LA CUEVA

BLUE TEAM

CUADERNO DE CAMPO

TCP/IP, DNS y HTTP en una sola historia

N1 · Redes / Clase + laboratorio práctico / GRATUITA

Una ficha premium, editable y orientada al trabajo: explica lo esencial, enseña los comandos y termina en una evidencia verificable.

5 páginas: mapa TKS · comandos · demostración · práctica · entregable

Aprender a investigar con evidencia.

01 / Contrato de aprendizaje

Seguir una navegación desde el nombre hasta la respuesta de la aplicación.

Campo	Compromiso verificable
Pregunta operativa	¿Qué necesito observar primero para investigar tcp/ip, dns y http en una sola historia sin adelantar una conclusión?
Objetivo	Ordenar los eventos de una solicitud web completa.
Producto	Timeline de flujo
Aplicación laboral	En un entorno profesional, esta competencia permite producir consulta dns, ip, puerto, conexión y código http sin ocultar las limitaciones de la fuente.

Mapa TKS

T - Tarea	K - Conocimiento	S - Habilidad
Ordenar los eventos de una solicitud web completa.	Consulta DNS, IP, puerto, conexión y código HTTP	Producir timeline de flujo

Roles NICE relacionados

- IO-WRL-004 · Network Operations
- PD-WRL-001 · Defensive Cybersecurity

Conceptos esenciales de esta clase

- Consulta DNS
- IP
- puerto
- conexión y código HTTP

Qué puede preguntarte una entrevista

En una entrevista: ¿cómo investigarías “TCP/IP, DNS y HTTP en una sola historia” sin confundir un indicio con una conclusión?

Criterio de salida

La clase se considera dominada cuando podés producir la evidencia indicada, explicar su fuente y declarar qué limitación impide una conclusión más fuerte.

02 / Guía completa de comandos

Cada tarjeta responde una pregunta concreta: propósito, sintaxis, ejemplo, salida, parámetros, equivalencias, riesgos y errores. Empezá por consultas de solo lectura.

01 curl -I

Observar cabeceras y estado sin descargar el cuerpo.

Sintaxis
`curl -I <url>`

Ejemplo
`curl -I https://portal.local`

Salida esperada
Status, servidor, redirecciones y cabeceras.

Parámetros
-I · <url>

Equivalencias
No existe una equivalencia exacta: compará la fuente y los campos disponibles en tu plataforma.

Riesgo / uso seguro
No consultes dominios desconocidos fuera del laboratorio. Empezá en modo lectura y conservá la salida original.

Error frecuente
Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.

02 http-inspect

Separar método, host, ruta y respuesta de una transacción sanitizada.

Sintaxis
`http-inspect <archivo>`

Ejemplo
`http-inspect web.log`

Salida esperada
Solicitud y respuesta relacionadas.

Parámetros
-inspect · <archivo>

Equivalencias
No existe una equivalencia exacta: compará la fuente y los campos disponibles en tu plataforma.

Riesgo / uso seguro
Una cabecera puede ser enviada por un intermediario. Empezá en modo lectura y conservá la salida original.

Error frecuente
Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.

03 tls-inspect

Revisar identidad y vigencia del certificado del caso.

Sintaxis
`tls-inspect <host>`

Ejemplo
`tls-inspect portal.local`

Salida esperada
SAN, emisor, validez y protocolo.

Parámetros
-inspect · <host>

Equivalencias
No existe una equivalencia exacta: compará la fuente y los campos disponibles en tu plataforma.

Riesgo / uso seguro
TLS válido protege transporte; no legitima el contenido. Empezá en modo lectura y conservá la salida original.

Error frecuente
Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.

04 grep

Localizar cookies, hosts o códigos dentro del registro.

Sintaxis
`grep -i <patrón> <archivo>`

Ejemplo
`grep -i set-cookie web.log`

Salida esperada
Transacciones coincidentes.

Parámetros
-i · <patrón> · <archivo>

Equivalencias
PowerShell: Select-String · CMD: findstr

Riesgo / uso seguro
Conservá la petición y la respuesta completas. Empezá en modo lectura y conservá la salida original.

Error frecuente
Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.

03 / Demostración y tres momentos prácticos

Seguir origen, destino, protocolo, estado y resultado en cada capa.

Paso	Señal	Pregunta	Limitación
01	Consulta DNS	¿Qué campo observar?	¿Qué todavía no demuestra?
02	IP	¿Qué campo observar?	¿Qué todavía no demuestra?
03	puerto	¿Qué campo observar?	¿Qué todavía no demuestra?
04	conexión y código HTTP	¿Qué campo observar?	¿Qué todavía no demuestra?

1. Demostración explicada

Seguir una navegación desde el nombre hasta la respuesta de la aplicación.

2. Práctica guiada

Practicá cómo escribir una conclusión sin ocultar incertidumbre.

- Copiar el dato exacto
- Nombrar la fuente
- Explicar la interpretación
- Proponer una alternativa
- Declarar qué falta

3. Investigación independiente

Repetí el procedimiento con ruido, un dato faltante y una hipótesis alternativa. La respuesta debe incluir fuente y limitación, no solo un identificador.

04 / Hoja editable de aplicación

Completá desde tu lector de PDF o imprimí la ficha. Usá datos ficticios o sanitizados y separá claramente observación de interpretación.

Evidencia observada - fuente, comando y timestamp

Razonamiento - hipótesis principal, alternativa y confianza

Decisión - preservación, limitación y próximo paso

Checklist de salida

- Conservo la fuente
- Registro fecha y alcance
- Separo evidencia de interpretación
- Documento el próximo paso

Revisión espaciada

- ¿Qué tres datos conservarías primero al trabajar tcp/ip, dns y http en una sola historia?
- ¿Cómo cambiaría tu procedimiento si faltara conexión y código http?
- Aplicá tcp/ip, dns y http en una sola historia dentro de un caso del módulo “Modelo de red y TCP/IP” y defendé una hipótesis alternativa.

Versión

Currículo 3.2.0 · NICE 2.2.0 · ATT&CK v19.2 · Actualizada 24 de agosto de 2026