

Actividad 2 - Wazuh

Módulo 3 - Gestión de incidentes

Diego Mucci

19/05/2024

Seguridad Informática

Actividad 2 - Wazuh

Wazuh es una plataforma de código abierto que proporciona detección de amenazas, monitorización de seguridad y respuesta a incidentes. Ofrece funcionalidades clave como la detección de intrusiones, gestión de incidentes, monitorización de integridad de archivos, análisis de vulnerabilidades y cumplimiento normativo. Además, es compatible con entornos en la nube como AWS, Azure y Google Cloud Platform, permitiendo una protección integral y adaptable a diferentes infraestructuras.

Para las organizaciones, Wazuh ofrece una protección proactiva al detectar y alertar sobre amenazas en tiempo real, facilitando respuestas rápidas y automatizadas. Proporciona visibilidad centralizada de la seguridad de todos los sistemas, ayuda a cumplir con regulaciones mediante informes detallado. Su capacidad para adaptarse a entornos locales, híbridos o en la nube y gestionar grandes volúmenes de datos lo convierte en una herramienta ideal para fortalecer la seguridad de los sistemas de información.

Actividad. - Implementación de Wazuh en Cloud

Objetivo:

Implementarás Wazuh en el cloud oficial, desplegarás agentes en una máquina virtual Windows y otra Kali, y activarás servicios de seguridad previamente configurados en la máquina Kali. Documentarás el proceso con capturas de pantalla y generarás eventos de seguridad para verificar la correcta configuración y funcionamiento.

Requisitos:

- Cuenta de correo temporal para registro
- Acceso a máquinas virtuales Windows y Kali
- Servicios de seguridad instalados y configurados en Kali (Snort, Suricata, WAF con mod-security)
- Opción alternativa: OVA oficial de Wazuh para instalación en máquina virtual

Pasos a seguir:

1. Registro en Wazuh Cloud

1. Accede a la página de registro de Wazuh Cloud.
2. Utiliza una cuenta de correo temporal para completar el registro.
3. Verifica tu cuenta a través del correo recibido y accede al portal de Wazuh Cloud.

2. Creación del Entorno en Wazuh

1. Inicia sesión en Wazuh Cloud.
2. Crea un nuevo entorno desde el dashboard principal.
3. Configura el entorno según las especificaciones necesarias.

3. Despliegue de Agentes

1. Máquina Virtual Windows:

- Crea un agente desde el portal de Wazuh Cloud e invoca con el comando necesario y desde la máquina virtual la instalación del agente de Wazuh.
- Inicia el servicio.

2. Máquina Virtual Kali:

- Crea un agente desde el portal de Wazuh Cloud e invoca con el comando necesario y desde la máquina virtual la instalación del agente de Wazuh.
- Inicia el servicio.

4. Activación de Servicios en Kali

Verifica y activa los servicios de seguridad previamente instalados:

- **Snort:** Configura y activa el servicio.
- **Suricata:** Configura y activa el servicio.
- **WAF (mod-security):** Configura y activa el servicio en el servidor web.

5. Verificación de Eventos en Wazuh Cloud

Accede al dashboard de Wazuh Cloud y verifica que los eventos de seguridad de las máquinas virtuales se reflejan correctamente.

6. Generación de Nuevos Eventos de Seguridad

- Máquina Windows:

- Genera varios intentos de inicio de sesión fallidos.

- Máquina Kali:

- Realiza un intento de inyección de código en un formulario web protegido por WAF.
- Ejecuta acciones para activar reglas de Snort y Suricata generando tráfico sospechoso.

7. Documentación del Proceso

- Compila todas las capturas de pantalla en un documento.
- Redacta una breve descripción para cada paso, explicando el proceso seguido y los resultados obtenidos.
- Asegúrate de incluir cualquier problema encontrado y cómo se resolvió.

