



Fuente: Microsoft Copilot

LABORATORIOS 3-4. CRIPTOGRAFÍA

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2024 – 2025 (V4.2 “S-81 Isaac Peral”)





Contenido

⬅ Infraestructura de este laboratorio	2
📁 Bloque 1: Usos prácticos de la criptografía	3
🛠 Ejercicio L34_CRYPTO_CTF_1: ¿Puedes resolver el desafío de criptografía que te planteamos?.....	3
📁 Bloque 2: Instrucciones de Entrega	6
👉 Insignias y Autoevaluación	7



BACK

1

2





BACK

Infraestructura de este laboratorio

Este laboratorio es un “juego” que consta de **varios pasos y da archivos y resultados diferentes para cada uno de vosotros** por lo que, por favor, entended los procesos, pero **no copiéis directamente el resultado de vuestros compañeros** porque entonces no podremos dar por buena vuestra evaluación.



BACK

1
2





Bloque 1: Usos prácticos de la criptografía

🛠 Ejercicio L34_CRYPTO_CTF_1: ¿Puedes resolver el desafío de criptografía que te planteamos?

👷 Descripción de la actividad / Aplicación práctica

Esta práctica de criptografía consiste en un CTF ([https://en.wikipedia.org/wiki/Capture_the_flag_\(cybersecurity\)](https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity))). Tendrás que realizar una serie de ejercicios (pasos), todos ellos relacionados con la criptografía (con los conocimientos vistos en las clases de teoría).

🔍 **Cuando superes un paso (capturar una bandera) obtendrás las instrucciones y/o recursos para continuar con el siguiente paso. ¡Lee las instrucciones con mucha atención para seguir avanzando!**

⭐ Resultados Esperados

Durante las fases de las que consta este CTF trabajarás con distintos conceptos de criptografía que veremos en la teoría. Debes asegurarte de que los comprendes y sabes aplicarlos por si tuvieras que reproducirlos en el futuro. Concretamente son estos:

- **Rotura de contraseñas en ficheros** mediante cracking (con o sin diccionarios).
- Uso de **herramientas de esteganografía**.
- Aplicación de algoritmos de **cifrado simétrico**.
- **Codificación y descodificación** de información.
- **Uso de criptografía asimétrica** para habilitar el acceso seguro por SSH.
- **Rotura de contraseñas de usuarios** de un SO Linux.
- **Generación de certificados digitales** para firmar ficheros.

❓ **Pregunta que debes resolver:** ¿Podrías reproducir alguno de los usos de criptografía que te planteamos en las distintas fases de este reto si te las planteamos de forma aislada? (Ej.: generar diccionarios, romper contraseñas...)

💻 Otra información necesaria para su realización

Para el primer paso **recibirás un correo electrónico** en el que se te informa de una URL a la que tienes que acceder junto a una clave. Tanto la URL como la clave **son personales** y te darán acceso a los recursos específicos para realizar la práctica.

Importante: El correo provendrá de la dirección ssi.eii.uniovi@gmail.com. Vigila tu spam por si acaba allí.

🔍 **Recuerda:** Cada estudiante tiene sus recursos individuales y son distintos de los de los demás estudiantes



Al acceder a esa URL personalizada descargas un fichero zip protegido por contraseña. El primer paso es **conseguir desencriptar ese fichero zip** con una herramienta adecuada que decidas usar, y acceder a sus contenidos. Como pista para lograr descifrar este zip, te decimos que la contraseña **no es mayor de seis caracteres** y que solo está formada por letras (mayúsculas o minúsculas) y nºs. Usa esto para ajustar los parámetros de la herramienta que elijas para descifrar el zip adecuadamente de manera que los tiempos de descifrado estén dentro de unos límites razonables.

Esto te muestra los objetivos de este laboratorio: debes investigar, pensar, discutir, revisar las diapositivas de teoría... Todo lo que puedes hacer para tratar de resolver el desafío (y entender cómo lo hiciste). Se trata de una serie de retos que pondrán a prueba tus conocimientos, asegurándose de que adquieras experiencia práctica con ellos.

Correo que recibirás

En el correo que recibirás (por favor, comprueba tu carpeta de “**Correo No Deseado**” por si acaso) se te proporcionará una URL y una clave. La URL será del estilo de **https://156.35.163.140/api/c1e45406** y para poder descargar el fichero zip debes hacer

```
curl -u UOXXXXXX:pass_XXXXXX https://156.35.163.140/api/c1e45406 --insecure --output  
UOXXXXXX.zip
```

NOTA: Si vas a acceder a esta IP desde fuera del laboratorio/red de la universidad, recuerda conectarte a la VPN de la Universidad, ya que se encuentra protegida por el firewall perimetral de Uniovi. Puedes encontrar un manual aquí: <https://torres.epv.uniovi.es/centon/acceso-forticlient.html>. Por problemas con las librerías de XFCE4, el cliente Fortinet no funciona en la MV de la asignatura, tendrás que instalarlo en tu host

1

2

3

4

Observaciones

En algunos casos tendrás que romper claves. Unas veces será por fuerza bruta, otras mediante uso de diccionarios, etc. En unos casos **os daremos pistas** de los posibles diccionarios a utilizar y en los que sean por fuerza bruta la longitud/complejidad de la contraseña será poca (mala contraseña) de tal forma que se pueda romper en poco tiempo con un ordenador normal (sin GPU ni gran potencia).

