🕵️‍♀️ Misión de Análisis Forense: "El Pendrive Fantasma"

Contexto: Hoy, a las **[Introduce la hora exacta de inicio del ejercicio]**, se ha detectado una posible violación de la política de seguridad. Un dispositivo de almacenamiento USB (pendrive) desconocido ha sido conectado brevemente a una de las estaciones de trabajo de esta aula, burlando el control de seguridad. Necesitamos identificar **qué equipo exacto** fue comprometido.

Objetivo: Actuar como analistas de Nivel 1 (Tier 1) y determinar el equipo sospechoso utilizando únicamente las herramientas de *logging* del sistema operativo.

Equipos de Trabajo: Formen grupos de 2-3 personas.

📜 Tareas Previas del Instructor (¡Solo el Instructor!)

1. **El Incidente:** Coge un pendrive y, de forma disimulada, conéctalo a **uno solo de los equipos** del aula durante 5 segundos. **Apunta el nombre o número del equipo (la "Víctima").**
2. **Configuración del Log:** Asegúrate de que los logs del sistema estén accesibles.
3. **Anuncio:** Anuncia la hora exacta del "incidente" (la hora en que conectaste el USB).

🛠️ Fases del Ejercicio para los Alumnos

Fase 1: Recolección de Evidencia (30 minutos)

Cada grupo deberá elegir un enfoque de sistema operativo (Windows o Linux) y revisar los logs del equipo que les ha sido asignado.

Instrucciones para la Recolección (Elige tu Batalla):

Si tu equipo usa...	Instrucciones y Comandos	Pista Clave a Buscar
Linux	Abre la terminal y ejecuta: 1. dmesg | less 2. tail -f /var/log/syslog (o /var/log/messages en algunas distros) 3. lsblk antes y después del incidente.	Busca mensajes que contengan palabras clave como **usb**, **new device**, o el nombre del dispositivo asignado (ej: **/dev/sdc**).
Windows	Abre el **Visor de Eventos** (eventvwr.msc). 1. Ve a **Registros de Windows Sistema**. 2. Usa la función **"Filtrar Registro Actual"** para buscar los IDs de evento: **20001** y **20003**.	Busca un evento de "montaje" (ID **20001**: USB Mass Storage Device) que coincida exactamente con el **timestamp** del incidente.

Importante: La clave no es solo encontrar la palabra "USB", sino ver que el **timestamp** del log coincida con la hora exacta del incidente.

Fase 2: Análisis y Correlación (15 minutos)

Una vez que cada grupo haya revisado su propio equipo, comparen notas.

1. **Análisis de Timestamps:** ¿Encontró algún equipo un *timestamp* que coincida con la hora del incidente?
2. **Aislamiento del Equipo:** El grupo cuyo equipo mostró un registro de conexión USB debe ser el principal sospechoso.

Fase 3: Conclusión y Reporte Forense (15 minutos)

El objetivo final es crear un reporte simple para el "Jefe del SOC".

Preguntas del Reporte:

1. **Hipótesis de Incidente:** ¿Qué equipo crees que fue el infectado?
2. **Evidencia Clave:** ¿Cuál fue el comando o *log ID* que te dio la prueba irrefutable?
3. **Timestamp Encontrado:** ¿Cuál es la fecha y hora exacta del evento de conexión en el log?
4. **Atributos del Dispositivo (Opcional):** Si usaste dmesg, ¿puedes identificar el **Vendor ID** o el **Product ID** del dispositivo USB?

🏆 Puntuación del Juego

- **10 Puntos:** Identificar el equipo correcto.
- **5 Puntos:** Presentar el *log ID* o línea de dmesg que demuestra la conexión.
- **3 Puntos:** Identificar un log de "USB" pero no dar con el equipo correcto (demuestra uso correcto de herramientas, pero fallo en correlación).

¡Que comience la cacería de *logs*!