WRITE-UP MARVEL – CTF UAM - HISPASEC

EPISODIO-3

Elaborado por: Arsenics

Misión:

Nos llevamos una muy grata sorpresa con el último rebelde. Este individuo posee unas capacidades extraordinarias. Su relación con Matrix parece mantener alguna forma de vigencia, aún encontrándose fuera de la simulación. De este modo, no sólo conseguimos anticiparnos a nuestros enemigos, sino que ahora contamos con un arma decisiva en nuestra filas.

Es hora de utilizar su poder para desconectar definitivamente el sistema y ocupar el lugar que nos corresponde en el nuevo mundo.

Los comandos que inician el proceso de desmantelamiento están almacenados de un modo que somos incapaces de comprender. El nuevo rebelde nos ha dado una valiosa pista: "Posiblemente, se requiera una mente que no esté tan limitada por los parámetros de la perfección". Necesitamos un razonamiento que no se apoye exclusivamente en la capacidad de cálculo, sino en aquel extraño atributo que los humanos llaman "intuición" y que, según ellos, les permite ver "más allá".

Hemos comprobado que ni los programas más involucrados en la seguridad de la simulación como El Oráculo o El Creador de Llaves tienen autorizado el acceso a este recurso crítico. Tampoco las suplantaciones de identidad con los datos rebeldes funcionan. Ni siquiera nuestros agentes dobles pueden acceder a él.

Es como si sólo alguien procedente de "FUERA DE LA SIMULACION" pudiera acceder al recurso sin disparar las alarmas.

Una vez que consigas acceso al recurso, recuerda que no todos escribimos de la misma manera...

Web: http://34.247.69.86/matrix/episodio3/index.php

Info: La flag tiene el formato UAM{md5}

Tools:

-Dirb: https://sourceforge.net/projects/dirb/

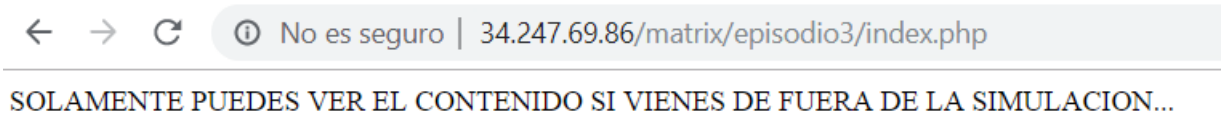
-Steghide: https://github.com/StefanoDeVuono/steghide

-Stegsolve: https://github.com/zardus/ctf-tools/tree/master/stegsolve

-Cyberchef: https://gchq.github.io/CyberChef/

Walktrough;

El enlace nos lleva a una web con una frase un tanto peculiar que recalca lo mismo que el enunciado “Solamente puedes acceder si vienes fuera de la simulación”



En primer lugar miramos el código fuente y comprobamos que está todo vacío… por esta vía va a ser que no. Tras ello realizo un poco de fuzzing con Dirb o Dirbuster y limitando la cantidad de Threats funcionaba pero me de devuelve ningun dato interesante...Me decanto por Nikto, miro SQL y tampoco. Pues empezamos bien….xD

Descartando las opciones anteriores pongo mis esfuerzos a revisar los métodos http, percantandome de que es vulnerable a header:

curl -v -H “newheader:headervalue:” http://34.247.69.86/episodio3/index.php

```
root@kali:~# curl -v -H "newheader: headervalue:" http://34.247.69.86/matrix/episodio3/index.php
*   Trying 34.247.69.86...
* TCP_NODELAY set
* Connected to 34.247.69.86 (34.247.69.86) port 80 (#0)
> GET /matrix/episodio3/index.php HTTP/1.1
> Host: 34.247.69.86
> User-Agent: curl/7.62.0
> Accept: */*
> newheader: headervalue:
>
< HTTP/1.1 200 OK
< Date: Sun, 19 May 2019 15:54:13 GMT
< Server: Apache/2.4.25 (Debian)
< Vary: Accept-Encoding
< Content-Length: 138
< Content-Type: text/html; charset=UTF-8
<

<html>
<head>
        <title>Le matrix</title>
</head>
<body>
SOLAMENTE PUEDES VER EL CONTENIDO SI VIENES DE FUERA DE LA SIMULACION...

</body>
* Connection #0 to host 34.247.69.86 left intact
```

