Lab Wazuh

Entorno

Ubuntu

Wazuh

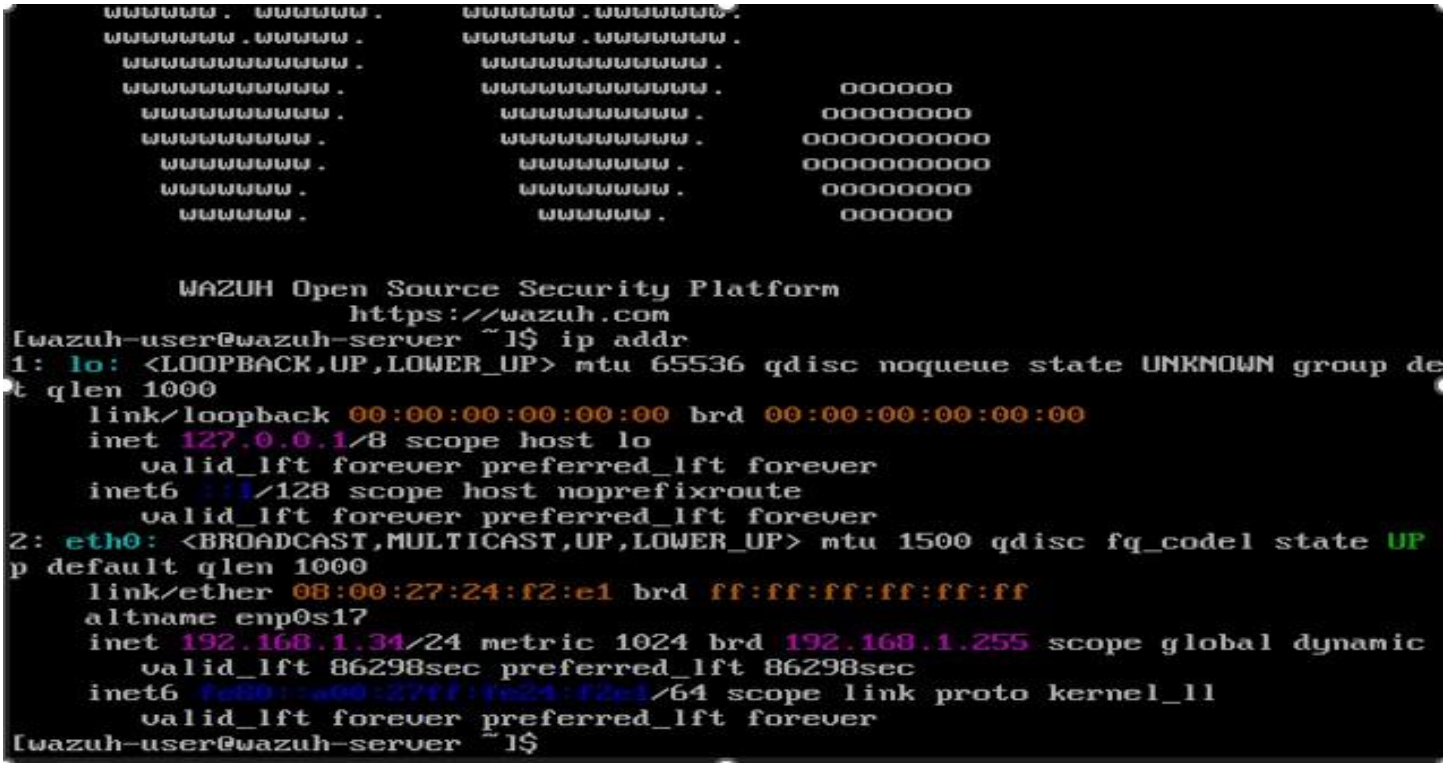
Virtual Box

Índice

1. Implementación de Wazuh

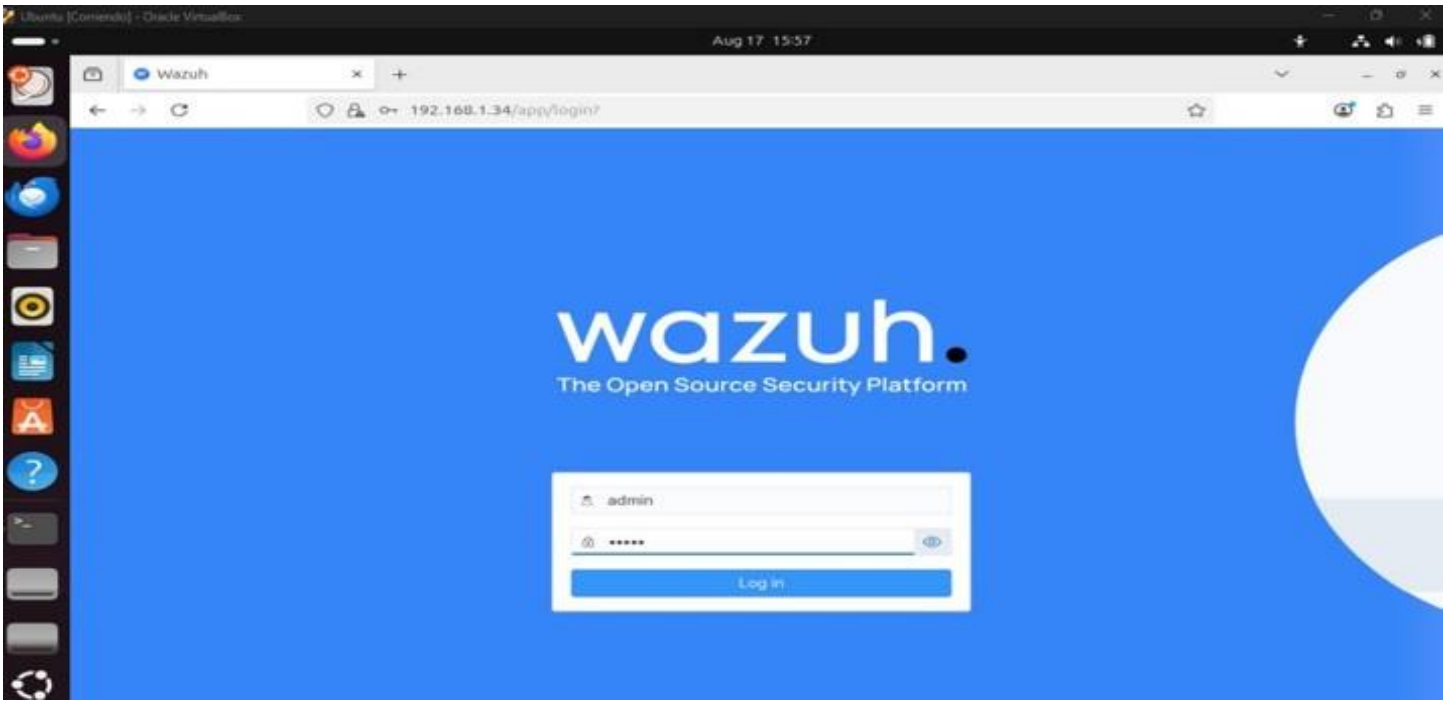
Maquina virtual iniciada, datos de acceso:

