LA CUEVA

BLUE TEAM

EXPEDIENTE DE INVESTIGACIÓN

La página que pedía credenciales

Redes / Network / 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	NET-1051 · Login interno servido por HTTP
Nivel	Redes
Dificultad	Inicial
Duración	50-70 min
Afectado	SOPORTE-05 · usuario de soporte
Alerta	Proxy: credential form over cleartext HTTP

Situación

El proxy observa que SOPORTE-05 visita portal-legacy.example por HTTP. El sitio se parece al portal interno, pero el inventario indica que la aplicación oficial usa HTTPS.

Objetivo

- Distinguir HTTP, HTTPS, DNS y certificado.
- Leer una solicitud y respuesta básica.
- Evaluar exposición sin afirmar compromiso prematuro.

Antes de empezar

- Reconocer puerto, protocolo y dominio.
- Conocer por qué TLS protege confidencialidad e integridad.

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 · PCAP	Actor, origen, timestamp y relación con la hipótesis.
02 · DNS logs	Actor, origen, timestamp y relación con la hipótesis.
03 · HTTP headers	Actor, origen, timestamp y relación con la hipótesis.
04 · Asset inventory	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 información puede quedar expuesta en HTTP?

Respuesta editable

02 · ¿Cómo confirmarías si el dominio es el oficial o una imitación?

Respuesta editable

03 · ¿Qué hosts y usuarios deben revisarse?

Respuesta editable

04 · ¿Qué control preventivo recomendarías?

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 credenciales.
- Diagrama del flujo HTTP/DNS.
- Recomendación de migración y control de proxy.
- Mensaje para el usuario afectado sin alarmismo.