Opción Alternativa: Instalación de Wazuh mediante OVA

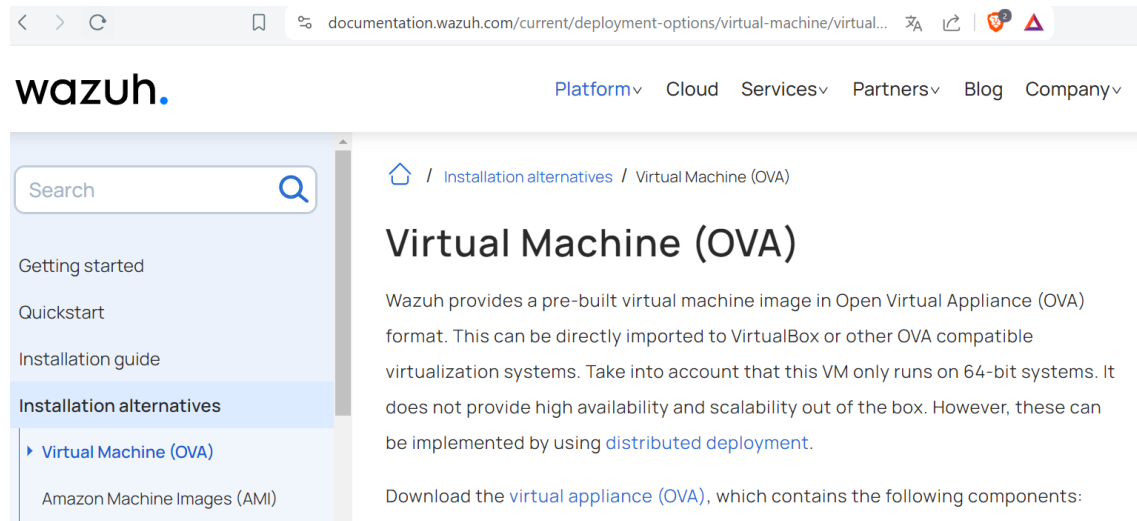
1. Descarga la OVA oficial de Wazuh desde el sitio web de Wazuh.
2. Importa la OVA en tu software de virtualización preferido (por ejemplo, VirtualBox, VMware).
3. Sigue las instrucciones de instalación y configuración para desplegar Wazuh en una máquina virtual.
4. Repite los pasos 3-6 para el despliegue de agentes y generación de eventos.

Entrega:

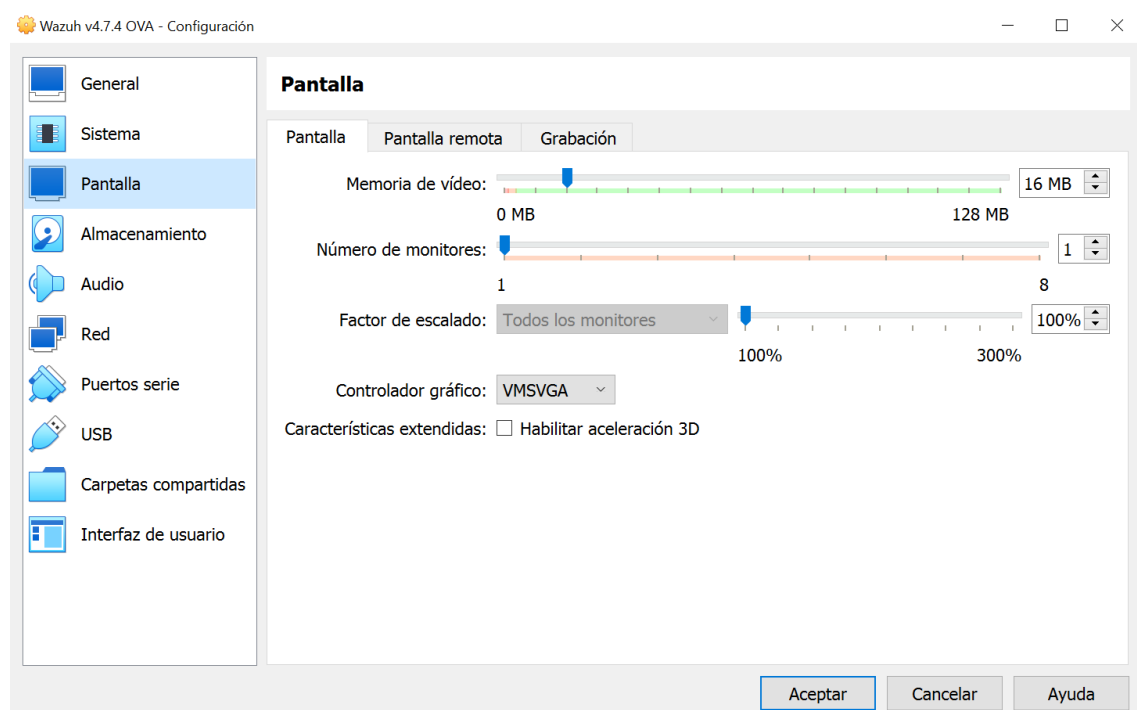
- Documento PDF con todas las capturas de pantalla y descripciones detalladas.