- User wazuh-user
- Password Wazuh

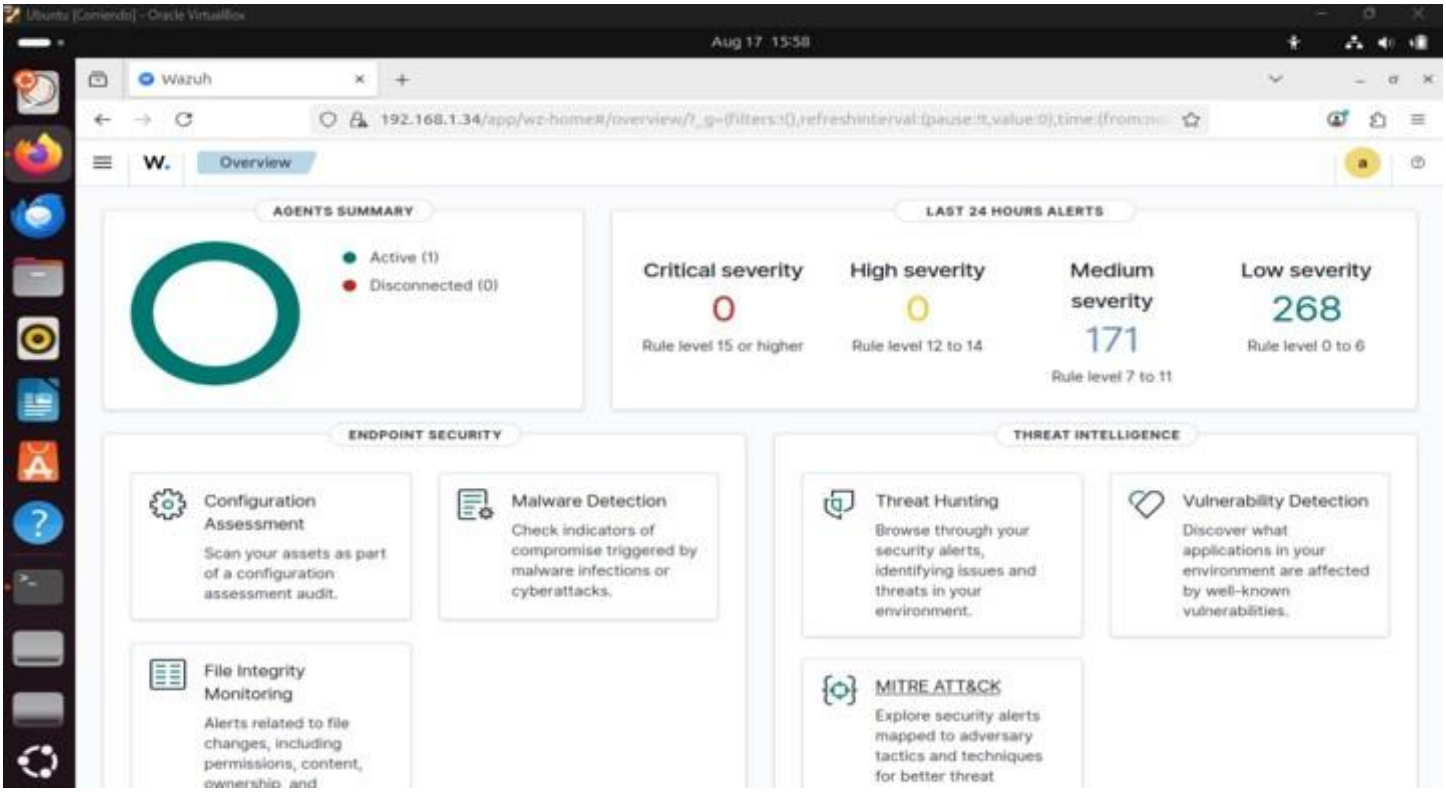


Acceso desde el navegador de Mozilla Firefox al servidor de Wazuh:

