

Cyber Security I

Cell 0-0. (y/o) - Buenos usuarios, como si se es de la guardería del ejército.
infectados

Cell 0-1 - Descubrir identidad real del usuario.
x concul. con posesión de datos. → x. tipo de firma.
con x concul.
San Sebastián de Argentina. (Zamora) → Buenos de El Paso 2020
Buenos Aires

Cell 0-2 - Descubrir base de datos como si se es de la policía.
Inteligencia de San Pedro (Argentina) SECRET

Cell 0-3 - Tenemos la foto y tenemos que encontrar el modelo de teléfono.
Red via Pote RTC

Cell 4-0. warez

http://cybersec.42urduliz.3318. para saber y que hasta contin → solo flag. → flag. → index.
para solucionar por servicios. 42 BCN {E156F/4g600200}

Cell 1-1. warez.

http://cybersec.[campus].[tld]:3318.
http://cybersec.42urduliz.com:3318/ordenar/flag.txt.
Se le pueden poner atributos. forcing. → como nombre local que de sea el correcto.

Cell 1-2. Desvar - Path Traversal o ruta de desvar.
prevención... // o /// etc

http://cybersec.[campus].[tld]:3319
Que una vulnerabilidad que permitiera acceder a los que no tendrían que tener acceso.
power o // flag.txt → solo flag.

Cell 1-3 - Inyección - inyección SQL

http://cybersec.[campus].[tld]:3320
El panel permite saltar el panel de autenticación sin estar autorizado por una vulnerabilidad de la web.
usuario. asdf' or 'a'='a
contraseña. asdf' or 'a'='a
También vale con 'or '1'='1' 49 BCN {welcomeHackerBlog}

Cell 2-0. Ghetto Basic. pista Cyber chef

Encontrar la codificación que está siendo utilizada para codificar la información y así poder decodificar el texto codificado → NDIC POSLY; Q 1 M 1 8 L N F B X N V G J
M O B S F P ==

coger prog. cyber chef, pegar input y le vamos cambiando la base en este caso From base64 y de 48BCN {6453-64-15-000}

Cell 2-1. Ghetto. Medium.

Puede haber ocasiones en las que se sucederan diferentes tipos de codificaciones. Aquí tendrías que identificar todas las codificaciones que se utilizan hasta llegar a texto plano. La tarea es descifrar el contenido de la cadena y escribirlo en flag.txt.

Cell. 1. Con Cyber chef → esta ciudad primera vez el que viene → From Hex

↓
From base 64

42BCN {6453-64-15-0001-but-
h3x-15-00013r}

Cell 2-2 Ghetto. Basic. pista — hashcat

Ahora no es de codificaciones sino de hashes. A diferencia de las codificaciones, los hashes no se pueden revertir. La única manera de saber el texto con hash es encontrar un texto que tenga el hash mismo.

Quien quiere investigar eso para resolver este desafío.

Deber entregar el texto codificado. Ten en cuenta que tendrás que ponerlo en la bandera (flag) .permuto. Por ejemplo si el texto hash era "barcelona", tendrías que entregarlo 42BCN {barcelona}

La tarea es descifrar el contenido de esta cadena. Cuando lo hayas logrado, debes escribirlo en un arch. flag.txt.

Aprender a comprender y detectar un código conocido

Se trata de un suceso al que se le da el nombre de hash, que identifica o representa a un conjunto determinado (p.e. documento, foto, video, etc.).

Con crackmapexec, se pone el código, e indica que es Tipo de B.S. y Resultado positivo.
También vale con hashes.com.

Cell 2-3 Geth - Hard. prueba de la Ripper

Gracias al equipo de seguridad de 42 uso veritas, encontraron algunos polibros que potencialmente podían ser parte del hash que buscamos, los contrastamos que queramos hacer. Tu objetivo es romper el hash y obtener la contraseña en texto plano.

Debes entregar el texto codificado. Ten en cuenta que tienes que ponerlo en formato. P.e. si el texto hash es "Barcelona" tendrías que entregar 42Bch Barcelona.

La tarea es descifrar el contenido de este código. Cuando lo tengas, debes escribirlo en un archivo flag.txt.

Busca de la lista de 3 polibros cuál es el código que nos indican.

Con hashes.com. meter el código y sale hiamup2v.

OSINT FRAMEWORK

Exif. tools → para extraer foto.

<https://start.me/p/q6uata/osint-tools>