Después de mucho pensamiento lateral y de mirarme muchas cosas me acabo dando cuenta que con el X-Forwarded For el parámetro que tenía que pasar lo tenía delante todo el tiempo. Nada si quieres esconder algo ponlo a la vista… Y yo rayandome con eso de venir fuera de la simulación. Pues pasandole esas palabras literalmente...Voilà!!! Ahí está lo que necesitaba!

```
root@kali:~# curl -v -H 'X-Forwarded-For: FUERA DE LA SIMULACION' http://34.247.69.86/matrix/episodio3/index.php
*   Trying 34.247.69.86...
* TCP_NODELAY set
* Connected to 34.247.69.86 (34.247.69.86) port 80 (#0)
> GET /matrix/episodio3/index.php HTTP/1.1
> Host: 34.247.69.86
> User-Agent: curl/7.62.0
> Accept: */*
> X-Forwarded-For: FUERA DE LA SIMULACION
>
< HTTP/1.1 200 OK
< Date: Sun, 19 May 2019 20:50:23 GMT
< Server: Apache/2.4.25 (Debian)
< Vary: Accept-Encoding
< Content-Length: 177
< Content-Type: text/html; charset=UTF-8
<

<html>
<head>
        <title>Le matrix</title>
</head>
<body>
http://34.247.69.86/matrix/episodio3/iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg
```

Recordamos que en burp también podemos trabajar los métodos http desde la pestaña del repeater aunque en este caso yo lo he realizado con curl.

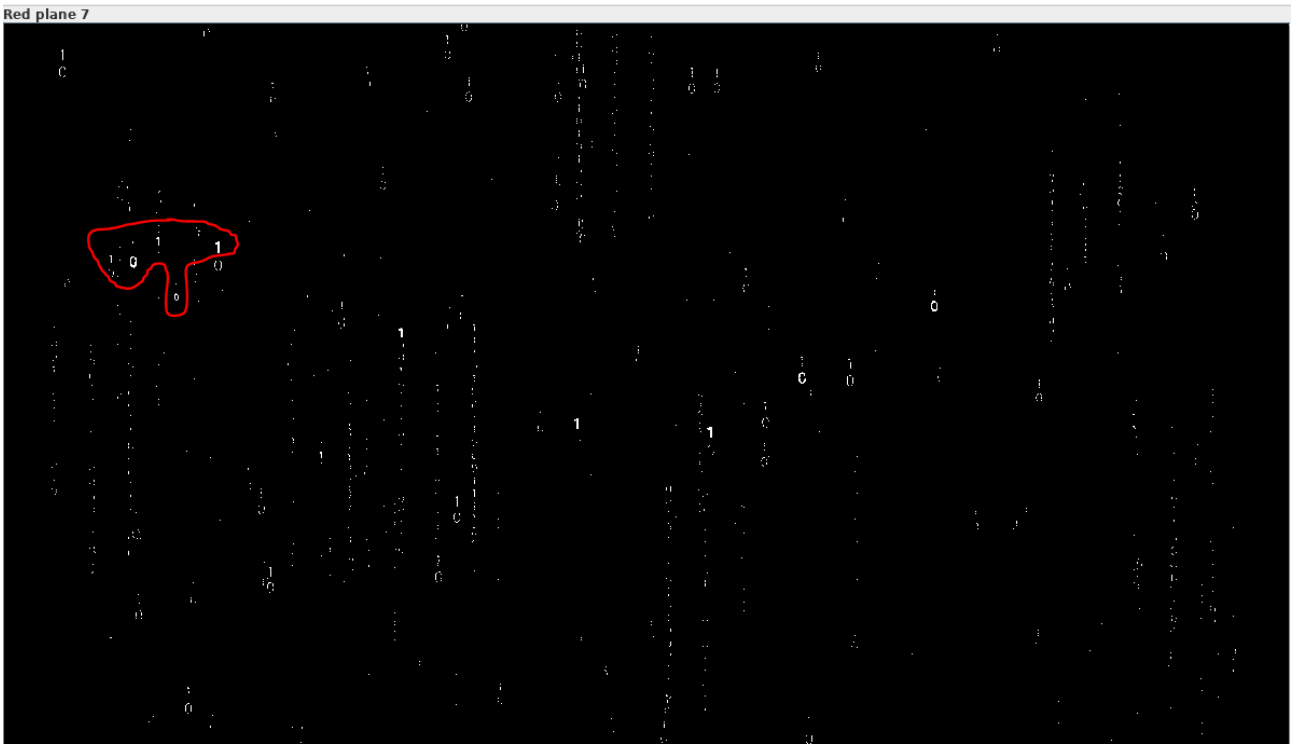
Con esta mítica imagen de Matrix nos adentramos en la prueba de Esteganografía, que llevabamos algunas uams sin ver. En esta ocasión de entrada veo algunos números en blanco que destacan formando 0111100 y pienso que puede ser alguna clave, lo pruebo con steghide y no funciona. Paso el exiftool a ver si me añade alguna información interesante sin suerte. Paso la imagen por varias páginas online de esteganografía sin éxito. Miro con Bless pero todo parece estar bien es un jpg que sale con la cabecera correcta y que acaba en FF D9 y no se ve que haya ningun zip ni imagen embebida.

