LA CUEVA

BLUE TEAM

EXPEDIENTE DE INVESTIGACIÓN

Los permisos que nadie revisó

Preparación informática / Sistemas / Acceso GRATUITO

Resolver, justificar y comunicar. Este pack es breve, editable y está pensado para producir una evidencia de trabajo reutilizable.

Formato: briefing · entorno seguro · preguntas · informe profesional

Aprender a investigar con evidencia.

01 / Contexto de misión

Leé el caso antes de consultar el entorno. Separá hechos, hipótesis y datos que todavía faltan.

Campo	Información
Ticket	HELP-1014 · Acceso inesperado a archivo financiero
Nivel	Preparación informática
Dificultad	Inicial
Duración	40-55 min
Afectado	FINANZAS_ARCHIVE · usuario nuevo
Alerta	File server: access outside role

Situación

Asteria Logistics recibe el ticket HELP-1014: una persona nueva puede abrir la carpeta FINANZAS_ARCHIVE aunque no pertenece al área. El equipo no sabe si el acceso viene de un permiso directo, un grupo o una herencia del directorio superior.

Objetivo

- Leer una ruta y su contexto de permisos.
- Distinguir capacidad de acceso y acceso efectivo.
- Documentar una recomendación reversible.

Antes de empezar

- Reconocer usuario, grupo, carpeta y archivo.
- Entender la diferencia entre lectura y escritura.

02 / Entorno controlado

Explorá una imagen ficticia de solo lectura y escribí cualquier comando que te ayude a investigar. La entrada se interpreta dentro del caso; no ejecuta procesos reales, toca tu equipo ni realiza conexiones externas.

Archivo virtual	Qué buscar
case-notes.txt	Hechos, fuente, tiempo y datos que todavía faltan.
evidence-index.txt	Hechos, fuente, tiempo y datos que todavía faltan.
timeline.txt	Hechos, fuente, tiempo y datos que todavía faltan.
readme.txt	Hechos, fuente, tiempo y datos que todavía faltan.

Fuentes disponibles

Archivo / consulta	Qué buscar
01 · Ticket	Actor, origen, timestamp y relación con la hipótesis.
02 · Árbol de carpetas	Actor, origen, timestamp y relación con la hipótesis.
03 · ACL	Actor, origen, timestamp y relación con la hipótesis.
04 · Usuarios	Actor, origen, timestamp y relación con la hipótesis.

Regla de oro

Un comando puede aportar un indicio, pero no reemplaza la correlación con el ticket, el activo, el usuario y el momento. No descargues muestras ni uses credenciales reales.

03 / Preguntas de evidencia y análisis

Respondé con hechos, fuente, timestamp, hipótesis y limitaciones. Si no podés confirmarlo, escribí qué dato pedirías.

01 · ¿Qué diferencia hay entre propietario, permiso directo, grupo y herencia?

Respuesta editable

02 · ¿Qué evidencia permite afirmar que una cuenta realmente puede leer un archivo?

Respuesta editable

03 · ¿Qué cambio harías y cuál no deberías hacer durante la investigación?

Respuesta editable

04 · ¿Cómo documentarías un permiso excesivo sin exponer el contenido del archivo?

Respuesta editable

04 / Informe profesional

Este documento debe permitir que otro analista retome el caso sin una explicación oral. Completalo después de usar el entorno.

Resumen ejecutivo · qué pasó y por qué importa

Hechos y evidencia · fuente + hora

Hipótesis · alternativa + nivel de confianza

Impacto, contención y próximo paso

Checklist de entrega

- Separé hechos, inferencias y datos pendientes.
- No afirmé ejecución o compromiso sin evidencia.
- Escribí impacto, contención y limitaciones.
- El siguiente paso tiene dueño y validación.

Entregable para portfolio

- Informe de exposición de permisos de una página.
- Tabla de acceso esperado versus efectivo.
- Diagrama simple de grupos y herencia.
- Recomendación de mínimo privilegio y validación posterior.