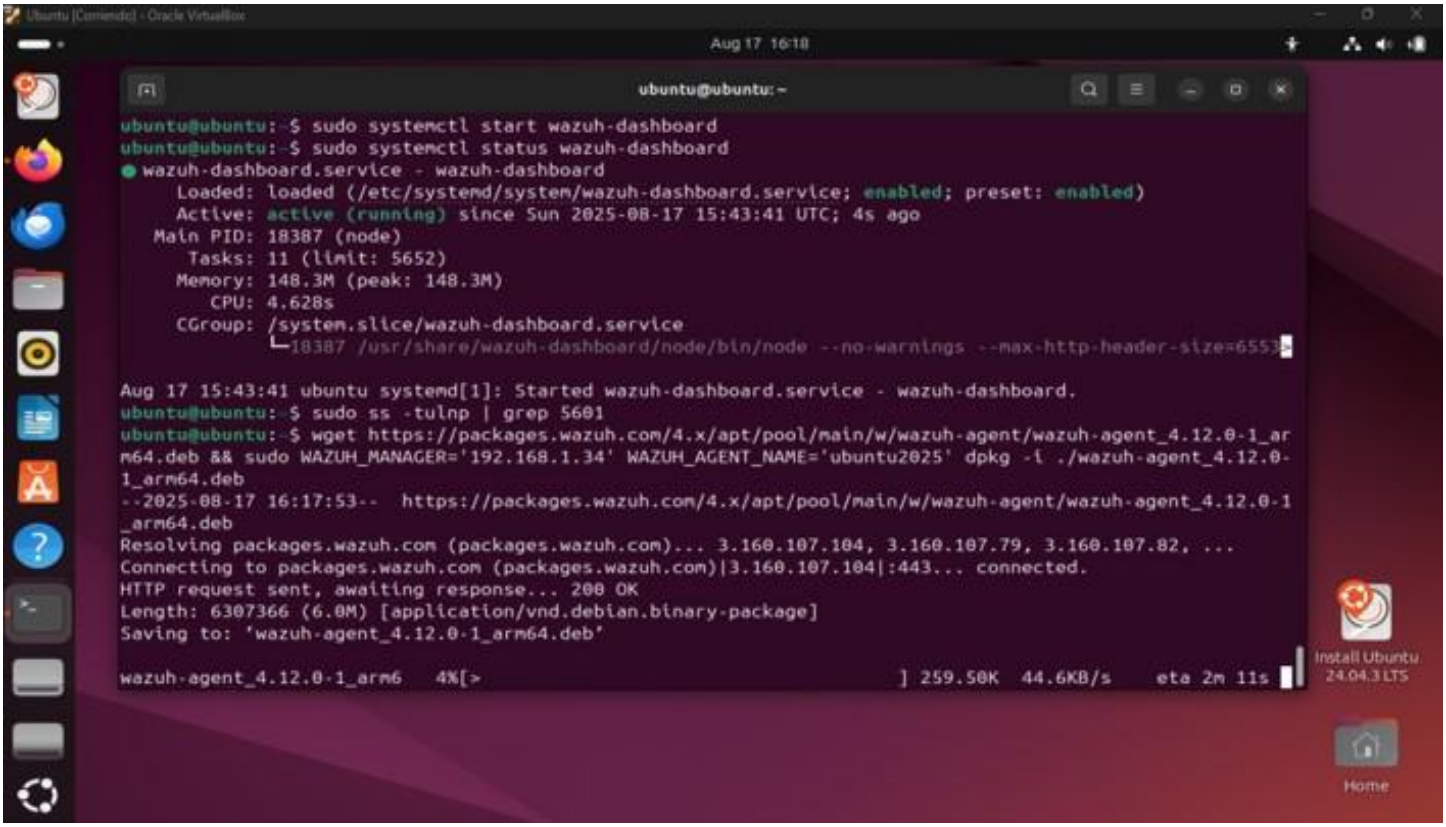
- user admin
- password admin

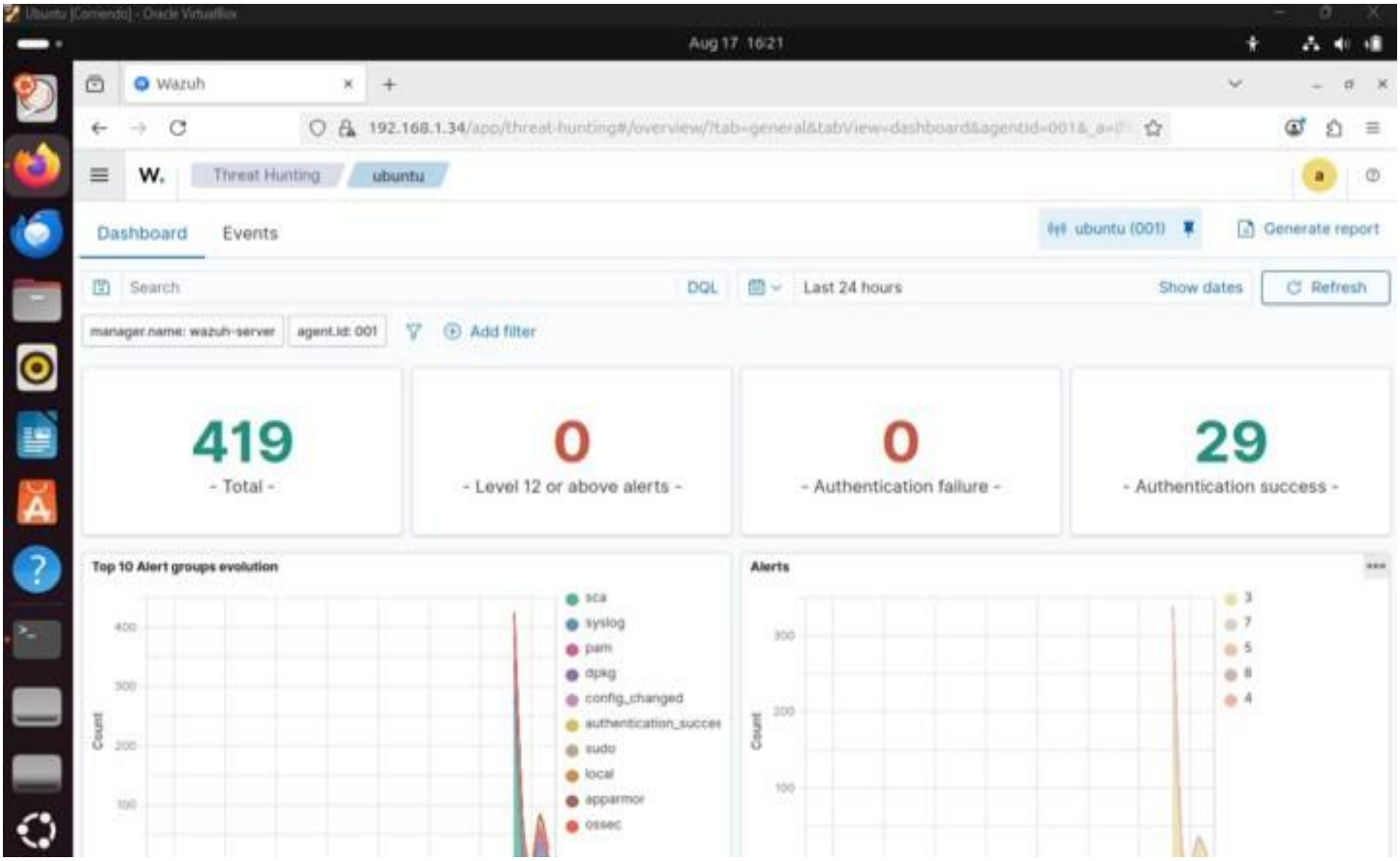


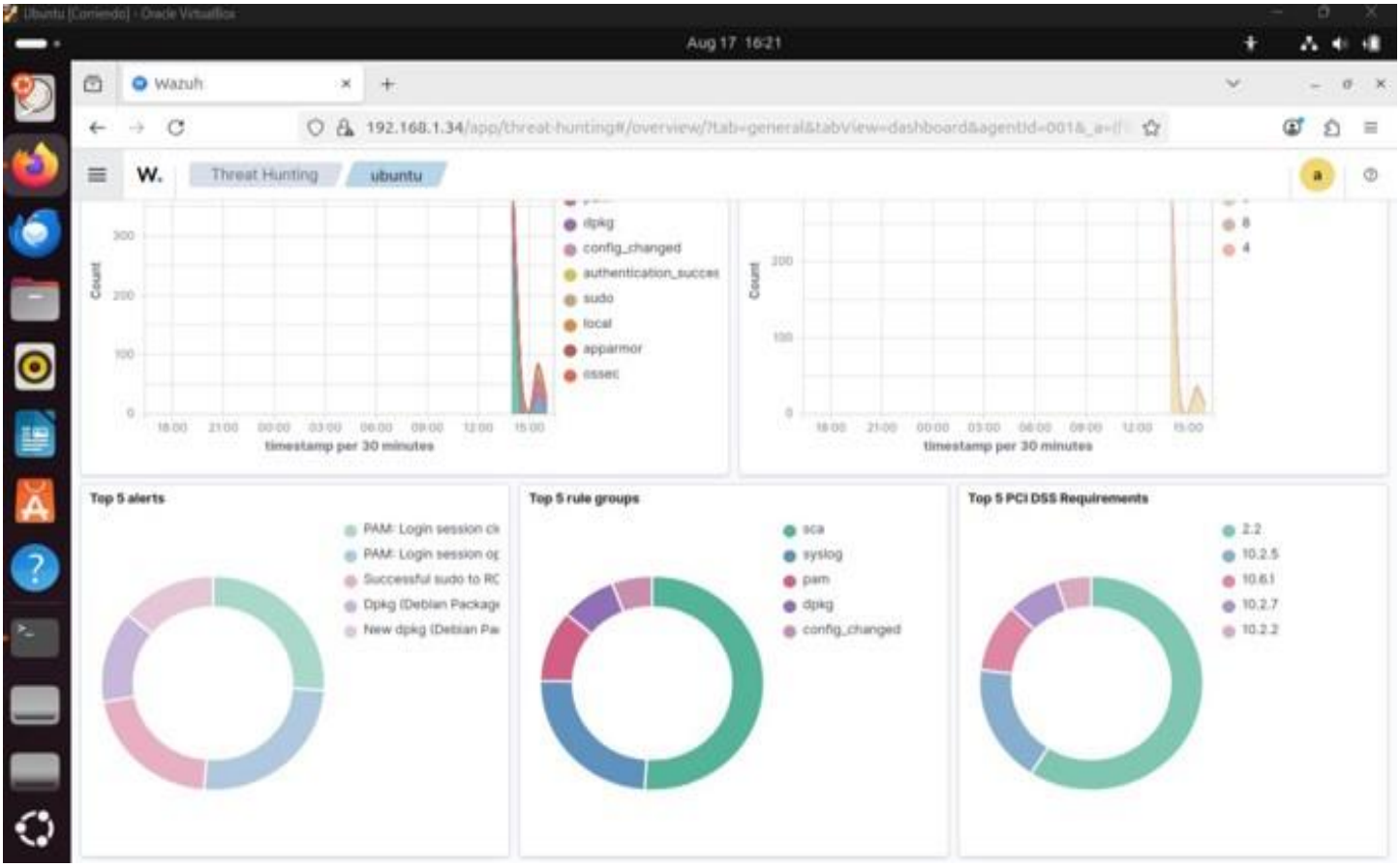
