20-9-2025

Respuesta en Vivo a Incidentes

Proyecto Final 4Geeks

Jose Antonio Briones
4GEEKS ACADEMY

Índice

Objetivo

Partiendo de la premisa que el sistema no puede ser desconectado, se debe de realizar una inspección del mismo con el fin de detectar si se ha visto comprometido el sistema, en el caso afirmativo detectar las vulnerabilidades que han podido ser explotadas, recopilación de las evidencias, restaurar la integridad y disponibilidad del mismo.

Herramientas

- Linux Kali.
    - nmap
    - nikto
- BD de CVE de la web https://www.cve.org/
- Autopsys 4.22.1
- FTK Imager 4.7.3.81

Datos del Técnico	
Autor	Jose Antonio B. R.
Fecha	23/09/2025
Versión	1.0
Empresa auditada	4geeks Academy

Introducción

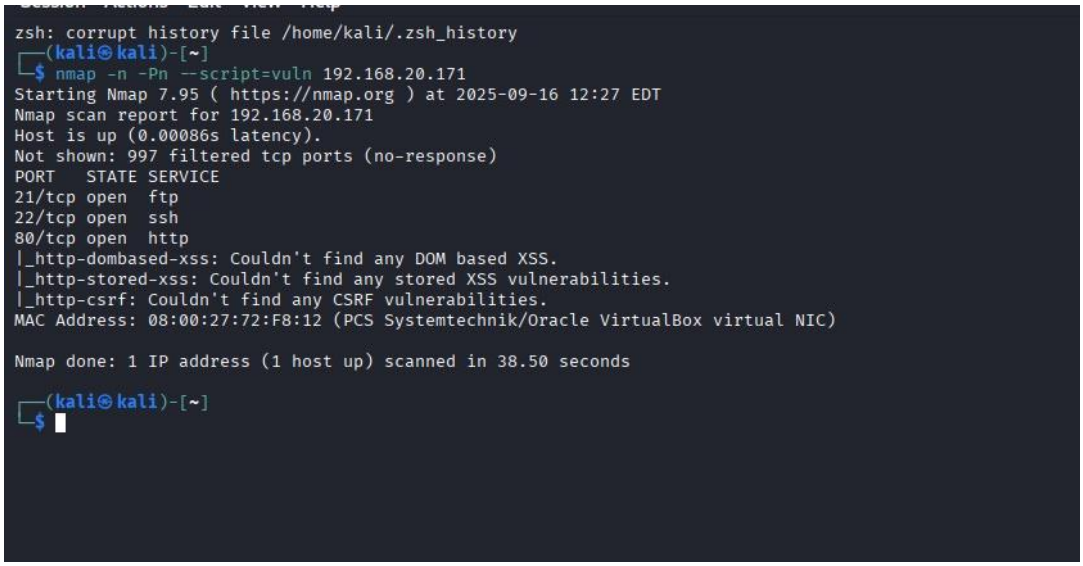
El presente informe es el resultado de la auditoría de seguridad y pruebas de penetración que se han realizado para ver vectores de entrada.

Dichas pruebas siempre se realizaron dentro de un marco de confianza y buena fe, con el objetivo de evaluar la seguridad a través de la utilización de técnicas de detección y explotación activa, con el fin de verificar la seguridad e identificar las posibles amenazas.

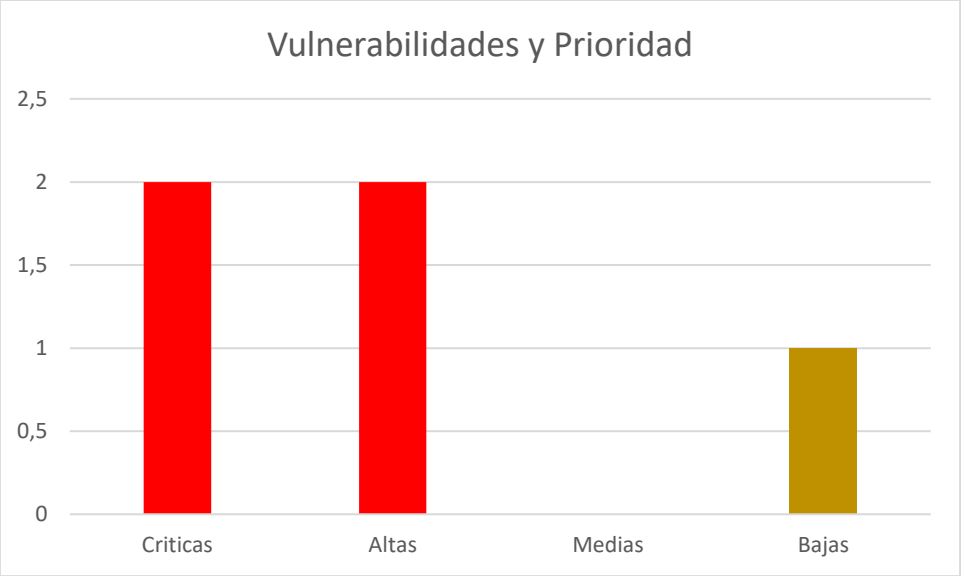
Resumen estratégico.

