

# Criptografía y Seguridad

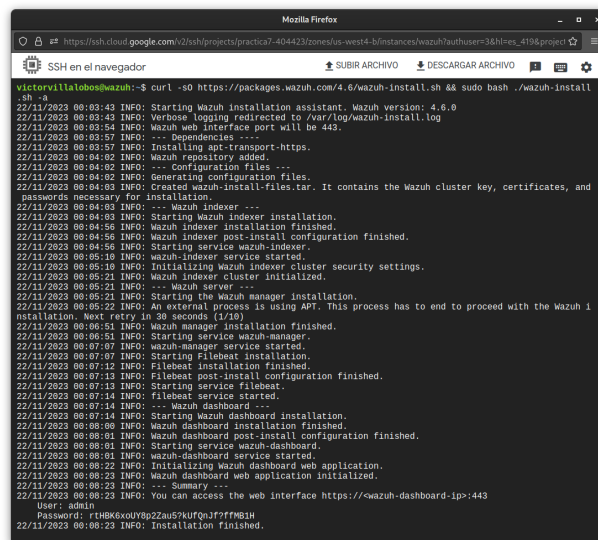
Equipo DragonCode

## Práctica 7

### Instalación de Wazuh

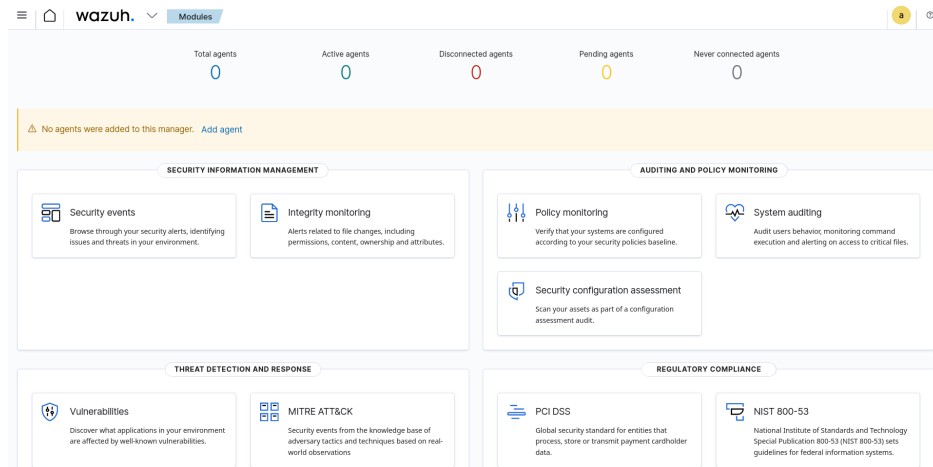
Reyes Ramos Luz Maria, 318211073      Sánchez Castro Gustavo, 318213888  
David Salvador Preciado Márquez, 421091670      Samantha Mora Abonce, 317010945  
Victor de Jesús Villalobos Ramírez 313098675

Con las instancias creadas, ejecutamos el asistente de instalación de Wazuh en la máquina correspondiente

