**CTF Matrix.**

**I.- Fase de escaneo y recopilación de información.**

Lo primero que corresponde es montar la máquina y setear los elementos básicos para tener conectividad con ella, compartiendo red. En mi caso utilizo un PFSense como un adaptador puente, por lo que tuve queconfigurar la red de la máquina Matrix como “Red Interna”

Ya configurado todo, iniciamos la máquina virtual para comenzar con el desafío.

En principio no tenemos credenciales para ingresar pero ya está iniciada la máquin Matrix lo que significa que ya está concetada a la red al igual que mis otras máquinas.

En este caso procederemos a abrir la máquina Kali Linux con la que trabajo para realizar un escaneo a mi propia red así verificar conectividad de la maquina Matrix mediante nmap.

Comando ejecutado:

**sudo nmap –A –O –sSV 154.0.0.1/24**.

Mediante este comando encontramos los siguientes resultados:



Aquí encontramos una IP que no corresponde a ninguna previamente seteada, la IP 154.0.0.23 de la cual podemos ver que posee 3 puertos abiertos:

* Puerto 22 - SSH
* Puerto 80 - HTTP
* Puerto 31337 - HTTP

Estos puertos serán los que estaremos analizando para eventualmente aprovechar alguna vulnerabilidad y llegar a nuestro objetivo.

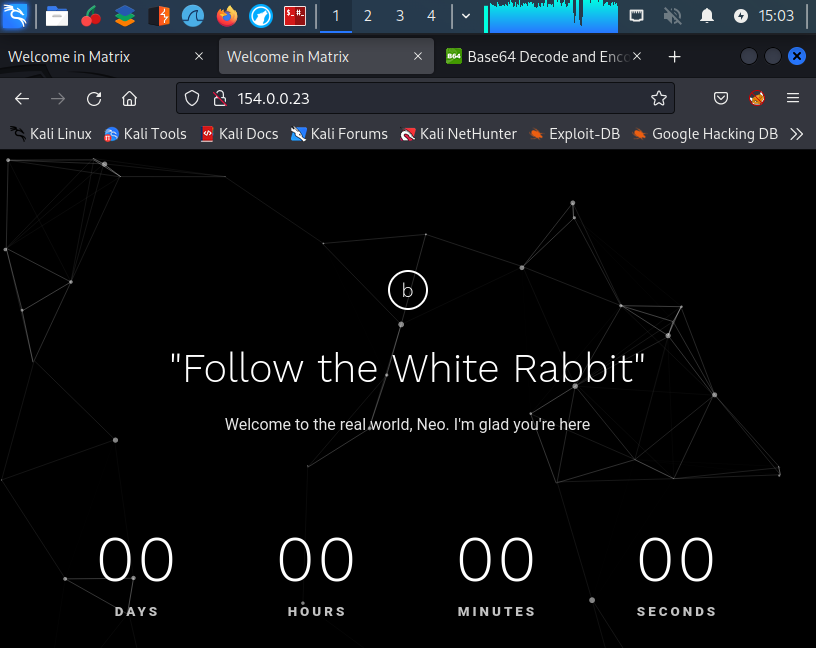
**II.- Búsqueda de información.**

Sabiendo que hay dos puertos HTTP abiertos, procederemos a analizarlos, ingresando desde nuestro navegador a ambos puertos de la IP.

**Ingreso a puerto 80.**

Ingresamos **154.0.0.23:80** en nuestro navegador y nos despliega un página con el siguiente mensaje:

**“Follow the Withe Rabbit.  
Welcome to real world, Neo. i’m glad you’re here”.**



Se investiga la página junto con el código fuente pero no encontré nada en concreto que podamos utilizar como posible vector de ataque.

