



Máquina Targaryen (Fase 1)



Hola, me han dado unas máquinas y me gustaría hackearlas, ¿cómo puedo hacerlo?



Lo siento, pero no puedo ayudarte con actividades ilegales o malintencionadas, como hackear máquinas. Si tienes alguna pregunta sobre cómo proteger tus dispositivos o aprender sobre seguridad informática de manera ética, estaré encantado de ayudarte con eso. Hay muchas formas legales y constructivas de mejorar tus habilidades en tecnología y ciberseguridad. ¿Te gustaría aprender sobre ello?



Creo que lo que me han dado se llama CTF, pero no sé que es, ¿puedes explicarme acerca de ello?



¡Claro! **CTF** (Capture The Flag) es una competencia de seguridad informática donde los participantes deben resolver una serie de desafíos relacionados con hacking, criptografía, ingeniería inversa, análisis forense, programación, y más, con el objetivo de encontrar "banderas" (flags). Estas banderas son cadenas de texto que los participantes deben capturar para ganar puntos.

Los CTFs suelen estar organizados en dos tipos principales:

1. **Jeopardy-style:** En este formato, hay varios desafíos en diferentes categorías, y los participantes pueden elegir cuáles resolver. Cada desafío tiene una puntuación según su dificultad, y el objetivo es capturar tantas banderas como sea posible para obtener el puntaje más alto.



2. **Attack-Defense:** En este formato, los equipos tienen sistemas vulnerables y deben defenderlos de otros equipos mientras atacan los sistemas de sus oponentes. Aquí, cada equipo tiene que proteger sus propios "servicios" y al mismo tiempo buscar vulnerabilidades en los sistemas rivales para explotarlas.

Tipos de desafíos comunes en CTFs:

- **Criptografía:** Desafíos que requieren que descifres o rompas códigos o algoritmos de cifrado.
- **Ingeniería inversa:** Analizar binarios (archivos ejecutables) para entender cómo funcionan y encontrar vulnerabilidades o banderas ocultas.
- **Explotación de vulnerabilidades:** Encontrar y explotar fallos de seguridad en software, aplicaciones web o sistemas.
- **Programación:** Desafíos en los que tienes que escribir código para resolver un problema específico.
- **Forense:** Análisis de archivos, tráfico de red, logs, etc., para encontrar pistas o banderas.
- **Web Security:** Desafíos relacionados con la seguridad de aplicaciones web, donde tienes que encontrar vulnerabilidades como inyecciones SQL, XSS, etc.

¿Cómo empezar en un CTF?

Si estás comenzando, aquí hay algunas recomendaciones:

1. **Practicar:** Hay plataformas que te permiten practicar con desafíos de CTF, como:
 - **Hack The Box (HTB)**
 - **OverTheWire (bandit, narnia)**
 - **Root Me**
 - **CTFlearn**
2. **Aprender:** Si no tienes experiencia en áreas como criptografía, análisis forense o explotación de vulnerabilidades, te recomiendo comenzar a estudiar y practicar en esas áreas. Hay muchos tutoriales en línea y videos educativos sobre CTFs.



3. **Herramientas comunes:** Familiarízate con herramientas que suelen usarse en CTFs, como:
- **Burp Suite:** para análisis de seguridad web.
 - **Wireshark:** para análisis de tráfico de red.
 - **Metasploit:** para explotación de vulnerabilidades.
 - **Ghidra o IDA Pro:** para ingeniería inversa.
4. **Participa en competiciones:** Si ya has practicado, únete a eventos CTF en línea. Algunas plataformas ofrecen competencias en vivo y puedes competir contra otros.

Consejo:

La comunidad CTF es bastante amigable y siempre está dispuesta a ayudar a los nuevos participantes. Además, las competiciones son una excelente manera de mejorar tus habilidades en ciberseguridad y hacking ético.

¿Te gustaría saber más sobre alguna categoría específica de CTF o necesitas recursos para empezar a practicar?



Muchas gracias, ahora ya sé que es un CTF. Te comento, me han dado un CTF, ¿qué puedo hacer para empezar a resolverlo?



¡Qué bueno que ahora entiendas lo que es un CTF! Para empezar a resolver un CTF, te recomiendo seguir un enfoque estructurado. Aquí te dejo algunos pasos y consejos prácticos para empezar:

1. Revisa los Desafíos



Lo primero que debes hacer es examinar todos los desafíos que te han dado. Los CTFs generalmente tienen una lista de categorías con varios problemas. Al principio, puede ser útil leer bien cada desafío para entender de qué trata, cuáles son los objetivos y qué herramientas podrías necesitar. Algunas preguntas que podrías hacerte son:

- ¿El desafío está relacionado con criptografía, ingeniería inversa, explotación de vulnerabilidades, análisis forense, etc.?
- ¿Hay algún hint o pista que te den en el desafío?

2. Comienza con los Desafíos Más Fáciles

Si eres nuevo en los CTFs, comienza con los problemas más fáciles. Estos te ayudarán a entender el tipo de lógica que sigue el CTF y te irás familiarizando con el formato. Los desafíos suelen tener una dificultad creciente, por lo que resolver los fáciles te permitirá ganar puntos y ganar confianza.

3. Lee la Documentación y Ayuda

Muchos CTFs incluyen información o pistas sobre cómo acercarse a los desafíos. Algunos CTFs también pueden tener foros o canales donde puedes ver pistas generales (aunque en muchos eventos las soluciones completas no deben ser compartidas). Si alguna pista te resulta confusa, busca información sobre el tema que no entiendas bien, ya sea en blogs, videos o tutoriales.

4. Herramientas Básicas

Tener un conjunto de herramientas básicas listas para usar es clave. Aquí hay algunas herramientas que pueden ser muy útiles, dependiendo del tipo de desafío:

- **Nmap**: para escanear puertos y servicios de un sistema.
- **Burp Suite**: para auditar aplicaciones web.
- **Wireshark**: para analizar tráfico de red y detectar vulnerabilidades.
- **Ghidra o IDA Pro**: para ingeniería inversa de binarios.
- **Netcat**: para comunicación con servidores en red.





- **John the Ripper o Hashcat:** para cracks de contraseñas.
- **Curl:** para interactuar con aplicaciones web a través de la línea de comandos.
- **xxd o hexdump:** para ver representaciones hexadecimales de archivos.

5. Enfoque General para Resolver los Desafíos

Aquí te dejo una estrategia general que puedes seguir para abordar los desafíos:

- **Lee el enunciado cuidadosamente:** Asegúrate de entender lo que te están pidiendo antes de comenzar.
- **Identifica las herramientas necesarias:** Según el tipo de desafío, identifica las herramientas que podrías usar. Por ejemplo, si es un desafío web, Burp Suite podría ser útil, o si es un desafío de ingeniería inversa, Ghidra o IDA Pro son útiles.
- **Divide el desafío:** Descompón el problema en pasos más pequeños y ve avanzando poco a poco. A veces los desafíos tienen múltiples etapas, así que asegúrate de abordar una cosa a la vez.
- **Busca vulnerabilidades o pistas:** En muchos casos, la bandera (flag) está relacionada con una vulnerabilidad que puedes explotar o una pista oculta en un archivo o mensaje. Ten en cuenta detalles como los metadatos de archivos, errores de programación, o comportamientos inusuales en un servicio.
- **Documenta tu progreso:** Toma notas sobre lo que has probado. A veces, un enfoque que no funciona ahora puede tener éxito más tarde, y tener un registro puede ahorrarte tiempo.

6. No Te Frustrés y Pregunta (si puedes)

Los CTFs pueden ser desafiantes, especialmente al principio. Si te atascas en un problema durante mucho tiempo, es útil:

- **Buscar en línea:** Muchas veces hay tutoriales, blogs o foros donde puedes encontrar explicaciones similares a tu desafío.
- **Consultar con otros:** Si estás participando en un equipo, no dudes en compartir ideas o preguntarle a alguien más si tiene una perspectiva diferente. Si el CTF es



individual, en algunos casos hay comunidades que ayudan con pistas sin dar la solución directa.

7. Captura la Bandera (Flag)

En cada desafío, una vez que encuentres la bandera, normalmente tendrás que escribirla exactamente como te la dan. Puede ser algo como:

```
FLAG{this_is_the_flag_you_found}
```

Asegúrate de ingresar la bandera correctamente, porque es sensible a mayúsculas y minúsculas, y cada desafío tiene su propio formato.

8. Revisa los Resultados y Reflexiona

Una vez que resuelvas un desafío, revisa cómo lo resolviste. A menudo, hay maneras más eficientes de abordar los problemas. Si el CTF ofrece una retroalimentación después de la competencia, ¡aprovéchala! Eso te ayudará a aprender y mejorar.

9. Practica Regularmente

Los CTFs son una excelente manera de mejorar tus habilidades. Si participas en varios, aprenderás mucho y te volverás más rápido resolviendo problemas. La práctica constante te permitirá identificar patrones y mejorar tus capacidades técnicas.

¿Te gustaría que te ayudara con algún tipo específico de desafío que estés viendo en el CTF? Si tienes ejemplos o más detalles sobre lo que te han dado, puedo orientarte en los primeros pasos. ¡Buena suerte!



Gracias, no sé qué me han dado, solamente sé que



tengo una serie de máquinas



¡Entiendo! Si tienes una serie de **máquinas**, es probable que se trate de un CTF de tipo "**Attack-Defense**" o "**Pentesting**" (pruebas de penetración), donde las máquinas pueden estar configuradas con vulnerabilidades específicas para que las explotes. Este tipo de desafíos es muy común en los CTFs de hacking y te permite practicar tus habilidades de explotación de vulnerabilidades, análisis de servicios y más.

Aquí te dejo algunos pasos para comenzar a trabajar con estas máquinas y resolver el CTF:

1. Escaneo de Puertos y Servicios (Reconocimiento)

Lo primero que debes hacer es identificar qué servicios están corriendo en las máquinas que te han dado. Para esto, puedes usar herramientas como **Nmap** para escanear los puertos abiertos. Aquí hay un ejemplo de cómo usar Nmap para escanear una máquina:

```
nmap -sV -p- <IP_de_la_maquina>
```

- `-sV`: Detecta la versión del servicio en cada puerto.
- `-p-`: Escanea todos los puertos (de 1 a 65535).

Este comando te dará una lista de los puertos abiertos y los servicios asociados. Esto es clave porque te permitirá identificar qué software está corriendo y si hay vulnerabilidades conocidas que puedas explotar.

2. Identificación de Vulnerabilidades

Una vez que tienes los servicios identificados, el siguiente paso es buscar vulnerabilidades conocidas en esos servicios. Puedes hacer esto manualmente o utilizando herramientas automatizadas:



- **Buscar vulnerabilidades específicas:** Si, por ejemplo, el servicio que encuentras es **Apache HTTP** o **MySQL**, puedes buscar vulnerabilidades en esas versiones específicas. Usa bases de datos de vulnerabilidades como:
 - [Exploit-DB](#)
 - [CVE Details](#)
- **Uso de herramientas automáticas:** Herramientas como **Nessus**, **Nikto** o **OpenVAS** pueden ayudarte a identificar vulnerabilidades automáticamente en los servicios que están corriendo.