El proceso de implementación de Wazuh se ha realizado instalando la OVA, dado que me resultaba interesante poder disponer de esta herramienta de manera indefinida, ya que si lo hacíamos en Wazuh Cloud este tenía un periodo de prueba gratuito de 14 días.

Así que nos descargamos la OVA de la página oficial de Wazuh:



Importamos la OVA en nuestra máquina virtual. El único cambio que debemos realizar es seleccionar el controlador gráfico a VMSVGA, el resto viene por defecto bien configurado:



Arrancamos el proceso de instalación. Introducimos el nombre de usuario “wazuh-user” y “wazuh” como contraseña.

Aquí nos hemos encontrado con un problema porque no se encontraba el símbolo “-“, ya que no estaba en la tecla que corresponde sino en la tecla del símbolo de interrogación.

```
Welcome to the Wazuh OVA version
Wazuh - 4.7.4
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login: wazuh-user
Password: █
```

Aplicamos el comando “ip a” para mostrar la IP del servicio Wazuh:

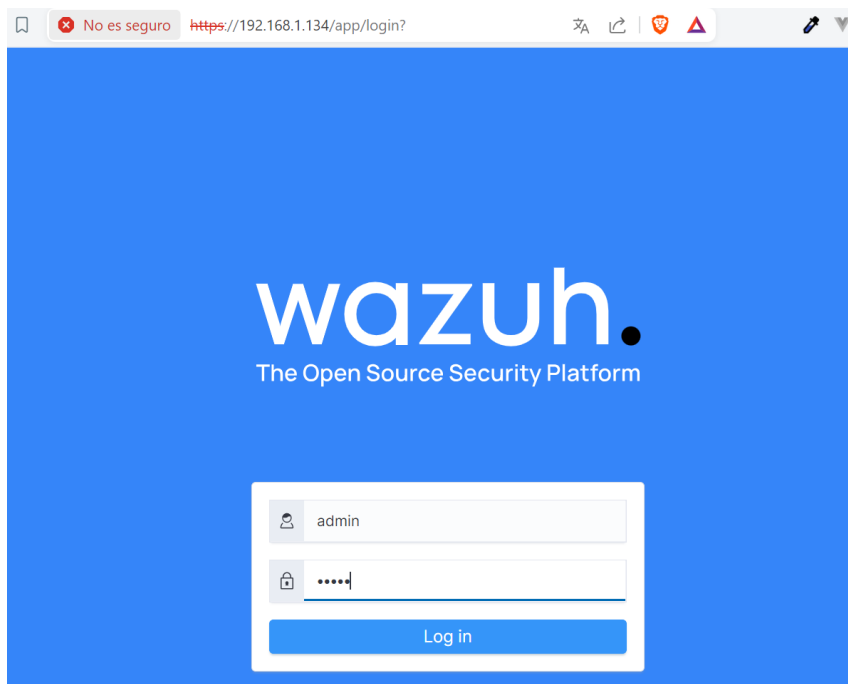
```

          WWWWWW.          WWWWWW.          0000000000
          WWWWWW.          WWWWWW.          00000000
          WWWWWW.          WWWWWW.          000000

WAZUH Open Source Security Platform
https://wazuh.com

[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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:1c:df:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.134/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 85946sec preferred_lft 85946sec
    inet6 fe80::a00:27ff:fe1c:dfae/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]# █
```

Copiamos la IP: 192.168.1.134 y la pegamos en nuestro navegador:

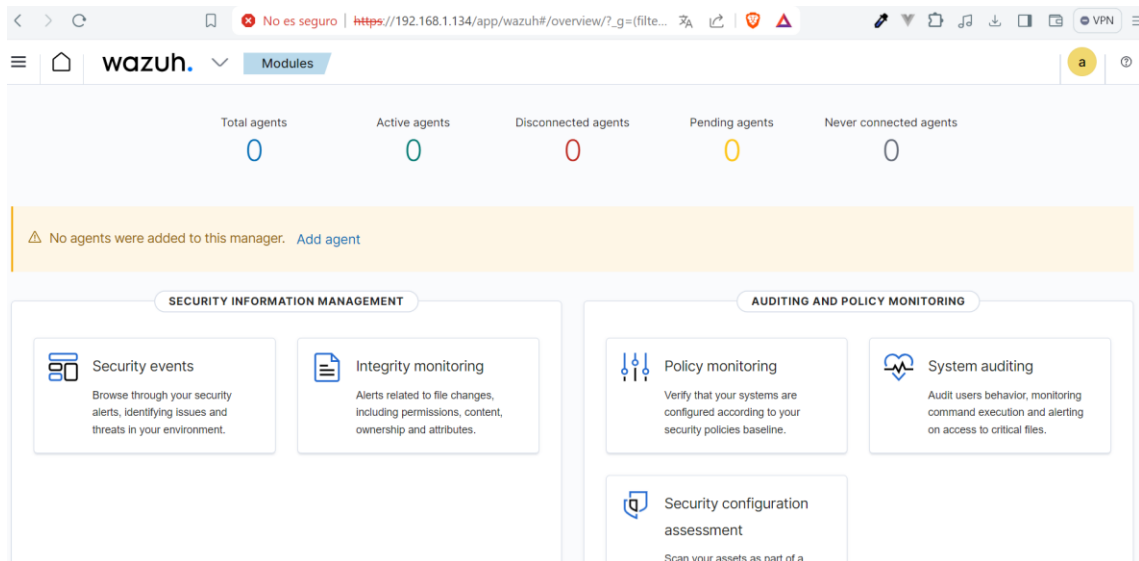


Nombre de usuario: admin

Contraseña: admin

Luego, estas credenciales se deben cambiar desde la plataforma.

Una vez dentro le damos a “Add agent”:



Seleccionamos Wazuh para Linux, escribimos la dirección IP que se le asignó a Wazuh en la máquina virtual y le asignamos un nombre al agente:

No es seguro

https://192.168.1.134/app/wazuh#/agents-previ...

wazuh.

Agents

LINUX

☐ RPM amd64

☐ RPM aarch64

☒ DEB amd64

☐ DEB aarch64

WINDOWS

☐ MSI 32/64 bits

macOS

☐ Intel

☐ Apple silicon

For additional systems and architectures, please check our documentation.

✓

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address:

192.168.1.134

✓

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Kali

Copiamos el siguiente comando en la consola de Kali:

✓

Run the following commands to download and install the agent:

Copy command

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Kali' dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb

Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

```
root@kali: ~# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb && sudo WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Kali' dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb
--2024-05-18 15:05:15-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 38.154.48.93, 38.154.48.249, 18.154.46.117, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.154.48.93|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9372734 (8.9M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.7.4-1_amd64.deb'

wazuh-agent_4.7.4-1_amd64.deb      100%[=====]
2024-05-18 15:05:15 (20.8 MB/s) - 'wazuh-agent_4.7.4-1_amd64.deb' saved [9372734/9372734]

Selecting previously unselected package wazuh-agent.
(Reading database ... 416241 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.4-1_amd64.deb ...
Unpacking wazuh-agent (4.7.4-1) ...
Setting up wazuh-agent (4.7.4-1) ...
```

Y ahora iniciamos el agente copiando este otro comando:

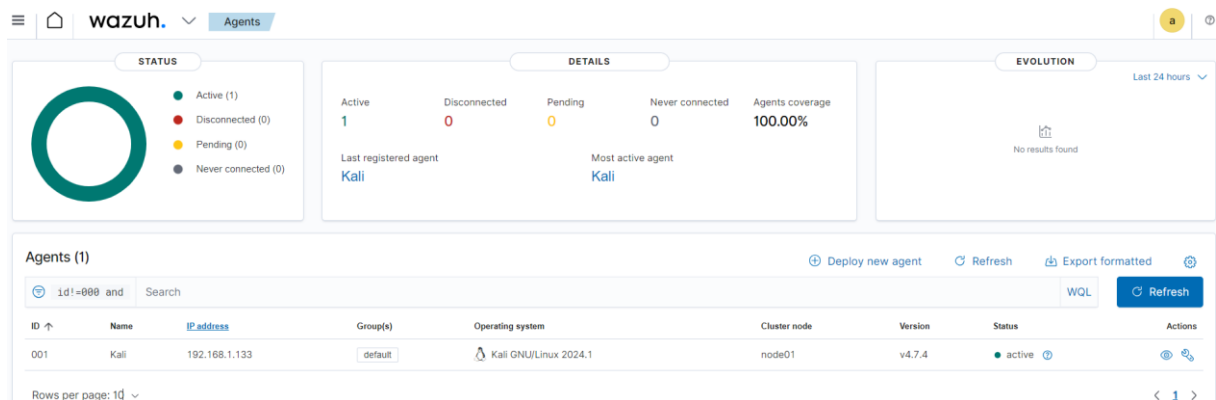
5 Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Close

```
(root@kali)-[/home/kali]
# sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
```