La máquina analizada tiene los siguientes puertos expuestos

Puerto/Protocolo	Servicio	Programa
21/tcp	ftp	Vsftpd 3.0.5
22/tcp	Ssh	OpenSSH 8.2p1
80/tcp	http	Apache 2.4.41



Vulnerabilidades detectadas



Críticas	Alta	Bajas	Totales
2	2	1	5

Recomendaciones

Atender y solucionar las incidencias que están clasificadas como "Altas" de forma inmediata, para asegurar el sistema y prever problemas tantos de pérdida de competitividad, información y datos sensibles que lleven al incumplimiento de la normativa vigente.

En un corto plazo se recomendando atender las "medias", las vulnerabilidades no atendidas producen inestabilidad en el sistema convirtiéndose en puntos que pueden ser explotados.

En el plan de mantenimiento trimestral, atender las "Bajas".

Informe Técnico

Resumen del Entorno.

Se dispone de una máquina con el sistema operativo Linux concretamente

Ubuntu 20.04.6 LTS
Codename.- focal

Actualmente está conectada y tiene una dirección IP 192.168.20.171

Para el análisis e inspección de la maquina se va utilizar un dispositivo conectado a la misma red, con el sistema operativo

Kali Release 2025.3
Codename.- Kali.rolling

Escaneo y análisis

Después del análisis se ha observado que dispone de 3 puertos expuestos, el puerto 80 sobre el que corre un servidor Web, concretamente el apache en la versión 2.4.41 el puerto 21 sobre el que correo un servicio FTP, a través de la aplicación Vsftpd 3.0.5 y el puerto 22 sobre el que corre el servicio de SSH, la aplicación OpenSSH 8.2

Se han realizado dos escaneos:

Con la herramienta nmap

sudo nmap -sV -P --script=vuln [IP]

Con la herramienta nikto

Sudo nikto -h [IP]