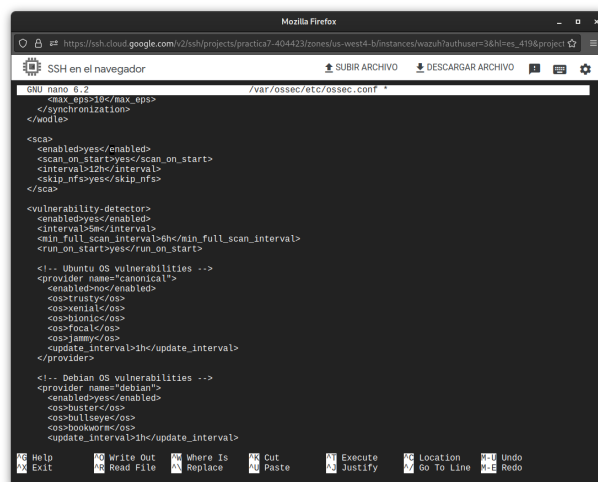


```
Victorvillalobos@wazuh:~$ curl -sO https://packages.wazuh.com/4.6/wazuh-install.sh && sudo bash ./wazuh-install.sh
22/11/2023 00:03:43 INFO: Starting Wazuh installation assistant. Wazuh version: 4.6.0
22/11/2023 00:03:43 INFO: Verbose logging redirected to /var/log/wazuh-install.log
22/11/2023 00:03:54 INFO: Wazuh web interface port will be 443.
22/11/2023 00:03:57 INFO: --- Dependencies ---
22/11/2023 00:03:57 INFO: Installing apt-transport-https.
22/11/2023 00:04:02 INFO: Wazuh repository added.
22/11/2023 00:04:02 INFO: --- Configuration files ---
22/11/2023 00:04:02 INFO: Generating configuration files.
22/11/2023 00:04:03 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
22/11/2023 00:04:03 INFO: --- Wazuh indexer ---
22/11/2023 00:04:03 INFO: Starting Wazuh indexer installation.
22/11/2023 00:04:06 INFO: Wazuh indexer installation finished.
22/11/2023 00:04:06 INFO: Wazuh indexer post-install configuration finished.
22/11/2023 00:04:06 INFO: Starting service wazuh-indexer.
22/11/2023 00:05:19 INFO: Wazuh-indexer service started.
22/11/2023 00:05:19 INFO: Initializing Wazuh indexer cluster security settings.
22/11/2023 00:05:21 INFO: Wazuh indexer cluster initialized.
22/11/2023 00:05:21 INFO: --- Wazuh manager ---
22/11/2023 00:05:21 INFO: Starting the Wazuh manager installation.
22/11/2023 00:05:22 INFO: An external process is using API. This process has to end to proceed with the Wazuh 1 installation. Next retry in 30 seconds (1/10)
22/11/2023 00:06:51 INFO: Wazuh manager installation finished.
22/11/2023 00:06:51 INFO: Starting service wazuh-manager.
22/11/2023 00:07:07 INFO: wazuh-manager service started.
22/11/2023 00:07:07 INFO: Starting Filebeat installation.
22/11/2023 00:07:12 INFO: Filebeat installation finished.
22/11/2023 00:07:13 INFO: Filebeat post-install configuration finished.
22/11/2023 00:07:13 INFO: Starting service filebeat.
22/11/2023 00:07:14 INFO: filebeat service started.
22/11/2023 00:07:14 INFO: --- Wazuh dashboard ---
22/11/2023 00:07:14 INFO: Starting Wazuh dashboard installation.
22/11/2023 00:08:09 INFO: Wazuh dashboard installation finished.
22/11/2023 00:08:09 INFO: Wazuh dashboard post-install configuration finished.
22/11/2023 00:08:09 INFO: Starting service wazuh-dashboard.
22/11/2023 00:08:09 INFO: wazuh-dashboard service started.
22/11/2023 00:08:22 INFO: Initializing Wazuh dashboard web application.
22/11/2023 00:08:23 INFO: Wazuh dashboard web application initialized.
22/11/2023 00:08:23 INFO: --- Summary ---
22/11/2023 00:08:23 INFO: You can access the web interface https://wazuh-dashboard-ip:443
User: admin
Password: r1NBK6c0H9p2Zau5KufQnZ7ffFWB1H
22/11/2023 00:08:23 INFO: Installation finished.
```

