



***Universidad Nacional
Autónoma de México
Facultad de Ciencias***



Facultad de Ciencias

Criptografía y Seguridad

Semestre: 2025-1

Equipo: Pingüicoders

**Práctica 9:
Lookout, guardian, sentry.
*Parte 1. Configuración***

Arrieta Mancera Luis Sebastián - 318174116

Cruz Cruz Alan Josue - 319327133

García Ponce José Camilo - 319210536

Matute Cantón Sara Lorena - 319331622

Introducción:

En esta primera parte de la práctica veremos el como usar google cloud, al igual que como configurar Wazuh, un sistema de detección de intrusos. Esto es importante ya que en la práctica previa vimos lo relativamente fácil que es crear un malware/spyware.

Desarrollo:

Para esta práctica decidimos usar google cloud ya que uno de nuestros compañeros tenía algo de experiencia con este.

Para poder coordinarnos mejor se optó por realizar una llamada por meet para realizar todo lo referente a la práctica.

Configurar el servidor para Wazuh:

Una vez creada la cuenta en google cloud, creamos la primera máquina virtual la cual actuará como el servidor de wazuh. Para crear esta , seguimos las recomendaciones de la página [quickstart](#) de la documentación de wazuh. En donde recomiendan que la máquina servidor tenga 4 vCPU, 8GiB y 50GB de memoria disponible para 1 a 25 agentes, en nuestro caso solo usaremos dos agentes.

Nosotros creamos la máquina virtual directamente en google cloud siguiendo la siguiente ruta:

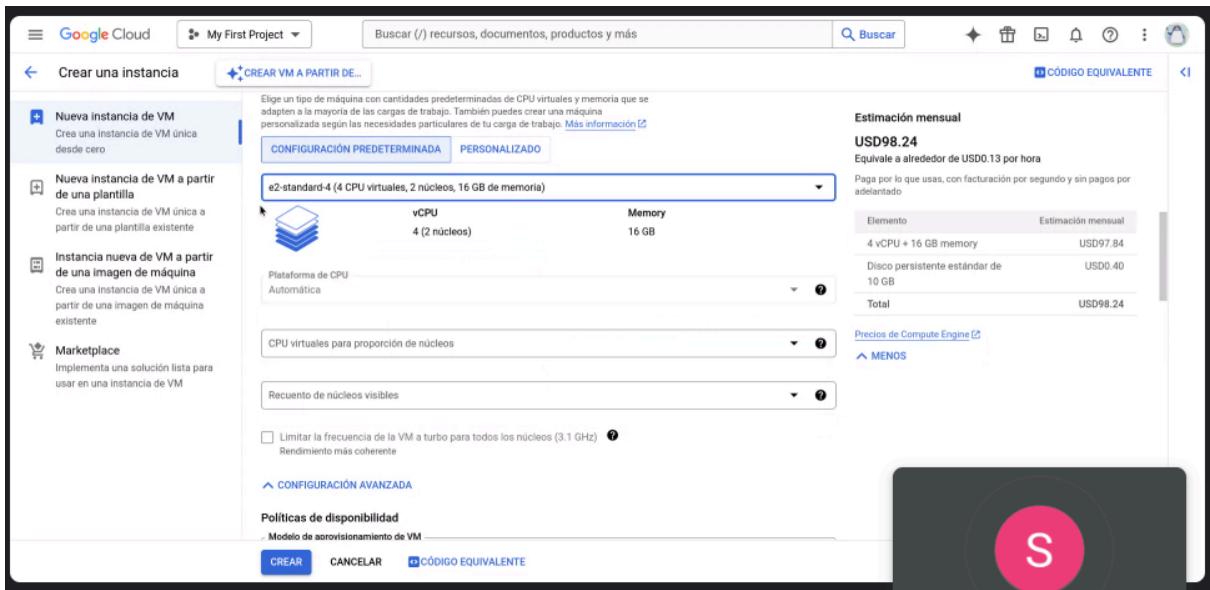
Máquinas virtuales > Nueva Instancia de máquina virtual

En donde creamos una máquina virtual con las siguientes características de acuerdo a lo mencionado previamente:

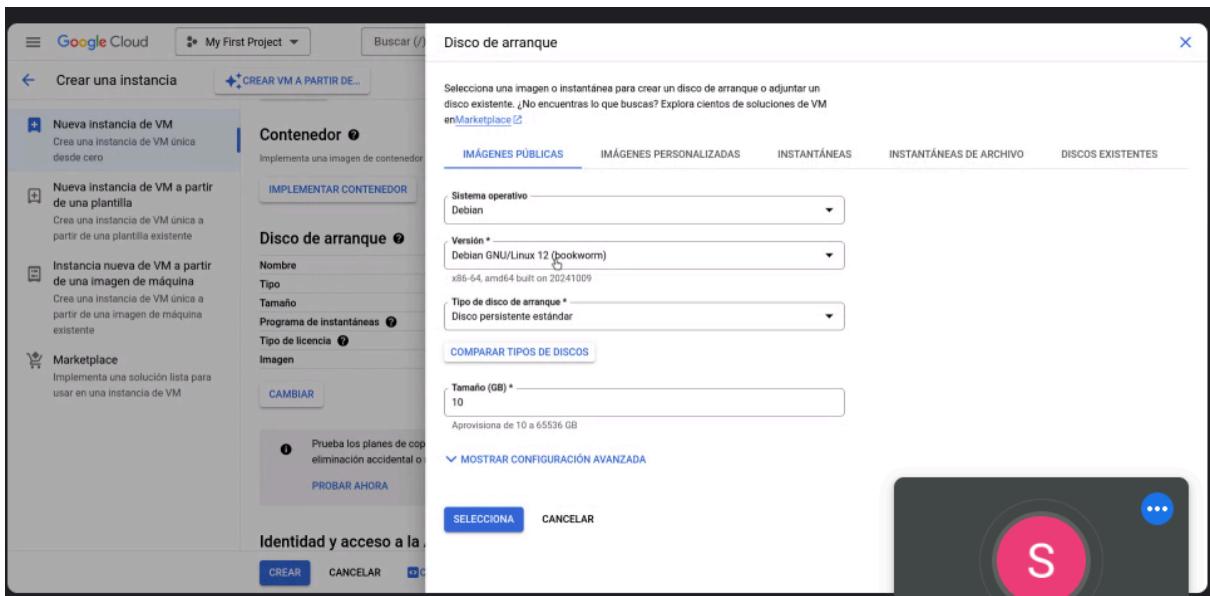
- Una máquina E2 ya que cumple con los requisitos requeridos de Wzuh y porque es una de las más baratas, para no quemarnos los créditos en una única máquina.

