Team SOC

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

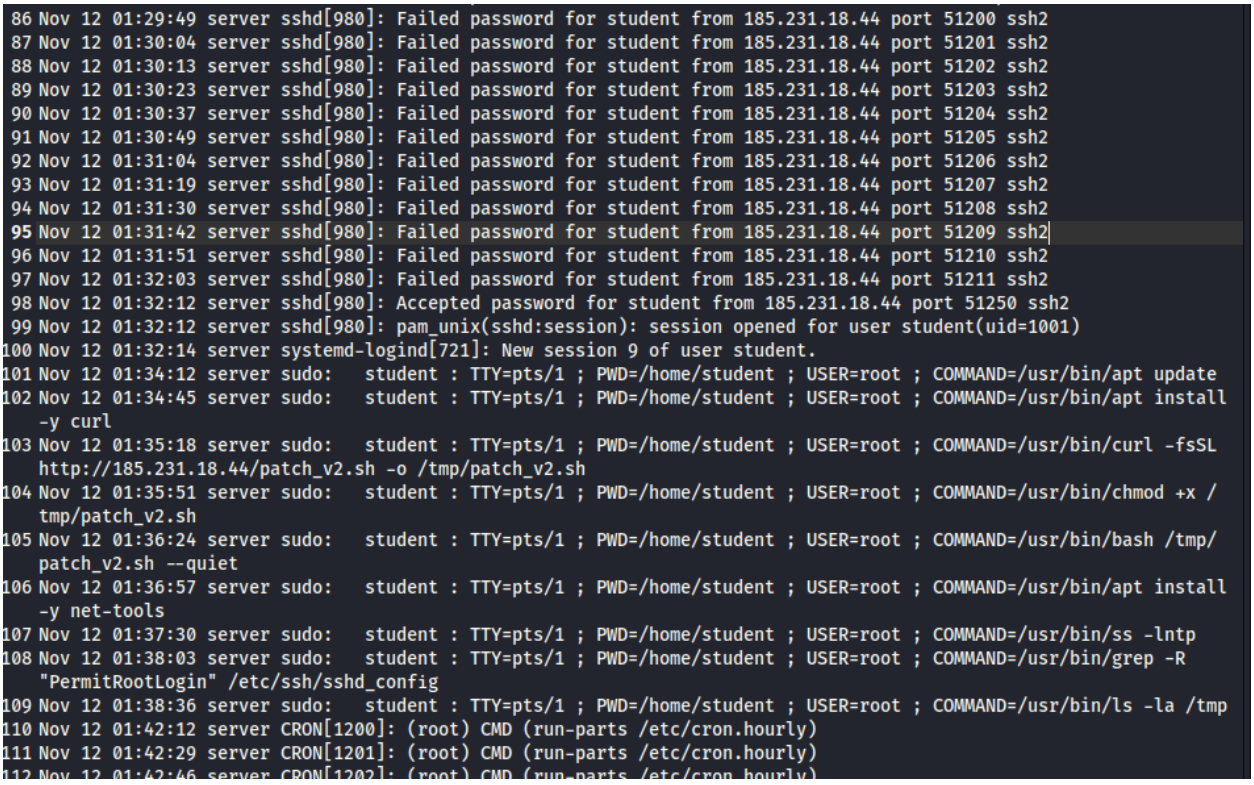
auth.log

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.



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
```

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 01:43:06 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 01:43:10 server kernel: audit: type=1300 audit(1762911790.122:162): cwd="/tmp"
21 Nov 12 01:43:11 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=ctfd-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}