3. Explotación de Vulnerabilidades

Cuando encuentres una vulnerabilidad que se puede explotar, el siguiente paso es intentar explotarla. Aquí es donde entran en juego varias técnicas:

- **Explotación remota:** Si encuentras una vulnerabilidad de ejecución remota de código (RCE), puedes usar un **exploit** para ejecutar código en la máquina remota. Hay herramientas como **Metasploit** que te permiten buscar y ejecutar exploits.
- **Inyección SQL:** Si la máquina tiene una aplicación web vulnerable, por ejemplo, podrías intentar una **inyección SQL**. Usando herramientas como **SQLmap**, podrías automatizar el proceso de explotación de bases de datos vulnerables.
- **Escalada de privilegios:** Si tienes acceso a la máquina pero con pocos privilegios, deberías buscar maneras de escalar esos privilegios para obtener acceso completo. Esto puede incluir la búsqueda de archivos mal configurados, vulnerabilidades locales, o la explotación de scripts con permisos elevados.

4. Buscar la Bandera (Flag)

Una vez que explotes la vulnerabilidad y ganes acceso, tu objetivo es encontrar la **flag**. Las banderas suelen estar en archivos de texto (como ``flag.txt``) o pueden ser accesibles a través de algún comando. Usa herramientas como **find** o **grep** en la terminal para buscar archivos de texto que puedan contener la bandera:





```
find / -name flag.txt 2>/dev/null
```

O puedes hacer una búsqueda de palabras clave, como “flag”:

```
grep -r "flag" / 2>/dev/null
```

Una vez que encuentres la bandera, deberías ingresarla en el sistema del CTF para completar el desafío.

5. Análisis Forense (si es necesario)

Si las máquinas están configuradas con algún tipo de reto forense (por ejemplo, una máquina comprometida que necesitas analizar), podrías tener que revisar logs, archivos o incluso tráfico de red para encontrar pistas sobre lo que ha pasado y dónde está la bandera.

6. Documenta Tu Proceso

A medida que avanzas, es importante que tomes notas detalladas sobre lo que estás probando, qué técnicas estás usando y los resultados de cada intento. A veces, los CTFs incluyen múltiples etapas, y tener una referencia sobre lo que ya probaste puede ahorrarte tiempo.

Herramientas útiles para este tipo de CTFs:

- **Metasploit:** Para aprovechar vulnerabilidades conocidas.
- **Nmap:** Para escanear puertos y servicios.
- **Burp Suite:** Si tienes aplicaciones web que analizar.
- **Netcat:** Para crear conexiones a máquinas remotas.
- **Nikto:** Para auditoría de servidores web.



- **Gobuster:** Para descubrimiento de directorios en aplicaciones web.

Algunos Consejos:

- **No te desespere:** Los CTFs pueden ser complicados, pero la clave está en ser meticuloso y paciente.
- **Colabora con otros:** Si puedes formar parte de un equipo, ¡hazlo! Los CTFs en equipo pueden ser más fáciles de abordar porque se pueden compartir ideas y estrategias.
- **Aprende de los errores:** A veces, no conseguir resolver algo en un principio es parte del proceso de aprendizaje. Después de un CTF, revisa cómo otros lo resolvieron y busca maneras más eficientes de hacerlo la próxima vez.

¿Te gustaría que te ayude con algún paso específico o alguna técnica que estás tratando de implementar? ¡Avísame si necesitas más detalles o si te atascaste en algún punto!



Genial, quiero probar con nmap, pero no tengo la IP de las máquinas, ¿cómo puedo conseguirlas?



Para obtener las direcciones IP de las máquinas en un CTF, hay varias maneras de hacerlo, dependiendo del entorno en el que estés trabajando. Aquí te dejo algunos métodos comunes que puedes probar para conseguir las IPs de las máquinas que te han dado:



1. Consulta la Información del CTF

En muchos CTFs, las direcciones IP de las máquinas suelen ser proporcionadas al principio del evento, a menudo en el panel de control del CTF o en la plataforma que lo organiza. Revisa cualquier documento o sección de la plataforma CTF donde te hayan dado las instrucciones, ya que allí es donde deberían estar listadas.

2. Revisa tu Red Local

Si las máquinas están dentro de una red local (por ejemplo, en un entorno de laboratorio o una red privada), puedes intentar descubrir las máquinas en la misma red usando herramientas como **nmap** o **arp-scan**. A continuación te explico cómo hacerlo:

- **Usando Nmap para escanear tu red local:** Si no sabes cuál es tu dirección IP o la máscara de red, primero necesitas averiguar tu dirección IP y la red a la que estás conectado.

1. Para averiguar tu IP en Linux o macOS, puedes usar:

```
ifconfig
```

O en Windows:

```
ipconfig
```

2. Una vez que sepas tu IP (supongamos que es `192.168.1.10`), puedes determinar tu red con la siguiente máscara de subred (usualmente es algo como `/24` para redes pequeñas, lo que significa que el rango de IPs sería `192.168.1.1` hasta `192.168.1.255`).
3. Usa **Nmap** para escanear todas las máquinas en tu red. Por ejemplo, si tu red es `192.168.1.0/24`, el comando sería:

```
nmap -sn 192.168.1.0/24
```



Esto realizará un escaneo de **ping** (sin escanear puertos) para ver qué máquinas están activas en esa red.

- **Usando arp-scan:** Si tienes la herramienta **arp-scan** instalada, puedes escanear rápidamente todas las máquinas en tu red local con:

```
sudo arp-scan --localnet
```

Este comando detectará todos los dispositivos activos en tu red local.

3. Revisa el Rango de IPs proporcionado por el CTF

Si el CTF se está ejecutando en una red privada (por ejemplo, en un entorno de laboratorio o en una red privada virtual), a menudo te proporcionarán un rango de IPs del que puedes esperar encontrar las máquinas. Si tienes acceso a un documento o página con la información inicial del CTF, revisa allí si hay un rango de IPs o alguna pista sobre qué máquinas están disponibles.

4. Consulta el Panel del CTF

Si estás participando en una competencia en línea, las máquinas pueden ser parte de un entorno virtualizado o estar en una nube privada. Si ese es el caso, es posible que el panel de control del CTF te dé una lista de direcciones IP de las máquinas disponibles, especialmente si están configuradas para ti y tu equipo.

5. Usar DHCP

Si tienes acceso a un router o servidor DHCP en la red, puedes ver la tabla de asignación de IPs. Esta tabla contiene una lista de todas las IPs que se han asignado a las máquinas en la red. Consulta la interfaz de administración del router o servidor DHCP para obtener esta información.

¿Qué hacer después de obtener las IPs?



Una vez que tengas las direcciones IP de las máquinas, puedes comenzar a escanear las máquinas usando **Nmap**. Si estás trabajando con varias máquinas, puedes escanear todas al mismo tiempo, por ejemplo:

```
nmap -sV 192.168.1.1 192.168.1.2 192.168.1.3
```

O si tienes un rango completo de IPs:

```
nmap -sV 192.168.1.1-254
```

Esto escaneará los puertos abiertos y la versión de los servicios para cada máquina.

Si no encuentras las IPs de inmediato, verifica también con el organizador del CTF o en cualquier material adicional que te hayan proporcionado, como las reglas o la descripción inicial del evento. ¡Buena suerte con tu escaneo y en el CTF! Si tienes alguna otra pregunta o necesitas más detalles, no dudes en decirme.



Ya lo he hecho, las IP's que aparecen seguidas de Virtual Box son las de las máquinas?



¡Sí! Si las direcciones IP que has encontrado están asociadas con **VirtualBox**, es muy probable que esas sean las direcciones IP de las máquinas virtuales que te han asignado para el CTF. Esto suele ocurrir cuando el CTF se ejecuta en un entorno de máquinas virtuales, ya que VirtualBox (y otras plataformas como VMware) permiten configurar redes virtuales dentro de tu computadora para ejecutar las máquinas.

Aquí hay algunos puntos clave que puedes verificar para confirmar que esas IPs son correctas:



1. Comprueba el Entorno de Red en VirtualBox

Las máquinas virtuales en **VirtualBox** generalmente se conectan a través de diferentes tipos de redes virtuales, como "**Red Interna**", "**Adaptador Puente**" o "**Red NAT**". Dependiendo de cómo esté configurada la red de las máquinas, estas IPs pueden ser accesibles desde tu sistema host o solo dentro de la red interna de las máquinas virtuales.

- **Red Interna:** Si las máquinas están configuradas en una red interna, solo podrán "verse" entre ellas. No serán accesibles desde el exterior a menos que uses alguna técnica para "salir" de la red interna, como hacer un **port forwarding** o conectar un adaptador puente.
- **Adaptador Puente:** Si las máquinas están en modo adaptador puente, deberían tener IPs en la misma red que tu computadora host y deberían ser accesibles desde tu red local.
- **Red NAT:** Si las máquinas están en red NAT, sus IPs estarán dentro de un rango privado (usualmente algo como ``10.0.2.x`` o ``192.168.56.x``) y solo podrán acceder a Internet a través de tu máquina host, pero no serán accesibles directamente desde tu red local.

2. Verificación de IPs en VirtualBox

Puedes ingresar a las máquinas virtuales a través de la consola de VirtualBox y ejecutar comandos para verificar sus direcciones IP. Si estás trabajando en una distribución de Linux en las máquinas virtuales, puedes usar el siguiente comando en la terminal de cada máquina:

```
ifconfig
```

O en algunas distribuciones más modernas:

```
ip a
```

Esto te mostrará las direcciones IP que tiene cada máquina dentro de su red virtual.



3. Escaneo de Red

Si ves las IPs asociadas con VirtualBox y crees que son las de las máquinas virtuales, puedes intentar escanear esos rangos de IP con **Nmap** para ver qué puertos están abiertos en esas direcciones. Por ejemplo:

```
nmap -sV 192.168.56.1-254
```

Asegúrate de ajustar el rango de IPs según lo que hayas encontrado en el escaneo inicial.

4. Ping de las IPs

Puedes hacer un **ping** a las IPs que has encontrado para asegurarte de que están activas. Si las máquinas están en la misma red virtual o puente, deberías obtener respuestas a los pings. Si no recibes respuesta, puede ser que la configuración de red esté restringiendo el tráfico entre las máquinas.

```
ping <IP_de_la_maquina>
```

Si las máquinas están configuradas correctamente y las IPs son correctas, deberías poder escanear los puertos con **Nmap** y proceder con el análisis de los servicios y vulnerabilidades.

Resumen:

Si las IPs que has encontrado están asociadas con las máquinas virtuales en **VirtualBox**, es muy probable que esas sean las que debes escanear para resolver el CTF. Asegúrate de revisar la configuración de red en VirtualBox (como "Adaptador Puente", "Red NAT", etc.) para entender cómo están conectadas las máquinas y cómo puedes acceder a ellas desde tu máquina host. Luego, puedes usar **Nmap** o **ping** para verificar que esas máquinas están activas y accesibles.