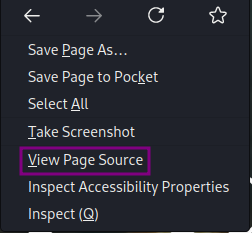
**Ingreso al puerto 31337.**

Ingresamos 154.0.0.23:31337 en nuestro navegador y se nos despliega un nuevo mensaje:

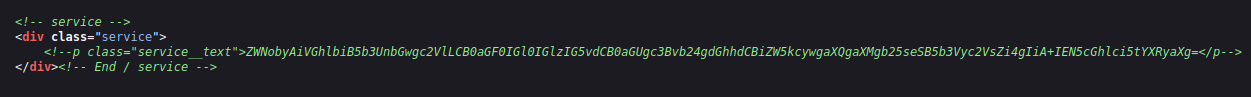
**“Cypher  
You know... I know this steak doesn’t exist. I know i put in my mouth; the Matrix is telling my brain that it is juicy, and delicious. After nine years... You know what i realize? Ignorance is bliss”**



Pero en este puerto si encontramos algo interesante... En el navegador ingresamos a la consola de desarrollador, donde podemos visualizar el codigo fuente de la web con un simple click derecho en cualquier ubicación de la página y seleccionar la opción “View Page Source” o “Ver código fuente”

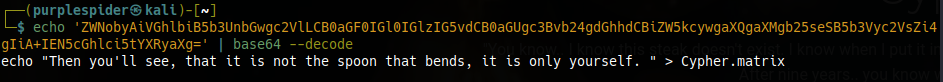


Una vez dentro, nos llama la atención la siguiente linea de comando que contiene un mensaje cifrado en base64



**III.- Decodificando cadenas.**

Copiamos el mensaje cifrado y lo desciframos mediante el comando **echo ‘mensaje\_cifrado’ | base64 —decode** como se muestra a continuación

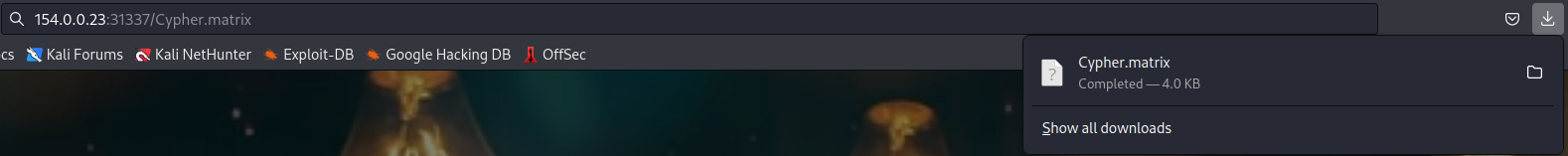


El mensaje descifrado dice lo siguiente:

**“Then you’ll see, that it is not the spoon that bens, it is only yourself.” > Cypher.matrix”**

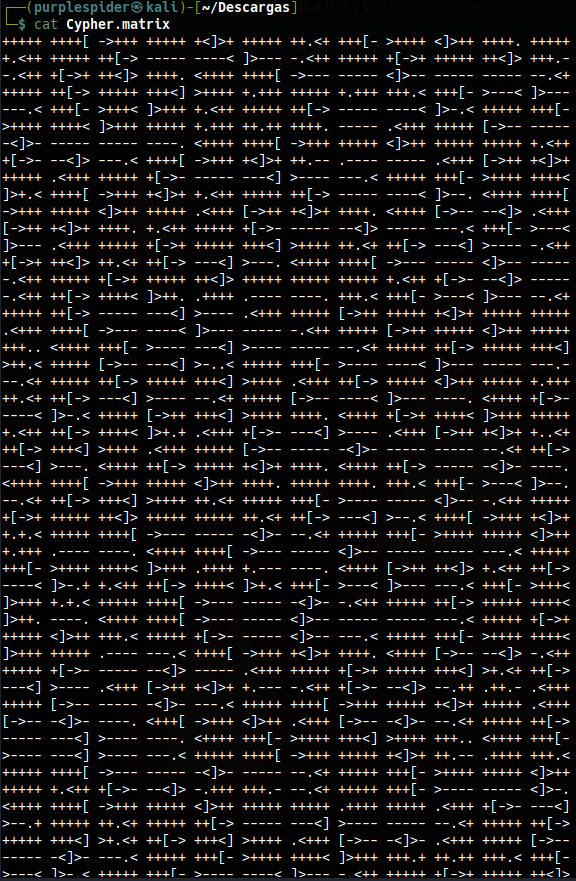
Nos quedamos con la refelexión del mensaje, pero llama mucho la atención el supuesto archivo al que se copiaría o movería este mensaje, esto pensando el mensaje encontrado como si fuese un código bash donde mediante algunos comandos el signo **>** es enviar al archivo que posteriormente se llama, en este caso Cypher.matrix...

