Piscine Discovery de Ciberseguridad

Tyto 01

by @alrodri2

Resumen: Continuando con OSINT ahora tendrás que investigar en el perfil para encontrar posibles nombres de usuario relacionados con este mismo usuario.

Versión: 2.00

Índice general

Capítulo I

Bienvenidx a la Piscina Discovery de Ciberseguridad

Hola!

Bienvenid@ a esta Piscine Discovery de ciberseguridad, un reto donde aprenderás los fundamentos de la ciberseguridad ofensiva mientras experimentas el modelo educativo único de 42. Aquí no encontrarás clases tradicionales ni una única solución correcta; el aprendizaje es colaborativo, práctico y centrado en tí.

Queremos que te sumerjas en el código que forma parte del software que usas cada día, desarrollando habilidades que van más allá de lo técnico: pensamiento lógico, resolución de problemas y aprendizaje autónomo. La programación no se trata de memorizar reglas, sino de ensamblar bloques de manera creativa para resolver problemas de forma única.

Durante esta experiencia, abordarás temas clave de la ciberseguridad:

- Manejo de la terminal: Aprende a navegar y operar con soltura en un sistema operativo utilizando comandos.
- OSINT (Open Source Intelligence): Descubre cómo recopilar información pública para identificar amenazas.
- Seguridad web: Comprende las vulnerabilidades más comunes de los sitios web y cómo se explotan.
- Criptografía: Familiarízate con los principios básicos de la protección de datos y comunicaciones.

En este proceso, la evaluación y el aprendizaje entre pares jugarán un papel crucial. Compartirás ideas, discutirás soluciones y descubrirás perspectivas diferentes al interactuar con tus compañeros. Esto no solo enriquecerá tu aprendizaje, sino que también te permitirá forjar conexiones y desarrollar habilidades clave para resolver desafíos futuros.

Recuerda que esta experiencia es tan única como tú: cada participante seguirá su propio camino, validará proyectos distintos y enfrentará retos únicos. Lo importante es lo que aprendas, tanto de tus aciertos como de tus errores.

¡Buena suerte! Esperamos que disfrutes este viaje hacia el mundo de la ciberseguridad y el aprendizaje colaborativo.

Capítulo II

Introducción

Probablemente hayas oído que "todo lo que está en internet es público", pero ¿te has preguntado hasta dónde llega esa información y cómo puedes encontrarla? OSINT (Open Source Intelligence) es la práctica de explorar, recopilar y analizar datos accesibles públicamente para obtener información valiosa.

En el mundo digital, aprender a buscar patrones, identificar conexiones y analizar fuentes abiertas te ayudará a entender cómo se genera y comparte la información en línea. Más allá de ser una simple búsqueda en Google, OSINT es una habilidad que combina creatividad, curiosidad y un enfoque analítico para descifrar datos y convertirlos en conocimiento útil.

En el mundo digital, los perfiles falsos son cada vez más comunes. Sin embargo, quienes los crean suelen cometer pequeños errores que pueden delatar su verdadera identidad. En este ejercicio, aprenderás cómo rastrear pistas ocultas y analizar información para identificar al creador detrás de un perfil falso.

Qué aprenderás en este ejercicio:

- Identificación de patrones y errores comunes en perfiles falsos.
- Cómo documentar y cruzar información para formar un perfil más completo.

Capítulo III

Instrucciones generales

Salvo que se especifique explícitamente, las siguientes reglas se aplicarán cada día de esta Piscine Discovery.

- Este enunciado es la única fuente confiable. No confíes en ningún rumor.
- Las tareas en un enunciado deben hacerse en el orden indicado. Las tareas posteriores no serán calificadas a menos que todas las anteriores estén perfectamente ejecutadas.
- Ten cuidado con los permisos de acceso de tus archivos y carpetas.
- Tus tareas serán evaluadas por tus compañeros de Piscine.
- Todas las tareas de shell deben ejecutarse usando `/bin/bash`.
- No debes dejar en tu entrega ningún archivo que no sea explícitamente solicitado por los enunciados.
- ¿Tienes una pregunta? Pregúntale a tu vecino de la izquierda. De lo contrario, prueba suerte con tu vecino de la derecha.
- Cualquier respuesta técnica que puedas necesitar está disponible en el `man` o en Internet.
- ¡Recuerda leer la documetación y Slack!
- Debes leer detenidamente los ejemplos. Pueden revelar requisitos que no son obvios en la descripción del enunciado.
- ¡Por Thor, por Odin! ¡Usa tu cerebro!

Capítulo IV

Ejercicio 01

	Ejercicio: 01
Doraemon	
Directorio de entrega: *ex*01/	
Archivos de entrega: `flag.txt`	
Funciones prohibidas: `Solo se permite el navegador`	

¡Fantástico! En el ejercicio anterior has localizado el perfil de esta persona, pero en realidad parece un perfil falso. ¿Puedes localizar la identidad real de este usuario?

Capítulo V

Entrega y evaluación entre pares

- Tu tarea es localizar la URL del usuario real que se esconde detrás de la cuenta falsa.
- Cuando la localices debes escribirla en un archivo `flag.txt`.
- El archivo `flag.txt` debe estar situado en `/tyto/ex01`.

Por favor, ten en cuenta que durante la evaluación lo que queremos comprobar es que has entendido lo que has hecho. Debes sabes explicarlo y argumentar las decisiones tomadas.