Piscine Discovery de Ciberseguridad

Gecko 03

by @alrodri2

Resumen: Verás que no todas las contraseñas se pueden encontrar tan fácilmente en listas de palabras preconstruidas. En este proyecto aprenderás a crear tus propias listas de palabras a partir de una lista base.

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

La criptografía está en el corazón de la protección de datos y comunicaciones en el mundo digital. Aunque a menudo se percibe como un campo reservado para matemáticos y expertos en seguridad, en realidad, muchas de las técnicas que la sustentan son herramientas que usamos (y dependemos de) todos los días, como cuando protegemos nuestras contraseñas, enviamos mensajes cifrados o verificamos la integridad de un archivo.

Entender cómo funcionan los principios básicos de la criptografía te permitirá no solo proteger mejor tu información, sino también reconocer las debilidades de los sistemas mal implementados. Desde los hashes y las codificaciones hasta los cifrados más complejos, este módulo te enseñará cómo se utilizan estas técnicas en el mundo real y cómo, si no se aplican correctamente, pueden ser explotadas.

Basándote en el ejercicio anterior, volverás a utilizar fuerza bruta para romper un hash. Esta vez, trabajarás con una lista proporcionada de contraseñas potenciales, poniendo a prueba tus habilidades mientras analizas y descifras el hash de manera eficiente.

Qué aprenderás en este ejercicio:

- Técnicas avanzadas de fuerza bruta para descifrar hashes.
- Cómo utilizar listas de contraseñas de forma eficaz.
- Experiencia práctica en analizar y romper sistemas basados en hashes.

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
Medium	
Directorio de entrega: *ex*01/	
Archivos de entrega: `flag.txt`	
Funciones prohibidas: `Ninguna`	

Gracias al equipo de seguridad de 42 hemos encontrado algunas palabras que potencialmente podrían ser parte del hash que almacena la contraseña que queremos obtener. Tu objetivo es romper el hash y conseguir la contraseña en texto plano.
La flag es el texto "deshasheado", pero ya sabes que "deshashear"no funciona.

Hash:

```
c967d488512ab5559b446f97843de1be0d615088
```

`TIENES que utilizar John the ripper.`

Capítulo V

Entrega y evaluación entre pares

- Has encontrado la flag? Cuando la tengas debes escribirla en un archivo `flag.txt`.
- El archivo `flag.txt` debe estar situado en `/gecko/ex03`.

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.