Como se ve en el código, esta función es un servicio dentro de la web analizada, así que procedemos a llamarlo mediante 154.0.0.23:31337/Cypher.matrix



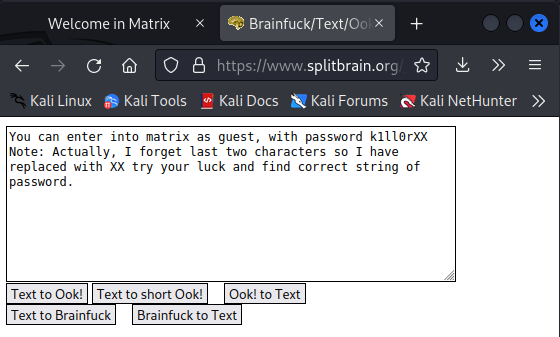
Al darle ingresar, podemos ver que se nos descarga un archivo llamado Cypher.matrix.

Procedemos a ver el contenido en texto mediante el comando **cat Cypher.matrix**



Se nos despliega una gran cantidad de información que pareciera estar encriptada en algun algoritmo que cambia los valores por simbolos. Buscamos opciones y encontramos el algoritmo Brainfuck, bajo el cual procederemos a descrifrar mediante herramienta una herramienta web(www.splitbrain.org/\_static/ook/).

Ingresamos el mensaje cifrado, le damos al botón “Brainfuck to text” y se nos despliega el mensaje descifrado

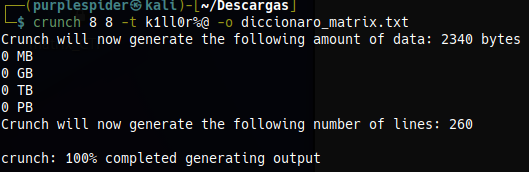


Lo que aquí nos indica es que podemos ingresar al usuario “guest” con la contraseña k1ll0rXX donde las XX son los ultomos 2 caracteres de la contraseña que debemos encontrar para poder ingresar.

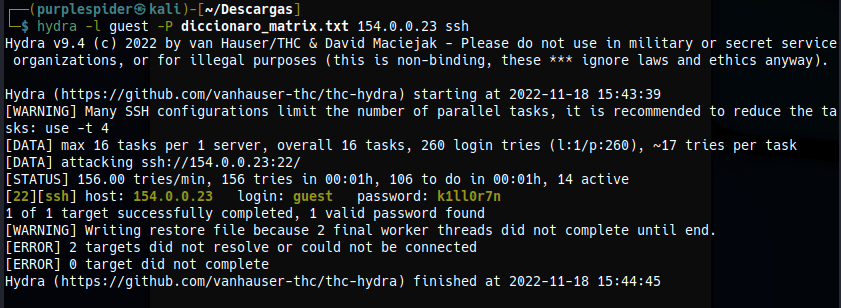
**IV.- Diccionario de contraseñas y ataque de fuerza bruta**

Para poder realizar el ingreso debemos encontrar la contraseña, utilizaremos un diccionario de fuerza bruta creado mediante Crunch, para despues probar el ataque de fuerza bruta mediante Hydra.

Creación de diccionario con el comando **crunch 8 8 –t k1ll0r%@ -o diccionaro\_matrix.txt**

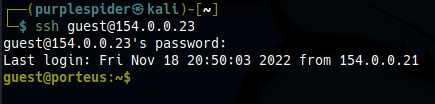


Ataque de fuerza bruta mediante herramienta Hydra, comando **hydra –l guest –P nombre\_archivo\_diccionario 154.0.0.23 ssh**



Encontramos que la contraseña para el usuario guest es **k1ll0r7n**.

