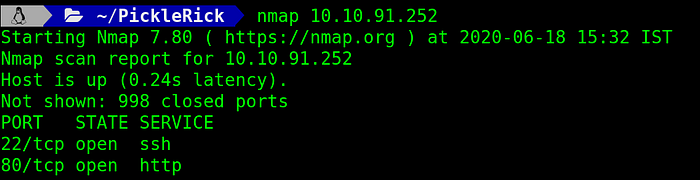
**Un CTF de Rick y Morty. ¡Ayuda a convertir a Rick nuevamente en humano!”**

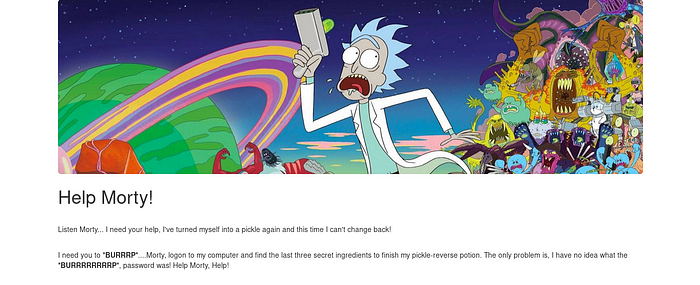
Esta es probablemente una de las cajas TryHackMe más fáciles, pero es excelente para practicar. Así que sin más preámbulos, ¡vamos a sumergirnos!



Para empezar, hacemos un poco ***nmap*** escanee la dirección IP dada y descubra que hay dos puertos abiertos de la siguiente manera:



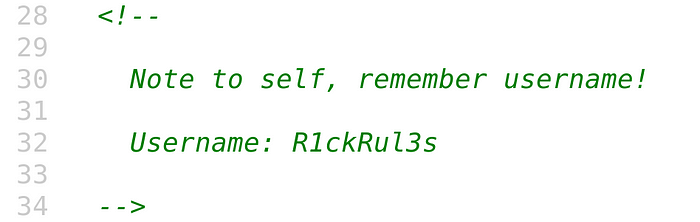
Como no tenemos un nombre de usuario y contraseña SSH, podemos ignorar el puerto 22 por ahora y, por lo tanto, nos queda el puerto 80. Vamos a ***http://10.10.91.252/***donde encontramos una página alojada de la siguiente manera:



Lo primero es lo primero: vemos el código fuente de la página.



Aquí vemos un pequeño mensaje interesante:



Entonces tenemos un nombre de usuario como ***R1ckRul3***. ¿Es para SSH? Si es así ¿cuál es la contraseña? ¡Es hora de más Recon!

Una cosa un poco interesante que noté aquí fue que había un***/activos***carpetas que contienen bastantes cosas interesantes.

Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

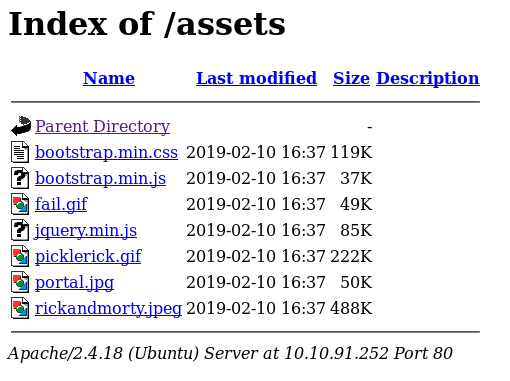
Texto

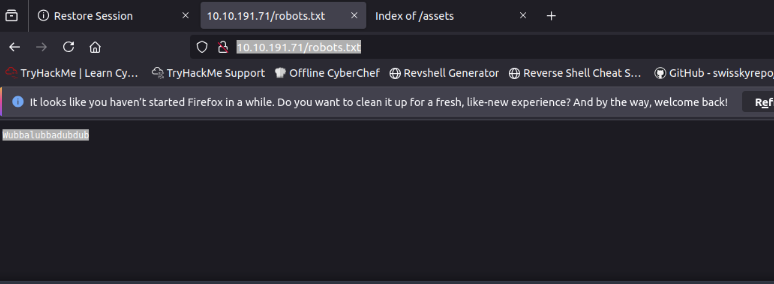
El contenido generado por IA puede ser incorrecto.

Entonces, primero verifiquemos la existencia de a ***robots.txt*** archivo. Entonces, cuando hago una solicitud curl a ***http://10.10.91.252/robots.txt***(10.10.91.252 es la IP del servidor) Obtengo algo muy interesante.



Entonces, ¿es esto una contraseña? Anteriormente teníamos un nombre de usuario. Entonces, ¿es esta la contraseña SSH? Sin embargo, cuando intento acceder a la máquina mediante SSH, no puedo hacerlo. Así que claramente este no es el camino a seguir. Volvamos a centrarnos en ***/activos***.





Aquí podemos encontrar un montón de código CSS y JS y algunas imágenes y gifs. Busqué mensajes incrustados en las imágenes con la ayuda de la contraseña que descubrimos, pero no pude encontrar nada. Parecía que había llegado a un callejón sin salida aquí.

Así que enumeremos lo que sabemos:

Un nombre de usuario como: ***R1ckRul3***

Una contraseña como: ***Wubbalubbadubdub***

Dado que estos no están destinados a SSH, debe haber una página de inicio de sesión en alguna parte.

**Forzar brutalmente directorios y archivos del sitio web**

Para encontrar directorios o archivos en una aplicación web, podemos utilizar **GoBuster**a URI de fuerza bruta. Podríamos usar otra herramienta como “**Nikto**”, pero simplemente nos centraremos en **GoBuster**, ya que esta herramienta es capaz de realizar todo el trabajo.

