**Hacking**

**ético**

| Índice |
| --- |
| [**Índice 2**](#_xr9rspeahkre)  [**Archivos 2**](#_u0jrf0gngatq)  [**Pasos 2**](#_m3miwj5ybiut)  [Formateo del archivo con rar2john 2](#_f5vzqadoettw)  [Fuerza bruta con John The Ripper 2](#_khg11bvceuoq)  [Análisis de ficheros 4](#_jwr4cylob3xi)  [Descifrado AES 6](#_gboxfr9n40z5)  [Doble base64 7](#_6a7cslw9zfay)  [Estenografía 7](#_u4u0eoy5t9vq)  [Cracking pdf 11](#_p08m12seub56) |
| Archivos |
|  |
| * RetoHackting.rar |
| Pasos |
| Formateo del archivo con rar2john |
| El archivo .rar tiene una contraseña con la que no contamos por lo que probamos a descubrirla por fuerza bruta. |
| Rar2john RetoHackting.rar > claves.txt |
|  |
|  |
| Fuerza bruta con John The Ripper |
| Uso del diccionario /usr/share/wordlist/rockyou.gz.txt para probar fuerza bruta. |
| John –wordlist=rockyou.txt claves.txt |
|  |
| unrar e RetoHackting.rar  # happyday |
| Resultado |
| * Pista1.html      * Pista2.pdf ( cifrado ) |
| Análisis de ficheros |
| El html se encuentra ofuscado. El crucigrama es dinámico pero no es posible completarlo al sobrar un carácter en la fila “fase de reconocimiento”.  Hemos de encontrar otra vía. |
| Encontramos el código fuente en búsqueda de la siguiente pista. |
|  |
| Se indica una máscara asi que probamos con un comando de john |
|  |
| No funciona. |
| Probamos con herramientas de [rainbow tables online](https://hashes.com/en/decrypt/hash) |
|  |
| Rinc0n88 |
| Descifrado AES |
| En la siguiente página añadimos la clave “Rinc0n88” para descifrar el texto. |
| <https://cifraronline.com/descifrar-aes> |
|  |
| Encriptación en : AES |
| Pista 2:  La Esteganografía es la ciencia de ocultar un mensaje en una imagen. Ya en Kali podemos instalar una herramienta que nos permite realizarla.  Sigue esta pista para seguir con el Reto.  Suerte e inténtalo al menos un par de veces ...  YUhSMGNITTZMeTlrY21sMlpTNW5iMjluYkdVdVkyOXRMMlpwYkdVdlpDOHhWSEkyWW5SbFF6SndZakpzYmxkSlduSmZNbEJ4WlVwVmRrSlpOVlpvY3pJdmRtbGxkejkxYzNBOWMyaGhjbVZmYkdsdWF3PT0= |
| Doble base64 |
| El signo al final hace sospechar de un formateo en base64 |
|  |
| Doble base 64 |
| Estenografía |
| Link |
| https://drive.google.com/file/d/1Tr6bteC2pb2lnWIZr\_2PqeJUvBY5Vhs2/view?usp=share\_link |
|  |
| Foto.jpg |
|  |
|  |
| Escaneo qr |
| “La clave para Extraer Mensage de Imagen es: TerorCity” |
| Hay un mensaje secreto escondido mediante estenografía. |
| Steghide –extract -sf Foto.jpg |
| Resultado: |
| Pista4.txt |
|  |
| Se trata de un mensaje en “BrainFuck” |
| <https://www.dcode.fr/brainfuck-language> |
|  |
| Final.rar |
| Cracking pdf |
|  |
| dolphins |
| Contenido |
|  |