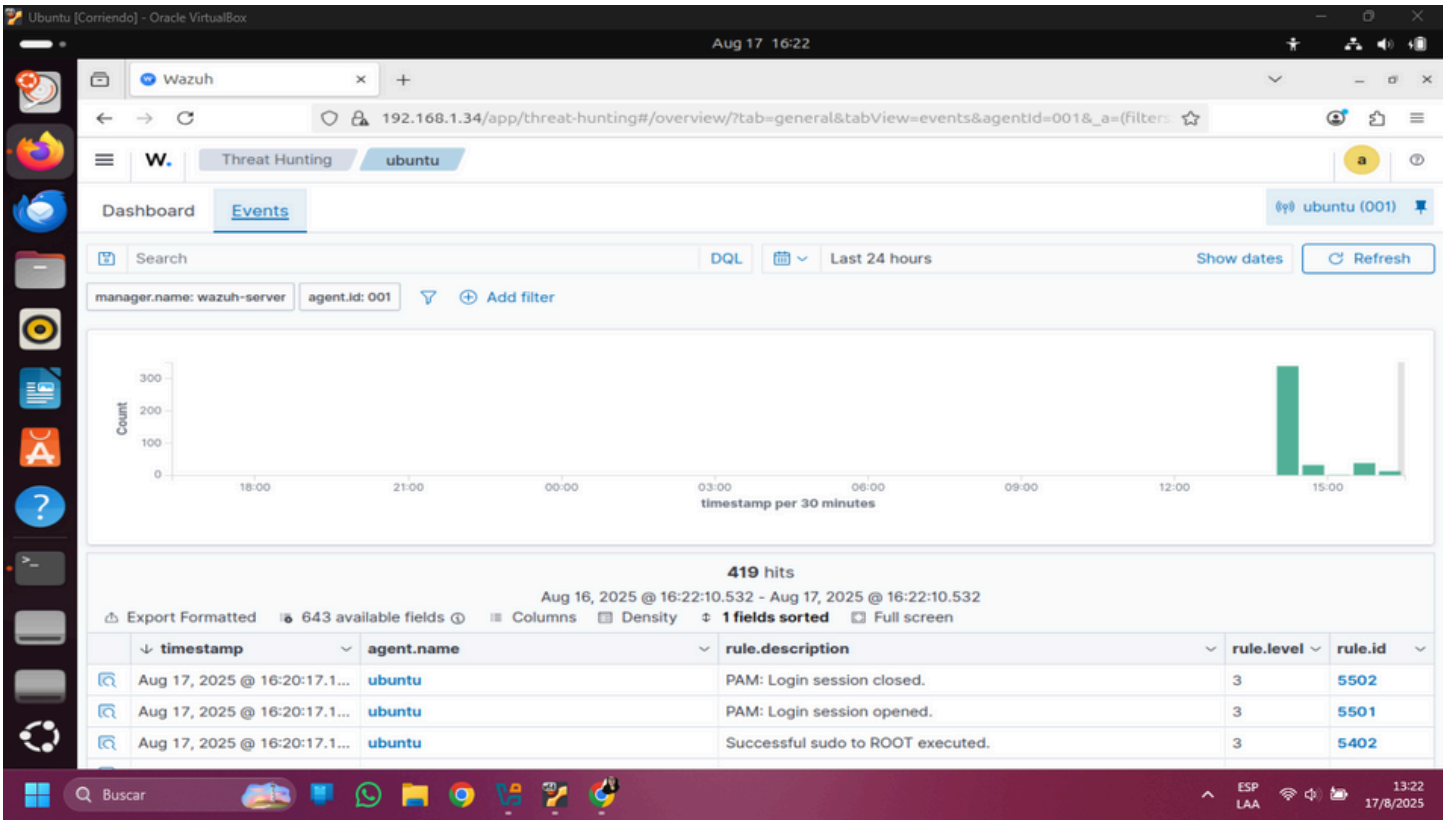
Evidencia N.º 5:

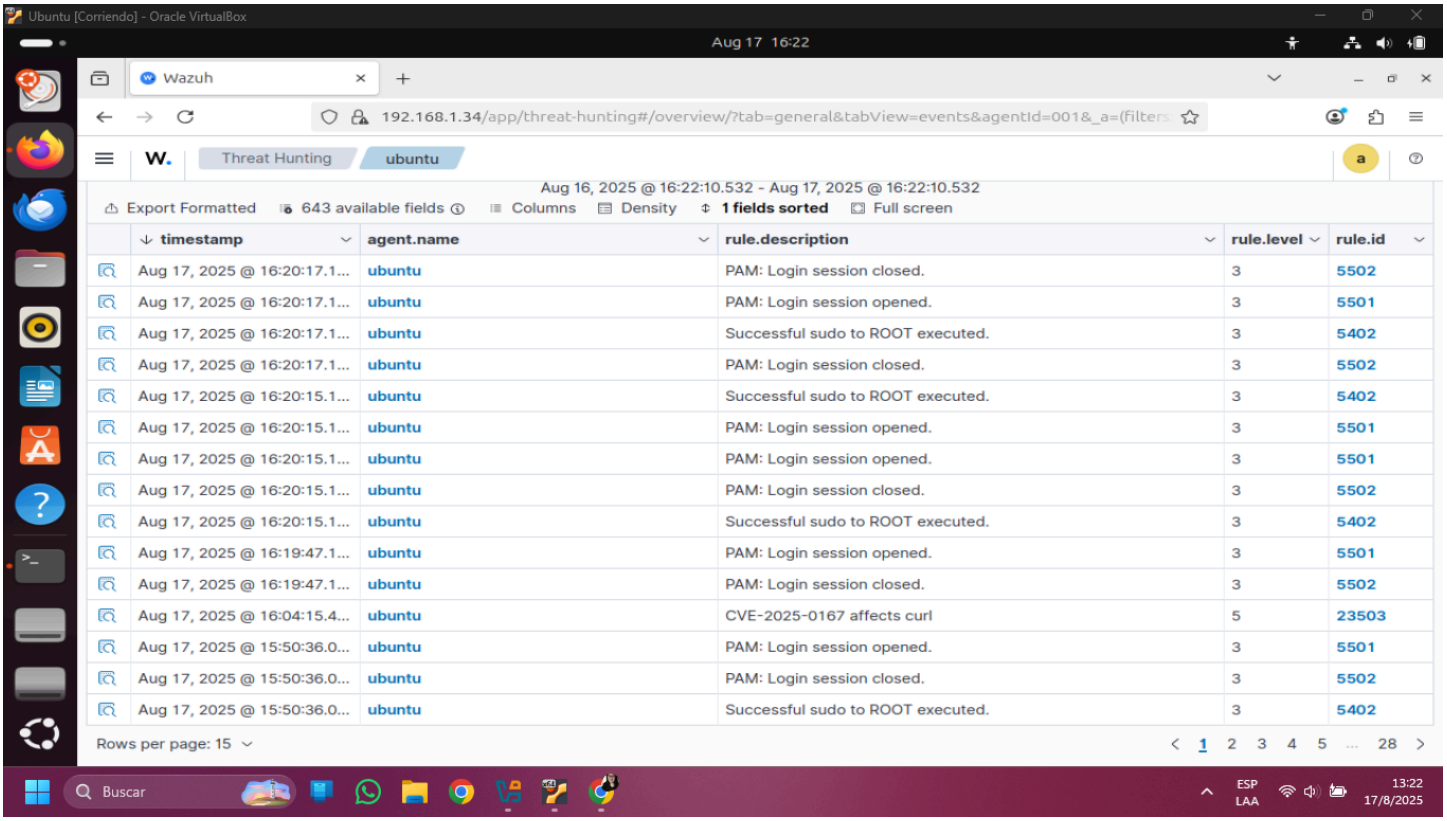
Luego de instalar los agentes necesarios para la recolección de logs, se utilizaron las opciones que posee Wazuh para Threat Hunting, detallando los eventos registrados.