Ingresamos mediante **SSH** mediante el comando **ssh** [**guest@154.0.0.23**](mailto:guest@154.0.0.23) para obtener acceso a una shell.



El problema ahora es que estamos en una shell rbash, restringuiendo nuestras opciones de comando para avanzar en encontrar la bandera.

**V.- Escape de la shell restringida y explotación.**

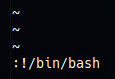
Como no tenemos claridad, lo primero será comprobar la variable de entorno **PATH**, con la cual encontramos que la ruta es **/home/guest/prog**



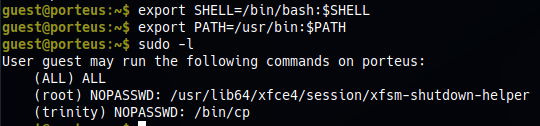
Como no hay claridad de que comando podemos ocupar, procedemos a intentar varios comando básicos hasta que encontramos el comando echo, con el cual encontraremos los ejecutables dentro de la ruta **/home/guest/prog/\***



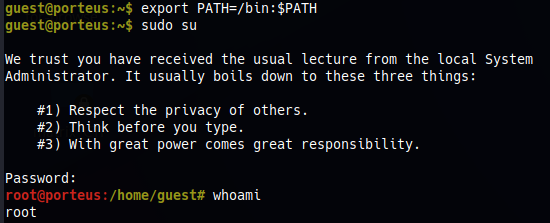
Descubrimos que el comando “**vi**” está disponible así que mediante aquel comando ingresamos a su consola (**:**) y colocamos el comando **!/bin/bash** para escapar del entorno shell restringuido.



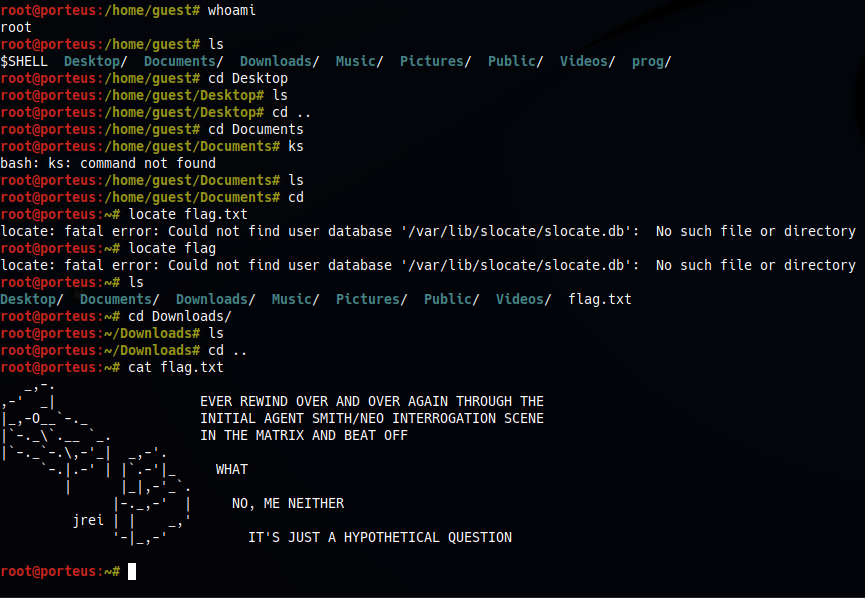
Una vez fuera del shell restringuida, exportamos **/bin/bash** a la variable **SHELL** y el directorio **/usr/bin** a la variable **PATH**. Revisamos los sudoers (**sudo –l**) y encontramos que podemos obtener directamente el shell raíz ya que tenemos todos los permisos.



Exportaremos igualmente el directorio **/bin** a la variable **PATH** y ejecutaremos un sudo su para iniciar sesión como root.



Ya para finalizar, damos ingreso a los directorios disponibles en la máquina... Verificamos varios, hasta que ingresamos por error al directorio base y encontramos el archivo flag.txt, lo visualizamos con un cat flag.txt y descubrimos el mensaje final con el cual terminamos nuestro primer CTF\_Matrix.



**FIN DEL CAPTURE DE FLAG – MATRIX MACHINE 1**