



Universidad
Francisco de Vitoria
UFV Madrid



Hacking Ético

Logros Atenea CCN-CERT



Nombre:	Fecha:	Edición:	Firma:
Gonzalo Pascual Romero	01/12/2023	1.0	



Índice

1. Alcance	3
2. Puntuación	6
3. Desarrollo del estudio	7
4. Conclusiones	96



Alcance

1. Básica	7
1. Hash.....	7
2. Hash 2	8
3. Hash 3	9
4. Base 64	11
5. ASCII	12
6. Hex	13
7. XOR	14
8. Entropía	15
9. Magic number	16
10. Strings	17
11. Metadatos	18
12. Metadatos 2	19
13. Variables	20
14. Variables 2	21
15. Python	22
16. C	24
17. Java.....	25
2.Básica: Red	26
1. Modelo TCP/IP	26
2. Dirección IP	27
3. Dirección IPv6	28
4. Direcciones IP privadas y públicas	29
5. DHCP	31
6. Mascara de red	32
7. Mascara de red 2	33
8. MAC	34



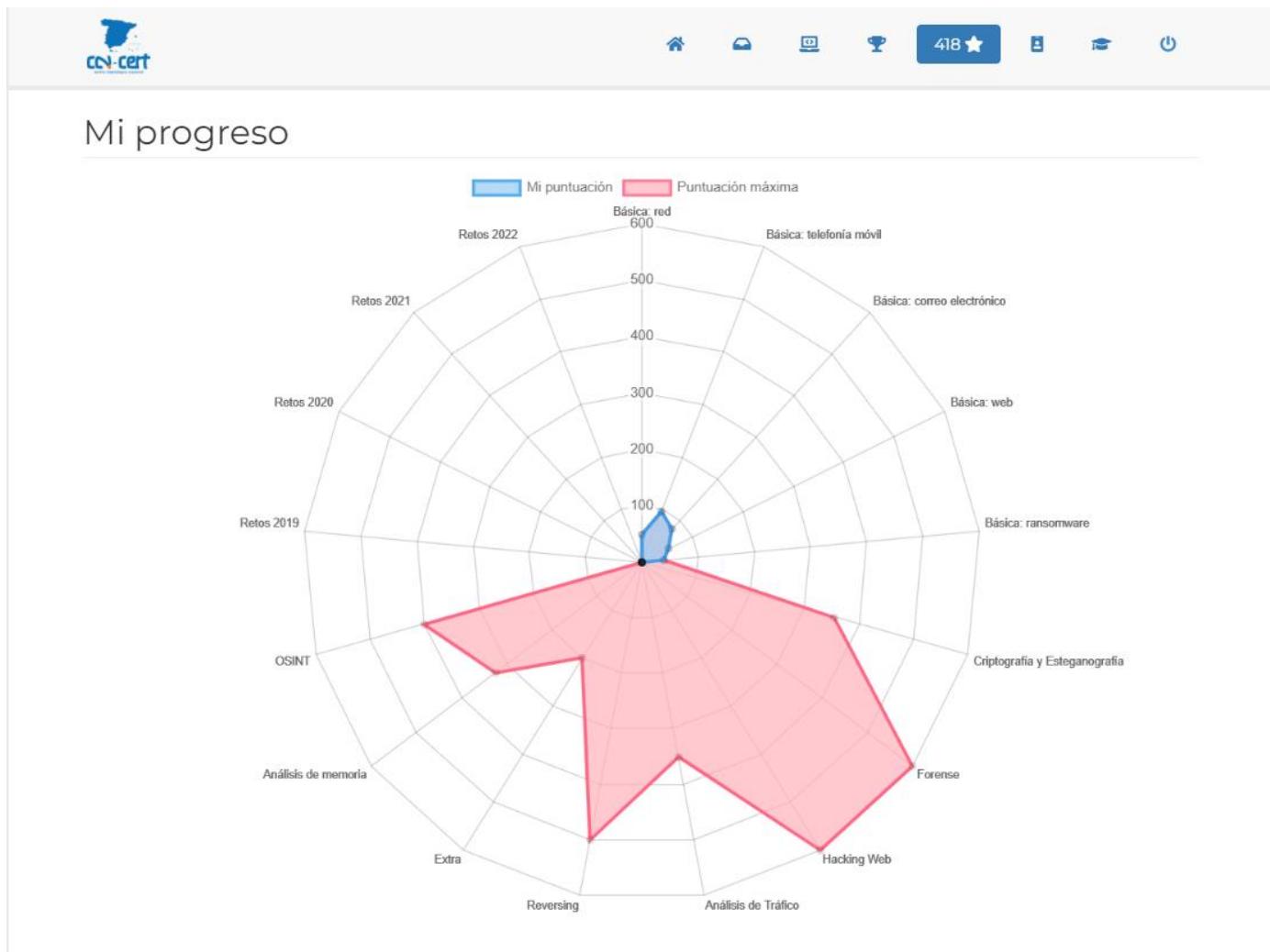
9. Puerto	35
10. Puerto 2	36
11. Puerto 3	37
12. DNS	38
13. DNS 2	39
14. Telenet	40
3.Básica: Telefonía móvil	42
1. Introducción	42
2. Versiones	43
3. Nombre interno	44
4. Permisos	45
5. Código PIN	46
6. Patrón de bloqueo.....	47
7. Permisos 2	48
8. Permisos 3	49
9. Credenciales	51
10. Credenciales 2	53
4.Básica: Correo electrónico	55
1. Phishing	55
2. Phishing 2	56
3. Phishing 3	57
4. Phishing 4	58
5. Phishing 5	59
6. Phishing 6	60
7. Phishing 7	62
8. Phishing 8	64
9. Phishing 9	66
10. Phishing 10	68
11. Carácter RLO	70



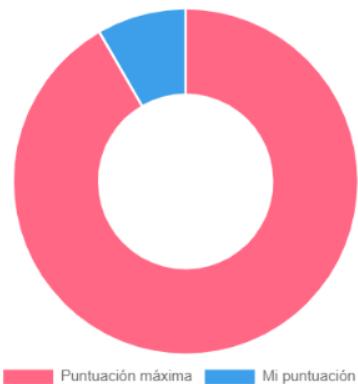
12. Macro	71
13. Compromiso de correo electrónico	72
14. Compromiso de correo electrónico 2	73
15. Compromiso de correo electrónico 3	74
5. Básica: Web	76
1. Tag HTML	76
2. Servidor web	77
3. Servidor web 2	78
4. País de origen	79
5. Código HTTP	80
6. Cookie	81
7. Certificado SSL	82
8. Ruta	83
9. JavaScript	84
10. PHP	85
11. XSS	86
6. Básica: Ransomware	87
1. Detección de ransomware	87
2. Identificación de la familia de ransomware	88
3. Recuperación de datos	90
4. Recuperación de datos 2	92
5. Recuperación de datos 3	93
6. WannaCry	95

Puntuación

Puntuación total: 418



Posición Global #386



#	Apodo	País	Puntos
383	Arz	ES	418
384	BeerMan	ES	418
385	Khane	ES	418
386	Gon	ES	418
387	Fishing	ES	418
388	juanxxx	ES	418
389	pablo97dr	ES	418



Desarrollo del estudio

Básica

Hash

Hash (1pts)



Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

La contraseña para superar este reto es **LearnTheHashFunction**

Tendrás que calcular su hash md5 y ponerla en el formato de la plataforma, esto es:
flag{md5}

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

Referencias:

<https://www.genbetadev.com/seuridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales>

<https://askubuntu.com/questions/53846/how-to-get-the-md5-hash-of-a-string-directly-in-the-terminal>

Solución:

Se puede hacer con páginas web en internet o con códigos de python

```
import hashlib
print('flag{' + hashlib.md5(b'LearnTheHashFunction').hexdigest() + '}')
```

Respuesta: [REDACTED]



Hash 2

Hash 2 (1pts)

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Existen diferentes algoritmos para calcular estas funciones resumen o hash, siendo los más extendidos md5 y sha256.

La contraseña para superar este reto es ThisIsAMoreSecureHashFunction

Tendrás que calcular su hash sha256 y posteriormente calcular su md5 para poder poner la solución en el formato de la plataforma, esto es: flag{md5}

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

Referencia:

<https://www.genbeta.dev.com/seuridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales>

Solución:

Con código de python lo paso a sha256 y después a md5

```
import hashlib
sha256 = hashlib.sha256()
sha256.update(b"ThisIsAMoreSecureHashFunction")
md5 = hashlib.md5()
md5.update(sha256.hexdigest().encode('utf-8'))
print("flag{" + md5.hexdigest() + "}")
```

Respuesta: [REDACTED]



Hash 3

Hash 3 (2pts)



Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Estas funciones son de un único sentido. Es decir, que a partir de un hash no es posible obtener su valor original de manera directa.

La única forma de calcular el valor correspondiente a un hash es mediante ataques de fuerza bruta, esto es, calcular el hash de todas las combinaciones posibles e ir comparándolo con el hash que tenemos. Afortunadamente hay servicios on-line que ya han calculado millones de hashes.

Para superar este reto deberás calcular la cadena de texto cuyo hash md5 se corresponde con el siguiente:

54f662a095fa3d5fbbdaac72d176701b

Una vez obtenida, deberás poner dicha cadena de texto en mayúsculas y calcular su hash md5 para poder enviar la solución siguiendo el formato de la plataforma: flag{md5}

Referencias:

<https://www.genbetadev.com/seuridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales>
<https://crackstation.net/>

Solución:

Se pasa de md5 a texto y sale master of puppets, se pasa a mayúsculas y de vuelta a md5

The screenshot shows a web-based tool for decoding MD5 hashes. On the left, there's a search bar with the placeholder "Search for a tool" and a keyword input field containing "e.g. type 'boolean'". Below the search bar is a link to "BROWSE THE FULL dCODE TOOLS' LIST". On the right, the main interface is titled "DESCIFRADO MD5". It displays the input hash "★ HASH MD5 54F662A095FA3D5FBBDAAC72D176701B" and two options fields: "★ SAL PREFIJO MD5 (PALABRA SAL)" and "★ SAL CON EL SUFIXO MD5 (PALABRA SAL)". A large green button labeled "► DESCIFRAR" is positioned below these fields. At the bottom, a link reads "Ver también : Hash Function – SHA-1 – Crypt() Hashing Function".



Página de descifrado md5

```
import hashlib
print('flag{'+hashlib.md5(b'').hexdigest()+'}')
```

Respuesta: [REDACTED]



Base64

Base64 (3pts)



Base64 es un grupo de esquemas de codificación de binario a texto que representa los datos binarios mediante una cadena ASCII, traduciéndolos en una representación radix-64. El término Base64 se origina de un sistema de codificación de transmisión de contenido MIME específico.

Los esquemas de codificación Base64 son comúnmente usados cuando se necesita codificar datos binarios para que sean almacenados y transferidos sobre un medio diseñado para tratar con datos textuales. Esto es para asegurar que los datos se mantienen intactos y sin modificaciones durante la transmisión. Base64 es comúnmente usado en muchas aplicaciones, incluyendo la escritura de emails vía MIME y el almacenamiento de datos complejos en XML.

Para superar este reto tendrás que descodificar el fichero adjunto y poner la contraseña en el formato de la plataforma, esto es: flag{md5}

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

Referencia:

https://developer.mozilla.org/es/docs/Web/API/WindowBase64/Base64_codificando_y_decodificando

Solución:

Se puede hacer por páginas de internet o por código de Python

```
Recuerda que cuando codificas algo en base64 NO lo estás cifrando,  
sino que simplemente lo estás codificando.  
La contraseña para superar este reto es: recuerdaquebase64NOescifrar
```

```
import hashlib  
print('flag{' + hashlib.md5(b'recuerdaquebase64NOescifrar').hexdigest() + '}')
```

Respuesta: [REDACTED]



ASCII

ASCII (3pts)



El código ASCII es una representación numérica de un carácter. Como otros códigos de formato de representación de caracteres, el ASCII es un método para una correspondencia entre cadenas de bits y una serie de símbolos (alfanuméricos y otros), permitiendo de esta forma la comunicación entre dispositivos digitales así como su procesado y almacenamiento.