Panel inicial (overview) de Wazuh

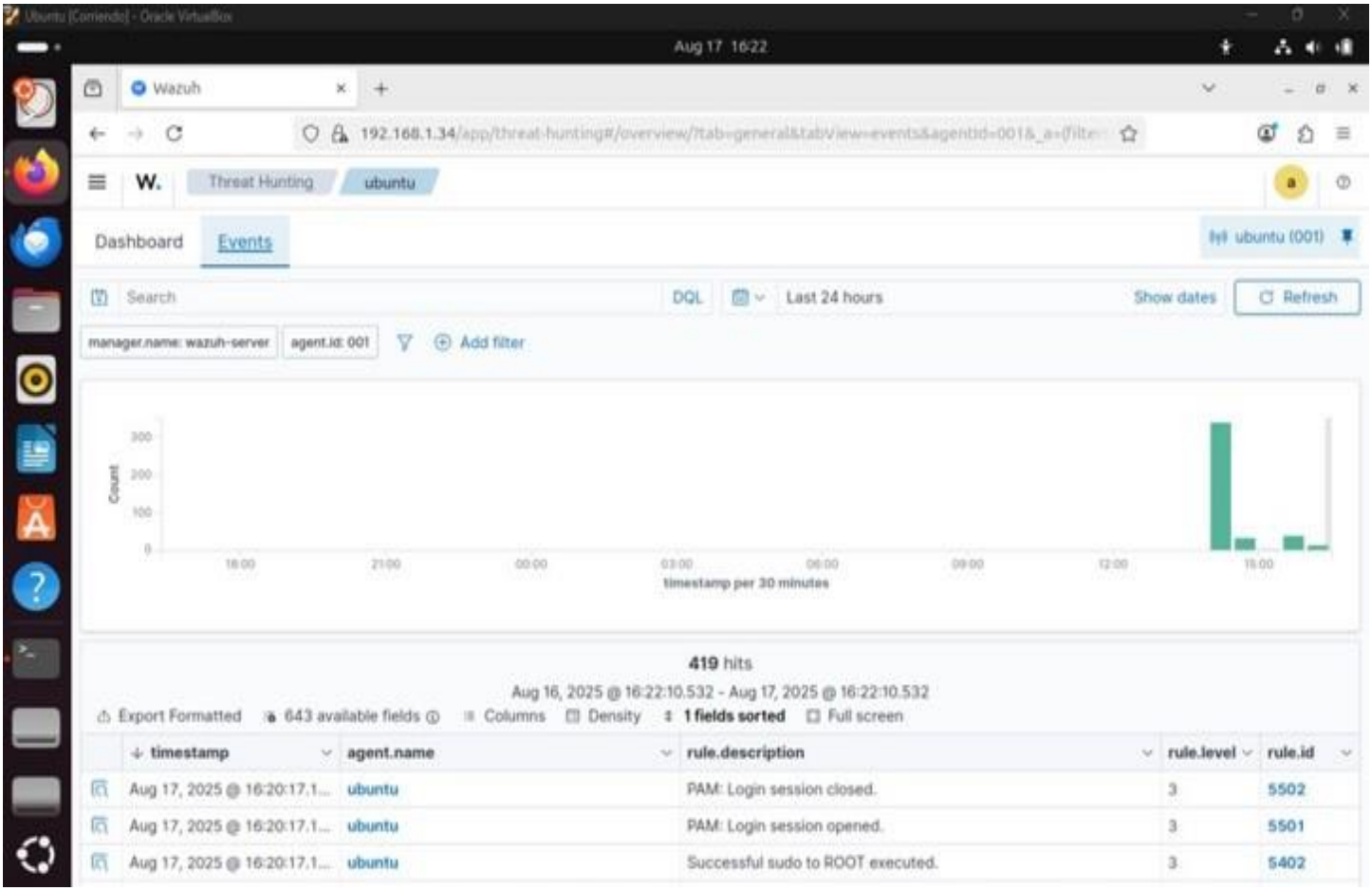


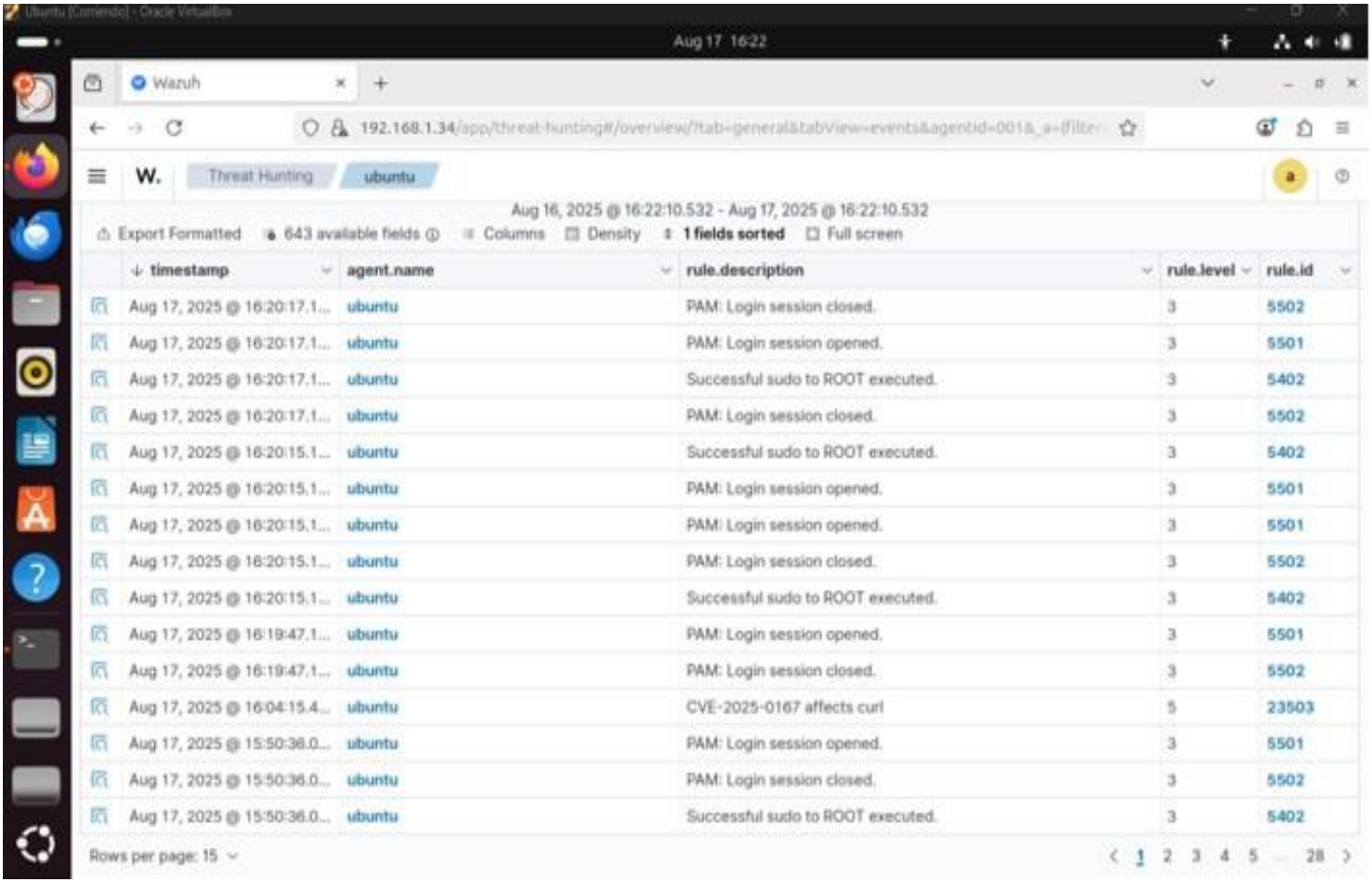
Luego de instalar los agentes necesarios para la recolección de logs, se utilizaron las opciones que posee Wazuh para Threat Hunting, detallando los eventos registrados