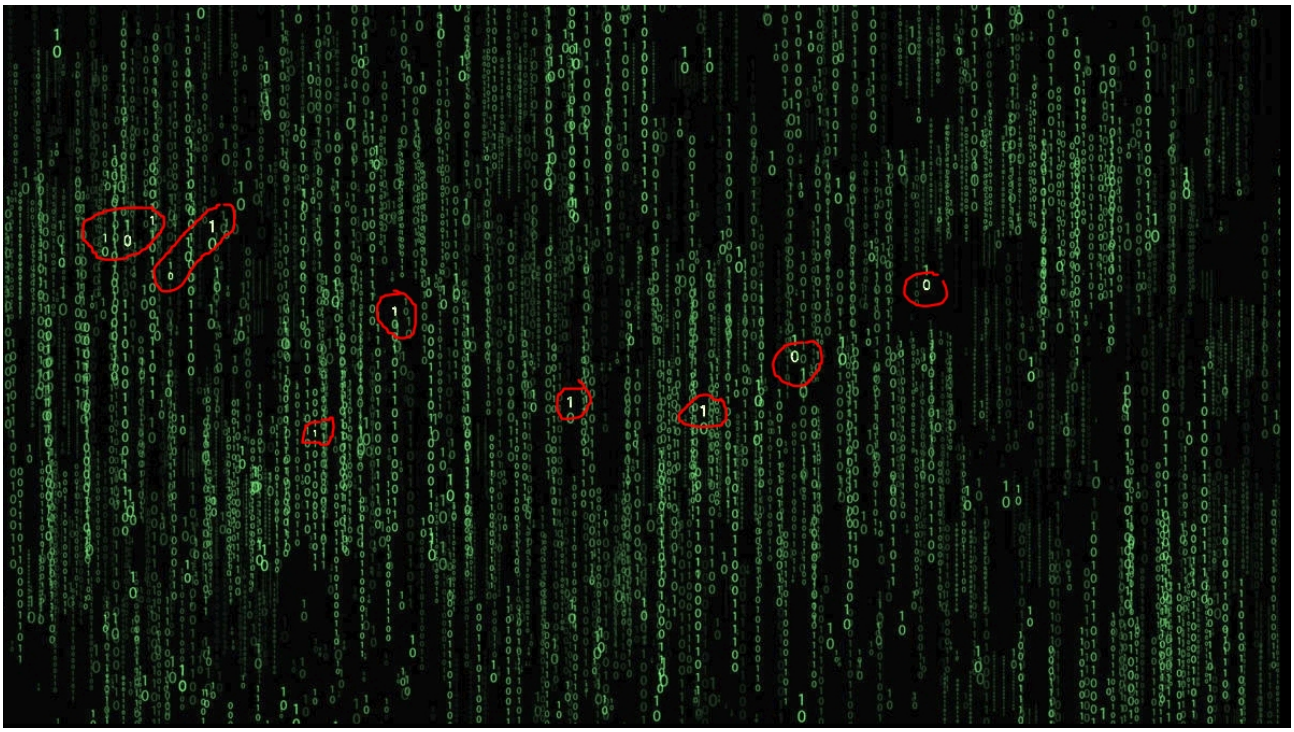
```
.....JFIF.....H.H.....C.....................
..........................................
..C.......................................
.....................................".....
..........................................
.....}.....!1A..Qa."q.2....#B...R..$3br...
.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstu
vwxyz.....................................
..........................................
.....................................w...
....!1..AQ.aq."2...B.....#3R..br...$4.%.....&
'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...
..........................................
.....................................?.....u.
%...X.r...r..T...p9.<..l.i.\.l^\\Mcao,S....X.
.X.....1..R..w.....#9/~...oK....~.Lz!.....*X.
```