El código ASCII reserva los primeros 32 códigos (numerados del 0 al 31 en decimal) para caracteres de control: códigos no pensados originalmente para representar información imprimible, sino para controlar dispositivos (como impresoras) que usaban ASCII.

Los códigos del 33 al 126 se conocen como caracteres imprimibles, y representan letras, dígitos, signos de puntuación y varios símbolos.

Para pasar este reto deberás encontrar los caracteres correspondientes a la siguiente codificación ASCII:

080 097 115 115 119 111 114 100 032 112 097 114 097 032 115 117 112 101 114 097 114
032 101 108 032 114 101 116 111 058 032 084 104 101 065 083 067 073 073 084 097 098
108 101 033

Referencias:

<https://es.wikipedia.org/wiki/ASCII>

<http://www.asciitable.com>

Solución:

Se puede hacer con páginas en internet o con códigos en Python

```
import hashlib
print('flag{' + hashlib.md5(b'TheASCIITable!').hexdigest() + '}')
```

Respuesta: [REDACTED]



Hex

Hex (3pts)



El sistema hexadecimal es el sistema de numeración posicional que tiene como base el 16. En principio, dado que el sistema usual de numeración es de base decimal y, por ello, sólo se dispone de diez dígitos, se adoptó la convención de usar las seis primeras letras del alfabeto latino para suplir los dígitos que nos faltan.

El conjunto de símbolos es el siguiente:

$$S = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F \}$$

Siendo A = 10, B = 11, C = 12, D = 13, E = 14 y F = 15. Para su representación se pueden utilizar tanto letras minúsculas como mayúsculas.

Para pasar este reto deberás decodificar la siguiente cadena hexadecimal:

50617373776f72643a2044346d7054686548337821

Referencias:

https://es.wikipedia.org/wiki/Sistema_hexadecimal
<http://www.asciitable.com>

Solución:

Directamente buscando en internet un conversor

HEXADECIMAL	ASCII
50617373776f72643a2044346d7054686548337821	Password: [REDACTED]

Respuesta: [REDACTED]
[REDACTED]



XOR

XOR (4pts)



En criptografía, el cifrado XOR es, como su nombre indica, un algoritmo de cifrado basado en el operador binario XOR:

$$\begin{aligned} A \text{ xor } 0 &= A \\ A \text{ xor } A &= 0 \\ (B \text{ xor } A) \text{ xor } A &= B \end{aligned}$$

Una cadena de texto puede ser cifrada aplicando el operador de bit XOR sobre cada uno de los caracteres utilizando una clave. Para descifrar la salida, sólo hay que volver a aplicar el operador XOR con la misma clave.

Usa la clave encryptXORkey para descifrar el siguiente mensaje:

HQERKhYCLDc9KgQX

Recuerda que la respuesta hay que ponerla en el formato correcto: flag{md5}

Referencias:

<https://gchq.github.io/CyberChef/>

Solución:

Código de Python que hace la operación XOR

```
import base64
# Mensaje cifrado en formato Base64
Mensaje = "HQERKhYCLDc9KgQX"
# Decodificar el mensaje Base64 a datos binarios
binario = base64.b64decode(Mensaje)
# Clave XOR
clave = "encryptXORkey"
# Realizar la operación XOR para descifrar
decrypted_data = bytes([a ^ ord(b) for a, b in zip(binario, clave)])
# Imprimir el mensaje descifrado como una cadena ASCII
print(decrypted_data.decode('ascii'))
```

Respuesta: [REDACTED]



Entropía

Entropía (5pts)



En el ámbito de la teoría de la información la entropía mide la incertidumbre de una fuente de información. La entropía también se puede considerar como la cantidad de información promedio que contienen los símbolos usados. Los símbolos con menor probabilidad son los que aportan mayor información. Llevando este concepto al campo informático, podemos decir que un fichero tiene una entropía alta (yendo ésta de 0 a 8), cuando sus bytes son más heterogéneos entre sí. Esto es especialmente interesante en seguridad informática porque los ficheros con una entropía muy alta (cerca de 8) suelen ser ficheros cifrados o comprimidos.

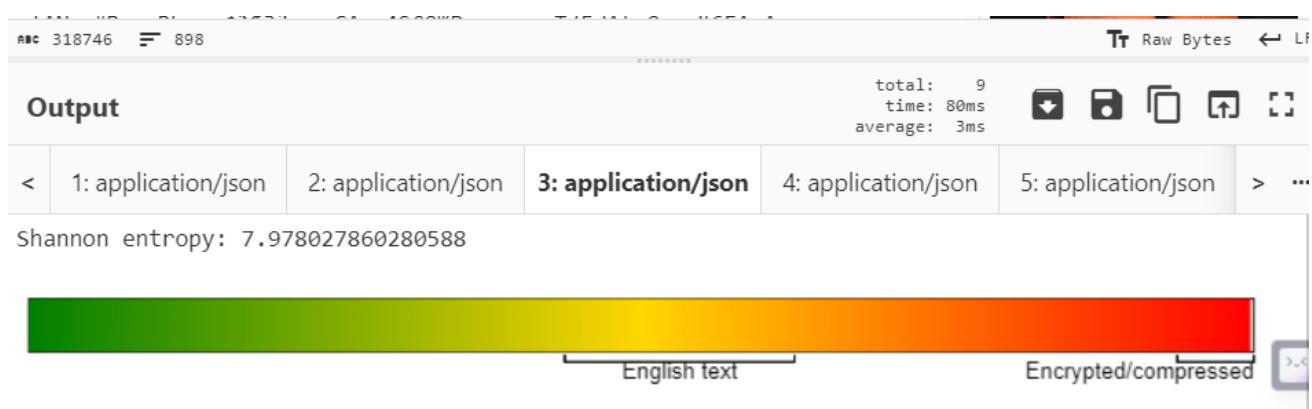
Teniendo en cuenta esto, para pasar este reto deberás encontrar cuál de las imágenes adjuntas tiene la mayor entropía. La solución al reto es el nombre del fichero de la imagen (incluyendo la extensión) en el formato habitual de la plataforma (por ejemplo: imagen25.jpg).

Referencia:

[https://es.wikipedia.org/wiki/Entrop%C3%ADa_\(informaci%C3%B3n\)](https://es.wikipedia.org/wiki/Entrop%C3%ADa_(informaci%C3%B3n))

<https://gchq.github.io/CyberChef>

Solución:



Buscando en el CyberChef y pasandole todos los archivos sale que el que más entropía tiene es el siguiente:

Respuesta: [REDACTED]



Magic number

Magic number (5pts)



Se le llama magic number a los primeros bytes de un fichero, los cuales son utilizados por los sistemas Linux para identificar el formato del mismo. En sistemas operativos Windows, sin embargo, basan la identificación del tipo de fichero en la extensión que tenga, siendo éste último método muy poco fiable.

Para superar el reto, debes averiguar qué magic number tiene el fichero sin extensión proporcionado (con letras mayúsculas. Por ejemplo: 0011DEADBEEFC0FFEEBABEFF)

Referencias:

<https://asecuritysite.com/forensics/magic>

Solución:

en la terminal de linux: xxd magicnumber-67351bf4490e9405b4195d544a1c290e y cogemos los 6 primeros bytes de la primera linea

```
[root@Gonzalo]# xxd magicnumber-67351bf4490e9405b4195d544a1c290e
00000000: [REDACTED]....
```

Respuesta: [REDACTED]



Strings

Strings (5pts)



Se denomina *string* a un conjunto de caracteres imprimibles (códigos 33 al 126 del alfabeto ASCII) que aparecen juntos. Podemos encontrarnos con multitud de *strings* dentro de cualquier fichero, independientemente de su tipo.

Cuando se trata de un ejecutable, por ejemplo un malware, estas cadenas de caracteres nos pueden dar pistas importantes sobre su funcionamiento sin tener que hacer ningún tipo de ingeniería inversa, ni tan siquiera tener que ejecutarlo; simplemente echando un vistazo a los *strings* que contiene.

Para superar este reto deberás averiguar cuál es el dominio al que se intenta conectar el binario de Linux que se adjunta (por ejemplo: www.dominio.com).

Referencias:

https://es.wikipedia.org/wiki/Cadena_de_caracteres

<http://www.linfo.org/strings.html>

<https://docs.microsoft.com/en-us/sysinternals/downloads/strings>

Solución:

Usando el comando strings lookinside-64d0177d2ee53c67e46d5748183d0098 | grep www filtramos por www y sale el dominio

```
(root@Gonzalo)-[/home/kali]
# strings lookinside-64d0177d2ee53c67e46d5748183d0098 | grep www
[REDACTED]
```

Respuesta: [REDACTED]



Metadatos

Metadatos (6pts)



Se define **metadato** como información estructurada que describe, explica, localiza y además hace más fácil recuperar, utilizar o gestionar un recurso de información. Los metadatos son comúnmente llamados "datos sobre los datos" o "información sobre la información".

Se define información o **datos ocultos** como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos programas, para su visualización.

Para superar este reto deberás averiguar quién es el autor del documento PDF.

Referencias:

https://www.adobe.com/digitalimag/pdfs/about_metadata.pdf

<https://helpx.adobe.com/acrobat/using/pdf-properties-metadata.html>

Solución:

La solución se saca haciendo desde Kali Linux un exiftool en el que te dice el autor

```
(kali㉿kali)-[~/Downloads]$ exiftool LoremIpsum-1e40fa12a5e7ce47ebcaaace81f6fd06.pdf
ExifTool Version Number      : 12.67
File Name                   : LoremIpsum-1e40fa12a5e7ce47ebcaaace81f6fd06.pdf
Directory                  : .
File Size                   : 31 kB
File Modification Date/Time: 2023:10:23 06:05:25-04:00
File Access Date/Time       : 2023:10:23 06:05:26-04:00
File Inode Change Date/Time: 2023:10:23 06:05:25-04:00
File Permissions            : -rw-r--r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.4
Linearized                  : No
Page Count                  : 1
XMP Toolkit                 : Image::ExifTool 10.55
Creator                     : John Doe
Language                    : none
Author                      : [REDACTED]
```

Respuesta: [REDACTED]



Metadatos 2

Metadatos 2 (6pts)



Cada vez que haces una fotografía digital se generan un montón de datos sobre la misma, como, por ejemplo, la fecha y hora en la que se hizo, el formato y el tamaño, marca y modelo de la cámara que has utilizado, etc. Si la fotografía se ha hecho con un móvil, dependiendo de la configuración del mismo, la imagen podría incluir también las coordenadas de la posición donde se tomó la fotografía.

Para superar este reto deberás averiguar el modelo de la cámara con la que se tomó la fotografía (la solución es sólo el modelo, sin incluir la marca, y todo en mayúsculas)

Referencias:

<https://www.pandasecurity.com/spain/mediacenter/consejos/fotos-metadatos-privacy/>
<https://www.sno.phy.queensu.ca/~phil/exiftool/>

Solución:

Igual que el anterior con el exiftool se busca la información y nos saldrá en el modelo de la cámara

```
(kali㉿kali)-[~/Downloads]
$ exiftool balloon-fc416bf4b40d82bcaa2b941bd38a42cd.jpg
ExifTool Version Number : 12.67
File Name : balloon-fc416bf4b40d82bcaa2b941bd38a42cd.jpg
Directory : .
File Size : 103 kB
File Modification Date/Time : 2023:10:23 06:16:58-04:00
File Access Date/Time : 2023:10:23 06:16:59-04:00
File Inode Change Date/Time : 2023:10:23 06:16:59-04:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : inches
X Resolution : 300
Y Resolution : 300
Exif Byte Order : Big-endian (Motorola, MM)
Make : SONY
Camera Model Name : [REDACTED]
```

Respuesta: [REDACTED]



Variable

Variable (7pts)



En programación, una variable está formada por un espacio en el sistema de almacenaje (memoria principal de un ordenador) y un nombre simbólico (un identificador) que está asociado a dicho espacio. Ese espacio contiene una cantidad de información conocida o desconocida, es decir un valor. El nombre de la variable es la forma usual de referirse al valor almacenado: esta separación entre nombre y contenido permite que el nombre sea usado independientemente de la información exacta que representa.