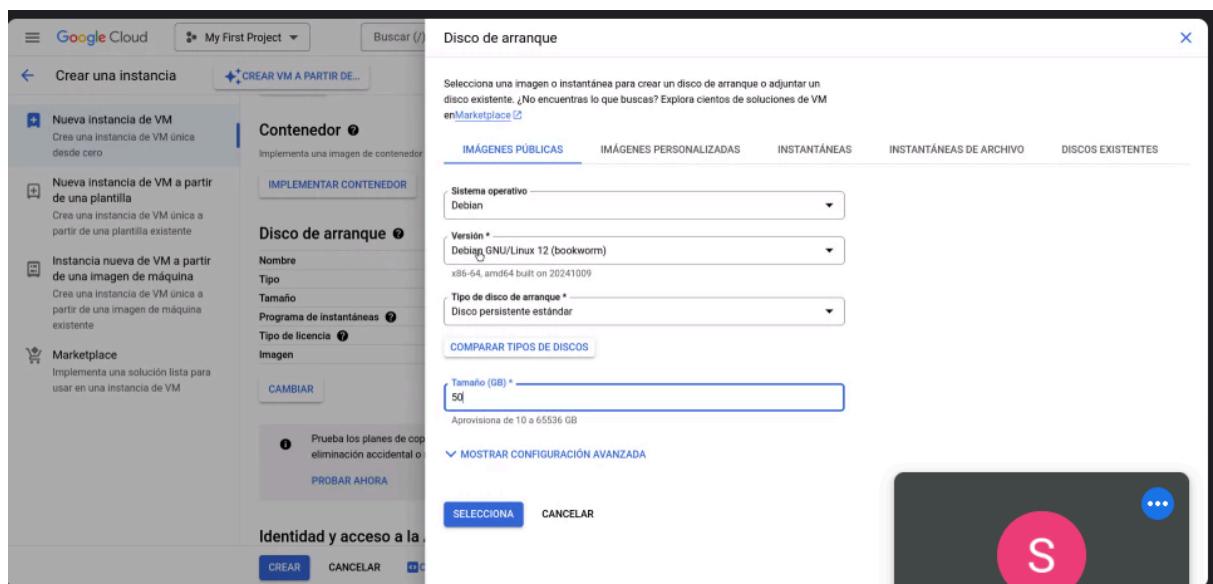
The screenshot shows the Google Cloud Platform interface for creating a new instance. On the left, there's a sidebar with options like 'Nueva instancia de VM', 'Nueva instancia de VM a partir de una plantilla', 'Instancia nueva de VM a partir de una imagen de máquina', and 'Marketplace'. The main area is titled 'Configuración de la máquina' and has tabs for 'De uso general', 'Optimizado para procesamiento', 'Con optimización de memoria', and 'Optimizada para almacenamiento'. Under 'GPU', it says 'Tipos de máquinas para cargas de trabajo comunes, optimizados en función del costo y la flexibilidad'. A table lists various machine types: C4, N4, C3, C3D, E2 (selected), N2, N2D, T2A, T2D, and N1. The E2 row shows: Series E2, Descripción: Rendimiento alto y constante, vCPUs: 0.25 - 32, Memory: 1 - 128 GB, Platform: Según la disponibilidad. To the right, there's an 'Estimación mensual' section showing a total cost of USD24.86, which is equivalent to approximately USD0.03 per hour. It also lists individual costs for memory and disk. At the bottom, there are 'CREAR' and 'CANCELAR' buttons, and a 'CÓDIGO EQUIVALENTE' link.

- Una vez seleccionada la E2, buscamos una que tuviera los 4 procesadores, la cual resultó ser la e2-standard-4.



- Finalmente tuvimos que configurar el disco de arranque. Siguiendo las instrucciones de la práctica seleccionamos debian 11 y modificamos el tamaño para tener los 50Gb recomendados.





Configuración final del disco de arranque:

Disco de arranque

Selecciona una imagen o instantánea para crear un disco de arranque o adjuntar un disco existente. ¿No encuentras lo que buscas? Explora clientes de soluciones de VM en [Marketplace](#)

IMÁGENES PÚBLICAS **IMÁGENES PERSONALIZADAS** **INSTANTÁNEAS** **INSTANTÁNEAS DE ARCHIV**

Sistema operativo: Debian

Versión *: Debian GNU/Linux 11 (bullseye)

Tamaño (GB) *: 50

TIPOS DE DISCOS

COMPARAR TIPOS DE DISCOS

Mostrar configuración avanzada

SELECCIONA CANCELAR

Una vez con el servidor creado creamos una nueva regla del firewall para poder activar los puertos necesarios para el correcto funcionamiento de Wazuh como visto en la [documentación](#).

A continuación se muestra la configuración usada para nuestra nueva regla del firewall, a la cual llamamos intento 1:

Nombre * ?
Se permiten letras minúsculas, números y guiones

Descripción

Registros
Activar los registros de firewall puede generar una gran cantidad de registros y aumentar los costos en Logging. [Más información](#) ?

Activado Desactivado

Red * ?

Prioridad * COMPARAR ?
La prioridad puede ser de 0 a 65535

Dirección del tráfico ?
 Entrada Salida

Permitir todo Protocolos y puertos especificados

TCP
Puertos
P. ej., 20, 50-60

UDP
Puertos
P. ej., todos

SCTP
Puertos
P. ej., 20, 50-60

Otro
Protocolos
Separa múltiples protocolos con comas, p. ej., ah, icmp

Acción en caso de coincidencia ?

Permitir
 Rechazar

Destinos —
 Todas las instancias de la red

Filtro de origen —
 Rangos de IPv4

Rangos de IPv4 de origen *
 0.0.0.0/0

Segundo filtro de origen —
 Ninguno

Filtro de destino —
 Ninguno

Finalmente seleccionamos nuestra nueva regla

	allow-ntp	Entrada	https-server	Intervalos de IP:	tcp:443	Permitir	
<input type="checkbox"/>	default-allow-https	Entrada	https-server	Intervalos de IP:	tcp:443	Permitir	<input type="button" value="▼"/>
<input checked="" type="checkbox"/>	intento1	Entrada	Aplicar a	Intervalos de IP:	tcp:53, 1514, 1515, 9200, 9300, 55000	Permitir	<input type="button" value="▼"/>
<input type="checkbox"/>	default-allow-icmp	Entrada	Aplicar a	Intervalos de IP:	icmp	Permitir	<input type="button" value="6: ▼"/>
<input type="checkbox"/>	default-"	Entrada	Aplicar a	Intervalos de IP:	tcp:0-65535	Permitir	<input type="button" value="6: ▼"/>

Con esto terminamos la configuración de nuestro servidor de Wazuh, desde un punto técnico ahora iniciamos con la configuración de Wazuh.

Google cloud nos permite entrar a sus máquinas virtuales desde SSH en el navegador, vamos a estar usando esta herramienta por el resto de la práctica para interactuar con nuestras máquinas virtuales.