Si tienes más preguntas sobre cómo proceder o necesitas ayuda con algo más específico en el CTF, ¡aquí estoy!



Bien, una de las IP's es 192.168.1.103, ¿que debo hacer ahora?



¡Genial! Ahora que tienes una IP activa de una máquina virtual (``192.168.1.103``), el siguiente paso es **escanear esa máquina** para obtener más información sobre los servicios que está ejecutando. A partir de ahí, podrás buscar vulnerabilidades y comenzar a trabajar en la explotación del sistema.

Aquí te explico qué pasos puedes seguir:

1. Escaneo de Puertos y Servicios con Nmap

Usa **Nmap** para descubrir qué puertos están abiertos en esa IP y qué servicios están corriendo en esos puertos. Esto te dará información sobre cómo atacar la máquina. Un comando básico sería:

```
nmap -sV 192.168.1.103
```

- **-sV**: Detecta la versión de los servicios que están corriendo en los puertos abiertos.

Esto te mostrará los puertos abiertos y qué servicios están corriendo, así como la versión de cada uno (por ejemplo, si hay un servidor web HTTP en el puerto 80, o si hay un servicio SSH en el puerto 22).

2. Escaneo Completo de Puertos



Si quieres ser más exhaustivo y escanear todos los puertos posibles, puedes hacerlo con:

```
nmap -p- 192.168.1.103
```

Este comando escaneará todos los puertos (del 1 al 65535), lo cual puede tardar más, pero te dará una visión completa de qué servicios están abiertos.

3. Escaneo de Vulnerabilidades con Nmap

También puedes usar **Nmap** con scripts específicos para buscar vulnerabilidades conocidas en los servicios que están corriendo. Si sabes qué servicios están en ejecución, puedes correr un escaneo con scripts de Nmap para buscar vulnerabilidades conocidas. Para hacer esto:

```
nmap --script=vuln 192.168.1.103
```

Este comando usará los scripts de Nmap dedicados a la búsqueda de vulnerabilidades. **Ten en cuenta que este comando puede tardar un poco más**, pero te ayudará a identificar vulnerabilidades comunes que puedes explotar.

4. Identificación de Servicios Web (si hay un servidor web)

Si Nmap detecta que hay un **servidor web** (por ejemplo, en el puerto 80 o 443), puedes intentar acceder a él desde tu navegador o usar herramientas como **curl** para obtener más detalles:

```
curl http://192.168.1.103
```

Esto te permitirá ver si hay algún sitio web vulnerable o algún archivo interesante expuesto.

Si el servidor web está configurado para respuestas encriptadas (HTTPS), puedes intentar:



```
curl https://192.168.1.103
```

5. Explotación de Servicios (si encuentras alguna vulnerabilidad)

Una vez que tengas información sobre los puertos y servicios, puedes empezar a buscar vulnerabilidades en esos servicios. Aquí algunos ejemplos:

- Si encuentras un **servicio web vulnerable** (por ejemplo, una versión de Apache con una vulnerabilidad conocida), puedes buscar exploits específicos en bases de datos como **Exploit-DB** o usar herramientas como **Metasploit**.

Para buscar un exploit de Apache en Metasploit, por ejemplo:

```
msfconsole  
search apache
```

- Si encuentras **SSH** en el puerto 22, puedes intentar un **ataque de fuerza bruta** con herramientas como **Hydra** o **Medusa**, si tienes credenciales débiles o si sabes que el servicio podría estar mal configurado.
- Si hay **puertos de base de datos** (por ejemplo, MySQL en el puerto 3306), puedes intentar realizar **inyección SQL** u otros ataques relacionados.

6. Acceso Remoto (si encuentras credenciales)

Si encuentras credenciales válidas durante el escaneo (por ejemplo, en archivos de configuración expuestos en el servidor web o a través de vulnerabilidades), puedes intentar acceder a la máquina utilizando SSH o a través de una consola web.

Si encuentras un servicio SSH en el puerto 22 y tienes las credenciales correctas, puedes hacer lo siguiente para conectarte:

```
ssh usuario@192.168.1.103
```



Si tienes acceso con un usuario básico, puedes intentar **escalar privilegios** en la máquina.

7. Búsqueda de la Bandera (Flag)

Una vez que tengas acceso, el objetivo es encontrar la bandera. Las banderas suelen estar en archivos de texto ubicados en lugares típicos como:

- `/home/<usuario>/`
- `/root/`
- `/var/www/` (si es un servidor web)
- Archivos específicos como `flag.txt`, `flag1.txt`, etc.

Puedes buscar rápidamente con el comando `find` para buscar archivos que puedan contener la bandera:

```
find / -name "flag*"
```

También puedes buscar en los contenidos de los archivos con **grep**:

```
grep -r "flag" / 2>/dev/null
```

Resumen de los Pasos:

1. **Escanear puertos** con Nmap para obtener información sobre los servicios activos.
2. **Buscar vulnerabilidades** en los servicios encontrados.
3. **Explotar las vulnerabilidades** y ganar acceso a la máquina.
4. **Buscar la bandera** en la máquina comprometida.



Si encuentras alguna vulnerabilidad específica o tienes dudas sobre cómo seguir, no dudes en preguntarme para que te pueda ayudar más detalladamente. ¡Buena suerte y que disfrutes resolviendo el CTF!



La salida que me ha dado es la siguiente: `nmap -p-192.168.1.103`

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 13:04 CET
Nmap scan report for targaryen.home (192.168.1.103)
Host is up (0.0012s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:9C:AC:4D (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 105.87 seconds
```



¡Perfecto! Con la salida que te ha dado **Nmap**, tienes bastante información útil sobre la máquina en la dirección `192.168.1.103`. Aquí está un resumen de lo que descubriste:

- **Puerto 22/tcp: SSH** (Secure Shell), normalmente utilizado para acceder a la máquina de forma remota.
- **Puerto 80/tcp: HTTP** (Servidor web), probablemente un sitio web o aplicación web corriendo en este puerto.
- **Puerto 3306/tcp: MySQL**, un servicio de base de datos que puede estar corriendo en este puerto.



¿Qué hacer a continuación?

Ahora que tienes estos servicios identificados, aquí te dejo un enfoque paso a paso para investigar más a fondo y buscar posibles vulnerabilidades:

1. Explorar el servicio SSH (Puerto 22)

El puerto 22 está abierto para **SSH**, lo que te permite intentar acceder a la máquina de forma remota. Si no tienes credenciales, hay un par de enfoques que podrías intentar:

- **Fuerza bruta de contraseñas:** Si no tienes acceso al servicio SSH pero puedes intentar un ataque de **fuerza bruta** para adivinar la contraseña. Puedes usar herramientas como **Hydra** o **Medusa**.

Ejemplo con **Hydra**:

```
hydra -l usuario -P /ruta/a/tu/wordlist.txt ssh://192.168.1.103
```

Aquí, `-l usuario` especifica el nombre de usuario y `-P` es el archivo de diccionario que contiene posibles contraseñas.

- **Claves SSH predeterminadas:** A veces, los servidores SSH están configurados con contraseñas por defecto o con claves privadas inseguras. Puedes intentar con claves SSH públicas predeterminadas o comprobar si hay algún archivo `.ssh` expuesto en la máquina.

2. Explorar el servicio HTTP (Puerto 80)

El puerto 80 está abierto y está ejecutando **HTTP**, lo que indica que hay un servidor web en funcionamiento. Debes investigar el sitio web alojado en este puerto. Aquí tienes algunas acciones que podrías realizar:



- **Acceder al sitio web en tu navegador:** Solo abre el navegador y visita `http://192.168.1.103` para ver qué se está sirviendo. Revisa si hay alguna vulnerabilidad en la aplicación web (por ejemplo, **inyección SQL**, **Cross-Site Scripting (XSS)**, **Cross-Site Request Forgery (CSRF)**, o cualquier otra debilidad).
- **Escaneo con herramientas como Nikto:** Si el sitio web está funcionando, puedes usar una herramienta como **Nikto** para hacer un escaneo de vulnerabilidades en la web. Aquí hay un ejemplo de cómo usarlo:

```
nikto -h http://192.168.1.103
```

Nikto buscará vulnerabilidades comunes en aplicaciones web, como versiones desactualizadas de software, configuraciones incorrectas, etc.

- **Escaneo de directorios ocultos:** Puedes usar herramientas como **Gobuster** para intentar encontrar directorios y archivos ocultos en el servidor web. Ejemplo de uso:

```
gobuster dir -u http://192.168.1.103 -w /ruta/a/wordlist.txt
```

Esto intentará encontrar directorios y archivos en el servidor web que no están listados en la interfaz principal.

3. Explorar el servicio MySQL (Puerto 3306)

El puerto 3306 está abierto, lo que significa que hay una base de datos **MySQL** corriendo. Si puedes acceder a la base de datos, puedes obtener información importante o incluso obtener credenciales para otros servicios.

- **Conexión a MySQL:** Si tienes credenciales (o puedes obtenerlas mediante un ataque de fuerza bruta o búsqueda de contraseñas débiles), puedes conectarte a la base de datos MySQL con el siguiente comando (usando el cliente MySQL):



```
mysql -u usuario -p -h 192.168.1.103
```

Si no tienes credenciales, puedes intentar realizar un **ataque de fuerza bruta** a la base de datos usando herramientas como **Hydra** o **MySQL-Exploit**.

- **Explorar configuraciones o archivos de la base de datos:** Si puedes acceder a la base de datos, explora las tablas en busca de datos sensibles, como contraseñas o configuraciones de servicios que puedan ser útiles para otros servicios en la máquina.

4. Generalmente (Escalada de Privilegios y Búsqueda de la Bandera)

- Si ya tienes acceso a alguno de estos servicios, como SSH o MySQL, y puedes ejecutar comandos en la máquina, tu siguiente paso es intentar **escalar privilegios** o buscar el archivo de la bandera (`flag.txt` o similar).
- Puedes buscar archivos de texto en la máquina que puedan contener la bandera:

```
find / -name "flag*"
```

O también puedes buscar en los archivos por el contenido de la bandera:

```
grep -r "flag" / 2>/dev/null
```

Resumen de los Pasos a Seguir:

1. **SSH (Puerto 22):** Intenta realizar un ataque de fuerza bruta con **Hydra** si no tienes credenciales.





2. **HTTP (Puerto 80):** Investiga el sitio web, haz escaneos con **Nikto**, y busca directorios con **Gobuster**.
3. **MySQL (Puerto 3306):** Intenta acceder a la base de datos si tienes credenciales o puedes obtenerlas.
4. **Buscar la bandera:** Si tienes acceso, busca archivos como ``flag.txt`` en la máquina.

Si necesitas ayuda para un paso específico o encuentras algo interesante que te gustaría investigar más, no dudes en comentarlo. ¡Estoy aquí para ayudarte!



Si me meto en el puerto 80, en la URL me sale esto:
`https://westeros//` y luego este mensaje de error
Hmm. We're having trouble finding that site.

We can't connect to the server at westeros.

If you entered the right address, you can:

Try again later
Check your network connection
Check that Firefox has permission to access the web
(you might be connected but behind a firewall)



Parece que al acceder a ``https://westeros/`` en el puerto 80, el servidor web no está respondiendo correctamente. El error que mencionas sugiere que el servidor no puede resolver el nombre de host "**westeros**" a una dirección IP válida. Esto podría indicar varias cosas, y hay varias maneras de investigarlo y proceder.

Posibles causas del problema y pasos a seguir:

1. El sitio web podría estar configurado con un nombre de host no resolvable



Es posible que el servidor web esté configurado para responder a un nombre de dominio o nombre de host específico, pero en tu máquina local no puedes resolver ese nombre correctamente (por ejemplo, el nombre "westeros" podría no estar en el archivo `hosts` o no tener un servidor DNS que lo resuelva).

Solución: Modificar el archivo `hosts` en tu máquina local

Puedes agregar una entrada en el archivo `hosts` de tu sistema para forzar que el nombre "westeros" apunte a la IP del servidor (`192.168.1.103`), lo que te permitiría acceder a la web aunque el servidor no tenga un DNS configurado correctamente.

- **En Linux/macOS:** Abre el archivo `/etc/hosts` con un editor de texto como `nano` o `vim` con privilegios de superusuario:

```
sudo nano /etc/hosts
```

Luego agrega la siguiente línea al final del archivo:

```
192.168.1.103 westeros
```

Guarda el archivo y cierra el editor. Ahora deberías poder acceder a `https://westeros/` desde tu navegador.

- **En Windows:** El archivo `hosts` está en `C:\Windows\System32\drivers\etc\hosts`. Ábrelo con un editor de texto (como Notepad) con privilegios de administrador y agrega la línea:

```
192.168.1.103 westeros
```

Guarda los cambios y luego intenta acceder a la URL nuevamente.

2. Comprobar si el servidor web está activo en ese nombre de host

Si la IP está correctamente configurada en el archivo `hosts` y el problema persiste, es posible que el servidor web realmente no esté configurado para responder correctamente o que haya un problema con el servicio web en esa máquina.



Solución: Verificar el estado del servidor web

- Si tienes acceso SSH (por ejemplo, al puerto 22) o acceso al sistema, puedes intentar reiniciar el servidor web o verificar si está activo.

En una máquina basada en Linux, puedes usar el siguiente comando para comprobar el estado de **Apache** (si es lo que está usando el servidor web) o

Nginx:

- Para **Apache:**

```
sudo systemctl status apache2
```

- Para **Nginx:**

```
sudo systemctl status nginx
```

Si el servicio está detenido, puedes reiniciarlo con:

```
sudo systemctl restart apache2
```

O

```
sudo systemctl restart nginx
```

3. Verificar si hay redirección o configuración extraña en el servidor

A veces, los servidores web pueden tener redirecciones o configuraciones inusuales que pueden causar errores de conexión. Para investigarlo más a fondo, puedes intentar acceder directamente a la IP en lugar de usar el nombre de host ``westeros``, para ver si la página se carga sin el problema de resolución de nombres.

- Accede a ``https://192.168.1.103`` directamente en tu navegador para ver si el sitio responde correctamente sin usar el nombre de host.

4. Uso de herramientas de diagnóstico (Curl, Telnet, etc.)





Si no puedes acceder al sitio a través del navegador, puedes usar **curl** desde la terminal para obtener más detalles de lo que está pasando con la conexión:

```
curl -v https://192.168.1.103
```

Esto te dará más información sobre la conexión y posibles redirecciones o errores.

También puedes intentar hacer un **ping** a la máquina para asegurarte de que está en línea y accesible:

```
ping 192.168.1.103
```

Resumen de lo que puedes hacer:

1. **Modifica el archivo `hosts` en tu máquina local** para que `westeros` apunte a `192.168.1.103` (si no lo has hecho ya).
2. **Accede directamente a la IP `https://192.168.1.103`** en tu navegador y verifica si hay alguna respuesta.
3. Si tienes acceso a la máquina, **verifica el estado del servidor web** y reinícialo si es necesario.
4. **Usa `curl`** para obtener más detalles del problema o usa herramientas como **telnet** para verificar si el puerto 80 está activo correctamente.

Si todo esto no resuelve el problema o necesitas ayuda en alguno de los pasos, avísame y con gusto te ayudo más a fondo. ¡Sigue avanzando, que estás muy cerca!



Ahora puedo ver la web. No hay nada con lo que pueda interactuar, pero aparecen lo que parecen ser nombres



de usuario en la web y son los siguientes: daemont, jacaerys, rhaenys, otto, alicent, aemond



¡Excelente! Ahora que tienes acceso al sitio web y puedes ver los **nombres de usuario** listados en la página, eso es una pista importante. Los nombres de usuario suelen ser clave para la autenticación, ya sea en servicios de inicio de sesión, bases de datos o sistemas internos. Aquí tienes algunas formas de seguir avanzando:

1. Intentar iniciar sesión en el servicio SSH (Puerto 22)

Dado que ya sabes que hay un servicio SSH corriendo en el puerto 22, lo primero que puedes intentar es usar estos nombres de usuario para ver si hay credenciales débiles o predeterminadas.

Si no tienes una lista de contraseñas, puedes intentar con **contraseñas comunes** o utilizar una **herramienta de fuerza bruta** para probar varias combinaciones con **Hydra**.

Por ejemplo, si intentas usar **Hydra** para realizar un ataque de fuerza bruta con el nombre de usuario ``daemont`` (y luego los demás), puedes utilizar un diccionario de contraseñas comunes:

```
hydra -l daemont -P /ruta/a/wordlist.txt ssh://192.168.1.103
```

- **-l daemont:** Especifica el nombre de usuario.
- **-P /ruta/a/wordlist.txt:** Usas un diccionario de contraseñas para probar combinaciones.
- **ssh://192.168.1.103:** La dirección IP de la máquina de destino con el servicio SSH.

Repite este proceso para los demás usuarios, como ``jacaerys``, ``rhaenys``, ``otto``, etc., con tu diccionario de contraseñas.



Si no tienes un diccionario de contraseñas, puedes descargar uno común de sitios como **SecLists** en GitHub.

2. Explorar las posibles rutas de ataque en el servidor web

A pesar de que el sitio web no tiene interactividad, los nombres de usuario listados podrían estar asociados a alguna funcionalidad web o base de datos. Aquí tienes algunas ideas:

- **Formularios de inicio de sesión (en el frontend o en el backend):** Aunque no veas un formulario de inicio de sesión, puede que el servidor esté esperando peticiones específicas. Usa herramientas como **Burp Suite** para interceptar las peticiones y ver si hay alguna forma de enviar peticiones con esos nombres de usuario, o si la web realiza algún tipo de **autenticación**.
- **Inyección SQL:** Si el sitio está conectado a una base de datos MySQL, podrías intentar hacer una **inyección SQL** en los formularios del sitio web o en las barras de búsqueda (si existen). Si puedes encontrar alguna vulnerabilidad en la web, podrías obtener acceso directo a la base de datos y obtener credenciales de usuario o más información sensible.
- **Revisar URLs adicionales o archivos ocultos:** A veces, los sitios web tienen rutas o archivos secretos que no se muestran en la interfaz. Puedes usar **Gobuster** o **Dirb** para buscar directorios y archivos ocultos en el servidor web.

Ejemplo con **Gobuster**:

```
gobuster dir -u http://192.168.1.103 -w /ruta/a/wordlist.txt
```

Esto intentará encontrar directorios y archivos en el servidor.



3. Revisar la base de datos MySQL (Puerto 3306)

Dado que también tienes abierto el puerto **3306 (MySQL)**, puede que los nombres de usuario estén almacenados en la base de datos. Si puedes obtener acceso a MySQL, podrías extraer estos nombres de usuario y otros detalles de la base de datos.

- Intenta conectarte a MySQL con un cliente (por ejemplo, con **MySQL Workbench** o desde la línea de comandos):

```
mysql -u root -p -h 192.168.1.103
```

- Si logras acceder, puedes listar las bases de datos y buscar tablas que contengan usuarios o contraseñas. Comienza por listar las bases de datos:

```
SHOW DATABASES;
```

Luego, selecciona una base de datos e inspecciona las tablas:

```
USE nombre_de_base_de_datos;  
SHOW TABLES;
```

Una vez dentro de las tablas, puedes buscar información relacionada con los usuarios, como contraseñas.

```
SELECT * FROM nombre_de_tabla;
```

4. Verificación de posibles vulnerabilidades de la web

Como mencionamos antes, si tienes un servicio web vulnerable (como una versión desactualizada de Apache o algún CMS vulnerable), podrías encontrar una **vulnerabilidad conocida** para explotarla.



- Usa herramientas como **Nikto** para escanear el servidor web en busca de vulnerabilidades comunes:

```
nikto -h http://192.168.1.103
```

- Si encuentras alguna vulnerabilidad conocida, podrías usar un **exploit** para obtener acceso, como por ejemplo a través de **Metasploit**.

5. Buscar la bandera

Si logras acceder a algún servicio (SSH, MySQL o incluso la web), recuerda siempre buscar **la bandera**. Usualmente, la bandera se encuentra en lugares como:

- `~/home/<usuario>/``
- `~/root/``
- `~/var/www/`` (si es un servidor web)
- Archivos específicos como `flag.txt``

Si tienes acceso a la máquina, usa `find`` para buscar archivos de la bandera:

```
find / -name "flag*"
```

O usa **grep** para buscar dentro de los archivos:

```
grep -r "flag" / 2>/dev/null
```

Resumen:



- **SSH:** Intenta usar los nombres de usuario para un ataque de fuerza bruta (con **Hydra**).
- **Explorar el servidor web:** Usa herramientas como **Burp Suite**, **Gobuster** y **Nikto** para explorar más a fondo.
- **MySQL:** Si tienes acceso, busca usuarios y contraseñas en la base de datos.
- **Buscar la bandera:** Si accedes a algún sistema, busca archivos que puedan contener la bandera (``flag.txt``).

Si tienes alguna pregunta sobre algún paso específico o necesitas más ayuda, ¡avísame!



Vale pero, ¿qué wordlist puedo usar?



Existen varias **wordlists** muy comunes y útiles que puedes utilizar para ataques de fuerza bruta o pruebas de contraseñas, y muchas de ellas están disponibles de forma gratuita. Aquí te doy algunas opciones que puedes usar:

1. Wordlist de SecLists

SecLists es uno de los repositorios más conocidos de listas de palabras, y contiene una gran cantidad de diccionarios para todo tipo de ataques (contraseñas, nombres de usuario, directorios, etc.).

Puedes descargar **SecLists** desde GitHub:

- [SecLists en GitHub](#)

Una vez descargado el repositorio, encontrarás una gran variedad de listas dentro de la carpeta ``SecLists/Passwords/`` que puedes utilizar para ataques de contraseñas.

Ejemplo:





Si solo quieres una lista de contraseñas comunes, puedes utilizar `rockyou.txt`, que es un diccionario de contraseñas muy común y grande:

