EPISODIO 3
963

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}

TOP 3: 1. 2. 3.

root@kali:~/uam/matrix_ep3# curl http://34.247.69.86/matrix/episodio3/index.php

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

</body>

En el enunciado ya nos hacía referencia a eso de “FUERA DE LA SIMULACION” por lo que entendemos que puede ser importante.

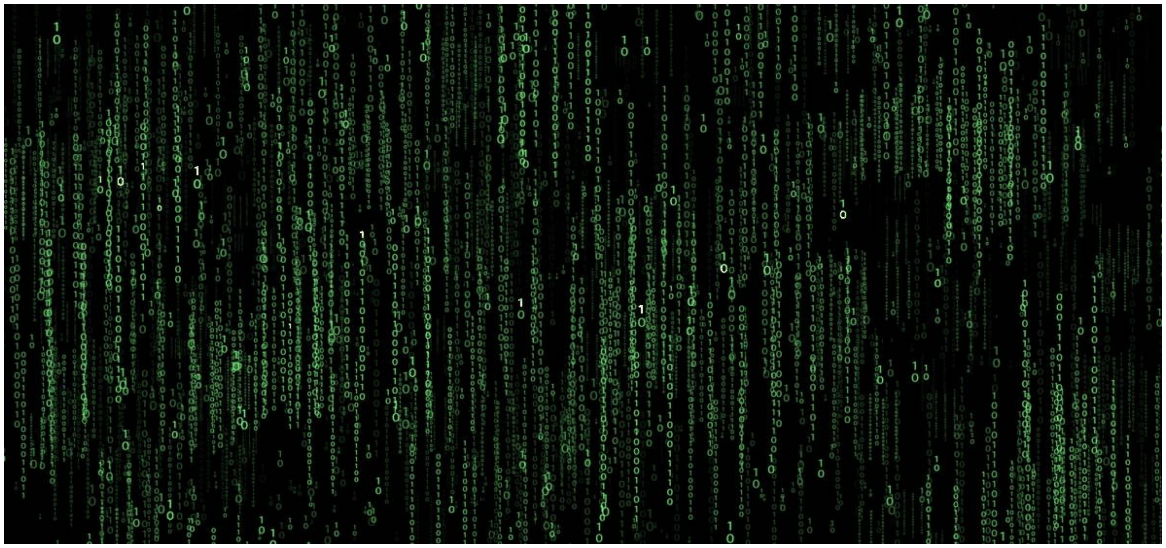
Después de varias pruebas, primero pensando en que podría referirse a un Virtual Host de Apache .. nos centramos en los HEADERS del HTTP.

root@kali:~/uam/matrix_ep3# curl -H 'X-Forwarded-For: FUERA DE LA SIMULACION' http://34.247.69.86/matrix/episodio3/index.php

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

</body>

Descargamos la imagen:



Y empezamos a hacer las pruebas básicas, file … exiftool, strings … y cuando le pasamos stegsolve (incluso antes) nos damos cuenta que hay 1 y 0 que resaltan más … por lo que probamos de ver cuales son y los introducimos como password en steghide.
Nos da error de contraseña … así que probamos a crear un diccionario para hacer después bruteforce (empecé con contraseña de 4 a 8 dígitos pero no salió aún, así que lo aumenté):

root@kali:~/uam/matrix_ep3# crunch 8 12 10 -o diccionari.txt
Crunch will now generate the following amount of data: 96512 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 7936

crunch: 100% completed generating output
root@kali:~/uam/matrix_ep3# steg_brute.py -b -d diccionari.txt -f iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg

[i] Searching...

30%|##
|

anot&#65533; los datos extra&#65533;dos e/"iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1_flag.txt".

[+] Information obtained with password: 10101111100

KGUB.;AfBI>2BhAfMI>4MmMfMhG5M;";M2KtF2UdRYedM;",u"]]

Una vez teniendo esta flag, tenía bastante claro que podía ser, gracias a la pista que se da en el enunciado: “Una vez que consigas acceso al recurso, recuerda que no todos escribimos de la misma manera…”

Me ha parecido muy evidente, así que lo primero que he probado ha sido pasar de dvorak a qwerty el mensaje:

Pasar de dvorak a qwerty:
http://wbic16.xedoloh.com/dvorak.html

Claramente el resultado que nos da es un base64, por lo que lo decodificamos:

root@kali:~/uam/matrix_ep3# echo -n 'VUFNezAyNGE2NjAyMGE4MmMyMjU5MzQzM2VkY2FhOTdhMzQwfQ==' | base64 -d

Flag: UAM{024a66020a82c22593433edcaa97a340}

DarkEagle