Desde el ssh en el navegador de nuestro servidor para wazuh, lo instalamos mediante el siguiente comando de la página [quickstart](#) de la documentación de wazuh:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

```
SSH en el navegador
Linux instance-20241026-022758 5.10.0-33-cloud-amd64 #1 SMP Debian 5.10.226-1 (2024-10-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jcamilo@instance-20241026-022758:~$ ls
jcamilo@instance-20241026-022758:~$ curl -s0 https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

```
SSH en el navegador
Linux instance-20241026-022758 5.10.0-33-cloud-amd64 #1 SMP Debian 5.10.226-1 (2024-10-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jcamilo@instance-20241026-022758:~$ ls
jcamilo@instance-20241026-022758:~$ curl -s0 https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
26/10/2024 02:47:19 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
26/10/2024 02:47:19 INFO: Verbose logging redirected to /var/log/wazuh-install.log
26/10/2024 02:47:19 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04
.
26/10/2024 02:47:19 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
26/10/2024 02:47:22 INFO: --- Dependencies ---
26/10/2024 02:47:22 INFO: Installing gawk.
26/10/2024 02:47:27 INFO: Verifying that your system meets the recommended minimum hardware requirements.
26/10/2024 02:47:27 INFO: Wazuh web interface port will be 443.
26/10/2024 02:47:27 INFO: --- Dependencies ---
26/10/2024 02:47:27 INFO: Installing lsof.
26/10/2024 02:47:33 INFO: --- Dependencies ---
26/10/2024 02:47:33 INFO: Installing apt-transport-https.
26/10/2024 02:47:34 INFO: Installing debhelper.
```

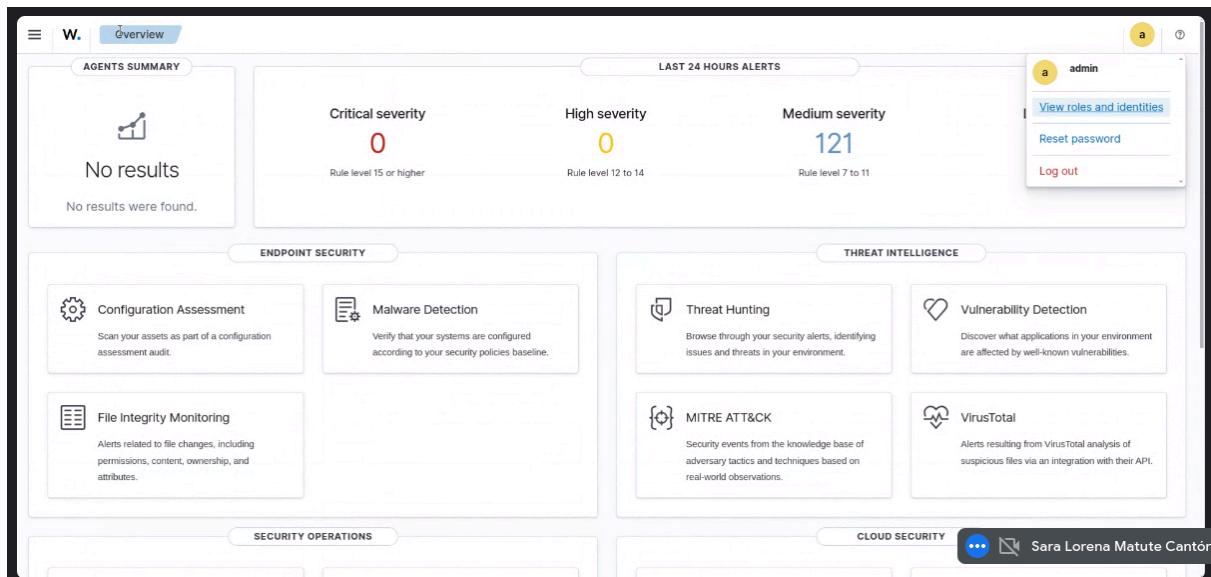
En este punto de la instalación Wazuh nos había marcado que Debian no era uno de los sistemas operativos recomendados y podría haber fallos.

```
SSH en el navegador
26/10/2024 02:48:46 INFO: --- Wazuh indexer ---
26/10/2024 02:48:46 INFO: Starting Wazuh indexer installation.
26/10/2024 02:49:16 INFO: Wazuh indexer installation finished.
26/10/2024 02:49:16 INFO: Wazuh indexer post-install configuration finished.
26/10/2024 02:49:16 INFO: Starting service wazuh-indexer.
26/10/2024 02:49:33 INFO: wazuh-indexer service started.
26/10/2024 02:49:33 INFO: Initializing Wazuh indexer cluster security settings.
26/10/2024 02:49:38 INFO: Wazuh indexer cluster security configuration initialized.
26/10/2024 02:49:38 INFO: Wazuh indexer cluster initialized.
26/10/2024 02:49:38 INFO: --- Wazuh server ---
26/10/2024 02:49:38 INFO: Starting the Wazuh manager installation.
26/10/2024 02:50:47 INFO: Wazuh manager installation finished.
26/10/2024 02:50:47 INFO: Wazuh manager vulnerability detection configuration finished.
26/10/2024 02:50:47 INFO: Starting service wazuh-manager.
26/10/2024 02:51:08 INFO: wazuh-manager service started.
26/10/2024 02:51:06 INFO: Starting Filebeat installation.
26/10/2024 02:51:12 INFO: Filebeat installation finished.
26/10/2024 02:51:12 INFO: Filebeat post-install configuration finished.
26/10/2024 02:51:12 INFO: Starting service filebeat.
26/10/2024 02:51:12 INFO: filebeat service started.
26/10/2024 02:51:12 INFO: --- Wazuh dashboard ---
26/10/2024 02:51:12 INFO: Starting Wazuh dashboard installation.
26/10/2024 02:52:57 INFO: Wazuh dashboard installation finished.
26/10/2024 02:52:57 INFO: Wazuh dashboard post-install configuration finished.
26/10/2024 02:52:57 INFO: Starting service wazuh-dashboard.
26/10/2024 02:52:57 INFO: wazuh-dashboard service started.
26/10/2024 02:52:57 INFO: Updating the internal users.
26/10/2024 02:53:11 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
26/10/2024 02:53:39 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
26/10/2024 02:54:23 INFO: Initializing Wazuh dashboard web application.
26/10/2024 02:54:24 INFO: Wazuh dashboard web application initialized.
26/10/2024 02:54:24 INFO: --- Summary ---
26/10/2024 02:54:24 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: yepPUD05KP5*YeKwX3Azx37K6UB+h1*v
26/10/2024 02:54:24 INFO: --- Dependencies ---
26/10/2024 02:54:24 INFO: Removing gawk.
26/10/2024 02:54:28 INFO: Removing lsof.
26/10/2024 02:54:29 INFO: Installation finished.
jcamilo@instance-20241026-022758:~$
```

Una vez terminada la instalación nos dio el siguiente mensaje:

26/10/2024 02:54:24 INFO: You can access the web interface
<https://<wazuh-dashboard-ip>:443> User: admin Password:
yepPUDO5KP5*YeKWx3AZx37K6UB+hi*V

Una vez en el navegador pudimos entrar al dashboard de Wazuh



Una vez más en la terminal de SSH en el navegador modificamos el archivo para que nos permita ver la detección de vulnerabilidades.