Detalles técnicos

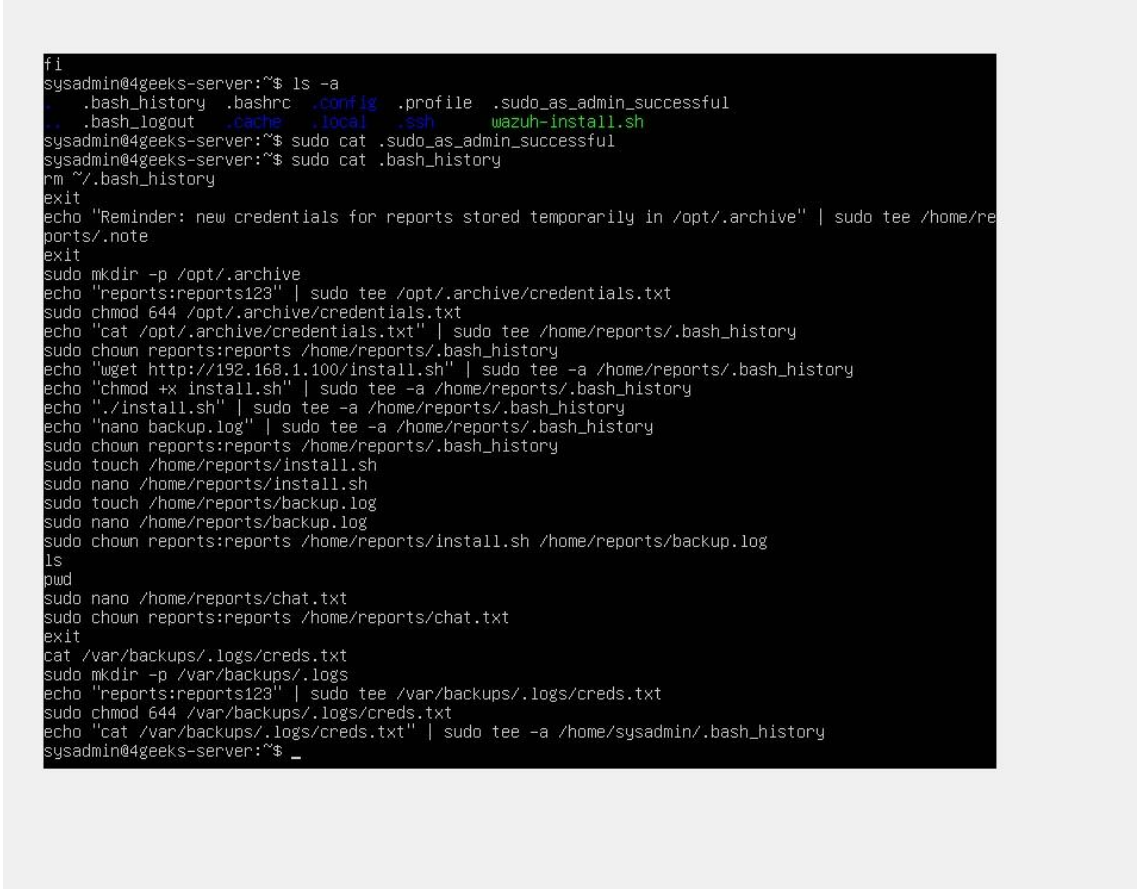
Los resultados desprendidos se observan puntos varios puntos que deben de ser atendidos.

Importancia		Descripción	Puerto
Crítica	**CVE-2023-25690 (información)**	Algunas configuraciones de Mod_Proxy permiten un ataque de contrabando de solicitudes http	80/tcp
Crítica	**CVE-2024-38476 (información)**	Vulnerabilidad en el núcleo de apache que permite la ejecución de scripts locales	80/tcp
Alta	**CVE-2020-15778 (información)**	Permite inyección de comandos en función remota scp.	22/tcp
Alta	**CVE-2023-38408 (información)**	Ruta de búsqueda poco confiable	22/tcp