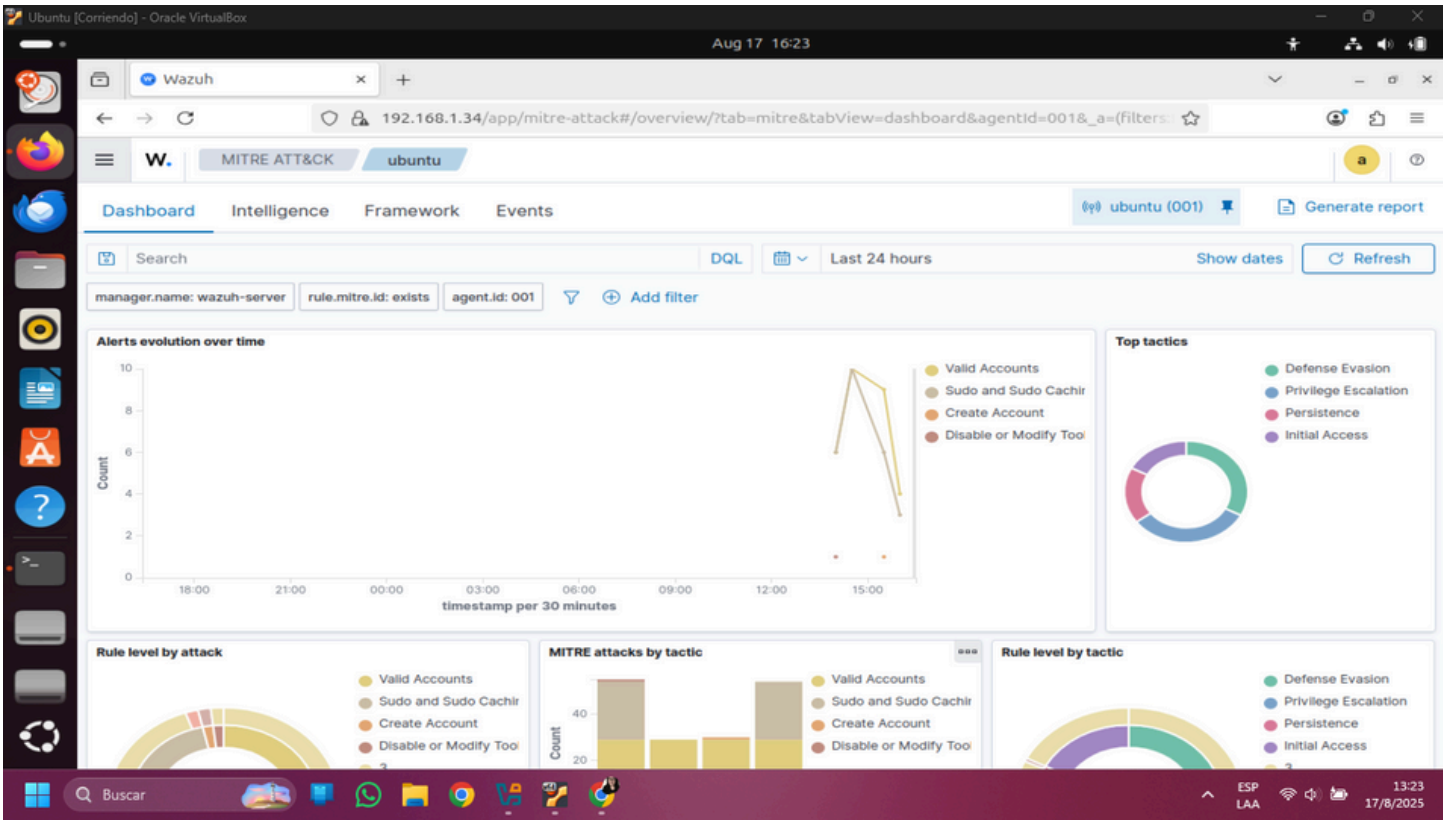


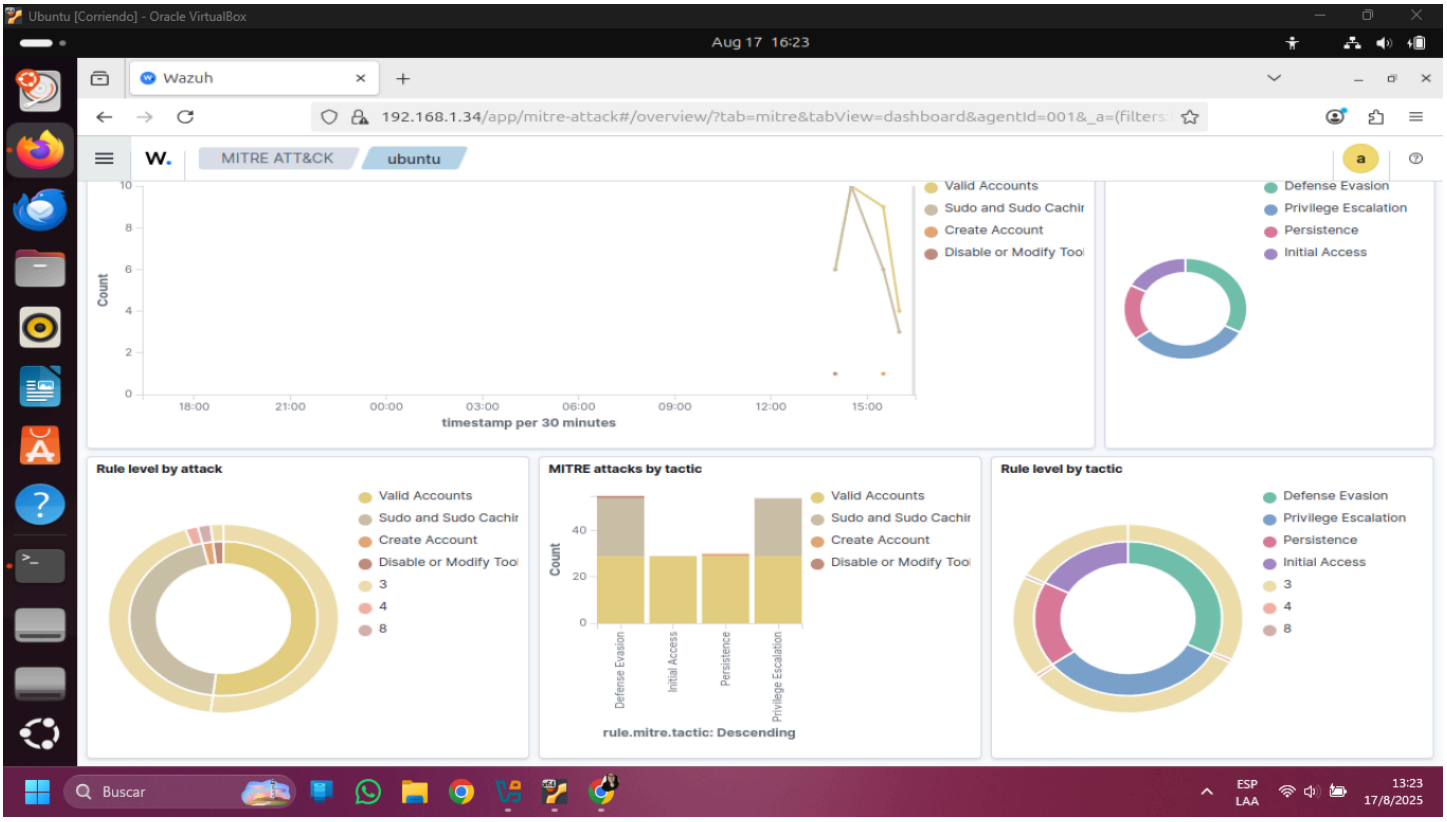

Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:21
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(Fil
Threat Hunting
ubuntu
Dashboard
Events
ubuntu (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 001
Add filter
419
- Total -
0
- Level 12 or above alerts -
0
- Authentication failure -
29
- Authentication success -