Desde luego no será porque no haya probado cosas...Sin embargo no dejo de intentarlo, paso el stegsolve a ver si me arroja algo más. Y entre varias opciones hay una que me desvela que me estaba dejando algunos números blancos la primera vez, aunque no me fío de ella porque me señala algunos verdes tambíen. Aun así hace un neteo bueno de la imagen y me arroja luz.

Java -jar stegsolve.jar

File/open y buscamos la imagen. Tras ello: en Red plane 7 detecto que me faltaban algunos números blancos al principio (los de la parte superior izquierda no los cuento porque son verdes De modo que la clave quedaría 1010111100



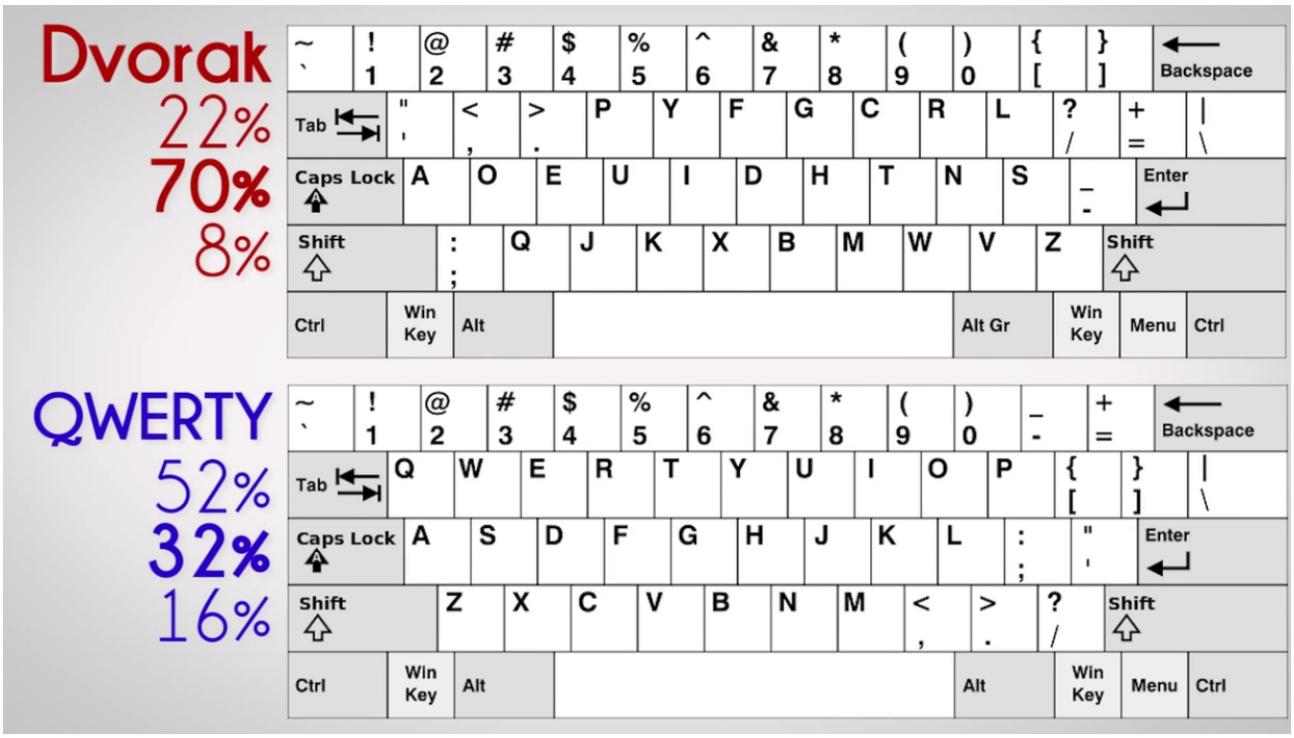


Vuelvo a probar suerte con steghide...No sale!! Me he debido dejar alguno. Jugando un poco con la clave 10101111100 nos deja un flag.txt. Bonito regalo, pero no puede ser tan fácil por supuesto. Que esto es la UAM !!! Evidentemente la clave ha de estar cifrada.

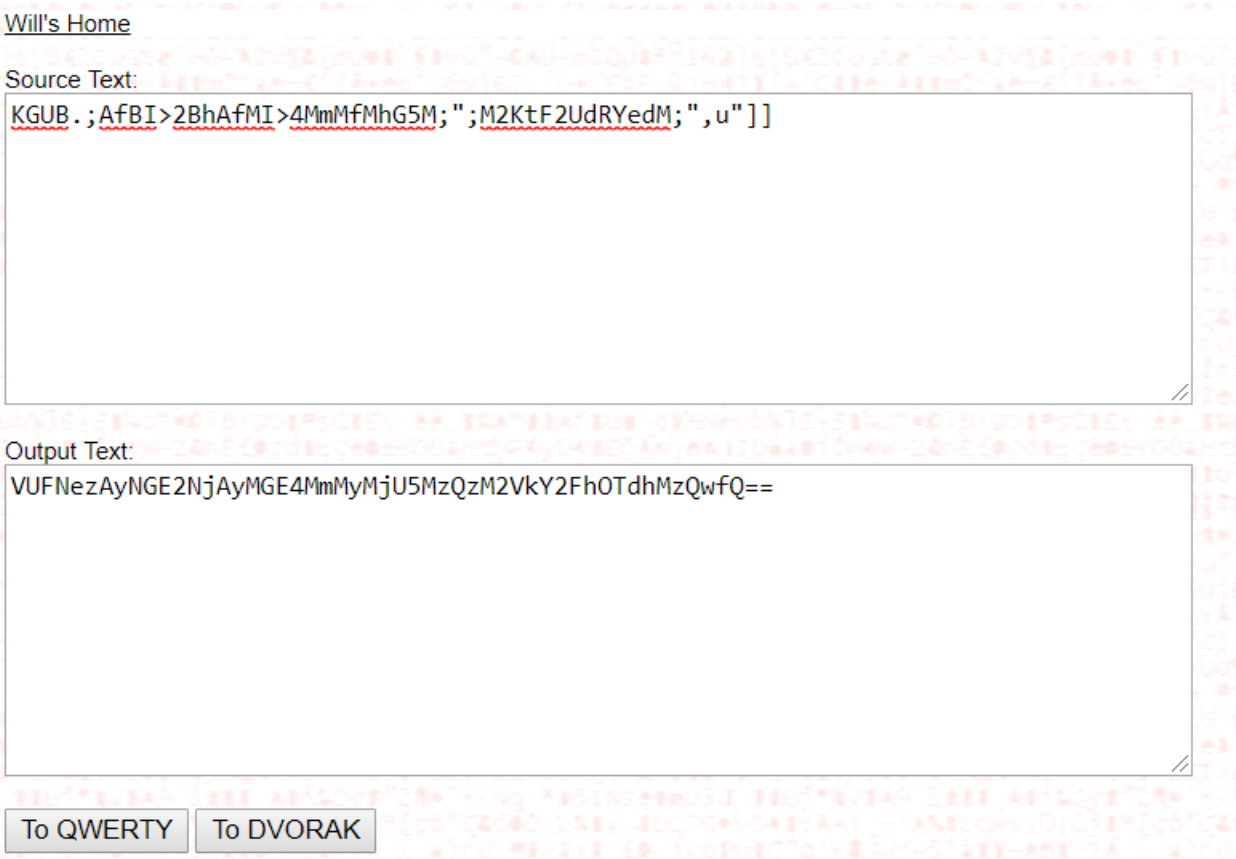
```
root@kali:~/Desktop# steghide --extract -sf matrix.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kali:~/Desktop# cat flag.txt
KGUB.;AfBI>2BhAfMI>4MmMfMhG5M;";M2KtF2UdRYedM;",u"]]
```