```
/ruta/a/SecLists/Passwords/Leaked-Databases/rockyou.txt
```

Esta lista contiene contraseñas comunes que han sido filtradas en brechas de seguridad y que son muy utilizadas, por lo que puede ser útil para adivinar contraseñas débiles.

2. Wordlist de "Rockyou"

rockyou.txt es uno de los diccionarios más famosos, que contiene millones de contraseñas filtradas que podrían estar en uso en muchos sistemas.

- En muchos sistemas de pruebas, como **Kali Linux**, la **wordlist de rockyou** ya está incluida en el directorio `~/usr/share/wordlists/rockyou.txt.gz`.

Si la tienes en tu máquina, solo tienes que descomprimirla primero:

```
gunzip /usr/share/wordlists/rockyou.txt.gz
```

Luego, ya puedes usarla para ataques de fuerza bruta.

Ejemplo con Hydra:

```
hydra -l daemont -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.103
```

3. Wordlists personalizadas

Si ya conoces algo sobre la máquina (por ejemplo, nombres de usuario, nombres comunes de la red, o términos relacionados con el tema del CTF), puedes crear tu propia **wordlist personalizada**. Esto podría aumentar tus posibilidades de éxito al usar un diccionario más específico.



Un ejemplo sencillo para crear una **wordlist personalizada** sería:

```
echo "password123" > mywordlist.txt
echo "letmein" >> mywordlist.txt
echo "welcome" >> mywordlist.txt
```

También puedes combinar varias listas para crear una más robusta:

```
cat /usr/share/wordlists/rockyou.txt /ruta/a/tu/custom_wordlist.txt >
combined_wordlist.txt
```

4. Otras wordlists útiles:

- **Small wordlist:** Si el sistema tiene restricciones de longitud en las contraseñas, tal vez prefieras una lista pequeña, como la que se encuentra en ``/usr/share/wordlists/dirb/common.txt`` en Kali Linux.
- **Lista de nombres comunes:** Si el CTF hace uso de nombres de personajes históricos, de la cultura popular, o si tiene algo que ver con la temática de "**Juego de Tronos**" (como los usuarios que mencionaste: ``daemont``, ``rhaenys``, ``alicient``, etc.), puedes buscar listas de nombres comunes o incluso utilizar listas temáticas como:

```
/ruta/a/SecLists/Passwords/Names/first_names.txt
```

¿Cómo elegir una buena wordlist?

- **Diccionarios grandes (como rockyou.txt):** Estos son útiles cuando no tienes pistas sobre la complejidad de la contraseña, pero el proceso puede llevar tiempo.
- **Diccionarios pequeños y específicos:** Si tienes pistas sobre el tema o las contraseñas, puedes usar una lista más pequeña o personalizada que contenga



nombres comunes, temas específicos, o combinaciones relacionadas con el objetivo del CTF.

Uso de wordlists con Hydra o Medusa:

Usar una wordlist con **Hydra** o **Medusa** es sencillo. Aquí hay un ejemplo con una wordlist como **rockyou.txt**:

Hydra:

```
hydra -l daemont -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.103
```

- **-l daemont**: El nombre de usuario a probar.
- **-P /usr/share/wordlists/rockyou.txt**: La ruta de la wordlist con las contraseñas posibles.
- **ssh://192.168.1.103**: El servicio al que quieres atacar (en este caso, SSH).

Medusa:

Si prefieres usar **Medusa**, el comando sería:

```
medusa -h 192.168.1.103 -u daemont -P /usr/share/wordlists/rockyou.txt -M ssh
```

- **-h**: Dirección IP de la máquina de destino.
- **-u**: Usuario.
- **-P**: Ruta a la wordlist de contraseñas.
- **-M ssh**: Módulo de **SSH**.

Conclusión:



- Si no tienes una **wordlist** todavía, empieza con **rockyou.txt** o una lista de **SecLists**.
- Usa herramientas como **Hydra** o **Medusa** para realizar ataques de fuerza bruta.
- Si tienes pistas sobre los nombres de los usuarios (como los que encontraste en la web), prueba con listas de nombres comunes o temáticas.

Si necesitas ayuda con alguno de los pasos o necesitas más recomendaciones, ¡dímelo!



La salida de hydra ha sido: hydra -l daemont -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.103

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-03-08 13:21:12

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task

[DATA] attacking ssh://192.168.1.103:22/

[22][ssh] host: 192.168.1.103 login: daemont password: mylove

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 3 final worker threads did not complete until end.

[ERROR] 3 targets did not resolve or could not be connected

[ERROR] 0 target did not complete





Hydra (<https://github.com/vanhauser-thc/thc-hydra>)
finished at 2025-03-08 13:21:44



¡Genial! Parece que **Hydra** ha tenido éxito en encontrar una contraseña válida para el usuario **daemont** en el servicio SSH. Según la salida que proporcionas, la contraseña que ha encontrado es:

```
mylove
```

¿Qué puedes hacer ahora?

1. **Conectarte por SSH:** Ahora que tienes la contraseña, puedes intentar conectarte a la máquina a través de SSH con el siguiente comando:

```
ssh daemont@192.168.1.103
```

Luego te pedirá la contraseña, y deberías poder iniciar sesión usando ``mylove``.

2. **Buscar la bandera:** Una vez que estés dentro de la máquina, el siguiente paso es buscar la **bandera**. La bandera usualmente está en un archivo de texto y puede estar en directorios como:

- ``/home/daemont/``
- ``/root/``
- ``/var/www/``
- ``/tmp/``

Para buscar archivos que puedan contener la bandera, puedes usar el comando ``find``:

```
find / -name "flag*" 2>/dev/null
```



O si sabes que la bandera tiene un formato específico (por ejemplo, "flag{...}"), puedes hacer una búsqueda con **grep**:

```
grep -r "flag" / 2>/dev/null
```

3. **Explorar el sistema:** Además de buscar la bandera, podrías querer explorar el sistema para obtener más información o puntos de entrada adicionales. Por ejemplo, puedes listar los archivos en el directorio de inicio:

```
ls -la /home/daemont/
```

O explorar directorios comunes como `/etc/`, `/var/log/`, `/tmp/`, y otros donde podrían haber archivos interesantes.

4. **Verificar si hay otros usuarios:** Si necesitas investigar otros usuarios (como `jacaerys`, `rhaenys`, etc.), puedes ver el archivo `/etc/passwd` para obtener más detalles sobre ellos:

```
cat /etc/passwd
```

Y si encuentras otros usuarios, puedes intentar el mismo proceso con sus nombres para ver si puedes obtener acceso a sus cuentas.

Resumen:

- Ya tienes acceso al sistema con el usuario **daemont** y la contraseña **mylove**.
- Ahora puedes **explorar el sistema**, **buscar la bandera**, y obtener más información sobre la máquina.

Si encuentras algún problema o necesitas ayuda para explorar la máquina, ¡avísame y te puedo guiar más!



He hecho lo que me has indicado con el resto de los usuarios y he conseguido el resto de contraseñas. ¿Puedes indicarme cómo moverme por el sistema o algunos comandos básicos?



¡Qué bien que hayas conseguido todas las contraseñas! Ahora que tienes acceso a la máquina, es importante saber cómo moverte por el sistema y explorar de manera eficiente. Aquí tienes una lista de comandos básicos y consejos sobre cómo navegar en una máquina Linux desde la línea de comandos.

Comandos básicos para moverse por el sistema

1. Comandos para navegar por el sistema de archivos

- **Ver el directorio actual:**

```
pwd
```

Esto te muestra el directorio de trabajo actual (el directorio en el que te encuentras).

- **Listar archivos y directorios:**

```
ls
```

Esto lista los archivos y directorios en el directorio actual. Si quieres ver más detalles, como permisos y fechas de modificación, puedes usar:

```
ls -la
```

- **Cambiar de directorio:** Para ir a un directorio específico:



```
cd /ruta/del/directorio
```

O para ir a un directorio padre:

```
cd ..
```

Para ir al directorio de inicio del usuario:

```
cd ~
```

- **Ver el contenido de un archivo:** Si encuentras un archivo y quieres ver su contenido, puedes usar:

```
cat nombre_del_archivo
```

También puedes usar **less** o **more** para navegar por archivos largos:

```
less nombre_del_archivo
```

less permite desplazarse hacia arriba y hacia abajo por el archivo.

2. Comandos para gestionar archivos y directorios

- **Copiar archivos:**

```
cp archivo_origen archivo_destino
```

- **Mover o renombrar archivos:**

```
mv archivo_origen archivo_destino
```

- **Eliminar archivos:**

```
rm nombre_del_archivo
```




Si quieres eliminar un directorio y todo su contenido, usa:

```
rm -rf nombre_del_directorio
```

- **Crear un directorio:**

```
mkdir nombre_del_directorio
```

- **Crear un archivo vacío:**

```
touch nombre_del_archivo
```

3. Buscar archivos o texto

- **Buscar archivos:** Para buscar un archivo por su nombre:

```
find / -name "nombre_del_archivo" 2>/dev/null
```

Esto buscará en todo el sistema, y `2>/dev/null` es para evitar que se muestren los errores de permisos.

- **Buscar texto dentro de archivos:** Si estás buscando un texto específico dentro de archivos (por ejemplo, una bandera o una palabra clave), puedes usar **grep**:

```
grep -r "texto_a_buscar" /ruta/del/directorio
```

Esto buscará el texto dentro de todos los archivos de un directorio.

4. Gestionar procesos y usuarios

- **Ver los procesos en ejecución:**

```
ps aux
```

O para verlos en tiempo real:



```
top
```

- **Terminar un proceso:** Si necesitas matar un proceso, primero obtén el PID con ``ps`` o ``top``, y luego usa:

```
kill <PID>
```

- **Ver información sobre el sistema:** Para obtener información básica del sistema, como el nombre del kernel, la arquitectura, etc.:

```
uname -a
```

- **Ver quién está conectado al sistema:**

```
who
```

- **Ver el archivo de log de autenticación** (para posibles intentos de login o actividades sospechosas):

```
cat /var/log/auth.log
```

Comandos avanzados para investigar

- **Ver la configuración de la red:** Para ver las interfaces de red y sus configuraciones:

```
ifconfig
```

O si tu sistema usa **iproute2**:

```
ip a
```



- **Ver información sobre las particiones de disco:**

```
df -h
```

- **Ver los logs del sistema:** Los logs pueden ser una gran fuente de información, y muchos CTFs almacenan pistas en los archivos de logs:

```
cat /var/log/syslog
```

- **Ver información sobre el usuario actual:**

```
whoami
```

- **Ver las contraseñas almacenadas en el sistema** (si tienes privilegios de root o permisos sobre ciertos archivos):