Debido a que las variables contienen o apuntan a valores de tipos determinados, las operaciones sobre las mismas y el dominio de sus propios valores están determinadas por el tipo de datos en cuestión.

Para superar este reto, deberás identificar, entre las siguientes declaraciones de variables, cuál de ellas tiene asociado un tipo de datos erróneo:

```
byte num = 44;  
short med = 1223;  
long lmax = 839492019487;  
float mreal = 112.31f;  
double rbig = 761132.4321;  
boolean bbin = true;  
int max = "1000";  
char lett = 'A';
```

La solución al reto es el nombre de la variable (por ejemplo: vbar), en el formato de la plataforma.

Referencias:

[https://es.wikipedia.org/wiki/Variable_\(programaci%C3%B3n\)](https://es.wikipedia.org/wiki/Variable_(programaci%C3%B3n))

https://es.wikipedia.org/wiki/Tipo_de_dato

Solución:

Respuesta: [REDACTED]



Variable 2

Variable 2 (7pts)



Cada lenguaje de programación tiene su propia sintaxis. Esto quiere decir que para obtener un mismo resultado, en un lenguaje de programación se expresará de manera diferente a otro.

Para superar este reto, deberás encontrar el equivalente en BASH, de la siguiente línea de código en BASIC:

PRINT "Atenea"

Referencia:

<https://www.geeksforgeeks.org/hello-world-in-30-different-languages/>

Solución:

Respuesta: [REDACTED]

[REDACTED]



Python

Python (10pts)



En informática, un script, archivo de órdenes, archivo de procesamiento por lotes, es un programa usualmente simple, que por regla general se almacena en un archivo de texto plano. Los script son casi siempre interpretados, esto es, que no se pueden ejecutar por sí mismos, sino que tienen que ser interpretados por el motor del lenguaje de programación correspondiente.

Para superar este reto deberás obtener el valor de la variable result del siguiente script en python, que te dará el password que necesitas.

Referencias:

<https://es.wikipedia.org/wiki/Script>
<https://es.wikipedia.org/wiki/Python>

Solución:

Para lograrlo hay que descargar unos módulos y cambiar el código

Descargar pycryptodome para que el modulo crypto funcione

```
(kali㉿kali)-[~/Downloads] $ pip install pycryptodome
Defaulting to user installation because normal site-packages is not writeable
Collecting pycryptodome
  Obtaining dependency information for pycryptodome from https://files.pythonhosted.org/packages/00/e6/73931df4046e34a6354d323b4a5b5c18e5184f4a08687806ee3353c81a6b/pycryptodome-3.19.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata
    Downloading pycryptodome-3.19.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (3.4 kB)
    Downloading pycryptodome-3.19.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
      2.1/2.1 MB 1.7 MB/s eta 0:00:00
Installing collected packages: pycryptodome
  Successfully installed pycryptodome-3.19.0
```

Se hace un cambio en las claves y se les pone la b delante para que se pase a bytes y un print final para que nos de el resultado:



```
(kali㉿kali)-[~/Downloads] $ cat script-6a21d37e6d6a4c87c06ba3ec40e28e0c.py
import base64
from Crypto import Random
from Crypto.Cipher import AES

AKEY = b'mysixteenbytekey'
iv = b'what_a_cool_iv!!'

def decode(cipher):
    obj2 = AES.new(AKEY, AES.MODE_CFB, iv)
    return obj2.decrypt(base64.urlsafe_b64decode(cipher))

result = decode("5fMfiISsxcG4gKWAXwkL1Bu6zW26FlhG1613")

print (result)

(kali㉿kali)-[~/Downloads] $ python script-6a21d37e6d6a4c87c06ba3ec40e28e0c.py
```

Respuesta: [REDACTED]



C

C (10pts)



A diferencia de python, que es un lenguaje de programación de scripting, el código fuente de un programa en C necesita ser compilado antes de poder ser ejecutado. Una vez compilado, podrá ser ejecutado sin necesidad de un intérprete.

Para poder superar este reto deberás compilar y ejecutar el siguiente código en C.

Referencias:

[https://es.wikipedia.org/wiki/C_\(lenguaje_de_programaci%C3%B3n\)](https://es.wikipedia.org/wiki/C_(lenguaje_de_programaci%C3%B3n))

https://es.wikibooks.org/wiki/Programaci%C3%B3n_en_C/Compilar_un_programa

Solución:

Ejecutandolo con un compilador de C sale el password directamente

```
8
9 #include <stdio.h>
10
11 void main() {
12     int a = 65535;
13
14     printf("Password : %d\n", a << 7);
15 }
```

>Password :

Respueta: [REDACTED]

[REDACTED]



Java

Java (25pts)



Java es un lenguaje de programación de propósito general, concurrente, orientado a objetos que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo, lo que quiere decir que el código que es ejecutado en una plataforma no tiene que ser recompilado para correr en otra.

En términos de seguridad informática, los programas escritos en Java puede ser descompilados muy fácilmente debido a las propias características de este lenguaje de programación.

Para poder superar este reto deberás descompilar, es decir, obtener el código fuente, del siguiente programa compilado de Java, para obtener el valor de una variable en concreto.

Referencias:

[https://es.wikipedia.org/wiki/Java_\(lenguaje_de_programaci%C3%B3n\)](https://es.wikipedia.org/wiki/Java_(lenguaje_de_programaci%C3%B3n))

<http://jd.benow.ca/>

<https://github.com/deathmarine/Luyten>

<http://www.javadecompilers.com>

Solución:

Igual que el anterior ejecutándolo con un compilador de Java sale el resultado

```
= "b0b9cb1e4b869109";
= "b0c35c246e7683db";
= "b1974843692d56e7";
= "b2242bdb30853506";
TheVariableYouAreLookingFor =
= "b27c3e217acd04bd";
= "b4d38fad34e8766b";
= "b6357550810cbff8";
```



Básica: Red

Modelo TCP/IP

Modelo TCP/IP (1pts)



TCP/IP es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa Protocolo de control de transmisión/Protocolo de Internet. Proviene de los nombres de dos protocolos importantes incluidos en el conjunto TCP/IP, es decir, del protocolo TCP y del protocolo IP.

Este modelo incluye cuatro capas. Para superar el reto indica el número de capa (en formato numérico, por ejemplo: 15) correspondiente a la capa de Internet.

Referencias:

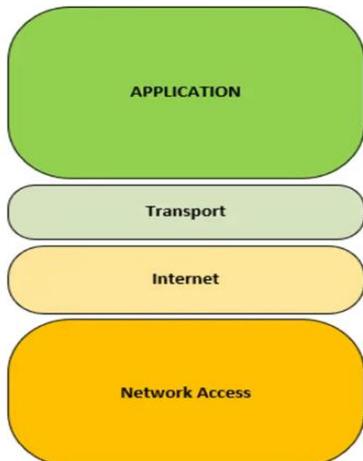
https://es.wikipedia.org/wiki/Modelo_TCP/IP

https://en.wikipedia.org/wiki/Internet_protocol_suite

https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet

Solución:

Modelo TCP/IP



Respuesta: [REDACTED]



Dirección IP

Dirección IP (2pts)



La dirección IP es un conjunto de números que identifica a un equipo dentro de una red que utilice el protocolo Internet Protocol (IP) o que corresponde al nivel de red del modelo TCP/IP.

La versión 4 de la dirección IP (IPv4) utiliza un formato de 4 números separados por un punto entre ellos.

Para superar este reto, indica cuál es una IPv4 válida:

- 45.2.6..1
- 192.1t8.32.8
- 8.8.8.8
- 3:4:5:6
- 212.27.123.45
- 00.25.350.56
- 128.76.64.258

Referencias:

https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

https://en.wikipedia.org/wiki/IP_address

Solución:

Respuesta: [REDACTED]



Dirección IPv6

Dirección IPv6 (2pts)



IPv6 es el sucesor del primer protocolo de direccionamiento de Internet, Internet Protocol versión 4 (IPv4). A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 tienen un tamaño de 128 bits. Por lo tanto, IPv6 tiene un espacio de direcciones mucho más amplio que IPv4.

Una dirección IPv6 (128 bits) se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bits (dos octetos). Los grupos se separan mediante dos puntos (:).

Para superar este reto, averigua la IPv6 válida:

192.168.1.1
80.40.32.112.0.0.1.12
ab00.12cd.4eef.2100.4e11.0a22.3333.1f44
2001:0aa8:13ed:0000:0000:ff7a:98ff:0001
2ae3::0::0233:1:
8.8.8.8
1aad:3aaa:13ej:0000:0000:ff7a:98ff:0001

Referencias:

https://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6

Solución:

Respuesta: [REDACTED]

[REDACTED]



Direcciones IP privadas y públicas

Direcciones IP privadas y públicas (2pts)



Una dirección IP puede ser privada o pública. Las IPs privadas se utilizan para las comunicaciones de los equipos dentro de una red local, mientras que las IPs públicas se utilizan para las comunicaciones a través de Internet.

Por ejemplo, en una red doméstica, en la que se tiene un router ADSL o de fibra, los equipos conectados a él mediante wifi o cable tendrán una dirección IP privada, pero saldrán a Internet usando la misma dirección IP pública.

Los rangos de IPs privadas están definidos dentro del RFC1918.

Para superar este reto, indica cuál de las siguientes IPs es una IP privada:

- 8.8.8.8
- 192.178.1.1
- 172.25.0.3
- 85.32.11.0
- 172.0.0.1
- 12.10.25.4
- 11.22.33.44
- 0.0.0.0

Referencias:

- https://es.wikipedia.org/wiki/Red_privada
- <https://tools.ietf.org/html/rfc1918>



Solución:

Las direcciones de Internet privadas son:

Nombre	Rango de direcciones IP	Cantidad de IP	N.º de Redes	Cantidad de IP por Red	Descripción de la clase de cada una de las redes	Mayor bloque de CIDR (máscara de subred)
Bloque de 24 bits	10.0.0.0 – 10.255.255.255	16.777.214	1	16.777.214	Clase A	10.0.0.0/8 (255.0.0.0)
Bloque de 20 bits	172.16.0.0 – 172.31.255.255	1.048.576	16	65.534	Clase B	172.16.0.0/12 (255.240.0.0)
Bloque de 16 bits	192.168.0.0 – 192.168.255.255	65.534	256	254	Clase C	192.168.0.0/16 (255.255.0.0)
Bloque de 16 bits	169.254.0.0 – 169.254.255.255	65.534	1	65.534	Clase B simple	169.254.0.0/16 (255.255.0.0)

Respuesta: [REDACTED]

[REDACTED]



DHCP

DHCP (3pts)



El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP. Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

En el fichero adjunto, el servidor DHCP asigna una IP privada a un equipo. Indica de qué IP se trata.

Referencias:

https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

<https://www.wireshark.org/>

Solución:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	[REDACTED]	DHCP	314	DHCP Discover - Transaction
2	0.000295	192.168.0.1	[REDACTED]	DHCP	342	DHCP Offer - Transaction
3	0.070031	0.0.0.0	[REDACTED]	DHCP	314	DHCP Request - Transaction
4	0.070345	192.168.0.1	[REDACTED]	DHCP	342	DHCP ACK - Transaction

Respuesta:

[REDACTED]



Máscara de red

Máscara de red (3pts)



La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Para superar este reto, indica la equivalencia en el formato CIDR de esta máscara de red (por ejemplo: 37):

255.255.255.0

Referencias:

https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

<https://en.wikipedia.org/wiki/Subnetwork>

https://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Solución:

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0000	0.0.0.0	127.255.255.255	255.0.0.0	
B	1000	128.0.0.0	191.255.255.255	255.255.0.0	
C	1100	192.0.0.0	223.255.255.255	255.255.255.0	
D	1110	224.0.0.0	239.255.255.255	255.255.255.255	
E	1111	240.0.0.0	255.255.255.255	255.255.255.255	

Respuesta:

[REDACTED]

[REDACTED]



Máscara de red 2

Máscara de red 2 (3pts)

La máscara de red se puede representar en diversos formatos.