Llegados a este punto para perder la cabeza provando todas las opciones de cyberchef más Maleboge, Caesar, Baconian, etc sin éxito ninguno. Volvemos a leer el enunciado. “No todos escribimos de la misma manera” mmmm A mano, a máquina, en braille, en morse, con pluma, en papyros, se me ocurren mil formas de escribir q nada tenían que ver. Estancarse es lo peor...Finalmente caigo en que no todos usamos las misma distribución de teclado...así que ...realmente no todos escribimos igual. Mirando varias disribuciones Azerty, Colemak sin embargo la más conocida es Dvorak.

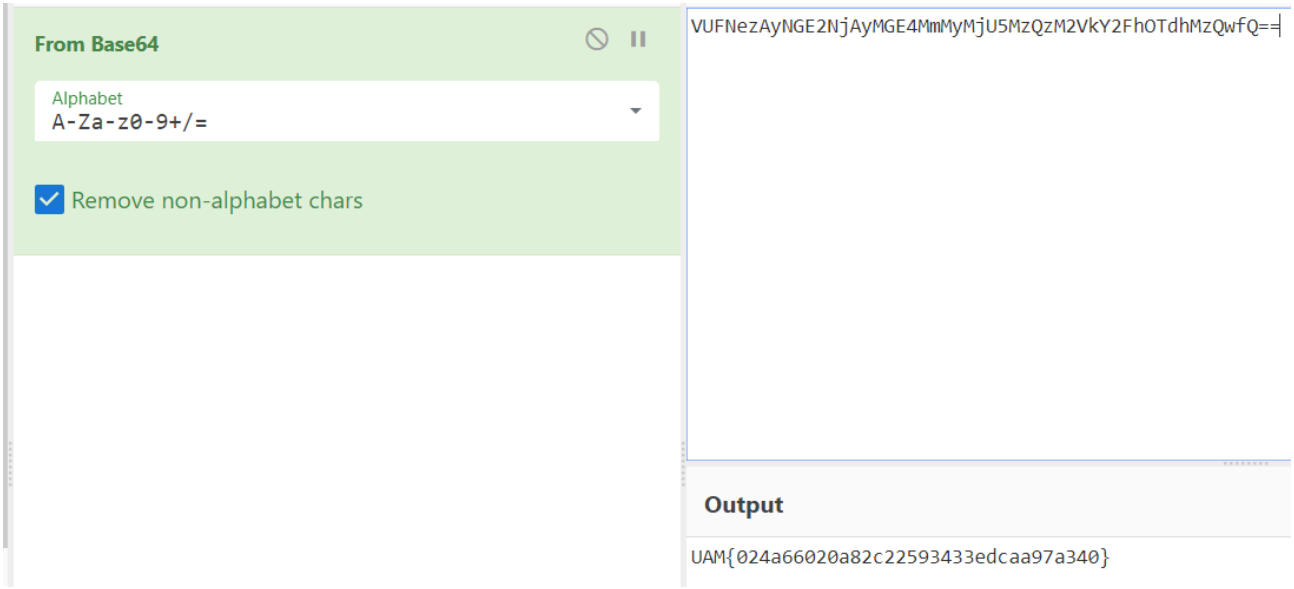
Se podría resolver a mano comparando nuestro teclado Qwerty:



O bien hay páginas online que te hacen la traducción como vemos a continuación.



Y tampoco tenemos la flag! He aquí un último pasito para el premio. Un rico base64 a descifrar en cyberchef con nuestra querida flag.



UAM{024a66020a82c22593433edcaa97a340}

Gracias Admins, nos vemos próximamente en la UAD360 !

Autoría: Arsenics