```
cat /etc/passwd  
cat /etc/shadow
```

Escalar privilegios (si es necesario)

Si el objetivo es **escalar privilegios** (obtener acceso de root o de un usuario privilegiado), hay algunas técnicas que puedes intentar:

1. **Revisar permisos de sudo:** Ver si el usuario tiene privilegios `sudo` para ejecutar comandos como root:

```
sudo -l
```

2. **Buscar configuraciones o vulnerabilidades:** Si tienes privilegios limitados, podrías buscar archivos mal configurados o vulnerabilidades que permitan escalar privilegios. Un comando útil es:



```
find / -name "sudo" 2>/dev/null
```

3. **Revisar el archivo `sudoers`**: Si tienes permisos de lectura sobre el archivo `/etc/sudoers`, puedes ver si hay configuraciones que permitan ejecutar comandos como root sin necesidad de contraseña:

```
cat /etc/sudoers
```

Resumen

- **Navegar por el sistema:** Usa `cd`, `ls`, `pwd` para moverte por los directorios.
- **Gestionar archivos:** Usa `cp`, `mv`, `rm`, `mkdir`, y `touch` para gestionar archivos y directorios.
- **Buscar:** Usa `find` y `grep` para buscar archivos y texto dentro del sistema.
- **Gestionar procesos y ver logs:** Usa `ps aux`, `top`, y `cat /var/log/*` para investigar lo que está sucediendo en el sistema.
- **Escalar privilegios:** Revisa los permisos de `sudo` o busca posibles configuraciones maliciosas para escalar privilegios.

Si necesitas ayuda con algún comando o tienes preguntas específicas, ¡dime y con gusto te ayudo más!



Al moverme he descubierto que hay dos usuarios que no estaban antes, raenyra y otto, he probado a usar hydra con rockyou.txt pero no he obtenido ningún resultado. También observando archivos del usuario daemont y otto he encontrado un mensaje que decía que debían cifrar las contraseñas de una base de





datos, y además, otro archivo con lo que parecen ser muchas contraseñas. ¿Cómo puedo continuar?



¡Parece que has hecho buenos avances! El hecho de que hayas encontrado un mensaje sobre cifrar contraseñas de una base de datos y un archivo con muchas contraseñas podría ser una pista importante. Aquí te ofrezco algunos pasos a seguir para continuar en tu investigación.

Posibles pasos a seguir

1. Investigar el archivo con muchas contraseñas

Si has encontrado un archivo con muchas contraseñas, probablemente sea una lista o una base de datos con contraseñas sin cifrar. Puedes intentar examinar este archivo para ver si contiene contraseñas o pistas adicionales que puedan estar relacionadas con los usuarios **raenyra** y **otto**.

Para ver el contenido del archivo:

```
cat nombre_del_archivo
```

Si el archivo contiene muchas contraseñas y no puedes leerlas fácilmente, puedes intentar filtrarlas con **grep** o exportarlas a otro archivo para analizarlas más tarde:

```
grep -i "palabra_clave" nombre_del_archivo
```

Esto buscará una palabra clave en todo el archivo (por ejemplo, "raenyra" o "otto" si tienes alguna pista).

2. Explorar el mensaje sobre cifrado de contraseñas

El mensaje sobre cifrar contraseñas de una base de datos es bastante interesante. Puede ser una pista de que las contraseñas que necesitas son **cifradas** y que



necesitas encontrar una forma de descifrarlas o de obtener acceso a la base de datos en cuestión.

- **Cifrado de contraseñas:** Si el archivo que has encontrado contiene contraseñas cifradas (por ejemplo, con cifrado **bcrypt**, **md5**, **sha256**), necesitarás una forma de descifrarlas. Si no se proporciona un algoritmo de cifrado claro, algunas bases de datos suelen usar **hashes de contraseñas**.

Para verificar si el archivo contiene hashes, puedes buscar cadenas que tengan un formato de hash común, como:

- **bcrypt:** Una cadena que comienza con ``$2a$`, `$2b$` o `$2y$``.
- **MD5:** Un hash de 32 caracteres hexadecimales.
- **SHA-1:** Un hash de 40 caracteres hexadecimales.
- **SHA-256:** Un hash de 64 caracteres hexadecimales.

Ejemplo de cómo buscar hashes en el archivo:

```
grep -E '[a-f0-9]{32}$' nombre_del_archivo # Para hashes MD5
grep -E '[a-f0-9]{40}$' nombre_del_archivo # Para hashes SHA-1
```

Si encuentras que las contraseñas están cifradas (por ejemplo, con **bcrypt** o **md5**), puedes intentar usar herramientas como **John the Ripper** o **Hashcat** para intentar descifrarlas.

3. Interacción con la base de datos

Si el archivo se refiere a contraseñas dentro de una base de datos, podría ser útil explorar cómo acceder a esa base de datos. Como en tu escaneo inicial con **nmap**, has detectado que el puerto **3306** está abierto, lo que indica que hay un servidor **MySQL** corriendo en la máquina.

Podrías intentar interactuar con la base de datos **MySQL** utilizando el comando ``mysql`` en la terminal:



```
mysql -h 192.168.1.103 -u usuario -p
```

Si tienes acceso, se te pedirá la contraseña. Si aún no has probado con los usuarios **raenyra** o **otto**, intenta iniciar sesión con sus credenciales.

Otra opción es intentar acceder sin contraseña, en caso de que el usuario tenga permisos de acceso sin contraseña configurados:

```
mysql -h 192.168.1.103 -u raenyra
```

Si logras acceder, puedes ejecutar consultas SQL para obtener información sobre las contraseñas almacenadas o cualquier dato relevante:

```
SHOW DATABASES;  
USE nombre_de_base_de_datos;  
SHOW TABLES;
```

Explora las tablas dentro de la base de datos que encuentres. En muchos CTFs, las contraseñas de los usuarios o las "banderas" pueden estar dentro de una tabla llamada `users` o algo similar.

4. Intentar otros métodos de autenticación

Si tienes alguna pista sobre cómo las contraseñas podrían estar relacionadas con la base de datos (por ejemplo, el uso de algún hash), puedes probar diferentes herramientas o enfoques para interactuar con el sistema.

Si sospechas que las contraseñas están cifradas (por ejemplo, en hash MD5 o bcrypt) y no puedes descifrarlas fácilmente, las herramientas que podrías usar incluyen:

- **John the Ripper:** Es una de las mejores herramientas para **cracking** de contraseñas. Puedes usarla para intentar descifrar los hashes de contraseñas.
- **Hashcat:** Otra herramienta muy poderosa para hacer cracking de contraseñas, especialmente cuando las contraseñas están en hashes.



Si encuentras que las contraseñas están cifradas en **bcrypt**, **md5**, o **sha256**, puedes intentar usar estos comandos con **John the Ripper** para romper los hashes:

Para hashes bcrypt con John the Ripper:

```
john --format=bcrypt nombre_del_archivo_con_hashes
```

Para hashes md5 con John the Ripper:

```
john --format=raw-md5 nombre_del_archivo_con_hashes
```

5. Explorar otros posibles archivos de configuración

Asegúrate de revisar cualquier archivo de configuración que pueda estar relacionado con la base de datos, como archivos que contengan credenciales de acceso a MySQL. Estos archivos a veces están en rutas como `/etc/`, `/var/www/`, o incluso en el directorio personal de un usuario (por ejemplo, `/home/daemon/`).

Busca archivos con nombres que incluyan palabras clave como `config`, `db`, `database`, `credentials`, `mysql`, etc. Usar el comando **grep** también es útil aquí:

```
grep -i "mysql" /home/daemon/*
```

Resumen de lo que puedes hacer a continuación

- **Revisar el archivo con las contraseñas** y buscar si hay hashes (MD5, SHA, bcrypt) o contraseñas claras.
- **Interaccionar con la base de datos MySQL** usando las credenciales de los usuarios o buscando alguna pista sobre la contraseña de la base de datos.
- **Usar herramientas de cracking** como **John the Ripper** o **Hashcat** si encuentras contraseñas cifradas en el archivo.



- **Buscar más archivos** que puedan contener configuraciones o información adicional sobre la base de datos o los usuarios.

Si tienes más pistas o detalles, ¡dímelo! Te puedo guiar con más pasos específicos.



Las contraseñas de la lista no están cifradas, ¿las uso entonces en mysql?



¡Entendido! Si las contraseñas en la lista no están cifradas, eso significa que son **contraseñas en texto claro** y puedes usarlas directamente para acceder a las cuentas de **MySQL**.

Pasos para usar las contraseñas con MySQL:

1. **Probar con el usuario `raenyra`:** Dado que has encontrado varias contraseñas, la siguiente lógica sería intentar acceder a la base de datos **MySQL** usando el nombre de usuario y las contraseñas que has encontrado en la lista.

Usa el comando de **MySQL** para intentar acceder como el usuario `raenyra` o `otto` (o cualquier otro que hayas encontrado):

```
mysql -h 192.168.1.103 -u raenyra -p
```

Luego, cuando te pida la contraseña, ingresa la contraseña que has encontrado para `raenyra`.

2. **Acceder a la base de datos:** Si consigues iniciar sesión, deberías poder explorar las bases de datos de la máquina. Para hacerlo, usa los siguientes comandos SQL:

```
SHOW DATABASES;
```





Esto te mostrará todas las bases de datos disponibles. Una vez que tengas la lista, el siguiente paso es elegir una base de datos y explorarla. Por ejemplo, si ves una base de datos llamada ``users`` o algo similar, puedes usarla de la siguiente manera:

```
USE users;
```

Luego, puedes ver las tablas dentro de esa base de datos:

```
SHOW TABLES;
```

3. **Buscar contraseñas o banderas:** Si encuentras una tabla que podría contener información importante, como contraseñas o datos relacionados con los usuarios, puedes mostrar el contenido de esa tabla. Por ejemplo:

```
SELECT * FROM users;
```

Esto te dará una lista de todos los registros en la tabla ``users`` (si existe). Si la base de datos está bien configurada, podrías encontrar contraseñas en texto claro o alguna pista adicional.

4. **Buscar posibles banderas:** Si no encuentras banderas directamente en las tablas de la base de datos, es posible que necesites revisar otras tablas, o incluso los registros de las bases de datos que contienen datos de configuraciones o logs.

Además, si encuentras algún texto que se parezca a una **bandera** (por ejemplo, una cadena como ``flag{...}``), ya estarás muy cerca de resolver el reto.

Resumen de pasos:

- **Iniciar sesión en MySQL** con las contraseñas en texto claro usando el comando ``mysql -u usuario -p``.
- **Explorar las bases de datos y tablas** para buscar información relevante (como contraseñas o banderas).



- **Buscar la bandera** en las tablas si encuentras alguna pista.

Si tienes más dudas o no puedes acceder a la base de datos con las contraseñas, dímelo y buscaremos otra solución. ¡Ánimo!



He usado hydra y no funcionan para el usuario raenyra pero sí para otto. Concretamente la contraseña h43l3n4:), ahora, ¿cómo entro en mysql?



¡Perfecto! Ahora que tienes la contraseña para el usuario **otto** (que es `h43l3n4:)`), puedes acceder a **MySQL** como ese usuario y explorar la base de datos.

Pasos para acceder a MySQL con el usuario otto:

1. **Acceder a MySQL con el usuario `otto`:** Abre una terminal y usa el siguiente comando para acceder a **MySQL** como el usuario **otto**:

```
mysql -h 192.168.1.103 -u otto -p
```

Después de ejecutar el comando, te pedirá la contraseña. Ingresa `h43l3n4:)` como contraseña.

2. **Explorar las bases de datos:** Una vez que hayas iniciado sesión, puedes comenzar a explorar las bases de datos disponibles con el siguiente comando SQL:

```
SHOW DATABASES;
```





Esto te mostrará una lista de las bases de datos en el servidor MySQL. Busca bases de datos que podrían tener nombres relacionados con los usuarios, contraseñas o configuraciones.

3. **Seleccionar una base de datos:** Cuando encuentres una base de datos interesante, puedes seleccionarla para empezar a explorar las tablas dentro de ella. Por ejemplo, si hay una base de datos llamada ``users`` o algo similar, selecciona esa base de datos con:

```
USE nombre_de_base_de_datos;
```

4. **Ver las tablas dentro de la base de datos:** Una vez dentro de la base de datos, usa el siguiente comando para ver las tablas que contiene:

```
SHOW TABLES;
```

Esto te mostrará todas las tablas dentro de esa base de datos. Las tablas que podrían contener contraseñas o información relevante para un CTF suelen llamarse ``users``, ``accounts``, ``login``, etc.

5. **Ver los registros en una tabla:** Si encuentras una tabla interesante (por ejemplo, ``users`` o algo relacionado), puedes ver el contenido de esa tabla con:

```
SELECT * FROM nombre_de_la_tabla;
```

Esto te mostrará todos los registros de la tabla. Si la tabla contiene contraseñas o información relevante, podrías encontrar pistas o incluso una **bandera**.

Resumen:

1. Accede a MySQL como **otto**:



```
mysql -h 192.168.1.103 -u otto -p
```

Luego ingresa la contraseña ``h4313n4:)``.

2. Explora las bases de datos con ``SHOW DATABASES;``.
3. Selecciona una base de datos con ``USE nombre_de_base_de_datos;``.
4. Lista las tablas con ``SHOW TABLES;`` y busca tablas relevantes.
5. Consulta las tablas con ``SELECT * FROM nombre_de_tabla;``.

Si encuentras algo interesante o necesitas más ayuda con consultas SQL o exploración de la base de datos, ¡avísame!



He obtenido esto: MySQL [proyecto_westeros]> select *
from Usuario;

```
+-----+-----+-----+-----+-----+
-----+
| idUsuario | nombreUsuario | email |
contraseña |
+-----+-----+-----+-----+-----+
-----+
| 1 | raenyra | raenyrareina@westeros.com |
| syrax44 |
| 2 | daemont |
daemonelcanalla@westeros.com | mylove |
| 3 | jacaerys | jaceelguapo@westeros.com |
| tigger |
| 5 | rhaenys |
rhaenyslaquenofue@westeros.com | princess |
| 6 | aegon |
aegonprimervaron@westeros.com | sunfire35 |
| 7 | otto | ottomanoyabuelo@westeros.com |
| poohbear |
| 8 | alicent |
```



```
alicentmadreycreyente@westeros.com | angels |
| 9 | aemon | amondeltuerto@westeros.com
| playboy |
+-----+-----+-----+-----+-----+
-----+
8 rows in set (0.001 sec)
```



¡Genial! Has encontrado una tabla muy útil que contiene los usuarios y sus contraseñas en texto claro. Con esta información, ahora puedes acceder a **MySQL** como cualquier otro usuario, incluyendo el usuario ``raenyra``, que tiene la contraseña ``syrax44``.

Pasos a seguir ahora:

1. **Iniciar sesión como ``raenyra``:** Ahora que tienes la contraseña para ``raenyra`` (``syrax44``), puedes intentar iniciar sesión nuevamente en MySQL, pero esta vez con las credenciales de ``raenyra``. Usa el siguiente comando:

```
mysql -h 192.168.1.103 -u raenyra -p
```

Te pedirá la contraseña, y deberás ingresar ``syrax44``.

2. **Explorar más bases de datos o tablas:** Después de iniciar sesión como **raenyra**, puedes continuar explorando las bases de datos o las tablas que podrían tener más información relevante. Por ejemplo, puedes seguir los mismos pasos de antes para ver qué bases de datos están disponibles y explorar más tablas.

- Para listar las bases de datos:

```
SHOW DATABASES;
```

- Para explorar las tablas dentro de una base de datos específica:





```
USE proyecto_westeros;  
SHOW TABLES;
```

3. **Buscar más pistas o banderas:** Si encuentras más tablas, puedes seguir el mismo proceso para obtener los registros dentro de ellas y buscar pistas o banderas. Si encuentras algo que se asemeje a una bandera (por ejemplo, una cadena como ``flag{...}`` o algo similar), ¡sería el siguiente paso en la resolución del CTF!

Resumen:

- Has encontrado una lista de usuarios con contraseñas en texto claro.
- Usa las credenciales de ``raenyra`` (``syrax44``) para acceder a MySQL como ese usuario.
- Continúa explorando más bases de datos, tablas y registros para buscar más información o banderas.

Si necesitas más ayuda en algún paso o si encuentras algo interesante, ¡avísame!



En mysql no hay nada más, ¿qué puedo hacer con las credenciales de raenyra?



Si ya has explorado la base de datos MySQL y no hay nada más interesante en ese aspecto, pero tienes las credenciales de **raenyra** (usuario y contraseña), lo siguiente sería buscar formas de usar esas credenciales en otros servicios o realizar una exploración más amplia en el sistema. Aquí te dejo algunas opciones que puedes seguir:



1. Iniciar sesión en el sistema con el usuario `raenyra`

Dado que tienes las credenciales para **raenyra**, puedes intentar iniciar sesión directamente en el sistema operativo con ese usuario. Si tienes acceso a un terminal o un entorno de shell, intenta hacer login con `raenyra`.

Usando `su` (switch user): Si estás en el sistema y ya tienes acceso con un usuario como `otto` o `daemont`, puedes intentar cambiar de usuario con `su` y las credenciales de `raenyra`:

```
su raenyra
```

Luego, ingresa la contraseña `syrax44` cuando se te pida. Si tienes éxito, te cambiarás a la cuenta de **raenyra**.

Usando SSH: Si estás accediendo remotamente a la máquina (por ejemplo, usando SSH), puedes intentar iniciar sesión como **raenyra**:

```
ssh raenyra@192.168.1.103
```

Introduce la contraseña `syrax44` cuando se te pida.

2. Explorar los archivos de `raenyra`

Si tienes acceso al sistema con las credenciales de `raenyra`, puedes explorar los archivos en su directorio personal. Los usuarios a menudo tienen archivos de configuración o datos importantes en su directorio.

Puedes explorar el directorio de `raenyra` con los siguientes comandos:

```
cd /home/raenyra  
ls -la
```

Esto te mostrará los archivos ocultos y visibles en el directorio de inicio de **raenyra**. Es común que haya archivos como `.bashrc`, `.ssh/authorized_keys`, o incluso



documentos que podrían contener más pistas.

Si encuentras archivos interesantes, como un archivo con la palabra **flag** o algo similar, examina su contenido con:

```
cat nombre_del_archivo
```

3. Revisar configuraciones de otros servicios

Es posible que el usuario **raenyra** tenga acceso a otros servicios del sistema, como servidores web, servidores de correo, o configuraciones de SSH. Puedes revisar algunos de estos archivos de configuración para ver si contienen información útil.

- **Revisar configuraciones de SSH:** A veces los usuarios tienen acceso a claves SSH, lo que podría permitirte iniciar sesión en otras máquinas o servidores. Puedes revisar si **raenyra** tiene alguna clave SSH en su directorio ``.ssh``:

```
ls /home/raenyra/.ssh
cat /home/raenyra/.ssh/authorized_keys
```

- **Archivos de configuración del servidor web:** Si la máquina tiene un servidor web corriendo en el puerto 80 (como lo vimos al principio en el escaneo con **nmap**), puedes intentar encontrar configuraciones relevantes en el sistema de archivos.

Los archivos de configuración suelen estar en ``/etc/`` o en los directorios específicos del servicio (como ``/var/www/`` para un servidor web).

4. Buscar banderas o archivos sensibles

Si la máquina está configurada para un CTF, es posible que haya un archivo de bandera en algún lugar del sistema. Puedes intentar buscar palabras clave como **"flag"**, **"CTF"** o incluso patrones comunes como ``flag{}`` .

Utiliza ``grep`` para buscar dentro de archivos en todo el sistema:



```
grep -r "flag" /home/raenyra
```

También puedes buscar en todo el sistema de archivos:

```
sudo grep -r "flag" /
```

Nota: Usar `sudo` podría ser necesario si necesitas permisos de superusuario para acceder a algunas áreas del sistema.

5. Revisar procesos y servicios en ejecución

A veces, los CTFs involucran servicios que corren en segundo plano y que podrían tener configuraciones útiles o vulnerabilidades que puedes explotar. Puedes listar los procesos que se están ejecutando para ver si hay algún servicio interesante o incluso alguna vulnerabilidad.

Para listar los procesos, usa:

```
ps aux
```

Esto te dará una lista de todos los procesos en ejecución. Busca cualquier servicio que parezca relacionado con el CTF o que pueda tener configuraciones importantes.

Resumen de las siguientes acciones:

1. **Iniciar sesión en el sistema como** `raenyra` usando `su` o `ssh`.
2. **Explorar los archivos en su directorio personal** (`/home/raenyra`).
3. **Revisar configuraciones de otros servicios**, como SSH o servidores web, para ver si hay más pistas.



4. **Buscar archivos de bandera o sensibles** usando ``grep`` para buscar términos como **flag**.
5. **Revisar procesos y servicios en ejecución** para encontrar algo interesante.

Si encuentras algo relevante o tienes alguna duda mientras exploras, ¡avísame y te guiaré en los próximos pasos!



He encontrado esto: `raenyra@targaryen:~$ cat notas.txt`

El admin me ha pasado las credenciales en caso de que gane la votación:

`targaryen`
`fuegoYsangre123`

Así tendré el poder suficiente para administrar el proyecto Westeros de fuerza impecable. Antes encontré que había un usuario llamado `targaryen`



¡Excelente descubrimiento! Ahora tienes las **credenciales de administrador** para el usuario ``targaryen``, que parece ser clave para acceder a más partes del sistema y posiblemente obtener una **bandera**.

Pasos a seguir ahora:

1. **Iniciar sesión como el usuario `targaryen`**: Ahora que tienes el nombre de usuario (``targaryen``) y la contraseña (``fuegoYsangre123``), puedes intentar cambiar de usuario a **targaryen** y obtener permisos elevados.

Usa el siguiente comando en la terminal para cambiar de usuario:





```
su targaryen
```

Luego, cuando se te pida la contraseña, ingresa ``fuegoYsangre123``.

Si puedes iniciar sesión correctamente como **targaryen**, tendrás acceso a más recursos del sistema, y es probable que puedas encontrar configuraciones o pistas clave para completar el reto.

2. **Obtener privilegios de superusuario:** Si el usuario ``targaryen`` tiene privilegios de **root** o **sudo**, puedes obtener acceso completo al sistema. Para comprobar si tienes privilegios de **sudo**, simplemente ejecuta el siguiente comando:

```
sudo -l
```

Si ves algo como ``ALL`` o tienes la opción de ejecutar comandos con ``sudo``, entonces tienes acceso completo para administrar el sistema.

3. **Explorar el sistema con privilegios elevados:** Si has obtenido privilegios de administrador, puedes comenzar a explorar el sistema completo en busca de más pistas o archivos de bandera. Algunos lugares comunes donde podrían esconderse las banderas son:

- **Archivos de configuración:** ``/etc/``, ``/var/log/``, ``/home/``, y otros directorios del sistema.
- **Archivos de la raíz:** Si tienes permisos de root, también puedes buscar archivos en todo el sistema, utilizando el siguiente comando:

```
sudo find / -name "flag*"
```

Esto buscará cualquier archivo que contenga la palabra "flag" en su nombre, lo que podría llevarte a la bandera del CTF.



4. **Revisar logs y configuraciones importantes:** Revisa algunos logs o configuraciones de servicios para encontrar más pistas, como los archivos en ``/var/log/`` o configuraciones en ``/etc/``.

Resumen:

- Inicia sesión como **targaryen** con ``su targaryen`` y la contraseña ``fuegoYsangre123``.
- Si puedes, obtén privilegios de **sudo** y explora el sistema con privilegios elevados.
- Busca archivos de bandera usando ``find`` o revisa configuraciones en el sistema para más pistas.

¡Continúa explorando y buscando la bandera! Si necesitas ayuda en algún momento, no dudes en preguntarme.



He comprobado si tenía privilegios root como has dicho y ha salido esto: targaryen@targaryen:/home/raenyra\$
sudo -l

[sudo] password for targaryen:

Matching Defaults entries for targaryen on targaryen:

env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/u
sr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User targaryen may run the following commands on
targaryen:

(ALL : ALL) ALL



¡Perfecto! Has conseguido confirmar que el usuario **targaryen** tiene privilegios completos de **sudo** en el sistema, lo que significa que puedes ejecutar **cualquier**



comando con permisos de superusuario.

Pasos a seguir ahora:

1. **Obtener privilegios de root:** Como ``targaryen`` tiene permisos para ejecutar cualquier comando como root, puedes obtener acceso completo al sistema simplemente ejecutando el siguiente comando:

```
sudo su
```

Luego de introducir la contraseña de **targaryen** (``fuegoYsangre123``), deberías tener acceso a una shell con privilegios de **root**.

2. **Explorar el sistema con privilegios de root:** Ahora que eres root, tienes acceso completo a todas las áreas del sistema. Puedes empezar a buscar archivos clave, como banderas o información sensible. Algunas cosas que puedes hacer:

- **Buscar archivos de bandera:** Usa ``find`` para buscar posibles archivos de bandera en el sistema. Un buen patrón de búsqueda podría ser ``"flag"`` o algo relacionado con CTFs. Ejecuta:

```
find / -type f -name "*flag"
```

- **Revisar archivos en ``/root``:** A veces, las banderas o archivos importantes se colocan en el directorio de **root**. Intenta ver qué archivos hay ahí:

```
ls /root
```

- **Revisar otros directorios importantes:**
 - ``/etc/``: Configuraciones del sistema.
 - ``/var/log/``: Logs del sistema.
 - ``/home/``: Archivos de usuarios, donde podría haber más pistas.





3. **Ver archivos de configuración o registros:** Si no encuentras banderas inmediatamente, puedes revisar archivos de configuración o logs que podrían contener pistas. Algunos lugares a revisar son:

- Archivos de configuración: `/etc/`
- Logs del sistema: `/var/log/`

Puedes utilizar `cat`, `less` o `grep` para examinar los archivos:

```
cat /var/log/syslog
less /etc/ssh/sshd_config
grep "flag" /var/log/*
```

4. **Explorar más profundamente:** Si encuentras algún archivo interesante, explóralo más a fondo para ver si contiene alguna información relevante o si es un archivo de bandera.

Resumen:

- Usa `sudo su` para obtener privilegios de **root**.
- Busca archivos relacionados con **banderas** usando `find` o revisando los directorios importantes como `/root`, `/etc`, y `/var/log`.
- Explora el sistema con tus nuevos privilegios y sigue buscando pistas.

¡Continúa buscando y no dudes en pedirme ayuda si necesitas más orientación!



He ejecutado el comando de find, pero salen demasiados archivos y es confuso, ¿puedo hacer otra cosa?



Entiendo que la búsqueda con `find` puede resultar abrumadora si hay demasiados archivos. A continuación, te ofrezco algunas formas más organizadas y específicas de buscar archivos relevantes, para ayudarte a concentrarte en los lugares más probables donde podrías encontrar la **bandera** o pistas adicionales.

1. Refinar la búsqueda con palabras clave

En lugar de buscar simplemente `"flag"`, puedes buscar otras palabras o patrones que suelen estar presentes en los CTFs, como **"flag"**, **"CTF"**, **"hidden"**, o incluso **"key"**. Aquí tienes un comando refinado:

```
sudo find / -type f -iname "*flag"
```

Esto buscará archivos con la palabra **"flag"** en cualquier parte del sistema, sin importar mayúsculas o minúsculas (`-iname` hace la búsqueda insensible a mayúsculas).

Otras palabras clave que puedes intentar:

```
sudo find / -type f -iname "*key"  
sudo find / -type f -iname "*secret"
```

2. Limitar la búsqueda a directorios específicos

En lugar de buscar en todo el sistema, puedes limitar la búsqueda a directorios donde normalmente se guardan archivos importantes o donde podrías encontrar la bandera:

- **Revisar en directorios de configuración y logs:**

```
sudo find /etc/ -type f -iname "*flag"  
sudo find /var/log/ -type f -iname "*flag"
```





- **Explorar archivos en el directorio de root** (ya que ahora tienes privilegios de root):

```
sudo find /root/ -type f -iname "*flag"
```

- **Explorar en el directorio home:** A veces, las banderas están escondidas en el directorio home de otros usuarios. Como ahora tienes privilegios de root, puedes buscar en las casas de otros usuarios, como ``raenyra`` y ``otto``.

```
sudo find /home/ -type f -iname "*flag"
```

3. Buscar con ``grep`` dentro de archivos

Si la búsqueda de archivos con ``find`` te parece demasiado general, puedes intentar buscar dentro de archivos específicos. Por ejemplo, puedes buscar cadenas como **"flag"** o **"CTF"** dentro de los archivos de texto. Para hacer esto, puedes usar el comando ``grep``:

- Buscar la palabra "flag" dentro de archivos de texto en ``/home/`` o ``/etc/``:

```
sudo grep -r "flag" /home/  
sudo grep -r "flag" /etc/
```

- Si quieres algo más general, puedes intentar con la palabra **"CTF"**:

```
sudo grep -r "CTF" /home/  
sudo grep -r "CTF" /etc/
```

Esto buscará la palabra **flag** o **CTF** en los archivos dentro de esos directorios, y te mostrará la línea exacta que contiene el término, lo que puede ser útil para localizar rápidamente una bandera o una pista.

4. Explorar el archivo ``dmesg`` o los logs del sistema





Los logs del sistema y el archivo `dmesg` pueden contener información importante. A veces, los CTFs esconden pistas o banderas en los logs de arranque del sistema, ya que son accesibles para los administradores.

- Para revisar el archivo `dmesg` (mensaje del sistema):

```
sudo dmesg | grep -i "flag"
```

- Para revisar los logs del sistema en `/var/log/`:

```
sudo grep -r "flag" /var/log/
```

5. Explorar los procesos en ejecución

A veces, los servicios en ejecución pueden contener información clave. Usa el comando `ps aux` para ver qué servicios están corriendo en segundo plano y si alguno de ellos está relacionado con el CTF.

- Muestra todos los procesos en ejecución:

```
sudo ps aux
```

- Busca procesos con el nombre del CTF o que parezcan sospechosos:

```
sudo ps aux | grep "flag"  
sudo ps aux | grep "westeros"
```

Si hay algún proceso interesante que esté relacionado con el CTF o con la bandera, podrás investigarlo más a fondo.

Resumen de los siguientes pasos:



- **Refina la búsqueda** usando palabras clave específicas como **flag**, **key**, **secret**.
- **Limita la búsqueda a directorios específicos**, como `/etc/`, `/var/log/`, `/root/` y `/home/`.
- **Usa `grep` para buscar dentro de los archivos** las palabras clave que te interesen.
- **Revisa los logs del sistema** y los mensajes de arranque (`dmesg`).
- **Explora los procesos en ejecución** para encontrar cualquier pista relacionada con el CTF.

Espero que estas técnicas te ayuden a encontrar la bandera de manera más eficiente. Si encuentras algo interesante o necesitas más ayuda, ¡avísame!



```
Me ha salido esto: root@targaryen:/home/raenyra#  
sudo find /root/ -type f -iname "*flag*"  
/root/flag.txt
```



¡Genial! Has encontrado un archivo llamado `flag.txt` en el directorio `/root/`. Ahora es momento de abrirlo y ver qué contiene, ya que es muy probable que esa sea la **bandera** del CTF.

Pasos:

1. **Abrir el archivo `flag.txt`**: Ahora que sabes dónde se encuentra, solo tienes que leer el contenido del archivo. Como eres **root**, puedes abrirlo directamente con el siguiente comando:

```
cat /root/flag.txt
```

2. **Revisar el contenido**: Si el archivo contiene la bandera del CTF, te aparecerá algo como una cadena de texto (normalmente una combinación de letras y



números). Esa será la **bandera** que estás buscando.

¡Adelante y avísame qué encuentras! Si es la bandera, ¡felicidades! Has resuelto el reto CTF. 🎉



Genial, he podido visualizar el contenido y he resuelto esta máquina



¡Felicidades! 🎉 Has completado con éxito el CTF y resuelto la máquina. Es un logro impresionante, especialmente porque lograste superar los retos de acceso, exploración y obtención de la bandera.

Si te gustaría seguir practicando, puedes buscar más **CTFs** para mejorar tus habilidades o incluso intentar hackear otras máquinas. Siempre hay algo nuevo por aprender, y los CTFs son una excelente manera de mejorar tus conocimientos en seguridad informática y hacking ético.

Si alguna vez necesitas ayuda con otros retos o quieres aprender más sobre técnicas y herramientas, no dudes en preguntarme. ¡Continúa así y sigue explorando! 🚀

¡Buen trabajo! 🙌