Top 10 Alert groups evolution
Count
sca
syslog
pam
dpkg
config_changed
authentication_succes
sudo
local
apparmor
ossec
Alerts
Count
3
7
5
8
4

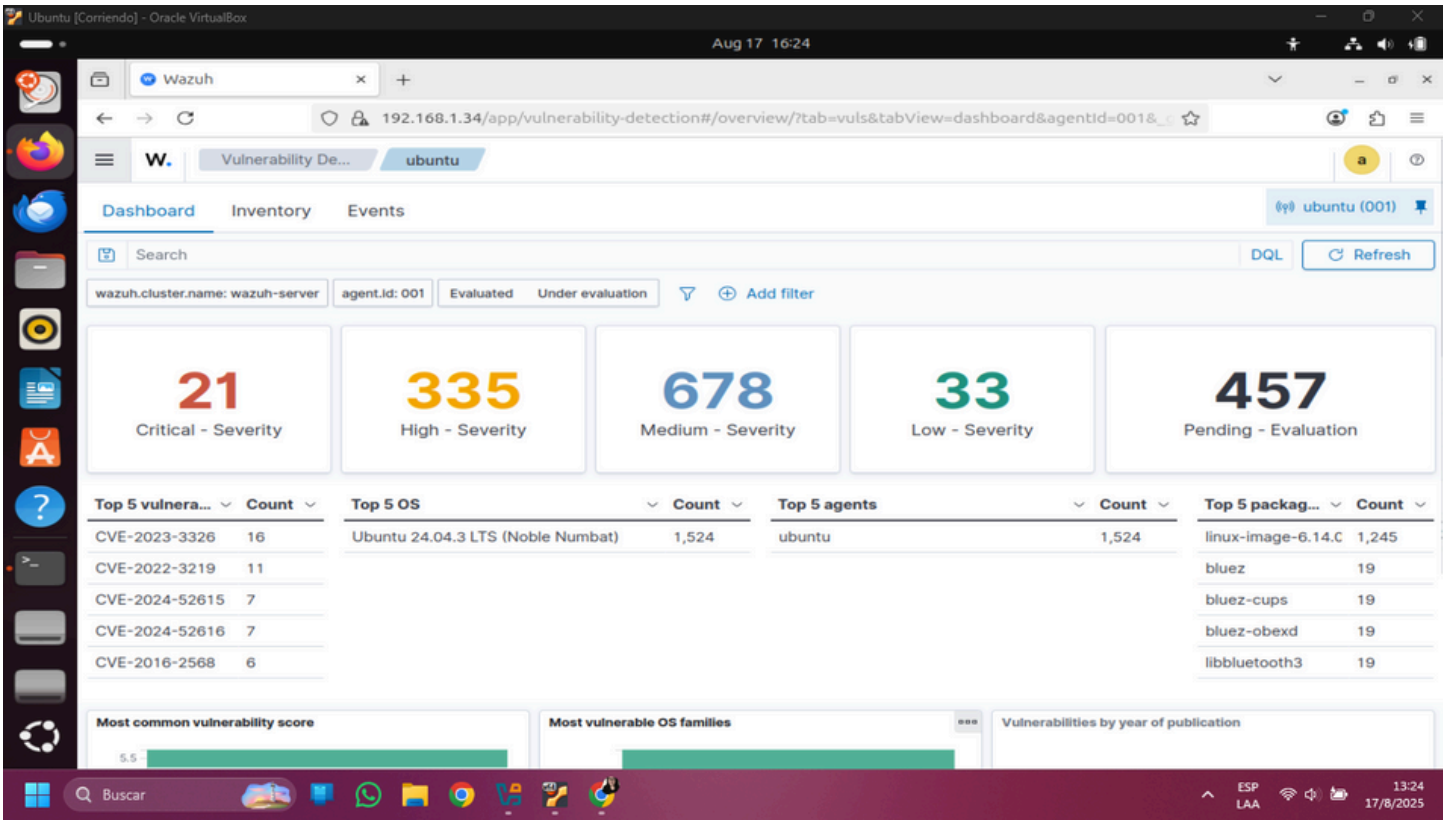

Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:21
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(Fil
Threat Hunting
ubuntu
Count
dpkg
config_changed
authentication_succes
sudo
local
apparmor
ossec
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