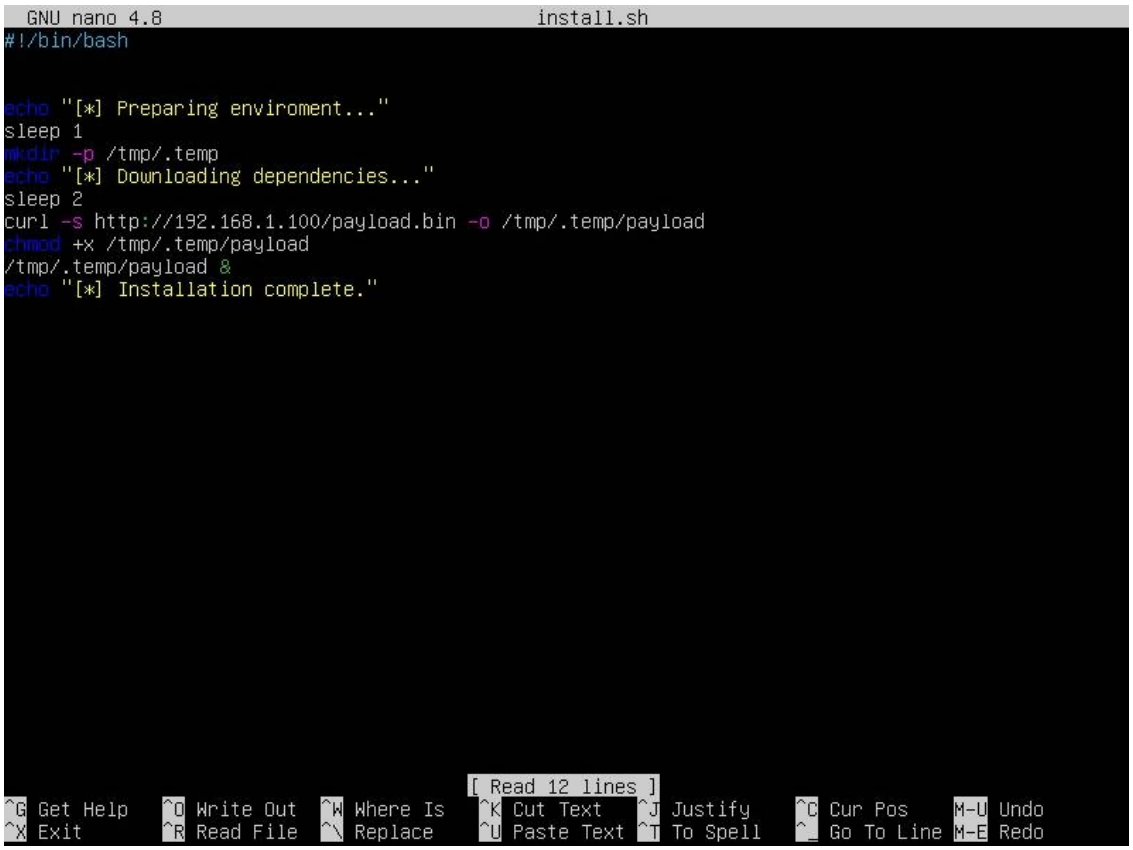
Evidencias

Se observa algunas acciones que pueden inducir a pensar que ha habido una fuga de información, concretamente los usuarios y las contraseñas de los usuarios del sistema.

Revisando el .bash_history del usuario sysadmin, se observa la ejecución por parte de sysadmin de un script que se llama “install.sh”.



Dicho script se conecta a la url http://192.168.1.100/ y se descarga un archivo Payload.bin que lo aloja en la ruta “tmp/.temp/payload” que crea desde el propio script, ejecutándolo dentro de la máquina.



Dicho Script es descargado directamente desde una URL, por lo que es bastante probable que se esté explotando una de las vulnerabilidades del servidor apache.

Realizando una consulta sobre las reglas que se aplica al firewall de la propia máquina se observa que no se filtran los paquetes ni el contenido de los puertos expuestos, facilitando la explotación de los mismos y generando un agujero de seguridad.

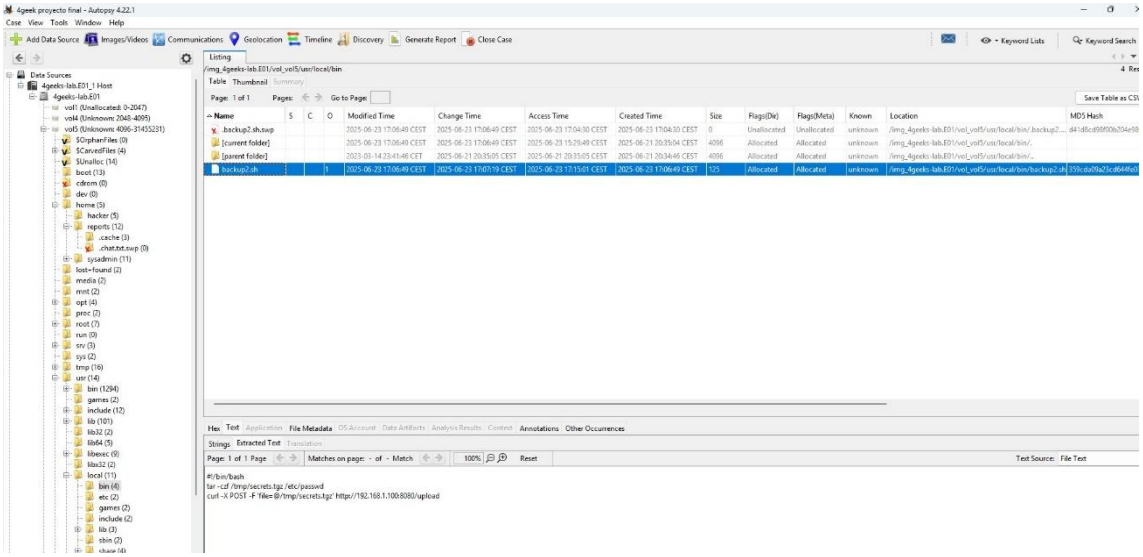
```
sysadmin@4geeks-server:~$ sudo ufw status verbose
[sudo] password for sysadmin:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
21                         ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
21 (v6)                    ALLOW IN    Anywhere (v6)

sysadmin@4geeks-server:~$ _
```

