Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 09/09/2023

Contacto: tomas.villaseca.c@gmail.com

Un archivo de registro o log es un archivo de texto que contiene una secuencia de eventos que ocurren en un sistema informático. Los archivos de registro pueden ser generados por una variedad de fuentes, incluyendo servidores, aplicaciones, dispositivos de red y sistemas operativos.

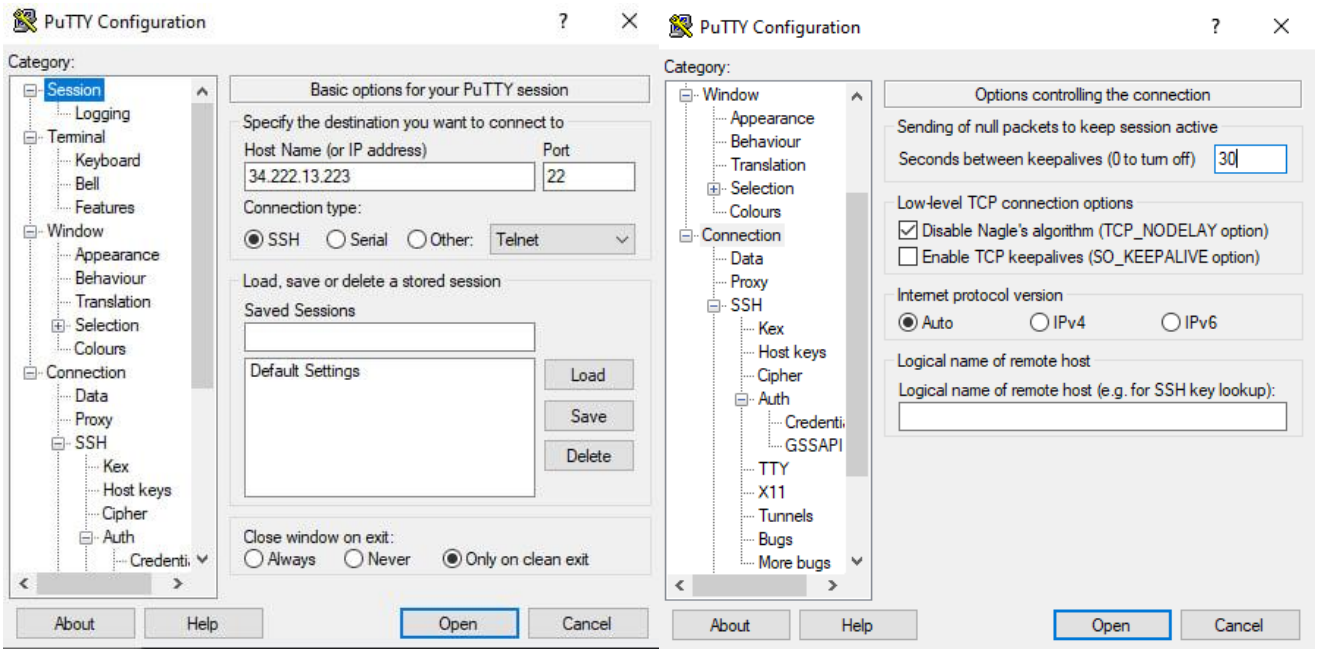
En este laboratorio, hará lo siguiente:

- Revisar el output de **lastlog** y secure log de la máquina de Linux

/var/log/secure = almacena información de autenticación para distribuciones de Linux derivadas de Red Hat (este laboratorio presenta una muestra de archivo secure log en /tmp/log/secure).

Tarea 1: conectarse a una instancia EC2 de Amazon Linux mediante SSH

1. Abrir Putty.exe: Se ingresa dirección IPv4 de la instancia EC2 en la sección Session.
2. En la sección Connection → SSH → Auth → Credentials se ingresa el archivo PPK descargado anteriormente.
3. En la sección Connection se establece **Seconds between keepalive en 30 (el valor predeterminado es 0).**