timestamp per 30 minutes
Top 5 alerts
PAM: Login session cl
PAM: Login session op
Successful sudo to RC
Dpkg (Debian Package
New dpkg (Debian Pac
Top 5 rule groups
sca
syslog
pam
dpkg
config_changed
Top 5 PCI DSS Requirements
2.2
10.2.5
10.6.1
10.2.7
10.2.2
Buscar
ESP
LAA
13:21
17/8/2025

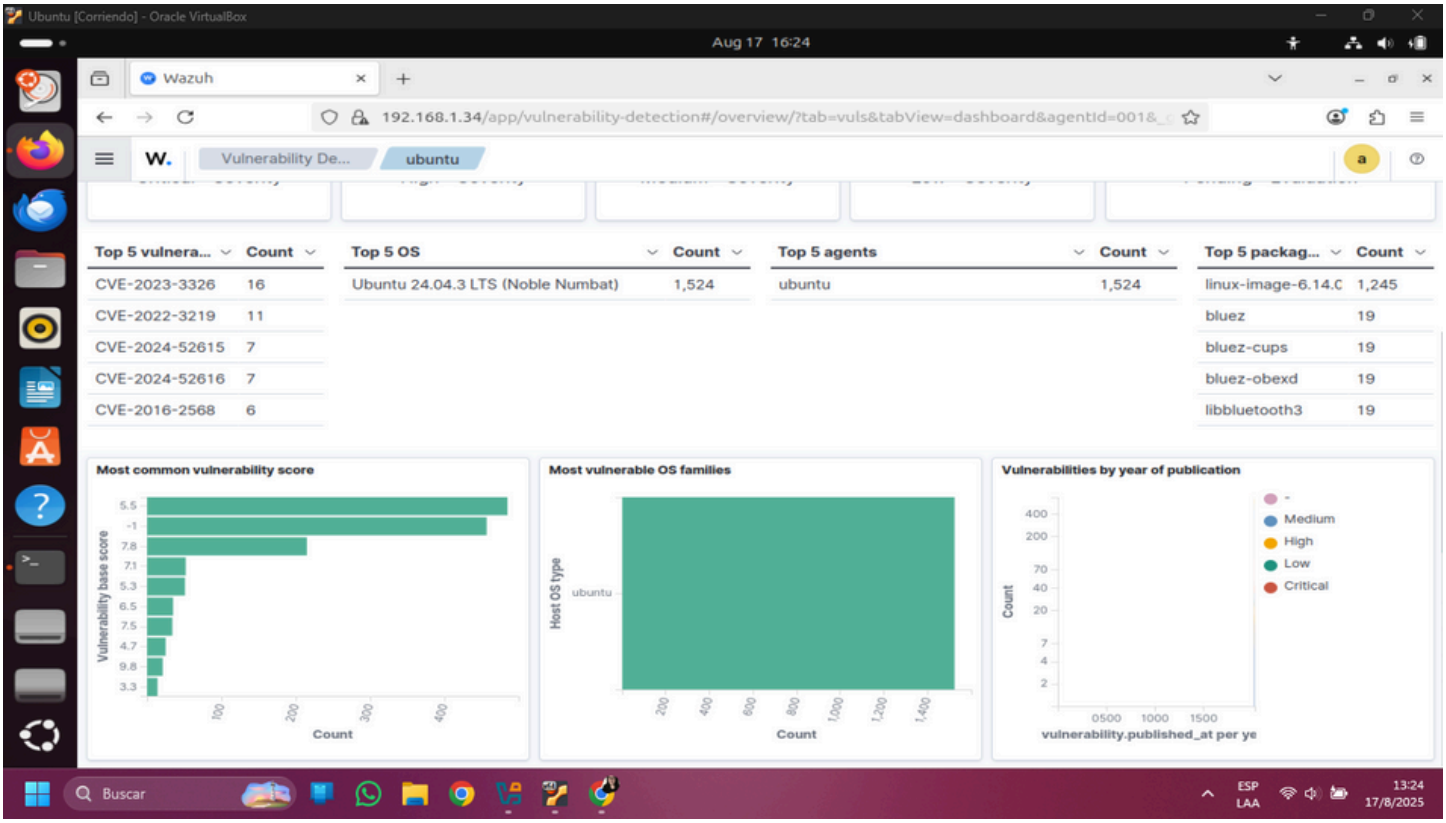

Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:22
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters
Threat Hunting
ubuntu
Dashboard
Events
ubuntu (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 001
Add filter
Count
300
200
100
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
timestamp per 30 minutes
419 hits
Aug 16, 2025 @ 16:22:10.532 - Aug 17, 2025 @ 16:22:10.532
Export Formatted
643 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Aug 17, 2025 @ 16:20:17.1...
ubuntu
PAM: Login session closed.