Abrimos el dashboard y nos encontramos con lo siguiente



Habilitamos el módulo de detección de vulnerabilidades



Luego instalamos el agente de Wazuh en el endpoint con Debian 11 y lo enrolamos al server.

```

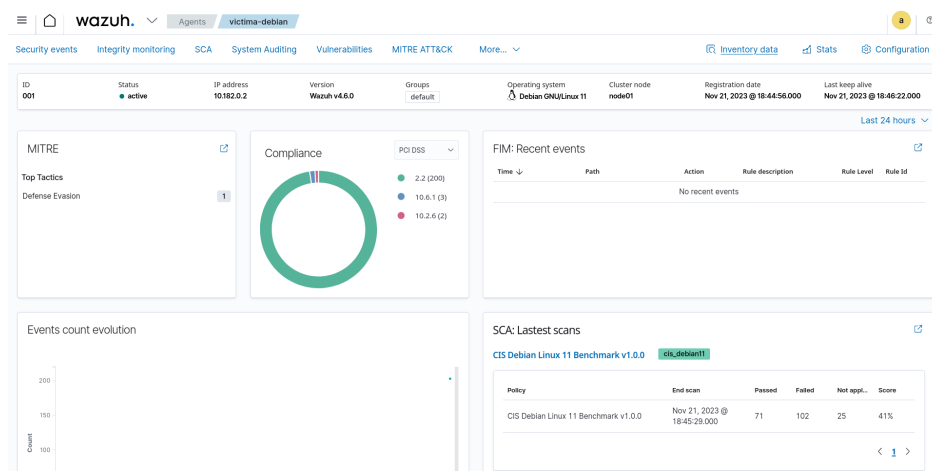
Mozilla Firefox
https://ssh.cloud.google.com/v2/ssh/projects/practica7-404423/zones/us-west4-b/instances/victima-debian/authusers36hmes_419
SSH en el navegador
SUBIR ARCHIVO DESCARGAR ARCHIVO
root@victima-debian:/home/victorvillalobos# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.6.0-1_amd64.deb && sudo WAZUH_MANAGER='10.182.0.3' WAZUH_AGENT_NAME='victima-debian' dpkg -i ./wazuh-agent_4.6.0-1_amd64.deb
--2023-11-22 00:44:44-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.6.0-1_amd64.d
eb
Resolving packages.wazuh.com (packages.wazuh.com)... 18.65.25.59, 18.65.25.48, 18.65.25.123, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.65.25.59|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9219888 (8.8M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.6.0-1_amd64.deb.1'

wazuh-agent_4.6.0-1_amd64.d 100%[=====] 8.79M --.-KB/s in 0.08s

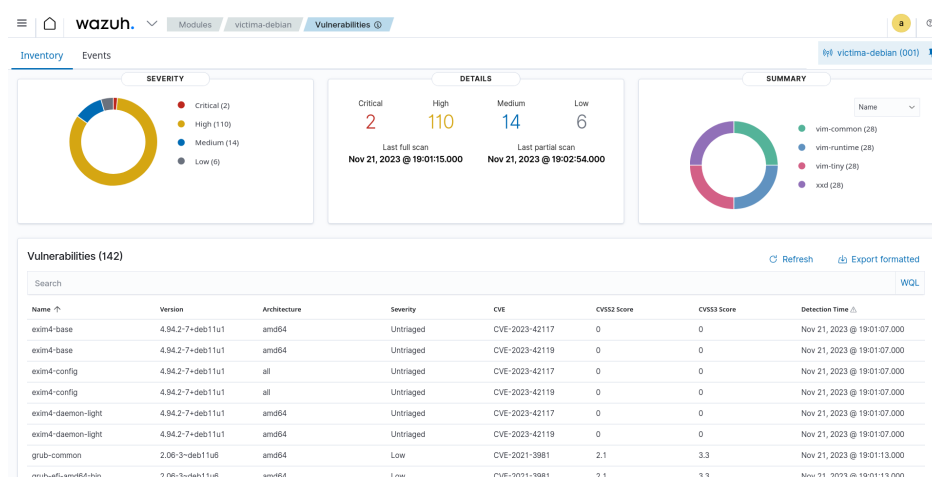
2023-11-22 00:44:44 (108 MB/s) - 'wazuh-agent_4.6.0-1_amd64.deb.1' saved [9219888/9219888]

Selecting previously unselected package wazuh-agent.
(Reading database ... 58563 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.6.0-1_amd64.deb ...
Unpacking wazuh-agent (4.6.0-1) ...
Setting up wazuh-agent (4.6.0-1) ...
root@victima-debian:/home/victorvillalobos# 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 - /lib/systemd/system/wazuh-age
nt.service.
root@victima-debian:/home/victorvillalobos#