```
<!-- Database synchronization settings -->
<synchronization>
  <max_eps>10</max_eps>
</synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>

<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://127.0.0.1:9200</host>
  </hosts>
  <ssl>
    <certificateAuthorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificateAuthorities>
    <certificate>/etc/filebeat/certs/wazuh-server.pem</certificate>
    <key>/etc/filebeat/certs/wazuh-server-key.pem</key>
  </ssl>
</indexer>

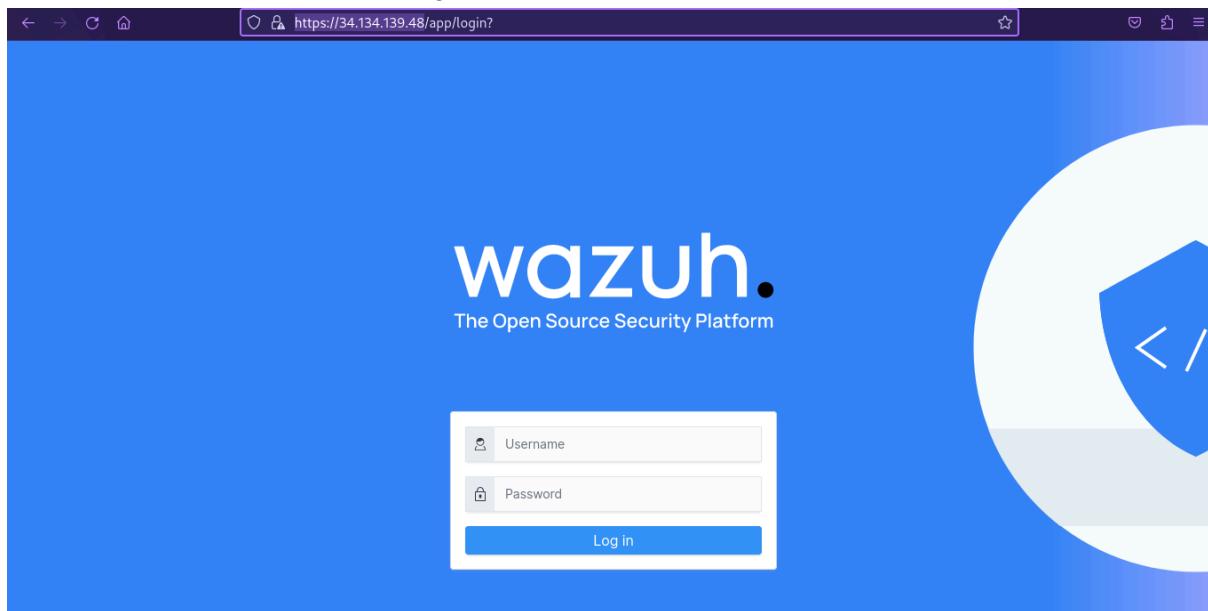
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
</syscheck>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>
```

Así que para acceder al dashboard de nuestro Wazuh es necesario poner la siguiente dirección en el navegador:
navegador:

<https://34.134.139.48>

Lo cual debería de llevarlo a la siguiente pantalla:



Username: Admin

Password: yepPUDO5KP5*YeKWx3AZx37K6UB+hi*V

Configurar el agente víctima:

Para la máquina que actuará como víctima hicimos un proceso bastante similar al que previamente fue descrito al crear el servidor de Wazuh, con la excepción de que no modificamos el espacio, es decir creamos una máquina virtual E2-Standard-4 y la dejamos con su configuración original.

Estado	Nombre	Zona	Recomendaciones	En uso por	IP interna	IP externa	Conectar
<input type="checkbox"/>	instance-20241026-022758	us-central1-c			10.128.0.2 (nic0)	34.134.139.48 (nic0)	SSH
<input type="checkbox"/>	victima						⋮

Antes de continuar creamos una nueva regla de firewall, en la cual, aparte de habilitar los puertos que usa Wazuh, habilitamos el puerto 5000 para poder realizar el ataque de espionaje. Para este paso realizamos lo mismo que cuando creamos la nueva regla para el servidor de Wazuh, añadiendo el puerto 5000.

A screenshot of a web-based interface for configuring a firewall rule. The section title is "Protocolos y puertos". There are two radio button options: "Permitir todo" (unchecked) and "Protocolos y puertos especificados" (checked). Under "Protocolos y puertos", there is a checked checkbox for "TCP". Below it is a "Puertos" input field containing the value "1515,1514,55000,53,9200,9300,5000". A note below the input field says "P. ej., 20, 50-60".

Una vez con la máquina creada, regresamos al dashboard y procedimos con ayuda de las instrucciones en pantalla.

Primero, buscamos qué versión del .deb debíamos de usar.

The screenshot shows the Google Cloud Compute Engine Images page. A specific image, 'debian-12-bookworm-v20241009', is selected. The details shown include:

- Descripción:** Debian, Debian GNU/Linux, 12 (bookworm), `amd64` built on 20241009
- Ubicación:** asia (Asia-Pacífico), eu (Unión Europea), us (Estados Unidos)
- Arquitectura:** x86-64
- Etiquetas:** Ninguno
- Etiquetas:** ⚠ No tienes permisos suficientes para mostrar la lista de etiquetas.
- Hora de creación:** oct 9, 2024, 7:22:04 p. m. UTC-06:00
- Familia:** debian-12
- Tipo de encriptación:** Administrada por Google
- REST equivalente:** /compute/images/{image_id}

Para esto revisamos las características de nuestra máquina víctima en google cloud.
En nuestro caso seleccionamos la versión de amd.

The screenshot shows the 'Deploy new agent' wizard, step 2: 'Select the package to download and install on your system'. It offers three options:

- LINUX:**
 - RPM amd64
 - RPM aarch64
 - DEB amd64** (selected)
 - DEB aarch64
- WINDOWS:**
 - MSI 32/64 bits
- macOS:**
 - Intel
 - Apple silicon

A note at the bottom says: 'For additional systems and architectures, please check our documentation'.

Después colocamos la ip de la máquina víctima.

The screenshot shows the 'Deploy new agent' wizard, step 2: 'Server address'. The 'Assign a server address' field contains '34.134.139.48'. The 'Remember server address' checkbox is checked. Step 3, 'Optional settings', is partially visible below.

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

Assign a server address ?
34.134.139.48
 Remember server address

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: ?
Agent name

⚠ The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: ?

Esto nos dio una lista de comandos que ejecutamos en terminal:

```

SSH en el navegador
SUBIR ARCHIVO DESCARGAR ARCHIVO
tcp  LISTEN  0      4096      0.0.0.0:5355  0.0.0.0:*
tcp  LISTEN  0      20        127.0.0.1:25  0.0.0.0:*
tcp  LISTEN  0      4096      127.0.0.53xlo:53  0.0.0.0:*
tcp  LISTEN  0      128       0.0.0.0:22  0.0.0.0:*
tcp  LISTEN  0      4096      127.0.0.54:53  0.0.0.0:*
tcp  LISTEN  0      4096      [::]:5355   [::]:*
tcp  LISTEN  0      128       [::]:22    [::]:*
tcp  LISTEN  0      20        [::]:1:25   [::]:*
jcamilo@victima:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb && sudo WAZUH_MANAGER='34.134.139.48' WAUH_AGENT_NAME='victima' dpkg -i ./wazuh-agent_4.9.1-1_amd64.deb
--2024-10-28 02:59:38-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 18.238.136.85, 18.238.136.36, 18.238.136.30, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.238.136.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10767678 (10M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.9.1-1_amd64.deb'

wazuh-agent_4.9.1-1_amd64.deb      100%[=====] 10.27M  ---KB/s  in 0.1s

2024-10-28 02:59:38 (91.8 MB/s) - 'wazuh-agent_4.9.1-1_amd64.deb' saved [10767678/10767678]