Para superar este reto, indica la equivalencia en formato decimal de la máscara /20 del formato CIDR (por ejemplo: 255.255.255.0)

Referencias:

https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

<https://en.wikipedia.org/wiki/Subnetwork>

https://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Solución:

Como en la siguiente tabla la respuesta es

Mask	IP Addresses	Hosts	Netmask
/31	2	2	
/30	4	2	
/29	8	6	
/28	16	14	
/27	32	30	
/26	64	62	
/25	128	126	
/24	256	254	
/23	512	510	
/22	1024	1022	
/21	2048	2046	
/20	4096	4094	

Respuesta:



MAC

MAC (4pts)



La dirección MAC (Media Access Control) es un identificador único para cada dispositivo de red. Se la conoce también como dirección física, y su valor depende del fabricante.

Para superar este reto, indica el fabricante (primera letra en mayúsculas) de la tarjeta de red con la siguiente dirección MAC:

fc:f8:ae:f1:fd:ec:8a:aa

Referencias:

https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC

https://en.wikipedia.org/wiki/MAC_address

Solución:

Buscando en internet me salió la respuesta

▀ OUI: FC:F8:AE
▀ Range: FC:F8:AE:00:00:00 - FC:F8:AE:FF:FF:FF
▀ Block Size: 16777215 (16.77 M)
∞ Universally administered addresses (UAA) : the a
▀ Type of transmission: Unicast
▀ WIRESHARK:
[REDACTED]

Respuesta: [REDACTED]
[REDACTED]



Puerto

Puerto (4pts)

En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan, por convenio, a ciertas aplicaciones particulares o servicios de carácter universal.

Para superar este reto, indica el puerto asignado por convenio para HTTP.

Referencias:

[https://es.wikipedia.org/wiki/Puerto_\(inform%C3%A1tica\)#Puertos_de_Internet](https://es.wikipedia.org/wiki/Puerto_(inform%C3%A1tica)#Puertos_de_Internet)

[https://en.wikipedia.org/wiki/Port_\(computer_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

Solución:

Como indica en la siguiente tabla el puerto es el

Number	Assignment
	File Transfer Protocol (FTP) Data Transfer
	File Transfer Protocol (FTP) Command Control
	Secure Shell (SSH) Secure Login
	Telnet remote login service, unencrypted text messages
	Simple Mail Transfer Protocol (SMTP) email delivery
	Domain Name System (DNS) service
	Dynamic Host Configuration Protocol (DHCP)
	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
	Post Office Protocol (POP3)

Respuesta:

[REDACTED]

[REDACTED]



Puerto 2

Puerto 2 (4pts)



En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan, por convenio, a ciertas aplicaciones particulares o servicios de carácter universal.

Para superar este reto, indica el puerto asignado por convenio para HTTPS.

Referencias:

[https://es.wikipedia.org/wiki/Puerto_\(inform%C3%A1tica\)#Puertos_de_Internet](https://es.wikipedia.org/wiki/Puerto_(inform%C3%A1tica)#Puertos_de_Internet)
[https://en.wikipedia.org/wiki/Port_\(computer_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

Solución:

Viendo la misma tabla del ejercicio anterior sale el puerto de HTTPS

	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
	Post Office Protocol (POP3)
	Network News Transfer Protocol (NNTP)
	Network Time Protocol (NTP)
	Internet Message Access Protocol (IMAP) Management of digital mail
	Simple Network Management Protocol (SNMP)
	Internet Relay Chat (IRC)
	HTTP Secure (HTTPS) HTTP over TLS/SSL
	DHCPv6 IPv6 version of DHCP

Respuesta:



Puerto 3

Puerto 3 (4pts)



En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan, por convenio, a ciertas aplicaciones particulares o servicios de carácter universal.

Para superar este reto, indica el puerto de origen más bajo utilizado para las comunicaciones en el fichero de captura de tráfico que se adjunta.

Referencias:

[https://es.wikipedia.org/wiki/Puerto_\(inform%C3%A1tica\)#Puertos_de_Internet](https://es.wikipedia.org/wiki/Puerto_(inform%C3%A1tica)#Puertos_de_Internet)

[https://en.wikipedia.org/wiki/Port_\(computer_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

<https://www.wireshark.org/>

Solución:

Lo abro con Wireshark y en uno de los registros sale el Source Port

Destination Address: 142.250

Transmission Control Protocol,

Source Port: [REDACTED]

Destination Port: 443

Respuesta: [REDACTED]
[REDACTED]



DNS

DNS (5pts)



El sistema de nombres de dominio (DNS) sirve como traductor de direcciones IP a nombres de dominio y viceversa. Se podría decir que es como una agenda de Internet.

Para pasar este reto indica el nombre de dominio correspondiente a la siguiente dirección IP:

8.8.8.8

Referencias:

https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio

https://en.wikipedia.org/wiki/Domain_Name_System

Solución:

Buscando por internet te sale el dominio

**Búsqueda de DNS para dns.google
(reverse DNS of 8.8.8.8)**

Tipo	Anfitrión	Clase	TTL	Datos
AAAA	[REDACTED]	IN	253	ipv6 = 2001:4860:4860::8844

Respuesta:



DNS 2

DNS 2 (5pts)

El sistema de nombres de dominio sirve como traductor de direcciones IP a nombres de dominio y viceversa. Es como una agenda de Internet.

Para pasar este reto indica la dirección IPv4 correspondiente al siguiente dominio:

reyes.ccn-cert.cni.es

Referencias:

https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio

https://en.wikipedia.org/wiki/Domain_Name_System

https://support.intermedia.com/app/articles/detail/a_id/24552/~how-do-i-use-the-nslookup-tool-provided-with-windows

Solución:

En la terminal de Windows lo busco con el comando nslookup seguido de la dirección

```
C:\Users\gonzalo>nslookup reyes.ccn-cert.cni.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: reyes.ccn-cert.cni.es
Address: [REDACTED]
```

Respuesta: [REDACTED]



Telnet

Telnet (6pts)



Telnet es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. El puerto que se utiliza generalmente es el 23. Debido a que las comunicaciones se realizan sin ningún tipo de cifrado, se considera un protocolo inseguro.

En la siguiente captura de tráfico un usuario se ha conectado remotamente a un servidor utilizando este protocolo. Para ello, ha tenido que autenticarse mediante usuario y contraseña. Para superar este reto, indica la contraseña utilizada.

Referencias:

<https://es.wikipedia.org/wiki/Telnet>
<https://en.wikipedia.org/wiki/Telnet>
<https://www.wireshark.org/>

Solución:

En Wireshark que nos da filtrado por `tcp.stream eq 0` seleccionamos cualquiera de los registros y le damos a seguir para que nos muestre la secuencia TCP y en el archivo que nos abre nos sale la contraseña



tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1254 → 23 [SYN] Seq=0
2	0.001690	192.168.0.1	192.168.0.2	TCP	74	23 → 1254 [SYN, ACK] Seq=1
3	0.001741	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=1
4	0.013173	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150283	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150351	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=28
7	0.150528					et Data ...
8	0.151908					1254 [ACK] Seq=4
9	0.153602					et Data ...
10	0.153816					et Data ...
11	0.154904					1254 [ACK] Seq=29
12	0.155418					et Data ...
13	0.155496					et Data ...
14	0.156474					1254 [ACK] Seq=47
15	0.158758					et Data ...
16	0.159498					1254 [ACK] Seq=71
17	0.160654					

.... .00 = Exp
Total Length: 53
Identification: 0x00000000
010. = Flags:
0... = Res:
.1... = Don:
.0... = Mor:
...0 0000 0000 0000
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x0000
[Header checksum : 0x0000]
Source Address: 192.168.0.2
Destination Address: 192.168.0.1
> Transmission Control
✓ Telnet
 Data: e

.....!...".'.....#..%..%.!...".'.....P..
.....".'.....#..&..\$.&..\$.#.#.
...DISPLAY.bam.zing.org:0.0.....xterm-color.....!
OpenBSD/i386 (oof) (tty1)

login: ..."....."ffaakkee
.
Password: [REDACTED]
.
Last login: Thu Dec 2 21:32:59 on ttym1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Len: 1

Respuesta: [REDACTED]



Básica: Telefonía Movil

Introducción

Introducción (1pts)



La adopción de los dispositivos y comunicaciones móviles, tanto en el ámbito personal como profesional, ha consolidado su nivel de madurez y estabilidad en la última década, en el que resulta difícil imaginar la realización de las actividades cotidianas sin hacer uso de estos.

Para superar este reto indica el nombre del sistema operativo para móviles más extendido en la actualidad (la primera letra en mayúsculas)

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6113-ccn-cert-ia-18-21-informe-anual-2020-dispositivos-moviles-1/file.html>

Solución:

Respuesta: [REDACTED]

[REDACTED]



Versiones

Versiones (1pts)

Google, creador del sistema operativo Android, le asocia un nombre interno a cada versión de este sistema operativo. Para superar este reto, indica el nombre interno asociado a la versión 7 de Android (por ejemplo: Chocolate Cake)

Referencias:

<https://developer.android.com/about/versions>

Solución:

Buscando en internet



Respuesta:



Nombre interno

Nombre interno (2pts)



Para superar este reto indica el número de la versión de Android correspondiente al nombre interno Snow Cone (por ejemplo: 5)

Solución:

Buscando en internet

[REDACTED] es Android Snow Cone

Respuesta: [REDACTED]
[REDACTED]



Permisos

Permisos (2pts)



Todas las aplicaciones para el sistema operativo Android requieren de un fichero XML en donde se definen, entre otras cosas, los permisos necesarios para ejecutar la aplicación. Indica el nombre de dicho fichero. (Por ejemplo: PermissionsAndroid.xml)

Referencias:

<https://developer.android.com/reference/android/Manifest.permission>

Solución:

Respuesta:



Código PIN

Código PIN (5pts)



La medida más básica de seguridad de acceso físico a nuestro dispositivo Android consiste en el establecimiento de un PIN de bloqueo. El hash de nuestro PIN se guarda dentro del siguiente fichero de nuestro móvil:

/data/system/password.key

Si quisieramos averiguar el PIN de un teléfono móvil necesitaríamos dicho fichero, junto con el SALT utilizado, el cual se puede consultar en la siguiente base de datos:

/data/system/locksettings.db

Mediante el siguiente comando:

SELECT value FROM locksettings WHERE name='lockscreen.password_salt'

Para superar este reto, deberás averiguar el PIN de un teléfono móvil del que conocemos lo siguiente:

Contenido del fichero /data/system/password.key

: 1136656D5C6718C1DEFC71B431B2CB5652A8AD550E20BDCF52B00002C8DF35C96
3B71298 Salt : 3582477098377895419

Referencias:

<https://github.com/georgenicolaou/androidlockcracker>

Solución:

Con Python abrimos el archivo escribimos crack pin y el fichero junto al salt

```
(kali㉿Gonzalo)-[~/Downloads/androidlockcracker-master]
$ python androidlockcracker.py crack pin 1136656D5C6718C1DEFC71B431B2CB5652A8AD550E20BDCF5
2B00002C8DF35C963B71298 3582477098377895419
Cracking ... (this might take a while)
Processing time: 0.0016 seconds
Password: [REDACTED]
```

Respuesta: [REDACTED]



Patrón de bloqueo

Patrón de bloqueo (5pts)



Otra medida básica de seguridad de acceso físico a nuestro dispositivo Android consiste en el establecimiento de un **PATRÓN** de bloqueo. El hash SHA1 de este patrón se guarda dentro del siguiente fichero de nuestro móvil:

/data/system/gesture.key

Para superar este reto, deberás averiguar el patrón de desbloqueo de un teléfono móvil del que conocemos lo siguiente:

Contenido del fichero /data/system/gesture.key
: **82790AD0ADEB07AC2A78AC07038BC93A26691F12**

Nota: la solución consiste en todos los números seguidos (por ejemplo: 56712)

Referencias:

<https://github.com/georgenicolaou/androidlockcracker>

Solución:

Como en el anterior abrimos con Python el archivo escribimos y escribimos en este caso crack gesture y el fichero junto al salt

```
(kali㉿Gonzalo)-[~/Downloads/androidlockcracker-master]$ python androidlockcracker.py crack gesture 82790AD0ADEB07AC2A78AC07038BC93A26691F12 3582  
477098377895419  
Cracking ... (this might take a while)  
Processing time: 0.8238 seconds  
Password: [REDACTED]
```

Respuesta: [REDACTED]
[REDACTED]



Permisos 2

Permisos 2 (5pts)



Como has visto anteriormente, todas las aplicaciones para el sistema operativo Android requieren de un fichero XML llamado AndroidManifest.xml en donde se definen, entre otras cosas, los permisos necesarios para ejecutar la aplicación. Es bastante habitual encontrarse con aplicaciones que solicitan más permisos de los que deberían (por ejemplo, el acceso a nuestros contactos solicitado por una aplicación cuya funcionalidad es la de hacer de linterna con el flash del móvil)

Para superar este reto, indica el permiso que está definido en el fichero AndroidManifest.xml adjunto que parezca más sospechoso teniendo en cuenta que el fichero es de una aplicación para móvil que muestra el tiempo metereológico.