```

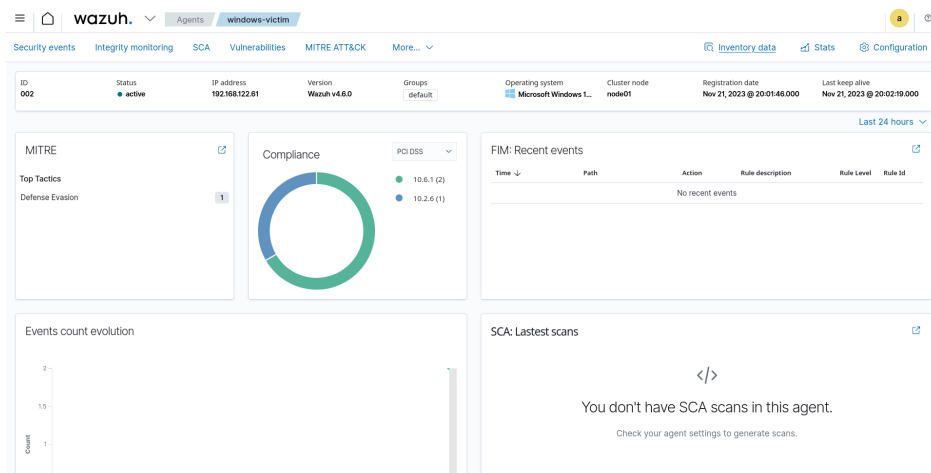


Notemos el módulo de vulnerabilidades funcionando

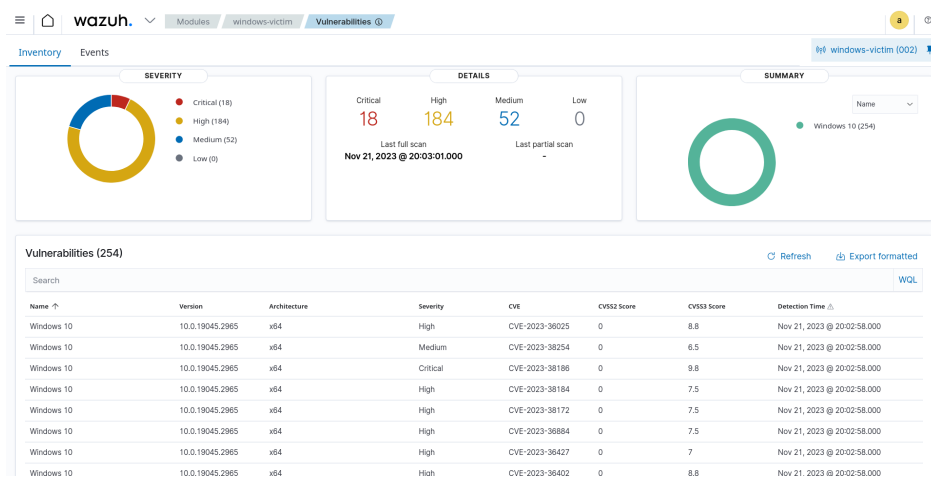


Posteriormente instalamos el agente de Wazuh en el endpoint con Windows 11 y lo enrolamos al server.

```
Select Administrator: Windows PowerShell
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.6.0-1.msi -OutFile .\wazuh-agent-4.6.0-1.msi
PS C:\Windows\system32> msisexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER="34.125.100.61" WAZUH_AGENT_NAME="windows-victim" WAZUH_REGISTRATION_SERVER="34.125.100.61"
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.
PS C:\Windows\system32>
```



Notamos también el módulo de vulnerabilidades funcionando.



Así queda finalmente la sección de agentes del dashboard.