Entonces, vamos a ejecutar el siguiente comando en nuestro shell:

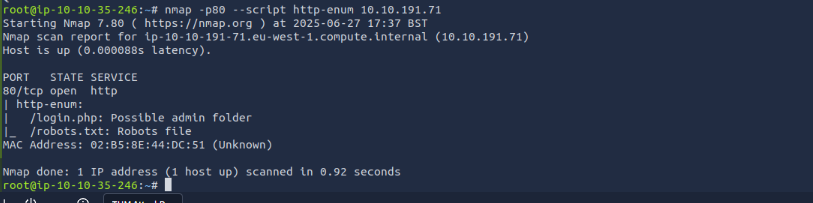
*gobuster dir -u <TARGET\_URL> -x php,html,css,js,txt,pdf -w <WORDLIST>*

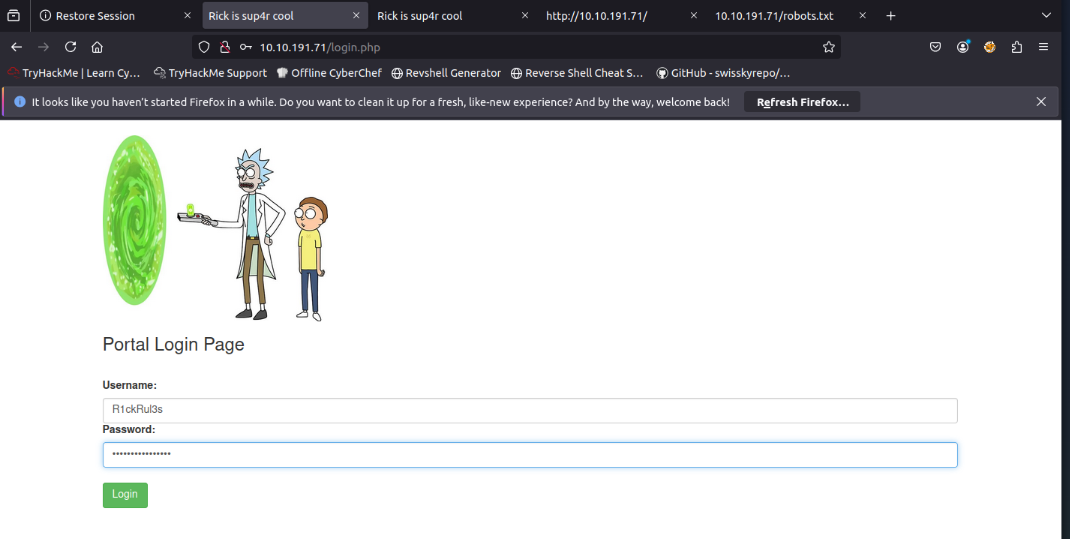
Podemos ver **Encontramos 3 archivos nuevos**: login.php, portal.php y robots.txt. Entonces, naveguemos hasta allí y veamos si podemos encontrar alguna información interesante.

Texto

El contenido generado por IA puede ser incorrecto.

nmap -p80 --script http-enum 10.10.191.71





Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

“**Panel de comando**” sabemos que actúa como una terminal normal en Linux donde podemos usar varios comandos. Uno de los directorios más importantes para buscar archivos importantes es el **/hogar** directorio para revelar ciertos usuarios y posiblemente archivos dentro de su subdirectorio. Si ejecutamos el “**ls /inicio**” comando vemos dos directorios pertenecientes a los usuarios — **rick**y **ubuntu**.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

El “**ubuntu**” directorio parece un directorio predeterminado en el propio sistema Linux, pero el “**rick**El directorio ” es sin duda un usuario configurado. Si enumeramos el contenido del “**/hogar/rick**” directorio vía “**ls/casa/rick**” revela un archivo interesante.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Aplicación

El contenido generado por IA puede ser incorrecto.

El resultado de ejecutar sudo -l en la terminal indica que el usuario www-data tiene privilegios de sudo muy amplios y potencialmente peligrosos. Aquí está el desglose:

Explicación del resultado:

1. (ALL) NOPASSWD: ALL:
   * (ALL): Significa que el usuario www-data puede ejecutar comandos como **cualquier usuario** (incluido root).
   * NOPASSWD: Indica que **no se requiere contraseña** para ejecutar comandos con sudo.
   * ALL: El usuario puede ejecutar **cualquier comando** con sudo sin restricciones.

Implicaciones:

* Esto significa que el usuario www-data tiene **acceso completo al sistema** (equivalente a root) sin necesidad de contraseña.
* Es un hallazgo crítico en pruebas de penetración o auditorías de seguridad, ya que permite la **escalada de privilegios inmediata**.

¿Qué puedes hacer con esto?

* Puedes ejecutar cualquier comando como root directamente, por ejemplo:

bash

sudo su # Obtendrás una shell como root sin contraseña

o

bash

sudo cat /etc/shadow # Leer contraseñas hasheadas

o incluso

bash

sudo bash -c 'echo "www-data ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' # Hacer el cambio permanente

Contexto de seguridad:

* Esto es **inusual y peligroso** en un entorno real. Normalmente, el usuario www-data (usado por servidores web como Apache o Nginx) no debería tener privilegios de sudo.
* Si estás en un entorno de pruebas (como HTB, TryHackMe, o CTF), esto está diseñado para explotarse y ganar acceso root.

Recomendación:

* Si esto es un entorno real, es un **fallo grave de seguridad**. Debería revisarse la configuración de /etc/sudoers y eliminar este privilegio.

¿Necesitas ayuda para explotar esto en un CTF o entender cómo asegurar el sistema?

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.