Volvemos a la pantalla inicial de wazuh y vemos como se ha agregado correctamente el agente:



Inicializamos *apache 2*, *mariadb*, *security2* y *headers* en Kali Linux:

```
(root@kali)-[/home/kali]
# systemctl start apache2

(root@kali)-[/home/kali]
# systemctl start mariadb

(root@kali)-[/home/kali]
# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled

(root@kali)-[/home/kali]
# a2enmod headers
Module headers already enabled
```

Realizamos una inyección de código para intentar lograr un login exitoso sin conocer las contraseñas. Esto lo haremos en el archivo `vuln.php` accesible desde el navegador de Kali.

← → ↻ 🏠 localhost/vuln.php
Kali Linux Kali Tools Kali Docs Kali Forums

Username:

Password:

Login

← → ↻ 🏠 localhost/vuln.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali N

Forbidden

You don't have permission to access this resource.

Ahora vamos al dashboard de Wazuh y vemos que nos aparece la alerta de seguridad de Modsecurity, el bloqueo al intento de login anterior:

Browser: No es seguro | https://192.168.1.134/app/wazuh#/agents?tab=...

wazuh. Agents Kali

Security events Integrity monitoring SCA System Auditing Vulnerabilities

ID: 001 Status: active IP address: 192.168.1.133 Version: Wazuh v4.7.4

MITRE: Discovery T1083

Compliance

Events count evolution

File and Directory Discovery

Technique details

ID: T1083

Tactics: Discovery

Version: 1.4

Recent events: 1 hits

Search: DQL Last 24 hours Show dates Refresh

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
May 18, 2024 @ 15:18:34.653	T1083	Discovery	7	30411	ModSecurity: Rejected a query

Rows per page: 10

Vemos que nos salen alertas de seguridad de cada proceso que realizamos en Kali. Iniciamos *Snort* en nuestro Kali y corroboramos este evento en las alertas de seguridad.

```
(kali@kali)-[~]
$ sudo systemctl status snort3-nic.service
[sudo] password for kali:
● snort3-nic.service - Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
   Loaded: loaded (/etc/systemd/system/snort3-nic.service; enabled; preset: disabled)
   Active: active (exited) since Sun 2024-05-19 23:28:22 CEST; 4min 16s ago
     Process: 724 ExecStart=/usr/sbin/ip link set dev eth0 promisc on (code=exited, status=0/SUCCESS)
     Process: 736 ExecStart=/usr/sbin/ethtool -K eth0 gro off lro off (code=exited, status=0/SUCCESS)
    Main PID: 736 (code=exited, status=0/SUCCESS)
      CPU: 59ms

May 19 23:28:22 kali.bosquempresa.local systemd[1]: Starting snort3-nic.service - Set Snort 3 NIC in promi
May 19 23:28:22 kali.bosquempresa.local systemd[1]: Finished snort3-nic.service - Set Snort 3 NIC in promi
log file:
zsh: suspended  sudo systemctl status snort3-nic.service
```

<https://192.168.1.134/app/wazuh#/overview/?tab=ge...>

[wazuh.](#)
[Modules](#)
[Kali](#)
[Security events](#)

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> May 18, 2024 @ 15:36:56.346			PAM: Login session closed.	3	5502
> May 18, 2024 @ 15:36:54.388	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> May 18, 2024 @ 15:36:54.345	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402

No es seguro | <https://192.168.1.134/app/wazuh#/agents-preview/?...>

wazuh.