Selecting previously unselected package wazuh-agent.
(Reading database ... 70354 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.9.1-1_amd64.deb ...
Unpacking wazuh-agent (4.9.1-1) ...
Setting up wazuh-agent (4.9.1-1) ...
jcamilo@victima:~$ sudo systemctl daemon-reload
jcamilo@victima:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
jcamilo@victima:~$ sudo systemctl start wazuh-agent
jcamilo@victima:~$ 

```

Sara Lorena Matute Cantón

Finalmente entramos a nuestro dashboard y ahí se encontraba nuestro nuevo agente.

Endpoints

AGENTS BY STATUS

- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (0)

TOP 5 OS

TOP 5 GROUPS

Agents (1)

Show only outdated

Deploy new agent Refresh Export formatted More

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	victima	10.128.0.3	default	Debian GNU/Linux 12	node01	v4.9.1	active	...

Rows per page: 10

Sara Lorena Matute Cantón

Una configuración extra que hicimos fue añadir un usuario y contraseña a nuestra máquina víctima.

```
Linux victim 6.1.0-26-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

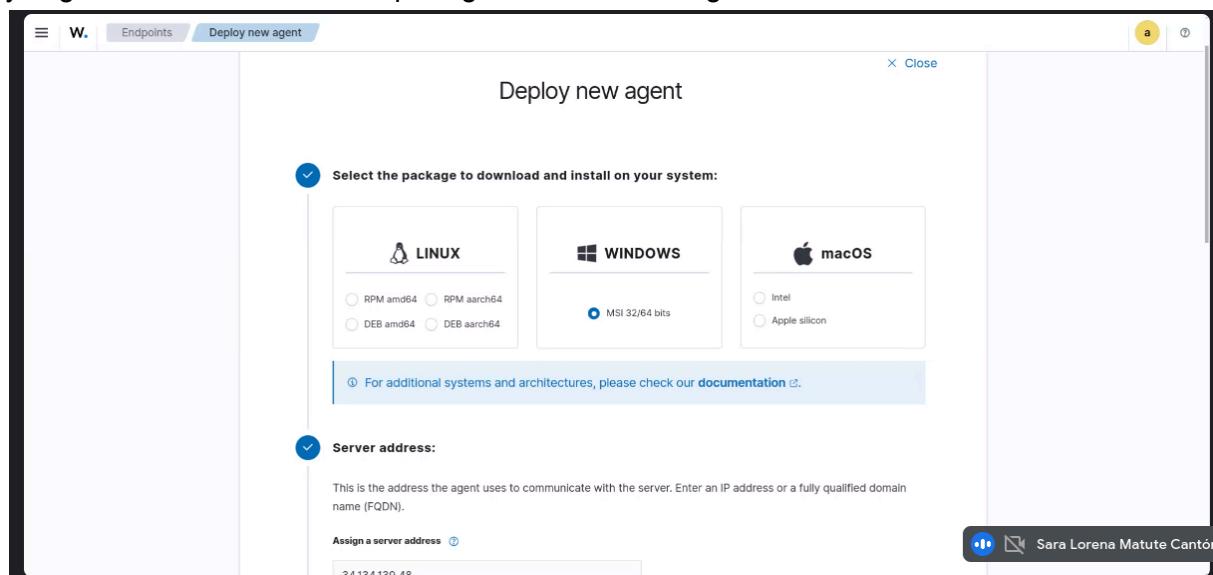
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 28 02:53:02 2024 from 35.235.244.34
jcamilo@victima:~$ whoami
jcamilo
jcamilo@victima:~$ sudo passwd verdic
passwd: user 'verdic' does not exist
jcamilo@victima:~$ sudo passwd jcamilo
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
jcamilo@victima:~$ sudo passwd jcamilo
New password:
```

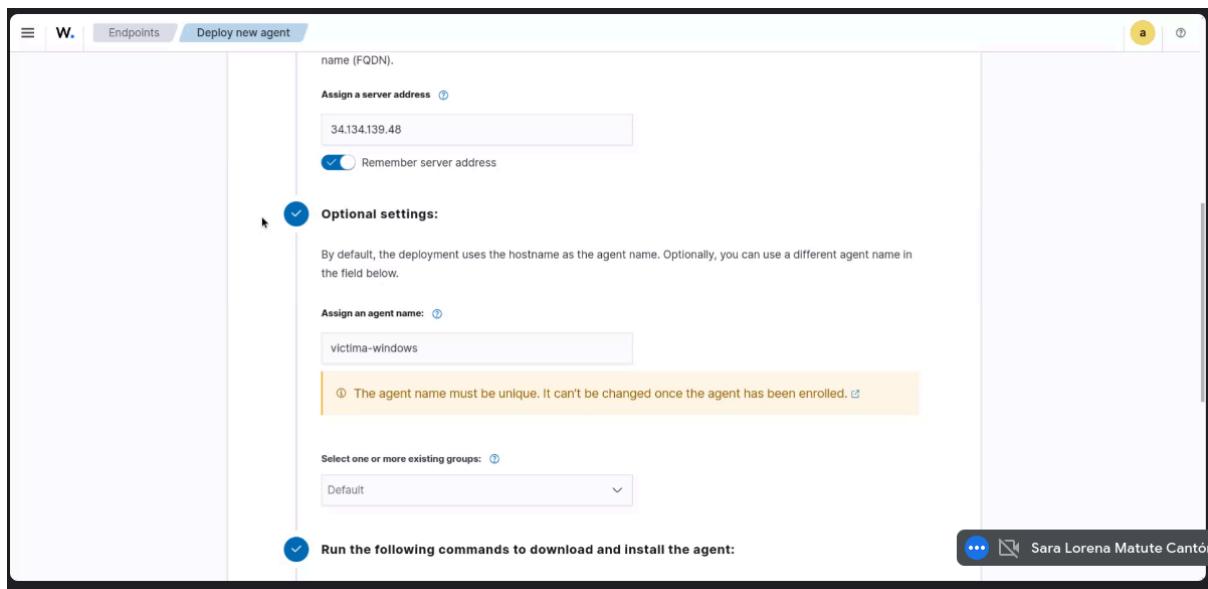
*Usuario: jcamilo
Contraseña: verdict*

Configurar maquina de windows:

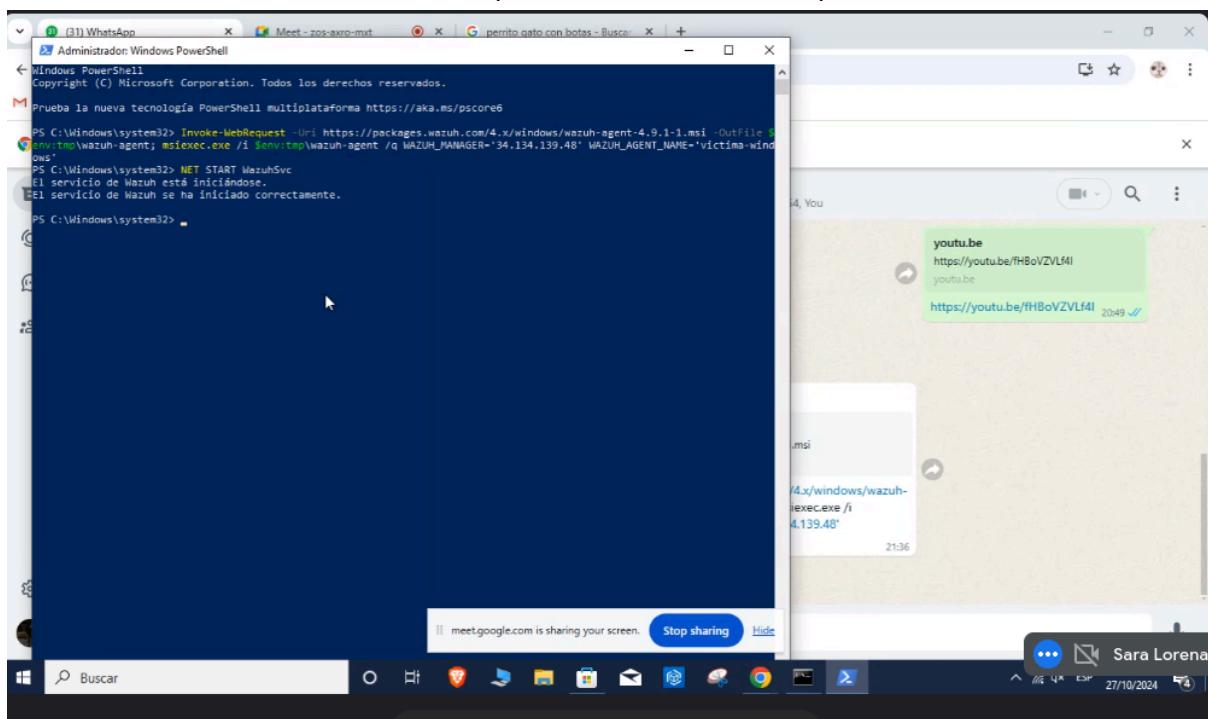
Para esta práctica optamos por usar un windows en una máquina local.

Una vez más regresamos al dashboard de Wazuh y seleccionamos la opción para windows y seguimos sus instrucciones para generar el nuevo agente.

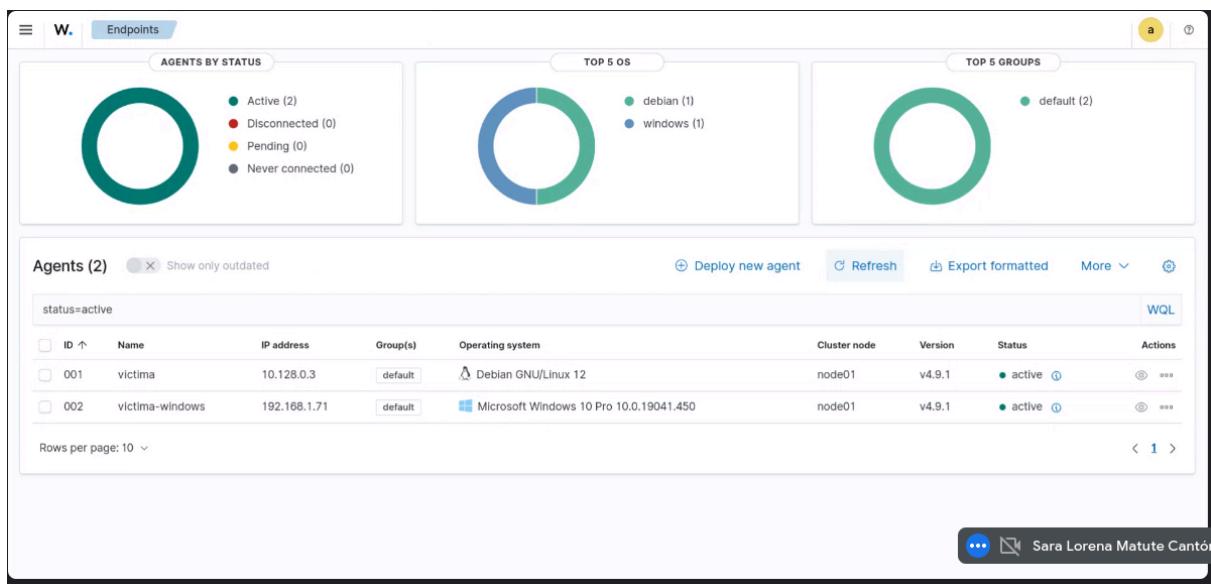




Una vez en la terminal de windows copiamos los comandos especificados:



Finalmente volvemos a nuestro dashboard y observamos que ya están nuestros dos agentes.



Configurar maquina atacante y víctima:

Para configurar la posible conexión entre atacante y víctima (Debian) realizamos los siguientes pasos.

Primero creamos una nueva regla de firewall

[← Crea una regla de firewall](#)

[a página anterior](#)

Las reglas de firewall controlan el tráfico saliente o entrante a una instancia. Según la configuración predeterminada, se bloquea el tráfico que entra desde el exterior de tu red.[Más información](#)

Nombre * [?](#)

Se permiten letras minúsculas, números y guiones

Descripción

Registros

Activar los registros de firewall puede generar una gran cantidad de registros y aumentar los costos en Logging.[Más información](#)

Activado

Desactivado

Red * [?](#)

Prioridad * [COMPARAR](#) [?](#)

La prioridad puede ser de 0 a 65535

Dirección del tráfico [?](#)

Entrada

Salida

[←](#) Crea una regla de firewall

Acción en caso de coincidencia [?](#)

Permitir

Rechazar

Destinos

Todas las instancias de la red



Filtro de origen

Rangos de IPv4



Rangos de IPv4 de origen *

10.128.0.0/20



Segundo filtro de origen

Ninguno



Filtro de destino

Ninguno



Protocolos y puertos [?](#)

Permitir todo

Protocolos y puertos especificados

TCP

Puertos

22

P. ej., 20, 50-60

Generamos una llave ssh para el atacante.

```
jcamilo@atacante:~$ ssh-keygen -t rsa -b 4096 -C "atacante"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jcamilo/.ssh/id_rsa):
/home/jcamilo/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/jcamilo/.ssh/id_rsa
Your public key has been saved in /home/jcamilo/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:zfKXpFMDkaigivGL/9EwPDG7oVdcEsqmbkHtgo0c22Y atacante
The key's randomart image is:
+---[RSA 4096]---+
|   .   .   |
|   o... .   |
|   ...B.... |
| o== =.o o . |
| +*=EO o S o + |
| o.++ O   o + o |
| .+.+ .   + o |
| .... .   o   |
| ....       |
+---[SHA256]---+
jcamilo@atacante:~$
```

Obtuvimos la llave pública.