NOTA: la solución deberá ponerse en mayúsculas. Por ejemplo, READ_CONTACTS

Referencias:

<https://developer.android.com/reference/android/Manifest.permission>

Solución:

Abriendo el AndroidManifest.xml salen todos y para una aplicación meteorológica no se necesita la camara

```
<uses-permission android:name="android.permission.CAMERA" />
```

Respuesta: [REDACTED]



Permisos 3

Permisos 3 (20pts)



Android fue diseñado con el lenguaje de programación Java, por lo que durante mucho tiempo este ha sido el lenguaje de programación por defecto para el desarrollo de aplicaciones en este sistema operativo. En cuanto a seguridad, hay que tener en cuenta que las aplicaciones programadas en este lenguaje pueden ser descompiladas fácilmente.

Para superar este reto, deberás descompilar el fichero APK adjunto y leer el fichero AndroidManifest.xml para indicar cuál de los siguientes permisos NO está definido en la aplicación adjunta:

BLUETOOTH
BIND_WALLPAPER
CALL_PHONE
CALL_PRIVILEGED
CAMERA
CAPTURE_AUDIO_OUTPUT
INTERNET
NFC
READ_CALENDAR
READ_CONTACTS
READ_SMS
REBOOT
RECORD_AUDIO
SEND_SMS
USE_BIOMETRIC

Referencias:

<https://developer.android.com/reference/android/Manifest.permission>

<https://ibotpeaches.github.io/Apktool/install/>

<https://ibotpeaches.github.io/Apktool/documentation/>

Solución:

Abriendo el archivo en android studio y examinando el .xml



```
<uses-permission
    android:name="android.permission.READ_CONTACTS" />

<uses-permission
    android:name="android.permission.READ_SMS" />

<uses-permission
    android:name="android.permission.REBOOT" />

<uses-permission
    android:name="android.permission.SEND_SMS" />

<uses-permission
    android:name="android.permission.USE_BIOMETRIC" />
```

Respuesta:



Credenciales

Credenciales (25pts)



En la siguiente aplicación para Android aparece un formulario de inicio de sesión donde se solicita un usuario y una contraseña. Para superar este reto deberás obtener un usuario válido.

Referencias:

<https://ibotpeaches.github.io/Apktool/install/>
<https://ibotpeaches.github.io/Apktool/documentation/>
<https://sourceforge.net/projects/dex2jar/>

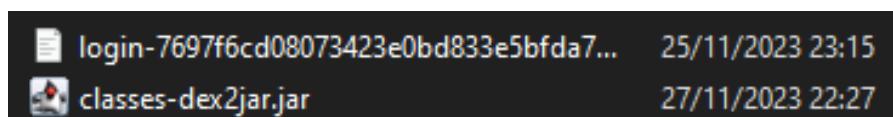
Solución:

Primero descargo los programas necesarios que son dex2jar y jd-gui

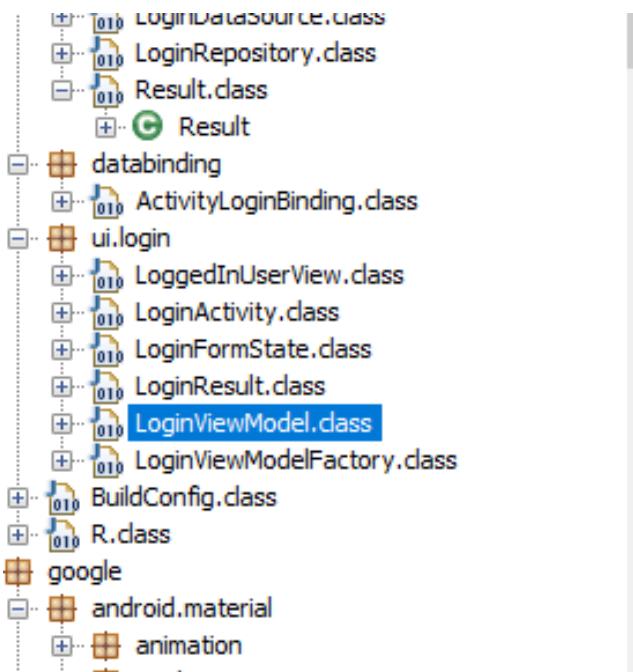


El programa dex2jar servirá para convertir el archivo .apk en un .jar

```
C:\Program Files\dex2jar>d2j-dex2jar.bat classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
Detail Error Information in File .\classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.
```



Y el jd-gui servirá para que de forma gráfica podamos investigar los archivos en busca del usuario y la contraseña. Lo encontré en el archivo LoginViewModel.class



```
public void login(String paramString1, String paramString2) {  
    boolean bool;  
    paramString2 = getMd5(paramString2);  
    if (paramString1.equals("████████████████████████████████████████")) &&  
        paramString2.equals("████████████████████████████████████████")) {
```

Respuesta:



Credenciales 2

Credenciales 2 (30pts)



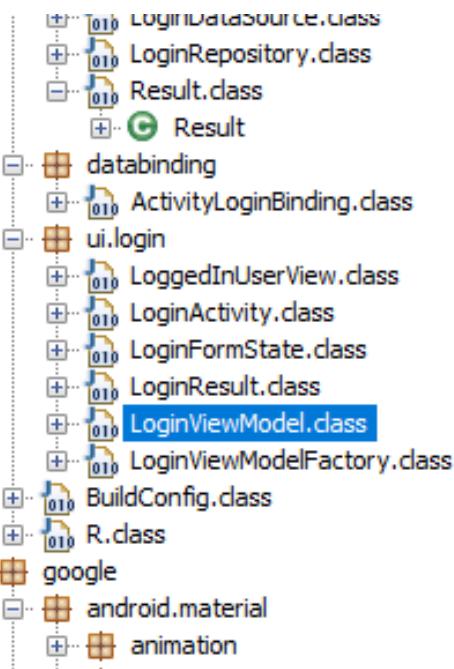
Continuando con el análisis de la aplicación para Android anterior, para superar este reto deberás encontrar la contraseña de acceso.

Referencias:

<https://ibotpeaches.github.io/Apktool/install/>
<https://ibotpeaches.github.io/Apktool/documentation/>
<https://sourceforge.net/projects/dex2jar/>

Solución:

Este es una adición del anterior en el que hay que poner la contraseña que ya antes salía



```
public void login(String paramString1, String paramString2) {  
    boolean bool;  
    paramString2 = getMd5(paramString2);  
    if (paramString1.equals(██████████)) && |  
        paramString2.equals("██████████")) {
```



Lo único que habría que hacer es desencriptar el md5 en el que esta para sacar la contraseña

The screenshot shows two side-by-side web pages. On the left, the 'dCode' search interface displays results for 'MD5'. It includes a search bar, a browse tools link, and a list of results with 'MD5' highlighted. On the right, a 'DESCIFRADO MD5' (MD5 Decryption) page is shown. It features a hash input field containing a redacted MD5 value, several decryption options (SAL PREFIX MD5, SAL SUFFIX MD5), and a large green 'DESCIFRAR' (Decrypt) button.

Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'boolean'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

MD5

MD5 - [dCode](#)
Tag(s) : Hashing Function, Modern Cryptography

DESCIFRADO MD5

★ HASH MD5 [REDACTED]

Opciones

★ SAL PREFIX MD5 (PALABRA SAL) [REDACTED]

★ SAL CON EL SUFIJO MD5 (PALABRA SAL) [REDACTED]

► DESCIFRAR

Ver también : Hash Function – SHA-1 – Crypt() Hashing Function

CIFRADO MD5

● DE UNA CADENA DE CARACTERES

Respuesta:



Básica: Correo electrónico

Phishing

Phishing (1pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El primer punto en el que tenemos que prestar atención es la dirección de correo electrónico del remitente, ya que existen varias técnicas que persiguen hacer creer que un correo electrónico proviene de una fuente legítima y confiable, cuando en realidad no lo es.

La más simple consiste en mandar un correo en el que el nombre del remitente parezca confiable.

Para superar este reto, indica el e-mail del remitente del correo adjunto.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

Solución:

Viéndolo con OutLook

Action de sécurité requise

Facebook < [REDACTED] >
To pierrenouveans@gmail.com

(i) Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Respuesta: [REDACTED]

[REDACTED]



Phishing 2

Phishing 2 (1pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El primer punto en el que tenemos que prestar atención es la dirección de correo electrónico del remitente, ya que existen varias técnicas que persiguen hacer creer que un correo electrónico proviene de una fuente legítima y confiable, cuando en realidad no lo es.

Una variación de la técnica anterior consiste en mandar un correo en el que el nombre del remitente sea el e-mail de una cuenta de correo confiable.

Para superar este reto, indica el e-mail del remitente del correo adjunto.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Viendolo con OutLook

Action de sécurité requise

security@facebook.com <[REDACTED]>
To pierrenouveans@gmail.com

ⓘ Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Respuesta: [REDACTED]

[REDACTED]



Phishing 3

Phishing 3 (1pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El primer punto en el que tenemos que prestar atención es la dirección de correo electrónico del remitente, ya que existen varias técnicas que persiguen hacer creer que un correo electrónico proviene de una fuente legítima y confiable, cuando en realidad no lo es.

Otra técnica muy común consiste en mandar el correo desde una cuenta de correo similar a un servicio legítimo.

Para superar este reto, indica el dominio registrado por el atacante para mandar el correo adjunto (se pide sólo el dominio. Por ejemplo: gmail.com)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Viendolo con OutLook

Password changed

To victim@gmail.com

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Respuesta: [REDACTED]

[REDACTED]



Phishing 4

Phishing 4 (2pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El primer punto en el que tenemos que prestar atención es la dirección de correo electrónico del remitente, ya que existen varias técnicas que persiguen hacer creer que un correo electrónico proviene de una fuente legítima y confiable, cuando en realidad no lo es.

Otra técnica utilizada consiste en mandar un correo desde una cuenta de correo legítima, pero poniendo en la cabecera "Reply-To" una cuenta controlada por el atacante. De esta manera, cuando se clique en responder al correo electrónico, la aplicación de correo electrónico, por defecto, pondrá como destinatario el e-mail que aparece en la cabecera "Reply-To" y no el de la cabecera "From".