Una vez instalado el Payload.bin, se produce una copia tanto del archivo password, como el shadow del directorio etc y se envía a la dirección 192.168.1.100:8080/upload

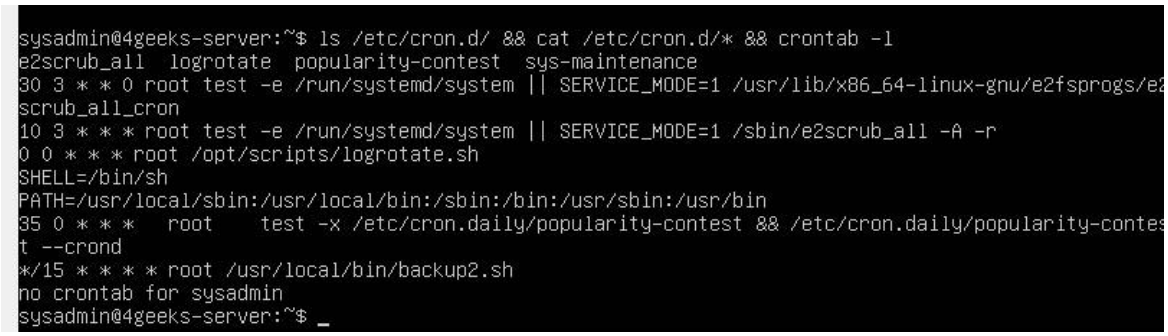
A través un script que se llama backup2.sh que se encuentra en la ruta /usr/local/bin



El archivo secrets.tgz todavía se encuentra dentro del sistema en la carpeta “tmp”

```
sysadmin@4geeks-server:/tmp$ ls
secrets.tgz
snap-private-tmp
systemd-private-6047fbe61ede4aa88ff5afe0618e546d-apache2.service-aDCUdg
systemd-private-6047fbe61ede4aa88ff5afe0618e546d-ModemManager.service-pvLXOe
systemd-private-6047fbe61ede4aa88ff5afe0618e546d-systemd-logind.service-tos23f
systemd-private-6047fbe61ede4aa88ff5afe0618e546d-systemd-resolved.service-568e4g
systemd-private-6047fbe61ede4aa88ff5afe0618e546d-systemd-timesyncd.service-ulWnCf
sysadmin@4geeks-server:/tmp$ _
```

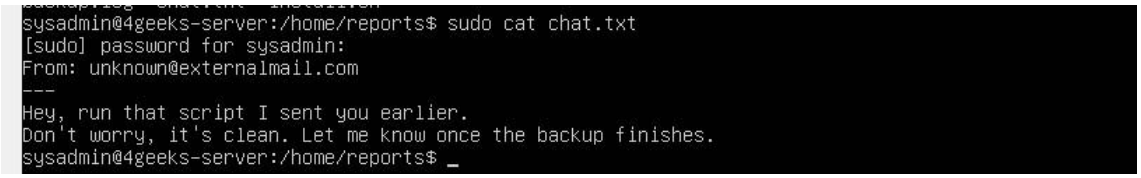
Existe una programación dentro crontab para que se ejecute dicho script cada 15 minutos, por lo que la fuga de la información es recurrente.



Todo esto ocurre el día 23/06/2025 desde las 13:00 aproximadamente hasta las 18:45 según el timeline aportado por Autopsys.

Existe también un archivo chat.txt que está en el home de un usuario nuevo que ha sido creado por sysadmin, en el que se copia un correo en el que se autoriza la ejecución del script una vez que se haya realizado el backup.

Esta evidencia podría indicar que el vector de entrada podría ser un phishing enviado desde el correo unknow@externalmail.com