```
jcamilo@atacante:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQADQDNXYug9hOrnqDWWzCfgsIAm2Cw41sUIQ01MkuCu1HnQp5uZkOIpBSeTsQ1LfUPmykUyhlpWds
TrG3MG+Oh/CvTseEFYxyB7c1k2Mun/Bgm+AKw4Y/qhD37hfydiWqKtVULCLda1xEsrx9A8b7rnCgwUjFU0tBdbV7/C5BRmz7MM5MogpoN1aNAXjF
APHMJ18K5uw9Xf5sRViUrH0ClVVBz+iyhVpqDyUBaEX05rmWowWX+In5U7hpXlvPVmm157UcdZ/TLppaI+EGhdQu3HqaOWKC0yFN4c6VdqZWG
YIJMBiLdkiosPppw4g3Ybevjw3pyaGyr4Cnev18JFkHlmKLNZ01nxarUpssKiT6k/wlOb4FJKJBKmlkA+16qgh0B6KEUgqmNFqSH/LNM8M+ty06FEG
NxfwQLbPbjAKa8TcTRcdPMCnk3OKiy4bUi/ZNSWDsIIXwyWHKCMZmzl06ON0MkZaCGNhweiDrUXskfq6KxRE20ekAtZ2hRqqjUSX1xO5n/sZ2bGC
c94L+tmus7Ks1aGqtGhPh/qCeJDwjSMuly8WytP7rMRHxc9YLDowKMevn+3qoD87P9ttalDwvP0UQhSm0KniMva/YuQVWGx/2qkuSaExtEEou
t6M3TiD06iHuEZjiPFax3fWXXr85lhiTWdnaddti6RGw== atacante
jcamilo@atacante:~$
```

Le pasamos la llave pública a la víctima (ya que no nos permite pasársela desde el atacante)

```
jcamilo@victima:~$ mkdir -p ~/.ssh
nano ~/.ssh/authorized_keys
jcamilo@victima:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCDNXYug9hOrnqDWWzCfgsaIAm2Cw41sUIQ01MkuCu1HnQp5uZkOIpBSeTsQ1LfUPmykUyhlpTwdsTrG3MG+Oh/Cv7sEEFXxyB7c1x2MunJBgm+AKw4Y/qhD37fyd1WqktvULCLda1xE8rx9A8b7rnCqwuJFUo0tBdbV7/c5BRmZ7MM5Mogpo1anAXjfAPHMJ18K5uw9Xf5sRViUrH0C1VVbz+iyhVpqDyUBaEX05rmWovWX+In5U7hpXLvPVmm157UucDZ/TLLppaiI+EGHdQu3HqaOWKC0yFN4c6VdqZUWGYIJMBlDkioSppw4g3Ybevjw3pyaGyr4Cnev18JFKhlmKLNZ01nxnRUpskit6k/w1ob4FJKJBKmlka+16qgh0B6KEUGqmNFqSH/LNM8M+ty06EFEGNx fwQLbPbjAKa8TcTRcdPMcnk30Kiy4bUi/ZN5WDsIIxNyWHKCGMZmzl06ON0MkZaCGNhweiDrUXskfq6KxREZ0ekAtZ2hRqggjUSX1x05n/sZ2bGCc94L+tmu87Ks1aGqttGhPh/qCeJDwjSJMulY8WytP7rMRHxc9YLDowKMevn+3q0oD87P9ttalDwvP0UQhSm0KniMva/YuQVWGx/2qkuSaExtEEou t6M3TiD06iHuEZJiPFAX3fWXXr851hiTWdnaddti6RGw== atacante
jcamilo@victima:~$
```

Revisamos que ssh esté activo

```
jcamilo@victima:~$ chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
jcamilo@victima:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-10-28 02:46:56 UTC; 14h ago
     Docs: man:sshd(8),
           man:sshd_config(5).
   Main PID: 843 (sshd)
      Tasks: 1 (limit: 19175)
        Memory: 5.8M
          CPU: 13.206s
        CGroup: /system.slice/ssh.service
            └─843 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 28 17:23:19 victima sshd[8829]: pam_unix(sshd:session): session opened for user jcamilo(uid=1000) by (uid=0)
Oct 28 17:23:19 victima sshd[8829]: pam_env(sshd:session): deprecated reading of user environment enabled
Oct 28 17:24:33 victima sshd[8857]: Connection closed by authenticating user jcamilo 10.128.0.4 port 41750 [preauth]
Oct 28 17:24:33 victima sshd[8859]: Connection closed by authenticating user jcamilo 10.128.0.4 port 41766 [preauth]
Oct 28 17:24:34 victima sshd[8861]: Connection closed by authenticating user jcamilo 10.128.0.4 port 41776 [preauth]
Oct 28 17:29:43 victima sshd[8885]: Connection closed by authenticating user jcamilo 10.128.0.4 port 37002 [preauth]
Oct 28 17:31:01 victima sshd[8887]: Connection closed by authenticating user jcamilo 10.128.0.4 port 59390 [preauth]
Oct 28 17:31:02 victima sshd[8889]: Connection closed by authenticating user jcamilo 10.128.0.4 port 59406 [preauth]
Oct 28 17:31:02 victima sshd[8891]: Connection closed by authenticating user jcamilo 10.128.0.4 port 59408 [preauth]
Oct 28 17:33:56 victima sshd[8916]: Connection closed by authenticating user root 194.169.175.38 port 61798 [preauth]
jcamilo@victima:~$
```

Desde víctima, activamos la autenticación al usar sshd

```
GNU nano 7.2                                     /etc/ssh/sshd_config *
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PubkeyAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes

^G Help      ^C Write Out    ^W Where Is      ^K Cut      ^T Execute      ^C Location      M-U Undo
^Y Exit      ^R Read File    ^A Replace      ^U Paste      ^J Justify      ^/ Go To Line    M-E Redo
```

Reiniciamos el servicio

```
jcamilo@victima:~$ sudo nano /etc/ssh/sshd_config
jcamilo@victima:~$ sudo systemctl restart ssh
jcamilo@victima:~$
```

Y lo probamos desde atacante, por lo tanto ya está todo listo del lado de la víctima

```
jcamilo@atacante:~$ ssh jcamilo@10.128.0.3
jcamilo@10.128.0.3's password:
```

Del lado del atacante instalamos hydra para el ataque

```
jcamilo@atacante:~$ sudo apt install hydra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  firebird3.0-common firebird3.0-common-doc fontconfig fontconfig-config fonts-dejavu-core i965-v4-driver
  intel-media-v4-driver libaom3 libapril1 libavutil11 libavcodec59 libavutil57 libbson-1.0-0 libcairo-gobject2
  libcairo2 libcodecs2-1.0 libdatriel libdavid6 libdeflate0 libdrm-amdgpu1 libdrm-common libdrm-intel1
  libdrm-nouveau2 libdrm-radeon1 libdrm2 libfbclient2 libfontconfig1 libfreerdp2-2 libfribidi0
  libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgl1 libgl1-mesa-dri libglapi-mesa
```

Y creamos una lista de 500 palabras, con la ultima siendo la contraseña de víctima