En el correo adjunto, un empleado de la empresa Capsule Corp. recibe un correo electrónico que parece provenir de su jefe. Para superar este reto, indica el correo electrónico que aparecería al darle a responder al mensaje.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

Solución:

Viéndolo con OutLook



Respuesta: [REDACTED]



Phishing 5

Phishing 5 (3pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El segundo punto en el que tenemos que prestar atención es si el cuerpo del correo electrónico incluye algún enlace a una web externa. La utilización de HTML para la construcción de mensajes de correo electrónico permite la creación de enlaces mediante la etiqueta <A HREF>. Para construir el enlace, hace falta el texto donde se clickará para acceder al enlace y la URL de la web a la que se desea acceder. Por ejemplo:

Access to Google

En el correo adjunto, el atacante, insta a clickar sobre un enlace. Para superar este reto, indica la URL a la que se accedería al clickar sobre el enlace indicado en el e-mail (por ejemplo: https://website.com)

Referencias:

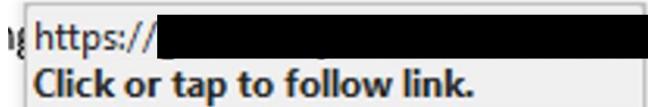
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Con el ratón por encima se puede ver el verdadero link



Respuesta: [REDACTED]



Phishing 6

Phishing 6 (3pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El segundo punto en el que tenemos que prestar atención es si el cuerpo del correo electrónico incluye algún enlace a una web externa. La utilización de HTML para la construcción de mensajes de correo electrónico permite la creación de enlaces mediante la etiqueta <A HREF>. Para construir el enlace, hace falta el texto donde se clickará para acceder al enlace y la URL de la web a la que se desea acceder. Por ejemplo:

Access to Google

El atacante puede haber mejorado su técnica anterior, incluyendo un acortado de URL en el enlace dañino, de manera que podría pasar inadvertido por las medidas de seguridad de la empresa objetivo.

Para superar este reto, indica la URL a la que se accedería al clickar sobre el acortador utilizado por el atacante en el correo de phishing (por ejemplo: https://website.com)

NOTA IMPORTANTE: nunca se debe clickar sobre un acortador de URL si no tiene la certeza absoluta de que es totalmente fiable. Existen servicios en Internet que te permiten mostrar una previsualización de la web destino antes de acceder a la misma.

Referencias:

<https://safecomputing.umich.edu/be-aware/phishing-and-suspicious-email/shortened-url-security>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Abriendo el html del correo sale el href del enlace, pero lo paso por un comprobador de URLs para confirmarlo



```
<p><a href="https://www.thebank.com/security/changepassword">https://www.thebank.com/security/changepassword</a></p>
<br>Thank you for your cooperation <br>
```

URL X-ray

Find out where shortened URLs lead to without clicking

<http://>



<https://>

Respuesta: [REDACTED]



Phishing 7

Phishing 7 (4pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El método clásico utilizado por los atacantes es incluir un fichero ejecutable (.exe) como adjunto a un correo. Para superar este reto deberás ejecutar el fichero adjunto en una máquina virtual (recuerda que ejecutar ficheros .exe de dudoso origen en tu equipo supone un grave riesgo para tu organización)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

<https://www.vmware.com/>

<https://www.virtualbox.org/>

Solución:

Abriendo el archivo con un lector de eml en una máquina virtual Windows 10 y ejecutándolo sale el siguiente mensaje



changePassword



Alert

X



Enhorabuena, has ejecutado este binario en un entorno seguro.

El flag para superar este reto es: [REDACTED]

Congratulations, you have run this binary in a secure environment.

The flag for this challenge is: [REDACTED]

Félicitations, vous avez exécuté ce binaire dans un environnement sûr.

Le flag pour surmonter ce défi est : [REDACTED]

Aceptar

Respuesta:

[REDACTED]



Phishing 8

Phishing 8 (4pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El método clásico utilizado por los atacantes es incluir un fichero ejecutable (.exe) como adjunto a un correo. Para mejorar la técnica de engaño, el atacante puede cambiar el icono del ejecutable para hacerlo pasar por un documento. Para superar este reto deberás abrir el fichero adjunto en una máquina virtual (recuerda que abrir ficheros de dudoso origen en tu equipo supone un grave riesgo para tu organización)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Abriendo el archivo con un lector de eml en una máquina virtual Windows 10 y ejecutándolo sale el siguiente mensaje

1599px-NATO_OTAN_landscape_logo.svg
 TopSecret



Alert

X



Enhorabuena, has ejecutado este binario en un entorno seguro.

El flag para superar este reto es: [REDACTED]

Congratulations, you have run this binary in a secure environment.

The flag for this challenge is: [REDACTED]

Félicitations, vous avez exécuté ce binaire dans un environnement sûr.

Le flag pour surmonter ce défi est : [REDACTED]

Aceptar

Respuesta: [REDACTED]
[REDACTED]



Phishing 9

Phishing 9 (4pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El método clásico utilizado por los atacantes es incluir un fichero ejecutable (.exe) como adjunto a un correo. Debido a que hoy en día cualquier solución antispam dispone de mecanismos para bloquear estos correos, el atacante puede mejorar la técnica utilizada y comprimir el fichero ejecutable en un fichero .zip para que el antivirus y filtros antispam de la víctima no pueda analizarlo. Para superar este reto deberás abrir el fichero adjunto en una máquina virtual (recuerda que abrir ficheros de dudoso origen en tu equipo supone un grave riesgo para tu organización)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>
<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>
<https://www.vmware.com/>
<https://www.virtualbox.org/>

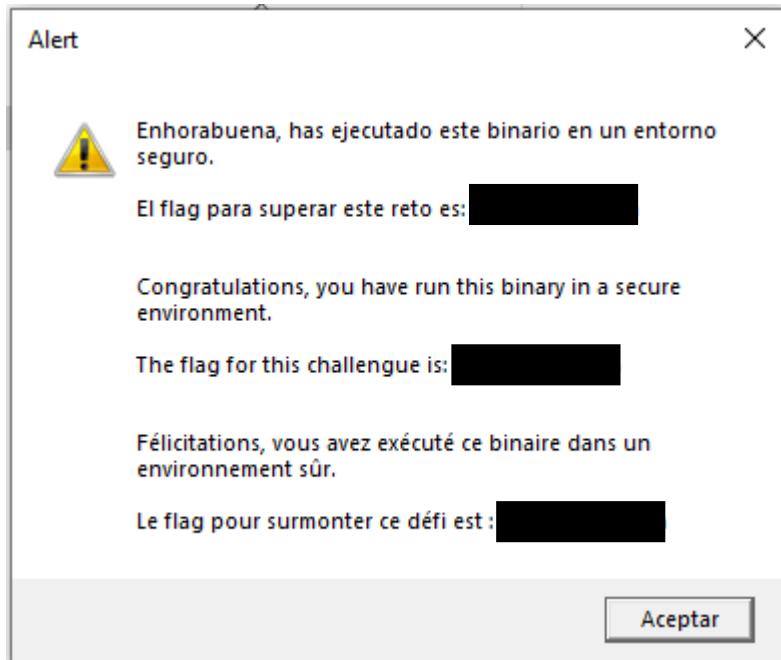
Solución:

Descargo el archivo

1599px-NATO_OTAN_landscape_logo.svg
documentation

Dentro de la carpeta zip

Agenda21.pdf
Information.exe
nato security briefing.pdf
RocketScience.pdf



Respuesta: [REDACTED]
[REDACTED]



Phishing 10

Phishing 10 (5pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

El método clásico utilizado por los atacantes es incluir un fichero ejecutable (.exe) como adjunto a un correo. Debido a que hoy en día cualquier solución antispam dispone de mecanismos para bloquear estos correos, el atacante puede mejorar la técnica utilizada y comprimir el fichero ejecutable en un fichero .zip para que el antivirus y filtros antispam de la víctima no pueda analizarlo. No obstante, debido a que hay soluciones de seguridad que descomprimen los ficheros comprimidos y analizan su contenido, el atacante ha decidido mandar un fichero comprimido con contraseña para saltarse estas restricciones. Para superar este reto deberás abrir el fichero adjunto en una máquina virtual (recuerda que abrir ficheros de dudoso origen en tu equipo supone un grave riesgo para tu organización)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

<https://www.vmware.com/>

<https://www.virtualbox.org/>

Solución:

Descargamos el archivo

1599px-NATO_OTAN_landscape_logo.svg.png
 restricted.zip

Se pone en el zip la contraseña: [REDACTED] se ejecuta el exe



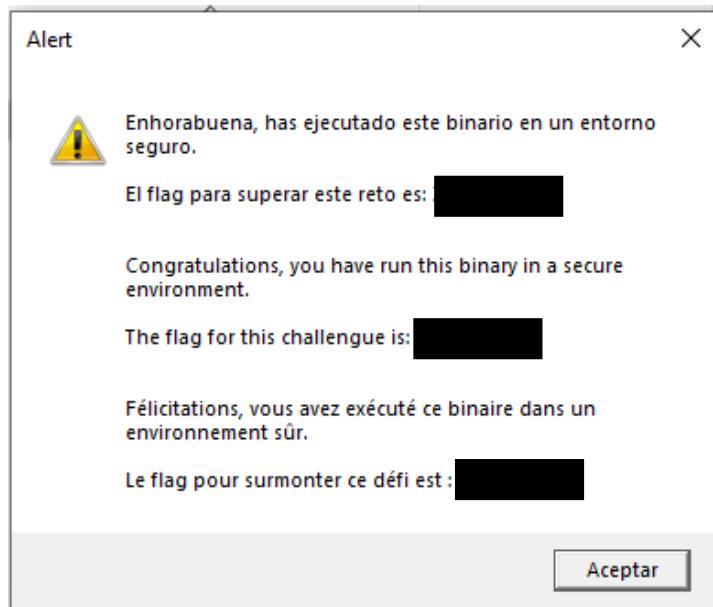
Agenda21.pdf

ImportantInformation.exe

nato security briefing.pdf

RocketScience.pdf

Y se ejecuta como el anterior



Respuesta: [REDACTED]



Carácter RLO

Carácter RLO (6pts)

El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

Otra de las técnicas utilizadas por los atacantes para ocultar la verdadera extensión del ejecutable dañino es la utilización del carácter RLO.

Para superar este reto, indica el nombre del fichero (sin la extensión) que hace uso de esta técnica (por ejemplo: A Long Tale)

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Buscando por .exe en el mismo buscador de Windows la saque



Respuesta: [REDACTED]



Macro

Macro (6pts)



El correo electrónico es la principal vía de infección utilizada por ciberdelincuentes de todo tipo para comprometer una red. Dependiendo de la capacitación técnica de los atacantes, será más o menos difícil detectar un correo electrónico dañino.

Una de las técnicas más comunes utilizadas últimamente son las macros dentro de documentos ofimáticos.

Para superar este reto deberás ver el código fuente de la macro del documento adjunto.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

Solución:

Abriendo el programa en forma desarrollador sale en VBA

```
Sub Macrol()
'
' Macrol Macro
'
' Flag for this challenge:
' El flag para este reto e
' Le flag de ce défi est:
'
End Sub
```

Respuesta: [REDACTED]



Compromiso de correo electrónico

Compromiso de correo electrónico (7pts)



La reutilización de contraseñas es una mala práctica, la cual es aprovechada por los atacantes para conseguir acceso, por ejemplo, a las cuentas de correo. Hay servicios en Internet que almacenan las contraseñas de e-mail robadas y te permite consultar si tu cuenta de correo ha sido comprometida.

Para superar este reto deberás indicar qué cuenta de correo ha sido comprometida de las que se adjuntan.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

<https://haveibeenpwned.com/>

Solución:

Con la web de las referencias te dice cuál ha sido comprometida

The screenshot shows a search result for an email address. At the top, there is a large black redacted area and a button labeled "pwned?". Below this, the text "Oh no — pwned!" is displayed in white on a dark background. Underneath, it says "Pwned in 67 data breaches and found 6 pastes (subscribe to search sensitive breaches)". At the bottom, there are social media sharing icons (Facebook, Twitter, LinkedIn, Pinterest) and a "Donate" button.

Respuesta: [REDACTED]



Compromiso de correo electrónico 2

Compromiso de correo electrónico 2 (7pts)



La reutilización de contraseñas es una mala práctica, la cual es aprovechada por los atacantes para conseguir acceso, por ejemplo, a las cuentas de correo. Hay servicios en Internet que almacenan las contraseñas de e-mail robadas y te permite consultar si tu cuenta de correo ha sido comprometida.

