Informe Forense de Seguridad

Fase 1. RECONOCIMIENTO Y RECOLECCIÓN DE EVIDENCIAS DE ATAQUE.

Como primer paso se comprobaron los logs con la herramienta "journalctl".

```
debian@debian:/var/log$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
```

Al ejecutar la herramienta lo primero que aparece es ese mensaje avisando carencia de permisos para poder ver todos los mensajes tanto de otros usuarios como del sistema. Para solucionar esto y poder ver todo se utiliza en este caso un comando para agregar el usuario actual al grupo “adm”, lo que otorgará permisos.

```
debian@debian:/var/log$ sudo usermod -aG adm debian
```

El siguiente paso es buscar en los logs conexiones, intentos de conexión, ejecución de servicios... que ha podido usar el atacante.

El analisis se inició revisando el servicio SSH ya que constituye el principal mecanismo para el acceso remoto y es uno de los objetivos de ataque más habituales.
Para ayudar en la lectura, ejecutaremos el comando: "journalctl -t sshd | tail -n 50".
Con esto filtraremos y nos proporcionará hasta los ultimos 50 logs de SSH.

```
debian@debian:~$ journalctl -t sshd | tail -n 50
Sep 30 12:25:16 debian sshd[51422]: Server listening on 0.0.0.0 port 22.
Sep 30 12:25:16 debian sshd[51422]: Server listening on :: port 22.
Sep 30 12:27:50 debian sshd[51422]: Received signal 15; terminating.
-- Boot 46ff5cf6df3d4f0e86b315592aaba2d0 --
Sep 30 15:09:51 debian sshd[560]: Server listening on 0.0.0.0 port 22.
Sep 30 15:09:51 debian sshd[560]: Server listening on :: port 22.
Oct 08 16:14:16 debian sshd[560]: Received signal 15; terminating.
Oct 08 16:14:16 debian sshd[5341]: Server listening on 0.0.0.0 port 22.
Oct 08 16:14:16 debian sshd[5341]: Server listening on :: port 22.
-- Boot 342683d8f35244b08c4f3863f2978eca --
Oct 08 16:43:18 debian sshd[543]: Server listening on 0.0.0.0 port 22.
Oct 08 16:43:18 debian sshd[543]: Server listening on :: port 22.
-- Boot d28e179bf5884b25bf94452c79fd0afa --
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot d6b8afd1c7154a5f9573e5a775bcb516 --
Dec 12 14:03:42 debian sshd[590]: Server listening on 0.0.0.0 port 22.
Dec 12 14:03:42 debian sshd[590]: Server listening on :: port 22.
```

Este análisis ha propocionado una información muy valiosa:

- Acceso con exito del atacante como ROOT a través del servicio SSH.

```
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
```

- IP del atacante: 192.168.0.134

Observaciones importantes:

- El atacante conectó de manera bastante facil y directa a través de SSH.
- Seguridad muy baja.
- El atacante descubrió la contraseña de manera muy fácil.

Se revisó el archivo /root/.bash_history, con el comando "cat /root/.bash_history" con el fin de encontrar evidencias de acciones hechas por el atacante:

```
debian@debian:~$ sudo cat /root/.bash_history
[sudo] password for debian:
sudo visudo
sudo systemctl stop speech-dispatcher
sudo systemctl disable speech-dispatcher
systemctl list-units --type=service
```

Observaciones:

- Normalmente el historial deberia contener muchas lineas de comandos pero en este caso sólo hay dos. Con ésto podemos pensar que el atacante borró el historial casi al completo.
- "sudo visudo" Este comando sirve para modificar la ruta (/etc/sudoers) y suele usarse para otorgar privilegios.
- "systemctl list-units --type=service" Es un comando común de reconocimiento tras penetrar en un sistema o equipo.
- Se realizó análisis del archivo /etc/sudoers y no se encontró nada extraño ni ninguna regla adicional.

Se revisó los registros del sistema en "journalctl" y se confirma que el atacante accedió a través de SSH consiguiendo conectar como root.

Escaneo de usuarios para encontrar posibles usuarios nuevos creados por el atacante.

Mediante el comando "sudo cat /etc/passwd" se comprueban los usuarios existentes y no se encuentra nada sospechoso. En este paso es importante destacar los usuarios en /bin/bash y se hizo busqueda específica.

```
debian@debian:~$ sudo grep "/bin/bash" /etc/passwd
[sudo] password for debian:
root:x:0:0:root:/root:/bin/bash
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
```

No se encontraron usuarios maliciosos.

Comprobación de permisos

No se encontraron permisos de usuarios fuera de lo normal.

Bloqueo de posibles backdoors.

Se realizó una busqueda de archivos con el bit SUID activado, este analisis no mostró binarios sospechosos, apareciendo binarios estándar del sistema.

```
debian@debian:~$ sudo find / -perm -4000 2>/dev/null
/usr/sbin/pppd
/usr/lib/xorg/Xorg.wrap
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/ntfs-3g
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/sudo
```

Como un método de controlar la posible conexión como root, se hizo una modificación del archivo ssh_config:
PermitRootLogin no
PasswordAuthentication no

CONCLUSION

Durante la Fase 1 del proyecto se llevó a cabo un análisis forense del sistema con el objetivo de identificar el vector de entrada del atacante, evaluar el alcance de la intrusión y

detectar posibles evidencias de persistencia o escalada de privilegios.

El análisis de los registros del sistema, centrado en el servicio SSH, confirmó un acceso no autorizado al usuario **root** mediante autenticación por contraseña desde una dirección IP externa. Ésto identifica al servicio SSH como el principal objetivo de entrada, permitiendo identificar una configuración insegura que permitía el inicio de sesión directo del usuario root.

Se revisaron los usuarios del sistema mediante el análisis del archivo `/etc/passwd`, no se detectaron cuentas adicionales con privilegios elevados ni usuarios creados de forma maliciosa.
Se comprobó que únicamente el usuario root posee UID 0 y que el resto de cuentas corresponden a usuarios de sistema con shells no interactivos, de esta manera pudiendo descartar persistencia con usuarios ocultos.

Como parte de la verificación de posibles backdoors, se realizó una búsqueda de binarios con el bit SUID activado, identificándose únicamente binarios estándar del sistema y necesarios para el funcionamiento normal del sistema. Del mismo modo, se comprobó la inexistencia de claves SSH configuradas para el usuario root, descartando mecanismos de persistencia basados en autenticación por clave.

El analisis forense permitió identificar el vector de entrada del ataque (SSH) y confirmar que, aunque el atacante obtuvo acceso completo al sistema, no se detectaron mecanismos de persistencia ni escaladas adicionales de privilegios.