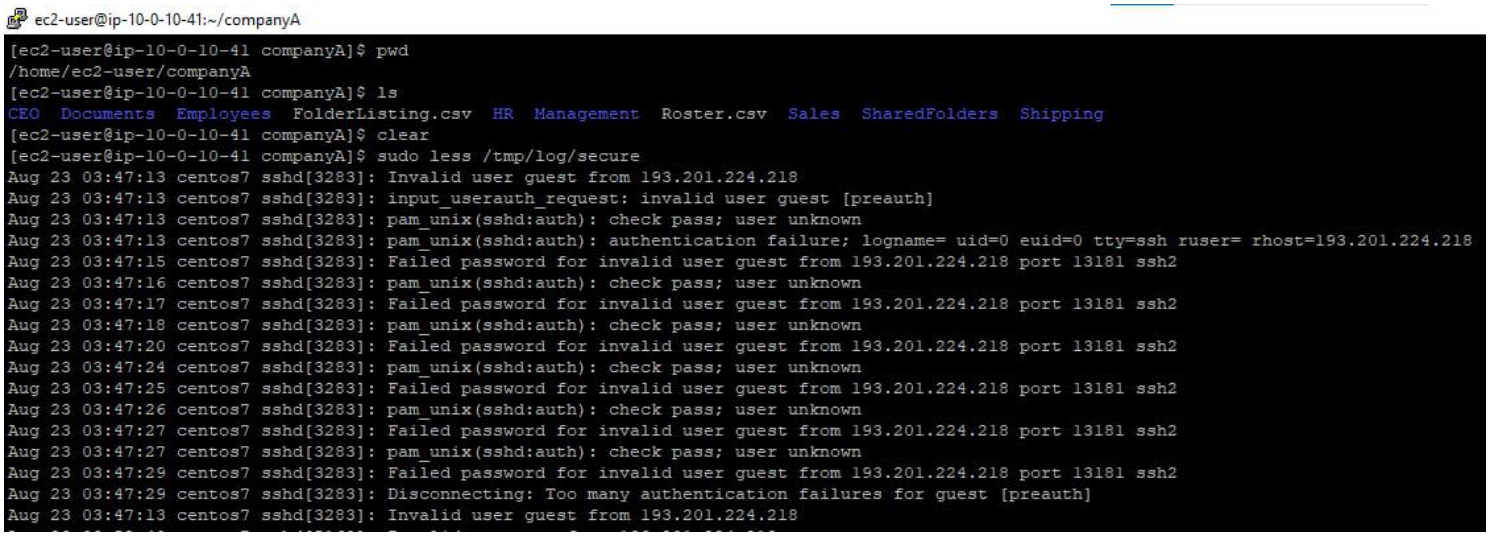


4. Se hace click en “Open” para validar y conectarse al Host.

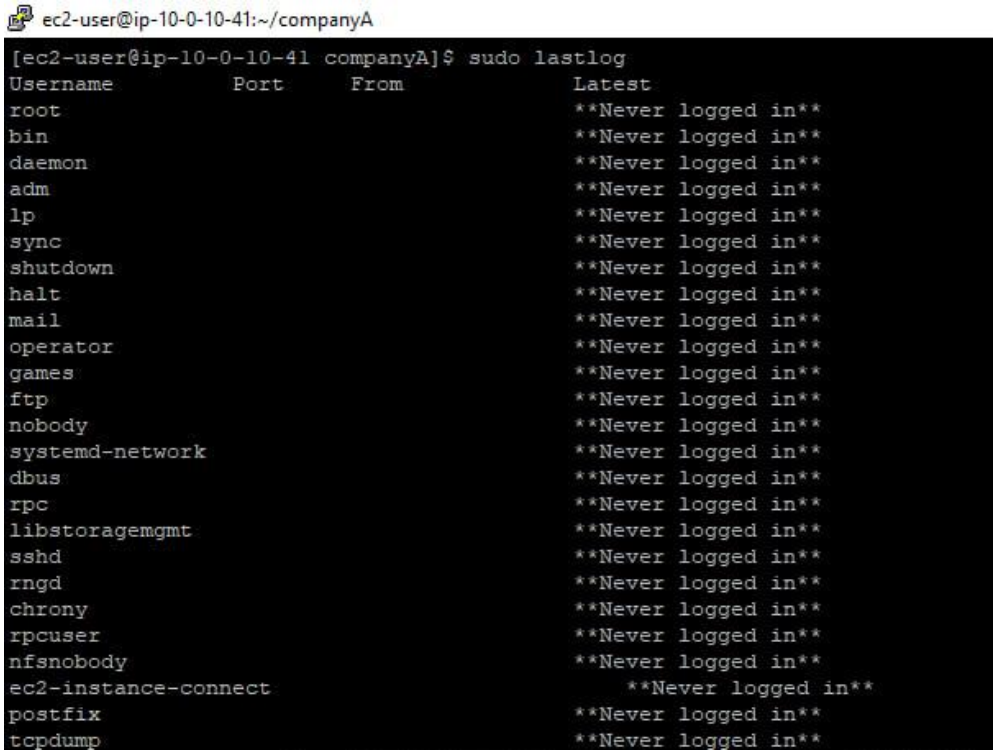
Tarea 2: Revisar archivos Secure Log

less = paginador que permite visualizar archivos de texto de gran tamaño

- Muestra el archivo de texto una pantalla a la vez



lastlog = entrega información sobre inicios de sesión recientes desde el archivo /var/log/lastlog



Desafío adicional

¿Qué información se puede extraer para algunos de los propósitos de su empresa?

Los archivos de registro o logs pueden proporcionar información valiosa sobre el rendimiento, la seguridad y el uso de su empresa. Al analizar los archivos de registro, puede identificar problemas potenciales, mejorar la eficiencia y garantizar que su empresa cumpla con los requisitos normativos.

Algunas de las formas en que puede utilizar los archivos de registro para los propósitos de su empresa incluyen:

- **Rendimiento:** Los archivos de registro pueden ayudarlo a identificar problemas de rendimiento, como cuellos de botella en la red o errores de software. Al analizar los archivos de registro, puede identificar los problemas que están causando el rendimiento lento y tomar medidas para corregirlos.
- **Seguridad**: Los archivos de registro pueden ayudarlo a detectar ataques y amenazas de seguridad. Al analizar los archivos de registro, puede identificar las vulnerabilidades que están siendo explotadas y tomar medidas para remediarlas.
- **Uso:** Los archivos de registro pueden ayudarlo a comprender cómo se utilizan sus recursos. Al analizar los archivos de registro, puede identificar las áreas donde se puede mejorar la eficiencia y tomar medidas para reducir los costos.