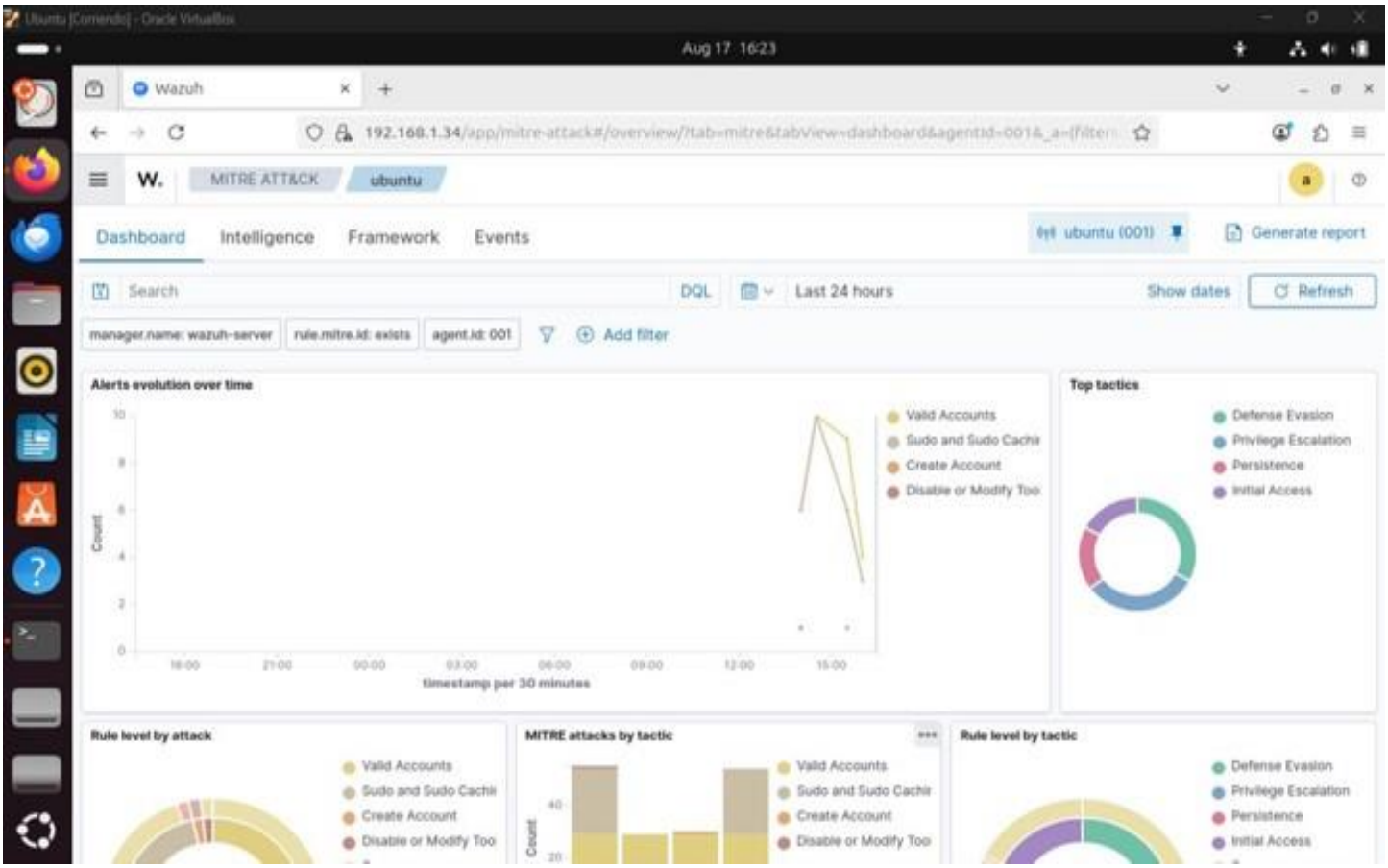


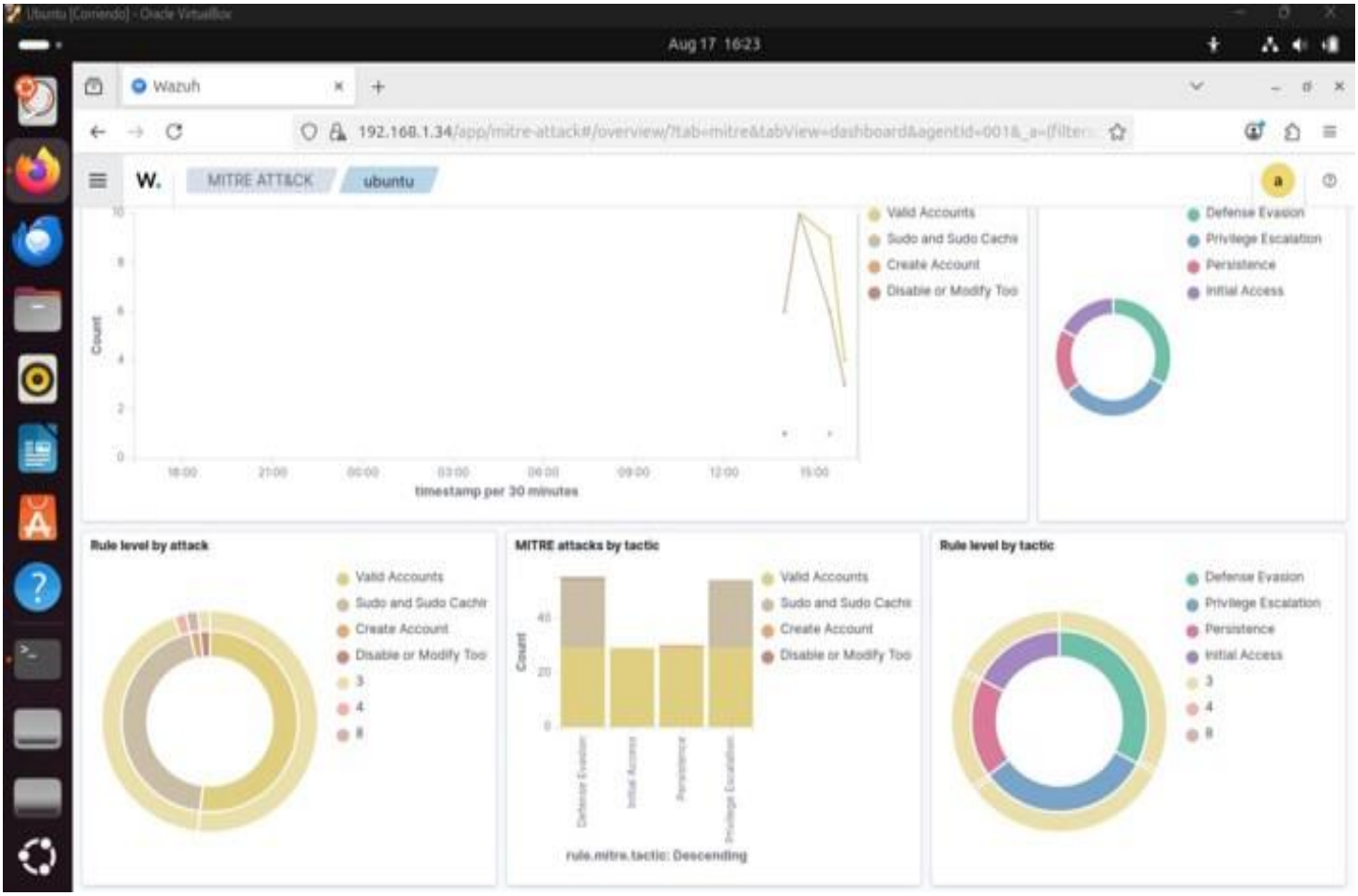


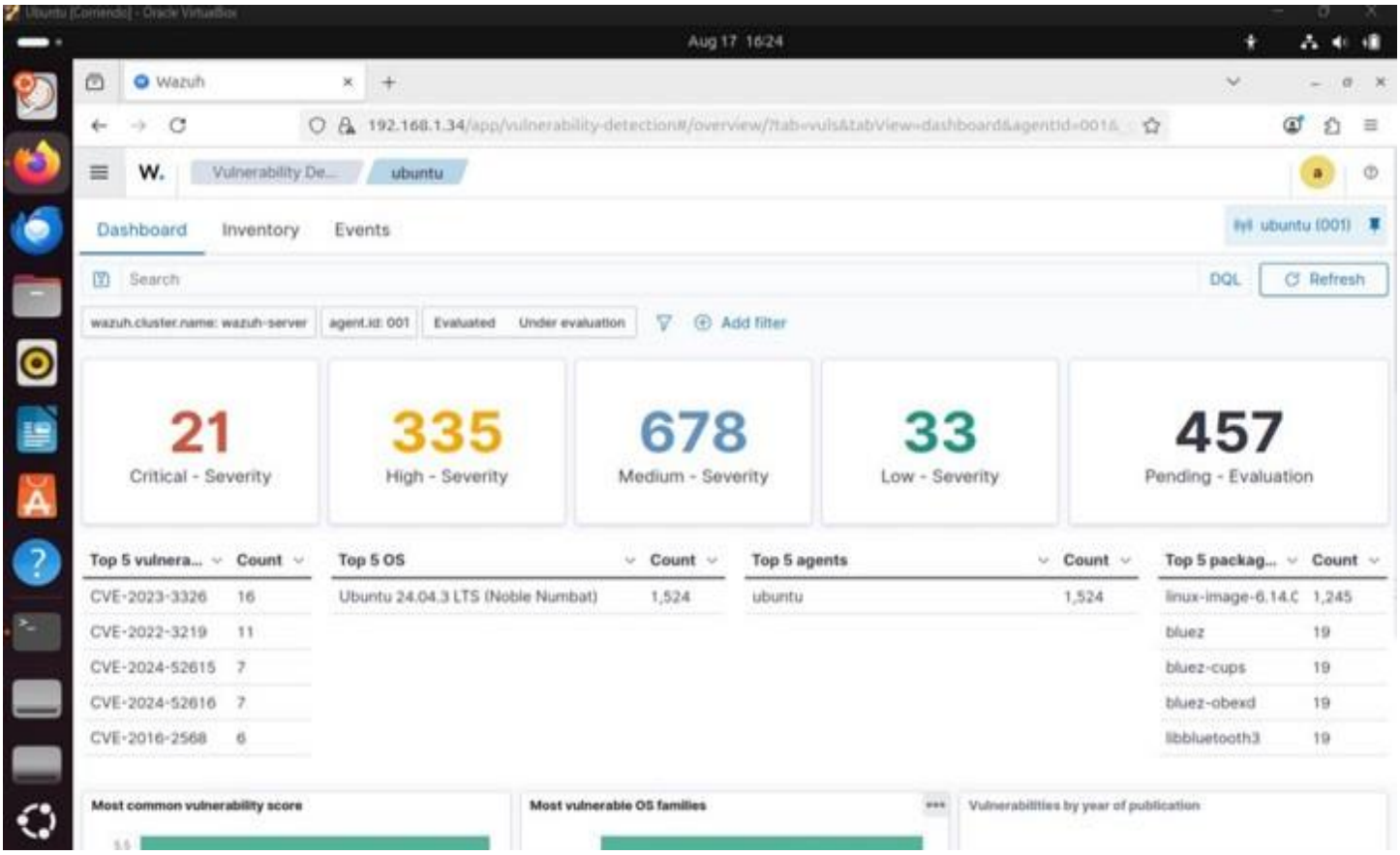

Aug 17 16:21
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(f
W.
Threat Hunting
ubuntu
dpkg
config_changed
authentication_succes
sudo
local
apparmor
ossec
Count
timestamp per 30 minutes
Top 5 alerts
PAM: Login session cl
PAM: Login session op
Successful sudo to RC
Dpkg (Debian Package
New dpkg (Debian Pa
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