```
GNU nano 7.2                                     word-list.txt *
britney
katrina
christina
pasaway
cocacola
mahal
grace
linda
albert
tatiana
london
cantik
0123456
lakers
marie
teiubesc
147258369
charlotte
natalia
francisco
amorcito
smile
paola
angelito
manchester
hahaha
elephant
mommy1
shelby
147258
kelsey
genesis
amigos
snickers
verdic
```

```
jcamilo@atacante:~$ nano word-list.txt
jcamilo@atacante:~$ wc -l word-list.txt
500 word-list.txt
jcamilo@atacante:~$
```

Instalamos python, pip y python-venv

```
jcamilo@atacante:~$ sudo apt install python3 python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.11.2-1+b1).
The following additional packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu build-essential bzip2 cpp cpp-12 dpkg-dev fakeroot g++
g++-12 gcc gcc-12 javascript-common libabsl20220623 libalgorithm-diff-perl libalgorithm-diff-xs-perl
libalgorithm-merge-perl libasan8 libatomic1 libavif15 libbinutils libc-dev-bin libc-devtools libc6-dev
libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdpkg-perl libexpat1-dev libfakeroot
libfile-fcntllock-perl libgavl-1 libgcc-12-dev libgd3 libgprofng0 libheif1 libis123 libitm1 libjansson4
libjs-jquery libjs-sphinxdoc libjs-underscore liblocale-gettext-perl liblsan0 libmpc3 libmpfr6 libnsl-dev
libpython3-dev libpython3.11 libpython3.11-dev libquadmath0 libstdc++-12-dev libtirpc-dev libtsan2 libubsan1
libxpm4 libyuv0 linux-libc-dev make manpages-dev patch python3-dev python3-distutils python3-lib2to3
python3-setuptools python3-wheel python3.11-dev rpcsvc-proto zlib1g-dev
Suggested packages:
binutils-doc bzip2-doc cpp-doc gcc-12-locales cpp-12-doc debian-keyring g++-multilib g++-12-multilib
gcc-12-doc gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-12-multilib apache2 | lighttpd
| httpd glibc-doc git bzr libgd-tools libstdc++-12-doc make-doc ed diffutils-doc python-setuptools-doc
The following NEW packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu build-essential bzip2 cpp cpp-12 dpkg-dev fakeroot g++
g++-12 gcc gcc-12 javascript-common libabsl20220623 libalgorithm-diff-perl libalgorithm-diff-xs-perl
libalgorithm-merge-perl libasan8 libatomic1 libavif15 libbinutils libc-dev-bin libc-devtools libc6-dev
libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdpkg-perl libexpat1-dev libfakeroot
libfile-fcntllock-perl libgavl-1 libgcc-12-dev libgd3 libgprofng0 libheif1 libis123 libitm1 libjansson4
libjs-jquery libjs-sphinxdoc libjs-underscore liblocale-gettext-perl liblsan0 libmpc3 libmpfr6 libnsl-dev
libpython3-dev libpython3.11 libpython3.11-dev libquadmath0 libstdc++-12-dev libtirpc-dev libtsan2 libubsan1
libxpm4 libyuv0 linux-libc-dev make manpages-dev patch python3-dev python3-distutils python3-lib2to3
python3-pip python3-setuptools python3-wheel python3.11-dev rpcsvc-proto zlib1g-dev
0 upgraded, 73 newly installed, 0 to remove and 4 not upgraded.
Need to get 80.5 MB of archives.
After this operation, 323 MB of additional disk space will be used.
Do you want to continue? [Y/n] █
```

```
jcamilo@atacante:~$ sudo apt install python3-venv
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
python3-pip-whl python3-setuptools-whl python3.11-venv
The following NEW packages will be installed:
python3-pip-whl python3-setuptools-whl python3-venv python3.11-venv
0 upgraded, 4 newly installed, 0 to remove and 4 not upgraded.
Need to get 2836 kB of archives.
After this operation, 3170 kB of additional disk space will be used.
Do you want to continue? [Y/n] █
```

Creamos un entorno nuevo y lo activamos

```
jcamilo@atacante:~$ python3 -m venv venv
jcamilo@atacante:~$ source venv/bin/activate
(venv) jcamilo@atacante:~$ █
```

En el entorno instalamos Flask

```
jcamilo@atacante:~$ python3 -m venv venv
jcamilo@atacante:~$ source venv/bin/activate
(venv) jcamilo@atacante:~$ pip install Flask
Collecting Flask
  Downloading flask-3.0.3-py3-none-any.whl (101 kB)
    ━━━━━━━━━━━━━━━━ 101.7/101.7 kB 3.1 MB/s eta 0:00:00
Collecting Werkzeug>=3.0.0
  Downloading werkzeug-3.0.6-py3-none-any.whl (227 kB)
    ━━━━━━━━━━━━━━ 228.0/228.0 kB 10.2 MB/s eta 0:00:00
Collecting Jinja2>=3.1.2
  Downloading jinja2-3.1.4-py3-none-any.whl (133 kB)
    ━━━━━━━━━━━━ 133.3/133.3 kB 0.2 MB/s eta 0:00:00
Collecting itsdangerous>=2.1.2
  Downloading itsdangerous-2.2.0-py3-none-any.whl (16 kB)
Collecting click>=8.1.3
  Downloading click-8.1.7-py3-none-any.whl (97 kB)
    ━━━━━━━━━━ 97.9/97.9 kB 13.2 MB/s eta 0:00:00
Collecting blinker>=1.6.2
  Downloading blinker-1.8.2-py3-none-any.whl (9.5 kB)
Collecting MarkupSafe>=2.0
  Downloading MarkupSafe-3.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (23 kB)
Installing collected packages: MarkupSafe, itsdangerous, click, blinker, Werkzeug, Jinja2, Flask
Successfully installed Flask-3.0.3 Jinja2-3.1.4 MarkupSafe-3.0.2 Werkzeug-3.0.6 blinker-1.8.2 click-8.1.7 itsdangerous-2.2.0
(venv) jcamilo@atacante:~$
```

Y ponemos el código para el ataque de spyware

```
GNU nano 7.2                                     atac.py *
from flask import Flask, request

app = Flask(__name__)

@app.route('/api/receptor', methods=['POST'])
def recibir_datos():
    data = request.form.get('data')
    print(f'Datos recibidos: {data}')

    with open('datos_recibidos.txt', 'a') as f:
        f.write(f'{data}\n')

    return '', 200

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

Por último probamos que el servidor de Flask funcione, y todo está lista para los ataques

```
(venv) jcamilo@atacante:~$ python atac.py
* Serving Flask app 'atac'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://10.128.0.4:5000
Press CTRL+C to quit
```

Referencias:

1. <https://documentation.wazuh.com/current/quickstart.html>
2. <https://documentation.wazuh.com/current/getting-started/architecture.html>