Agents

Deploy new agent

Linux

☐ RPM amd64

☐ RPM aarch64

☐ DEB amd64

☐ DEB aarch64

Windows

☒ MSI 32/64 bits

macOS

☐ Intel

☐ Apple silicon

For additional systems and architectures, please check our [documentation](#).

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address:

192.168.1.134

Select one or more existing groups: ⓘ

Default ▾

✓

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile $(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='192.168.1.134'
```

ⓘ Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5

Start the agent:

```
NET START WazuhSvc
```

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Escribiendo solicitud web
Escribiendo secuencia de solicitud... (Número de bytes escritos: 474570)

(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='192.168.1.134'^C
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile $(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='192.168.1.134'
```

Una vez finaliza, inicializamos el agente escribiendo el comando “NET START WazuhSvc”:

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

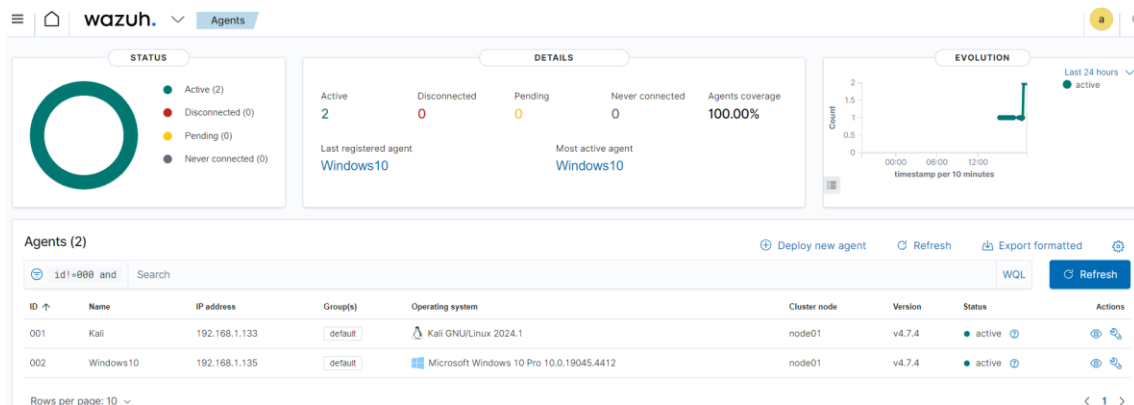
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile $(env.tmp)\wazuh-agent; msixec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.134' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='192.168.1.134'
PS C:\Windows\system32> NET START WazuhSvc
El servicio solicitado ya ha sido iniciado.

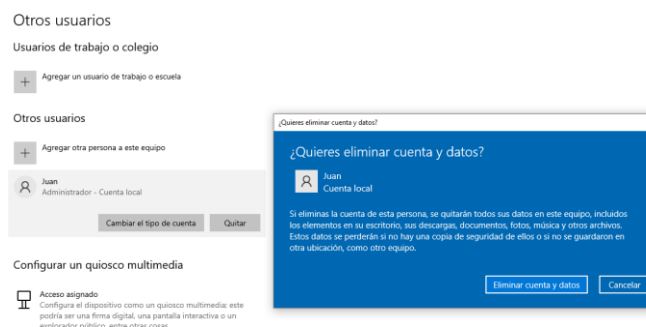
Puede obtener más ayuda con el comando NET HELPMSG 2182.