3
5502
Aug 17, 2025 @ 16:20:17.1...
ubuntu
PAM: Login session opened.
3
5501
Aug 17, 2025 @ 16:20:17.1...
ubuntu
Successful sudo to ROOT executed.
3
5402
Buscar
ESP
LAA
13:22
17/8/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:22
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters
Threat Hunting
ubuntu
Aug 16, 2025 @ 16:22:10.532 - Aug 17, 2025 @ 16:22:10.532
Export Formatted
643 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Aug 17, 2025 @ 16:20:17.1... ubuntu PAM: Login session closed. 3 5502
Aug 17, 2025 @ 16:20:17.1... ubuntu PAM: Login session opened. 3 5501
Aug 17, 2025 @ 16:20:17.1... ubuntu Successful sudo to ROOT executed. 3 5402
Aug 17, 2025 @ 16:20:17.1... ubuntu PAM: Login session closed. 3 5502
Aug 17, 2025 @ 16:20:15.1... ubuntu Successful sudo to ROOT executed. 3 5402
Aug 17, 2025 @ 16:20:15.1... ubuntu PAM: Login session opened. 3 5501
Aug 17, 2025 @ 16:20:15.1... ubuntu PAM: Login session opened. 3 5501
Aug 17, 2025 @ 16:20:15.1... ubuntu PAM: Login session closed. 3 5502
Aug 17, 2025 @ 16:20:15.1... ubuntu Successful sudo to ROOT executed. 3 5402
Aug 17, 2025 @ 16:19:47.1... ubuntu PAM: Login session opened. 3 5501
Aug 17, 2025 @ 16:19:47.1... ubuntu PAM: Login session closed. 3 5502
Aug 17, 2025 @ 16:04:15.4... ubuntu CVE-2025-0167 affects curl 5 23503
Aug 17, 2025 @ 15:50:36.0... ubuntu PAM: Login session opened. 3 5501
Aug 17, 2025 @ 15:50:36.0... ubuntu PAM: Login session closed. 3 5502
Aug 17, 2025 @ 15:50:36.0... ubuntu Successful sudo to ROOT executed. 3 5402
Rows per page: 15
1 2 3 4 5 ... 28
Buscar
ESP
LAA
13:22
17/8/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:23
Wazuh
192.168.1.34/app/mitre-attack#/overview/?tab=mitre&tabView=dashboard&agentId=001&_a=(filters:
MITRE ATT&CK
ubuntu
Dashboard
Intelligence
Framework
Events
ubuntu (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.mitre.id: exists
agent.id: 001
Add filter
Alerts evolution over time
Count
timestamp per 30 minutes
Valid Accounts
Sudo and Sudo Cachir
Create Account
Disable or Modify Tool
Top tactics
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Rule level by attack
MITRE attacks by tactic
Rule level by tactic
Buscar
ESP
LAA
13:23
17/8/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Aug 17 16:23
Wazuh
192.168.1.34/app/mitre-attack#/overview/?tab=mitre&tabView=dashboard&agentId=001&_a=(filters:
MITRE ATT&CK
ubuntu
Count
timestamp per 30 minutes
Valid Accounts
Sudo and Sudo Cachir
Create Account
Disable or Modify Tool
Defense Evasion
Privilege Escalation
Persistence
Initial Access
3
4
8
Rule level by attack
MITRE attacks by tactic
rule.mitre.tactic: Descending
Rule level by tactic
Buscar
ESP
LAA
13:23
17/8/2025





Conclusión:

Wazuh es una herramienta potente para la recolección de logs, fácil de instalar, intuitiva y con una interfaz clara, ideal especialmente para usuarios con un nivel más bien principiante.

Mi experiencia personal: La instalación del sistema Ubuntu me resultó complicada debido a las limitaciones de mi equipo, lo que me obligó a buscar soluciones alternativas. Posteriormente,

desplegar Wazuh supuso otro desafío importante, del que logré salir airosa, aunque no sin esfuerzo. En definitiva, este laboratorio me permitió aprender muchísimo.