Por tanto, en caso de que se te pida descifrar por fuerza bruta, las contraseñas están ajustadas para que no tarden demasiado tiempo, incluso en hardware modesto. En general, si el proceso de descifrado por fuerza bruta tarda más de cinco minutos, puedes considerar que algo has hecho mal y que el proceso que has usado no es el adecuado para ese paso.

Programas/webs que te pueden ser útiles durante alguna de las fases del ejercicio

En caso de ser una herramienta, comprueba primero si se puede instalar directamente mediante el sistema de paquetes de la MV Ubuntu (**snap** o **apt**) para no perder el tiempo con eso. No tienes que usar cada herramienta. Solo son algunas posibilidades que te damos para que investigues y determines si podrían resultarte útiles para lo que tienes que hacer, en lugar de ir “a ciegas”.

- **Cewl.** <https://www.kali.org/tools/cewl/>
- **Crunch.** <https://www.kali.org/tools/crunch/>
- **John the Ripper.** <https://www.kali.org/tools/john/>
- **Fcrackzip.** <https://www.kali.org/tools/fcrackzip/>
- **Hashcat.** <https://www.kali.org/tools/hashcat/>
- **Steghide.** <https://www.kali.org/tools/steghide/>
- **Stegseek:** <https://github.com/RickdeJager/stegseek>



- **Stegcracker:** <https://github.com/Paradoxis/StegCracker>
- **Hashid:** Una herramienta de línea de comandos que detecta tipos de hashes. <https://www.kali.org/tools/hashid/>
- https://hashes.com/en/tools/hash_identifier: detecta tipos de hashes
- <https://www.tunnelsup.com/hash-analyzer>: detecta tipos de hashes
- **OpenSSL:** <https://www.openssl.org/>
- **CyberChef:** <https://gchq.github.io/CyberChef/>
- **Curl**
- **Crackstation:** <https://crackstation.net/>
- **RainbowCrack:** <http://project-rainbowcrack.com/index.htm>
- **xxd**

Algoritmos de hashing que podemos haber usado para generar hashes si te encuentras con una

- MD5
- SHA1
- SHA224
- SHA256
- SHA384
- SHA512

Algoritmos simétricos que podemos haber utilizado si te encuentras con información cifrada

- AES 192 CBC
- AES 192 CTR
- ARIA 256 CBC
- ARIA 256 CTR
- AES 256 CBC
- AES 256 ECB
- AES 256 OFB
- AES 256 CTR
- Camellia 256 CBC
- ChaCha20

caso de que el algoritmo requiera un Vector de Inicialización (IV Initialization Vector), lo podrás encontrar en el fichero zip inicial. Un vector de inicialización es un dato aleatorio que algunos algoritmos de cifrado (no todos) necesitan para calcular información que necesitan para el proceso de cifrado como "semilla" del proceso.

Algoritmos de codificación que podemos haber usado si te encuentras con información codificada

- Base64
- Hex
- Rot13
- Base32
- Base85



Bloque 2: Instrucciones de Entrega

Debes entregar los resultados de este laboratorio. Debes acceder a la dirección <https://156.35.163.140:444/xxxxxxxx> siendo la parte final la misma que usaste para descargar el zip (fíjate que es sin la parte de `/api`). En el ejemplo sería <https://156.35.163.140:444/c1e45406>

Se te presentará un formulario donde **debes poner las respuestas a todas las preguntas** y también puedes subir los ficheros correspondientes a los ejercicios. Se te pide una clave que es **la misma que usaste para descargar el zip en el paso inicial**. Además, **debes subir al Campus Virtual un PDF con la memoria** de todo lo realizado, en una tarea de entrega que se creará al efecto. En esta memoria deberás incluir:

- Cada paso en un apartado independiente, con un título “Paso 1”, “Paso 2”, y dentro de los mismos los siguientes contenidos
- El comando o comandos que has usado para hacer el proceso
- Una captura de la salida donde se vea el dato que se te pide obtener
- Si lo consideras necesario, el texto de alguna aclaración breve que quieras hacer.



BACK

1

2





Insignias y Autoevaluación

NOTA: Tienes una versión de esta tabla de insignias en formato editable disponible en el *Campus Virtual*. Puedes usar este archivo para crear un documento en el formato que deseas y tomar notas extendidas de tus actividades para crear un log de lo que has hecho. Recuerda que el material que elaboras se puede llevar a los exámenes de laboratorio.

Nivel de insignia	Desbloqueado cuando	¿Desbloqueado?
	Puedes extraer mensajes ocultos en imágenes usando técnicas de esteganografía y <i>hashing</i>	
	Puedes descifrar un mensaje con una clave simétrica usando algún algoritmo de cifrado popular	
	Puedes decodificar un mensaje usando algún algoritmo de codificación popular	
	Puedes entender el concepto de hash como medio para identificar inequívocamente ficheros concretos	
	Puedes romper un fichero zip protegido por contraseña con una herramienta adecuada	
	Puedes construir un diccionario con palabras extraídas del contenido de una página web y entender cómo se usan en herramientas que los admitan como entrada	
	Puedes romper la contraseña de un usuario de un SO <i>Linux</i> mediante técnicas de <i>cracking</i> de contraseñas	
	Sabes conectarte de manera segura vía SSH usando cifrado simétrico	
	Puedes generar certificados digitales a tu nombre y enviarlos a una autoridad certificadora para que te los firmen	

BACK

1

2

3