PS C:\Windows\system32>
```

Ahora, en el dashboard de Wazuh, vemos como se han instalado correctamente los dos agentes:



Eliminamos el usuario Juan creado en nuestra máquina virtual Windows 10 para que se genere actividad:



Comprobamos que se haya creado la alerta de seguridad correctamente:

Windows10Security events

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 18, 2024 @ 19:07:26.036	T1098 T1531	Persistence, Impact	User account disabled or deleted.	8	60111

Table

JSONRule

@timestamp	2024-05-18T17:07:26.036Z
_id	XXXkj8BAy1slGnN2ev
agent.id	002
agent.ip	192.168.1.135
agent.name	Windows10
data.win.eventdata.subjectDomainName	WINDOWS10
data.win.eventdata.subjectLogonId	0x36efb
data.win.eventdata.subjectUserName	Admin
data.win.eventdata.subjectUserSid	S-1-5-21-2588876185-3704041075-2818194894-1001
data.win.eventdata.targetDomainName	WINDOWS10

Creamos un usuario llamado Pedro en nuestra máquina virtual Windows10 para generar otra alerta de seguridad:

Otros usuarios

Usuarios de trabajo o colegio

+ Agregar un usuario de trabajo o escuela

Otros usuarios

+ Agregar otra persona a este equipo

Configurar un quiosco multimedia

Acceso asignado
Configura el dispositivo como un quiosco. Podría ser una firma digital, una pantalla explorador público, entre otras cosas.

Cuenta de Microsoft

Crear un usuario para este equipo

Si quieres usar una contraseña, elige algo que te resulte fácil de recordar, pero que sea difícil de adivinar para los demás.

¿Quién va a usar este PC?

Pedro

Dale seguridad.

••••••••

••••••••

En caso de que olvides la contraseña

Primera pregunta de seguridad

Respuesta

Siguiente

Atrás

Vemos que se ha generado correctamente la alerta de la creación de una nueva cuenta, indicándonos el nombre del usuario creado:

Wazuh

ModulesWindows10Security events ⓘ

May 18, 2024 @ 19:19:01.275

T1098

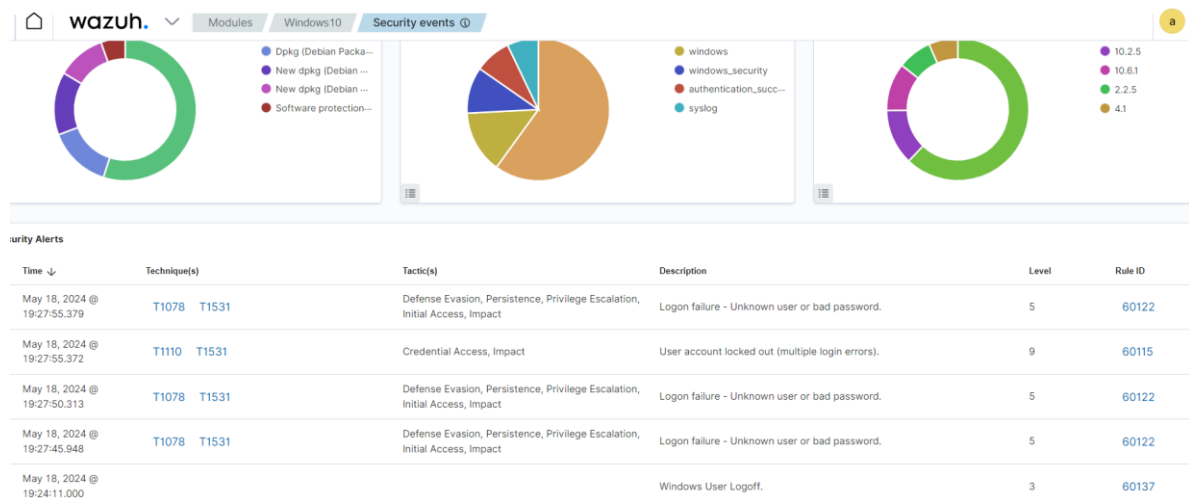
Persistence

User account enabled or created.

Table	JSON	Rule
@timestamp	2024-05-18T17:19:01.275Z	
_id	bHK2j8BAy1iisGn82fK	
agent.id	002	
agent.ip	192.168.1.135	
agent.name	Windows10	
data.win.eventdata.subjectDomainName	WINDOWS10	
data.win.eventdata.subjectLogonId	0x36efb	
data.win.eventdata.subjectUserName	Admin	
data.win.eventdata.subjectUserSid	S-1-5-21-2588876185-3704041075-2818194894-1001	
data.win.eventdata.targetDomainName	WINDOWS10	
data.win.eventdata.targetSid	S-1-5-21-2588876185-3704041075-2818194894-1003	
data.win.eventdata.targetUserName	Pedro	
data.win.system.channel	Security	
data.win.system.computer	Windows10.bosquempresa.local	
data.win.system.eventID	4722	

Por último, cerraremos sesión y volveremos a intentar iniciar sesión en nuestro Windows 10 de la máquina virtual, probando varios inicios de sesión hasta bloquear la cuenta.

Comprobamos, y vemos que se han creado correctamente todas estas alertas de seguridad:



Buen trabajo 10/10