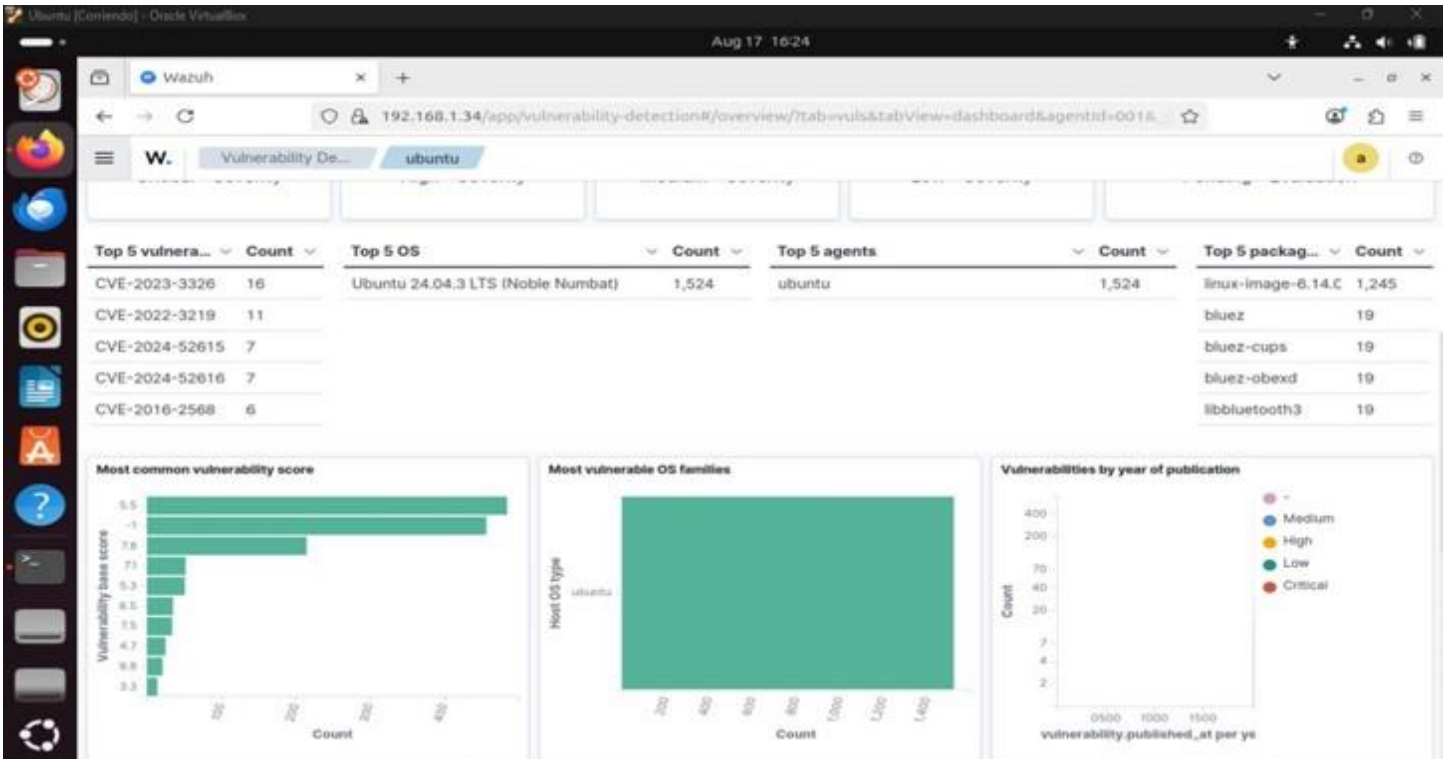

Aug 17 16:22
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filter
W.
Threat Hunting
ubuntu
Dashboard
Events
ubuntu (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 001
Add filter
Count
timestamp per 30 minutes
419 hits
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


Aug 17 16:22
Wazuh
192.168.1.34/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filter
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


Aug 17 16:23
Wazuh
192.168.1.34/app/mitre-attack#/overview/?tab=mitre&tabView=dashboard&agentId=001&_a=(filter
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 Cachi
Create Account
Disable or Modify Too
Top tactics
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Rule level by attack
MITRE attacks by tactic
Rule level by tactic


Aug 17 16:23
Wazuh
192.168.1.34/app/mitre-attack#/overview/?tab=mitre&tabView=dashboard&agentId=001&_a=(filter
MITRE ATT&CK
ubuntu
Valid Accounts
Sudo and Sudo Cachi
Create Account
Disable or Modify Too
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Count
timestamp per 30 minutes
Rule level by attack
MITRE attacks by tactic
Rule level by tactic
3
4
8
rule.mitre.tactic: Descending


Aug 17 16:24
Wazuh
192.168.1.34/app/vulnerability-detection#/overview/?tab=vuls&tabView=dashboard&agentId=001&
Vulnerability De...
ubuntu
Dashboard
Inventory
Events
ubuntu (001)
Search
DQL
Refresh
wazuh.cluster.name: wazuh-server
agent.id: 001
Evaluated
Under evaluation
Add filter
21
Critical - Severity
335
High - Severity
678
Medium - Severity
33
Low - Severity
457
Pending - Evaluation
Top 5 vulnera...
Count
CVE-2023-3326 16
CVE-2022-3219 11
CVE-2024-52615 7
CVE-2024-52616 7
CVE-2016-2568 6
Top 5 OS
Ubuntu 24.04.3 LTS (Noble Numbat) 1,524
Top 5 agents
ubuntu 1,524
Top 5 packag...
linux-image-6.14.0 1,245
bluez 19
bluez-cups 19
bluez-obexd 19
libbluetooth3 19
Most common vulnerability score
Most vulnerable OS families
Vulnerabilities by year of publication



2. Resumen final

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