Para superar este reto deberás indicar en cuántos leaks aparece la cuenta de correo verdi@gmail.com (por ejemplo: 8).

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

<https://haveibeenpwned.com/>

Solución:

Como en el anterior buscamos en la página que nos proporcionan

Oh no — pwned!
Pwned in 16 data breaches and found no pastes (subscribe to search sensitive breaches)

Respuesta: [REDACTED]



Compromiso de correo electrónico 3

Compromiso de correo electrónico 3 (25pts)



La reutilización de contraseñas es una mala práctica, la cual es aprovechada por los atacantes para conseguir acceso, por ejemplo, a las cuentas de correo. Hay servicios en Internet que almacenan las contraseñas de e-mail robadas y te permite consultar si tu cuenta de correo ha sido comprometida.

Para superar este reto, descárgate el leak Collection #1 y encuentra la contraseña asociada a la cuenta de correo comprometida del reto anterior que está formada por dos letras y varios números.

Referencias:

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5939-ccn-cert-bp-02-courrier-electronique/file.html>

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-buenas-practicas-bp/5936-ccn-cert-bp-02-e-mail-address/file.html>

<https://haveibeenpwned.com/>

Solución:

Accediendo a este repositorio nos sale el link para en UTorrent poder descargarlo.

<https://gist.github.com/fawazahmed0/79764af8a026a9a5b380728e67f786d4>

Collection 1

31 Files, 36.26 GB (57.39 GB available on your hard drive)

Peers: 46 | Seeds: 21

Name	Size
Collection #1_BTC combos.tar.gz	338 MB
Collection #1_Dumps - dehashed.tar.gz	82 MB
Collection #1_EU combos.tar.gz	3 GB
Collection #1_EU combos_1tar.gz	2 GB
Collection #1_Games combos.tar.gz	1 GB

Download this torrent to:

C:\Users\Equipo\Downloads

Start downloading when torrent is added

Don't show this dialog next time I add a torrent



Una vez descargado lo abrimos con el buscador Astro Grep

● C:\Users\gonza\Documents\Collection1\Collection #1_EU combos - AstroGrep

Archivo Edición Ver Herramientas Ayuda

Búsqueda con AstroGrep

Ruta de búsqueda
C:\Users\gonza\Documents\Collection1\Collection #1_EU combos

Tipos de archivo
.txt

Texto de la búsqueda
verdi@gmail.com

Búsqueda Cancelar

Opciones de búsqueda

Nombre	Localizado en	Extensión
1571.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1586.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1592.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1615.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1715.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1716.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1717.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1719.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1721.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt
1724.txt	C:\Users\gonza\Documents\Collection1\Collection #1_EU combos	.txt

Líneas adyacetes 2

verdi@gmail.com:p1314361497

Respuesta:

[REDACTED]

[REDACTED]



Básica: Web

Tag HTML

Tag HTML (1pts)



Para superar este reto, deberás indicar cuál es el tag que se utiliza en HTML para establecer el título de una página web. (Deberás poner la solución en mayúsculas, por ejemplo: DATA)

Referencias:

<https://www.w3schools.com/TAGS/default.ASP>

Solución:

Respuesta: [REDACTED]

[REDACTED]



Servidor Web

Servidor web (2pts)



El fichero adjunto contiene el tráfico intercambiado contra un servidor web. Identifica de qué servidor web se trata (por ejemplo: Apache/1.2.7)

Referencias:

<https://www.wireshark.org/>

<http://www.steves-internet-guide.com/http-basics/>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers>

Solución:

Examinándolo con Wireshark y buscandolo en el HTTP salen las especificaciones de la conexión

```
2 0.002079      172.16.33.129      172.16.33.129      HTTP      5387 HTTP/1.1 200 OK  (text/html)

> Internet Protocol Version 4, Src: 172.16.33.129, Dst: 172.16.33.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 5387
└─ Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
        Date: Mon, 01 Nov 2021 08:54:46 GMT\r\n
        Server: [REDACTED]
        Last-Modified: Tue, 04 Dec 2018 03:05:48 GMT\r\n
```

Respuesta: [REDACTED]



Servidor Web 2

Servidor web 2 (2pts)



Indica el navegador que se ha usado para realizar la navegación al servidor web (por ejemplo: Chrome/95.0)

Referencias:

<https://www.wireshark.org/>

<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/User-Agent>

<https://developers.whatismybrowser.com/useragents/parse/>

Solución:

Buscando igual que en el anterior con Wireshark

```
Host: 172.16.33.129\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) [REDACTED]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
```

Respuesta: [REDACTED]



Pais de origen

País de origen (3pts)



A partir de la captura de tráfico adjunta, deduce cuál es el idioma que habla la persona que está realizando la navegación web. La solución a este reto es el país donde más se habla dicho idioma (introduce el país con la primera letra en mayúsculas y en inglés. Por ejemplo: Spain)

Referencias:

<https://www.wireshark.org/>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Accept-Language>

https://docs.oracle.com/cd/E13214_01/wli/docs92/xref/xqisocodes.html

Solución:

Buscando el lenguaje en el que esta el teclado y después comprobándolo por internet

```
Accept: text/html,application/xhtml+xml
Accept-Language: [REDACTED]
Accept-Encoding: gzip, deflate\r\n
```

Respuesta: [REDACTED]



Código HTTP

Código HTTP (4pts)



Indica cuál es el código devuelto por el servidor web cuando el usuario intenta acceder al recurso unknown.jpg (por ejemplo: 501)

Referencias:

<https://www.wireshark.org/>

<https://www.restapitutorial.com/httpstatuscodes.html>

Solución:

Buscando igual que en el anterior con Wireshark en el archivo que dice que no se ha encontrado

104 37.185707	172.16.33.129	172.16.33.129	HTTP	413 GET /unknown.jpg HTTP/1
105 37.186174	172.16.33.129	172.16.33.129	HTTP	550 HTTP/1.1 404 Not Found
106 61.344460	172.16.33.129	172.16.33.129	HTTP	376 GET /img/gallery-img-03
107 61.345253	172.16.33.129	172.16.33.129	TCP	32836 80 → 59932 [ACK] Seq=1
[Header checksum status: Unverified]				
Source Address: 172.16.33.129				
Destination Address: 172.16.33.129				
Transmission Control Protocol, Src Port: 80, Dst Port: 59928, Seq: 1, Ack: 346, Len: 482				
Hypertext Transfer Protocol				
▼ HTTP/1.1				

Respuesta: [REDACTED]



Cookies

Cookie (5pts)



Identifica el nombre de la cookie que se está utilizando en la captura de tráfico adjunta.

Referencias:

<https://www.wireshark.org/>

<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/Cookie>

Solución:

Buscando igual que en el anterior con Wireshark y filtrando por las coockies sale el nombre

```
http.cookie
No. Time Source Destination Protocol
71 3.339201 172.16.33.129 172.16.33.129 HTTP

Frame 71: 297 bytes on wire (2376 bits), 297 bytes captured (2376 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.16.33.129, Dst: 172.16.33.129
Transmission Control Protocol, Src Port: 60348, Dst Port: 80, Seq: 1, Ack: 1, Len: 297
Hypertext Transfer Protocol
  GET /index.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /index.html HTTP/1.1\r\n]
      [GET /index.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /index.html
      Request Version: HTTP/1.1
      Host: 172.16.33.129\r\n
      Accept: */*\r\n
  Cookie:
    Cooki
```

Respuesta: [REDACTED]



Certificado SSL

Certificado SSL (6pts)

Indica el valor del campo organización del certificado de la web de Google:

<http://www.google.com>

Referencias:

<https://www.google.com>

<https://www.venafi.com/education-center/ssl/how-to-check-ssl-certificate>

<https://securitytrails.com/blog/extract-ssl-data>

Solución:

Buscando por internet

Emitido por

Nombre común (CN)

GTS CA 1C3

Organización (O)

[REDACTED]

Unidad organizativa (OU)

<No incluido en el certificado>

Respuesta: [REDACTED]
[REDACTED]



Ruta

Ruta (6pts)



Encuentra la ruta completa donde se encuentra la hoja de estilos custom.css de la web:

<https://www.ccn-cert.cni.es>

Referencias:

<https://www.ccn-cert.cni.es>

<https://www.dummies.com/web-design-development/site-development/how-to-view-source-code-on-a-web-page/>

https://www.w3schools.com/html/html_css.asp

Solución:

Buscando en las carpetas de la fuente con el inspector

The screenshot shows the Chrome DevTools Sources tab. On the left, there's a tree view of files under 'custom.css'. The 'css' folder contains 'joomla-fontawesome.css'. The 'js' folder contains 'core.min.js?576eb51'. The 'custom.css' file itself is selected and shown on the right. Its content is as follows:

```
#astroid-header a{  
    color: #303030;  
    font-size: 1rem  
}  
  
.buscador.visible{  
    margin-top: 0px !important;  
}  
  
.buscadoricon{  
    cursor: pointer;  
    margin-left: 10px;  
}  
  
#language_btn_132,.buscadorcontainer{  
    background: #ff0000;  
    color: #0f70b3;  
    border-radius: 2px;  
    border-color: #0f70b3;  

```

Respuesta: [REDACTED]



JavaScript

JavaScript (7pts)



Indica el resultado tras ejecutar el siguiente código JavaScript:

```
<html>
<body>
<script>
    var contador;
    var result = 0;
    for (contador = 1; contador <= 10; contador++)
    {
        if (contador % 5 == 0)
            result += contador;
    }
    document.write(result);
</script>
</body>
</html>
```

Referencias:

<https://developer.mozilla.org/en-US/docs/Web/JavaScript>
<https://onecompiler.com/javascript/>

Solución:

Ejecutandolo en un compilador de código HTML ya que esta entre comillas html y sale la respuesta

Respuesta: [REDACTED]



PHP

PHP (7pts)



PHP es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. En lugar de usar muchos comandos para mostrar HTML (como en C o en Perl), las páginas de PHP consisten en HTML con código incrustado, encerrado entre las etiquetas especiales de comienzo y final <?php y ?>.

Lo que distingue a PHP de algo del lado del cliente como Javascript es que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente.

Indica el resultado de ejecutar el siguiente código PHP:

```
<?php
for ($num=5; $num<=11; $num++)
{
}
echo $num;
?>
```

Referencias:

<https://en.wikipedia.org/wiki/PHP>
<https://sandbox.onlinephpfunctions.com/>
<https://onecompiler.com/php>

Solución:

Ejecutandolo en un compilador de código HTML ya que esta entre comillas html y sale la respuesta

Respuesta: [REDACTED]



XSS

XSS (10pts)



El Cross Site Scripting o XSS es un tipo de ataque por el cual se buscan vulnerabilidades en una aplicación web para introducir un script dañino y atacar sus visitantes. En su versión más inocua abre ventanas emergentes y en el peor de los casos son utilizados por atacantes para acceder a información sensible o comprometer el equipo del usuario.

Para superar este reto, provoca un ataque de XSS en el siguiente servidor web:

<http://85.159.210.133/xss1/>

Referencias:

<https://medium.com/spidernitt/xss-for-dummies-eeb1a4133e52>
https://www.owasp.org/index.php/Testing_for_Cross_site_scripting
[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

Solución:

Para ello escribo en el buscador el script: <script>alert("hacked")</script> y lo busco y saldrá un alert con el flag



<script>alert("hacked")</script>

85.159.210.133 dice

Felicidades, has injectado una ventana emergente:

hacked

El flag que necesitas es: [REDACTED]

Respuesta: [REDACTED]



Básica: Ransomware

Detección de ransomware

Detección de ransomware (1pts)



El antivirus de nuestra organización ha detectado un ransomware en un equipo y lo ha detenido. En el informe del antivirus, entre otras cosas, aparece el hash MD5 correspondiente al malware:

07fad006486953439ce0092651fd7a6

Para superar este reto, indica el nombre de la familia de ransomware responsable del incidente (todo en minúsculas)

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5966-ccn-cert-bp-04-ransomware-en-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5969-ccn-cert-bp-04-ransomware-fr-1/file.html>

Respuesta:

Ransomware Sample Download Signatures

Family: Win32:Malware-gen

MD5: 07fad006486953439ce0092651fd7a6

SHA256: d77378dcc42b912e514d3bd4466cdda050dda9b57799a6c97f70e8489dd8c8d0

Respuesta: [REDACTED]



Identificación de la familia de ransomware

Identificación de la familia de ransomware (2pts)

Si hemos sido víctimas de un ataque de ransomware el primer paso consiste en identificar la familia a la que pertenece dicho malware. Una vez identificada es posible realizar una búsqueda sobre los detalles y comportamiento de dicho código dañino, pudiendo obtener información valiosa, como conocer si existe o no una herramienta de descifrado y recuperación de ficheros.