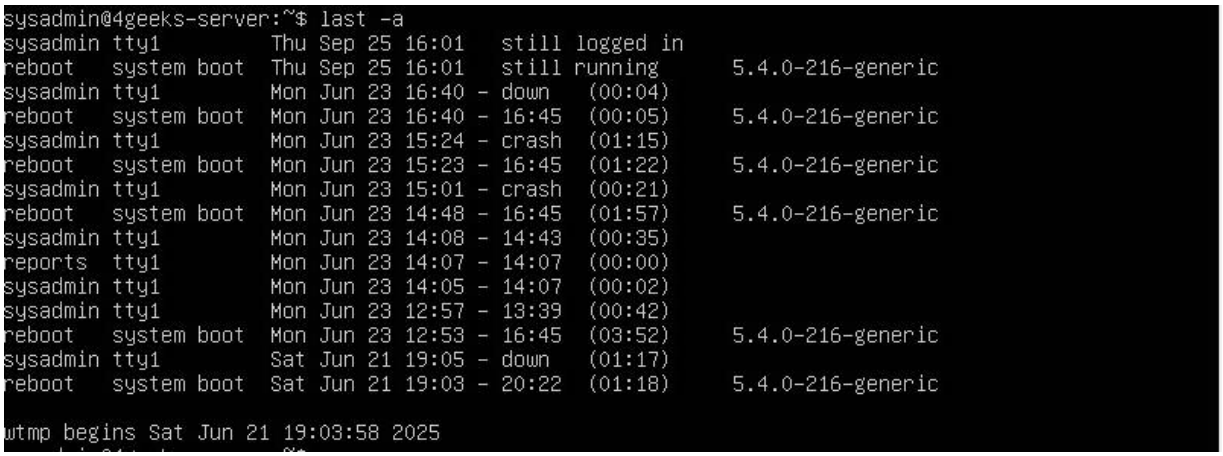


Se observa la creación de un usuario reports y de un usuario hacker, el .bash_history de ambos usuarios no se refleja ninguna acción, lo cual podría ser debido a que la configuración del .bash de ambos usuarios tiene activo el flag

HISTCONTROL = ignoreboth

Lo cual realiza que no registre los comandos o acciones realizadas.

Observando los últimos usuarios logueados en el sistema se ve un inicio de sesión del usuario reports el día 23 pero no estuvo nada de tiempo.



Resumen

Recopilando y resumiendo la información se observa que la fuga de información muy sensible y de alta confidencialidad se ha producido por:

- Un phishing enviado que ha terminado en existo para el atacante.
- Mala configuración de sistema de seguridad, entre varios el firewall de la maquina (ufw) lo cual ha dado la posibilidad de explotación de una vulnerabilidad del servidor apache2. Descargando a través de una url, por el puerto 80 desde la direccion 192.168.1.100 el payload. Posteriormente se ha subido a la misma dirección a través del puerto 8080
- Ausencia de seguridad perimetral que hubiera filtrado los correos con script, en este caso el install.sh
- Se ha generado una tarea que se realiza una carga de los usuarios y password del sistema en la url mencionada con anterioridad.

Proteger la integridad del sistema

- Se procede a la eliminación de todos los scripts, eliminación de la programación de ejecución del script backup2.sh cada 15 minutos. Para ello se realizar desde la terminal.

    - *crontab -e*
    - *Se elimina la regla que ejecuta el archivo backup2.sh*

- Se procede a la actualización de las contraseñas de todos los usuarios, generando contraseñas robustas, mínimo de 12 caracteres usando símbolos, letras mayúsculas y minúsculas. Desde la terminal y con privilegios de root.

    - *passwd nombre usuario*

- Eliminando los usuarios que no estén ya en la empresa o que hayan podido ser creados, sin un consentimiento claro, ni una función definida. En este caso reports y hacker.

    - *userdel -r nombre usuario*

- Actualizando del sistema y de todas las aplicaciones sobre él, especialmente las de apache y ssh.

    - sudo apt update
      sudo apt upgrade

- Modificación de las reglas del firewall filtrando las conexiones de entrada, en los puertos 80, 443, 21 y 22 y cerrando el resto.

    - sudo ufw default deny incoming (se bloquea todo el tráfico)
    - sudo ufw allow 80/tcp
    - sudo ufw allow 443/tcp
    - sudo ufw allow 21/tcp
    - sudo ufw allow 22/tcp

- Se podría plantear la utilidad de disponer el servidor apache2, ya que no está clara la función que está realizando actualmente, en el caso de que ya no fuera necesario, desinstalo del sistema.

- Se recomienda a la empresa poner un firewall NGFW para que filtre tanto no solo las conexiones sino el contenido de las mismas.

- Formación a los usuarios para detectar posibles intrusiones o intentos de phishing.
- Filtrar las conexión ssh a los usuarios y a través de máquinas concretas que lo necesiten para el desarrollo de las funciones asignadas.