El fichero adjunto incluye la nota de rescate creada por un ransomware tras infectar un equipo, junto con uno de los ficheros cifrados. Para superar este reto deberás identificar el nombre de dicho malware (todo en minúsculas)

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html>

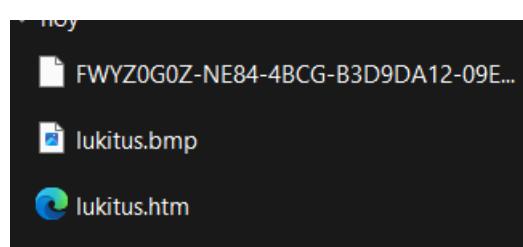
<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5966-ccn-cert-bp-04-ransomware-en-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5969-ccn-cert-bp-04-ransomware-fr-1/file.html>

<https://id-ransomware.malwarehunterteam.com/>

Respuesta:

Descargamos el .zip, lo descomprimimos y nos aparecerá una foto la cual subiremos a este enlace que nos proporcionan <https://id-ransomware.malwarehunterteam.com/>



Y nos dará el siguiente resultado donde nos dice el nombre del ransomware



1 Result



Este ransomware no tiene ninguna forma conocida para descifrar los datos en este momento.

Se recomienda hacer una copia de seguridad de sus archivos cifrados, con la esperanza de una solución a futuro.

Identificado por

- **ransomnote_filename:** lukitus.bmp

Haga clic aquí para obtener más información acerca de [REDACTED]

🔔 Would you like to be notified if there is any development regarding this ransomware? [Click here.](#)

Respuesta: [REDACTED]
[REDACTED]



Recuperación de los datos

Recuperación de los datos (3pts)



Dependiendo de la familia de ransomware, es posible recuperar los datos cifrados mediante alguna herramienta. Desgraciadamente en la mayoría de los casos esto no es posible y la única solución posible es restaurar el equipo a partir de un backup.

Para superar este reto, indica cuál de las siguientes familias de ransomware NO dispone de una herramienta para el descifrado de ficheros:

Avaddon
Babuk
Bitcryptor
Coinvault
Dharma
Eking
Hakbit
Hive
Jigsaw
Lortok
Nemucod
Pylocky
Ragnarok
Sodinokibi

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5966-ccn-cert-bp-04-ransomware-en-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5969-ccn-cert-bp-04-ransomware-fr-1/file.html>

<https://www.nomoreransom.org/en/decryption-tools.html>

Respuesta:

Buscando en la página que nos proporcionan:

<https://www.nomoreransom.org/en/decryption-tools.html>

Vemos que la única que no aparece es



[TO TOP](#)

Respuesta:



Recuperación de los datos 2

Recuperación de los datos 2 (3pts)



Dependiendo de la familia de ransomware, es posible recuperar los datos cifrados mediante alguna herramienta. Desgraciadamente en la mayoría de los casos esto no es posible y la única solución posible es restaurar el equipo a partir de un backup.

Windows dispone de una utilidad que permite restaurar el equipo a un estado anterior, denominada Shadow Copies, (para, por ejemplo, restaurar el equipo al momento antes de ser infectado por el malware). Algunos atacantes, conocedores de esta característica, suelen programar el ransomware para que inhabilite este sistema de backup.

Para superar este reto, introduce el binario de Windows encargado de gestionar las Shadow Copies (todo en minúsculas, por ejemplo: shadowcopies.exe).

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5966-ccn-cert-bp-04-ransomware-en-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5969-ccn-cert-bp-04-ransomware-fr-1/file.html>

Respuesta:

Buscando en internet encontré que es vssadmin.exe



Nombre de proceso: Command Line Interface for Microsoft® Volume Shadow Copy Service

Respuesta: [REDACTED]



Recuperación de los datos 3

Recuperación de los datos 3 (5pts)



Dependiendo de la familia de ransomware, es posible recuperar los datos cifrados mediante alguna herramienta.

En el fichero adjunto se incluye la nota de rescate del ransomware junto con un fichero cifrado tras la infección de un equipo. La solución a este reto está dentro del fichero cifrado.

Referencias:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5966-ccn-cert-bp-04-ransomware-en-1/file.html>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5969-ccn-cert-bp-04-ransomware-fr-1/file.html>

<https://id-ransomware.malwarehunterteam.com/>

<https://www.nomoreransom.org/en/decryption-tools.html>

Respuesta:

Desencriptamos el zip y subimos el archivo a la página que nos dan en las referencias y nos dice información sobre el

1 Result

GandCrab v4.0 / v5.0

✓ Este ransomware es descriptable!

Identificado por

- sample_bytes: [0x224 - 0x22C] 0x1829899381820300

Haga clic aquí para obtener más información acerca de GandCrab v4.0 / v5.0

Buscamos en la página del ejercicio de Recuperación de datos 1 y nos sale un .exe para desencriptar el archivo.



GandCrab (V1, V4 and V5 up to V5.2 versions) Ransom

BDGandCrabDecryptTool Decryptor is designed to decrypt files encrypted by GandCrab (V1, V4 and V5 up to V5.2 versions) Ransom.

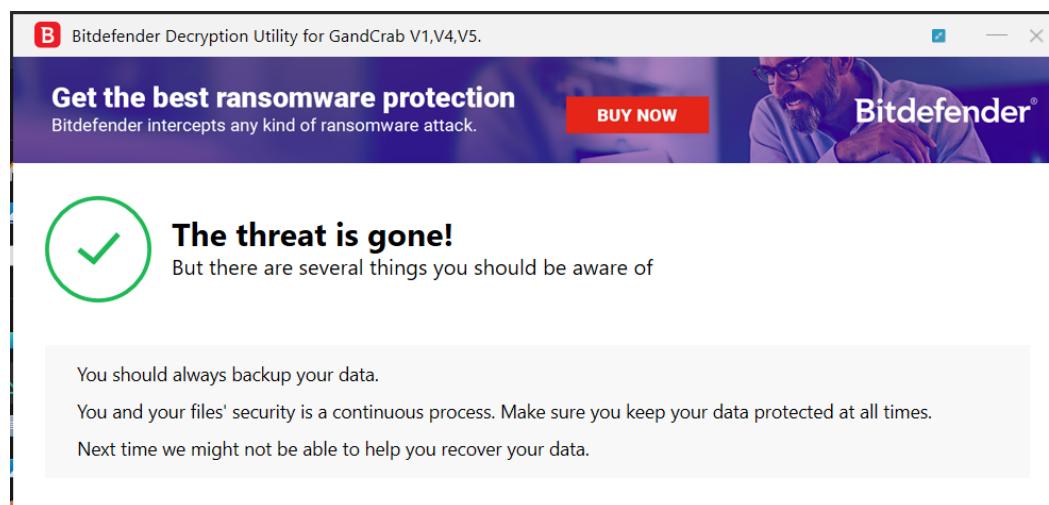
For more information please see this [how-to guide](#).

[download](#)

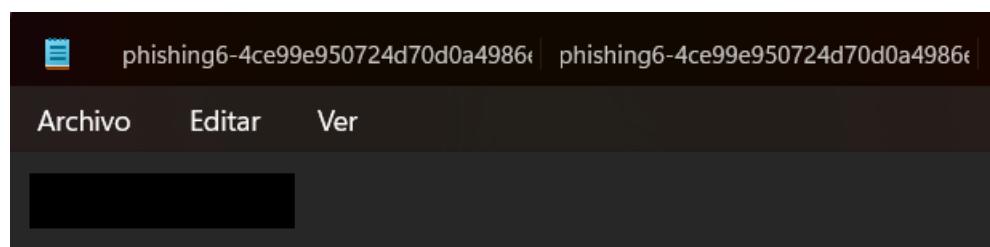
Tool made by Bitdefender

[TO TOP](#)

Una vez descargado y ejecutado nos dirá que se ha desencriptado



Y cuando nos vayamos al .txt nos saldrá el flag



Respuesta: [REDACTED]



Wanna Cry

WannaCry (25pts)



La red de tu organización ha sido comprometida por el ransomware WannaCry. Afortunadamente, se realizan copias de seguridad diarias y se han podido restaurar todos los equipos y servidores. Además, se han aplicado los parches de seguridad correspondientes que mitigan la propagación de este malware a través de la red interna.

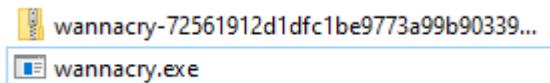
Este malware presenta la peculiaridad de que dispone de un kill switch, consistente en un dominio al que el malware se conecta antes de hacer nada y, si este dominio existe, para su ejecución.

Tu objetivo consiste en encontrar dicho dominio (sin http://) para poder salvar al mundo.

NOTA: es importante que ejecutes el binario en un entorno virtual.
El password del zip es infected

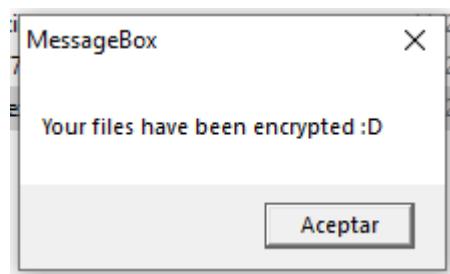
Respuesta:

Primero descargamos el archivo .zip y lo descomprimimos, aunque tendremos que desactivar el firewall y todos los sistemas de defensa o no nos dejará.



Después encendemos wireshark con el que analizaremos la red en busca del DNS de la página.

Abrimos el .exe y nos saldrá el mensaje



Por último en wireshark filtramos por DNS y miramos los destacados que son los que tienen el dominio.



No.	Time	Source	Destination	Protocol
27	0.141997	192.168.1.62	80.58.61.250	DNS
28	0.148568	80.58.61.250	192.168.1.62	DNS
58	0.205694	192.168.1.62	80.58.61.250	DNS
59	0.211776	80.58.61.250	192.168.1.62	DNS
149	4.216974	192.168.1.62	80.58.61.250	DNS
150	4.248372	192.168.1.62	80.58.61.254	DNS
151	4.285904	80.58.61.250	192.168.1.62	DNS
152	4.296059	80.58.61.254	192.168.1.62	DNS
153	4.296103	192.168.1.62	80.58.61.254	ICMP
199	12.538118	192.168.1.62	80.58.61.250	DNS
200	12.560503	192.168.1.62	80.58.61.254	DNS
201	12.568098	80.58.61.250	192.168.1.62	DNS
202	12.602328	80.58.61.254	192.168.1.62	DNS
203	12.602452	192.168.1.62	80.58.61.254	ICMP

```
> Frame 203: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
> Ethernet II, Src: PcsCompu_40:16:c8 (08:00:27:40:16:c8), Dst: Mitra
> Internet Protocol Version 4, Src: 192.168.1.62, Dst: 80.58.61.254
> Internet Control Message Protocol
▼ Domain Name System (response)
  Transaction ID: 0x6ce4
> Flags: 0x8183 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
▼ Queries
  ▼ www.ccncertnomorecryanrtifaderesddferrrqdfwa.com: type A, cl
    Name: [REDACTED]
    [Name Length: 49]
    [Label Count: 3]
```

Respuesta:



Conclusiones

Atenea es una plataforma del CCN-CERT con retos de seguridad informática que incluyen muchos campos en los que aprender diferentes herramientas de diferentes dificultades desde más simples a más complejas, estos retos son muy útiles para aprender a buscar y resolver todo tipo de problemas.

