**Mr Robot – Vulnhub**





Contenido

[Descripción 2](#_Toc156506293)

[Objetivo 2](#_Toc156506294)

[Herramientas utilizadas 2](#_Toc156506295)

[Reconocimiento 2](#_Toc156506296)

[Escaneo 3](#_Toc156506297)

[Explotación 7](#_Toc156506298)

[Escalada de privilegios 12](#_Toc156506299)

# Descripción

Basado en la serie Mr. Robot. Máquina virtual WordPress.

# Objetivo

Esta VM tiene tres claves ocultas en diferentes ubicaciones. El objetivo es encontrarlas. Cada clave es progresivamente difícil de encontrar.

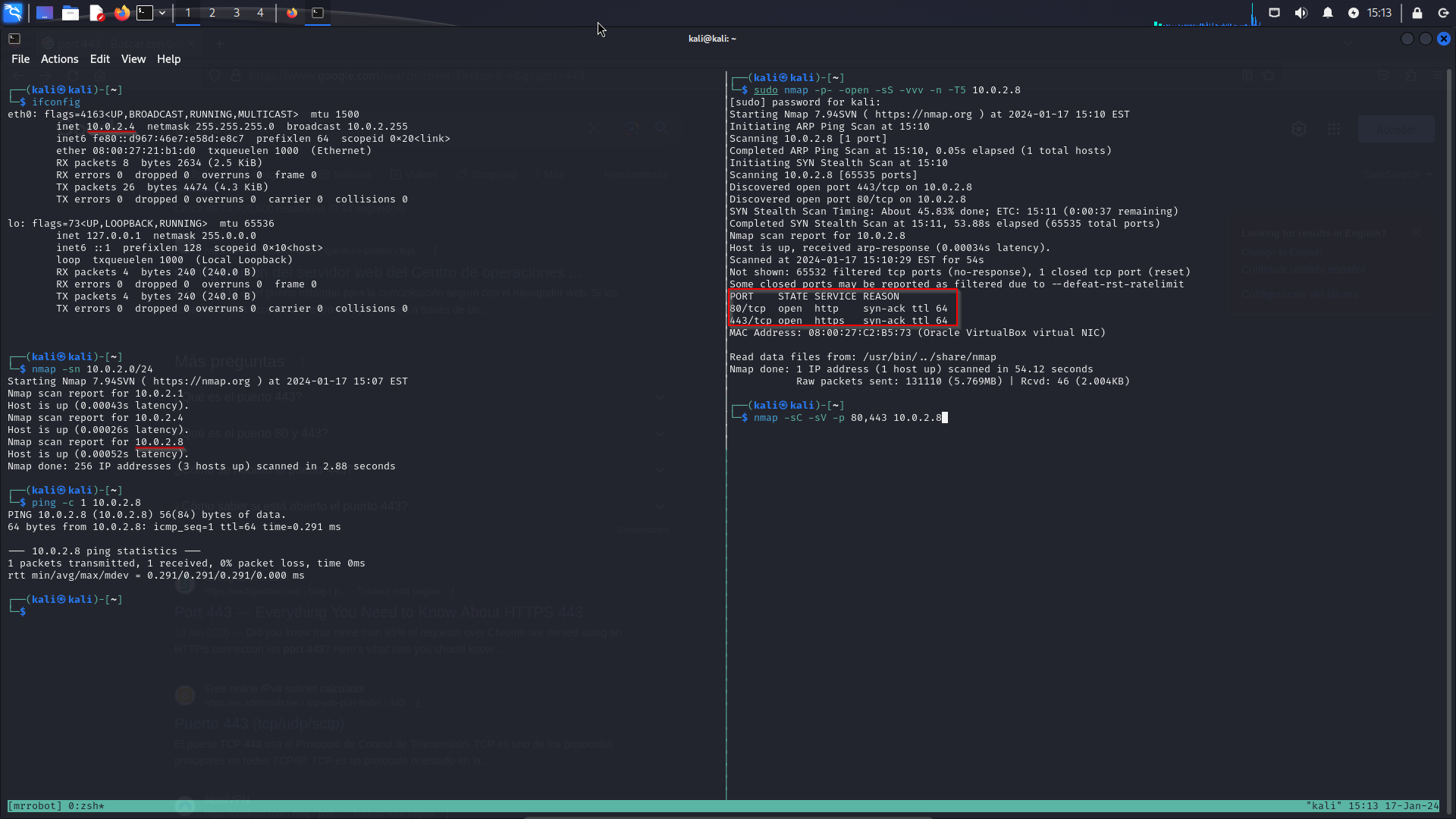
La VM no es demasiado difícil. No existe ninguna explotación avanzada ni ingeniería inversa. El nivel se considera principiante-intermedio.

# Herramientas utilizadas

* Nmap
* Whatweb
* Wpscan
* Gobuster
* [*Blog informativo*](https://nitesculucian.github.io/2019/07/01/exploiting-the-xmlrpc-php-on-all-wordpress-versions/)
* [*php-reverse-shell-pentestmonkey*](https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php.)
* [*crackstation*](https://crackstation.net/)

# Reconocimiento

Ejecuto *ifconfig* para saber la dirección ip de la máquina atacante (Kali Linux) e iniciar el reconocimiento de dispositivos en la red mediante el comando *nmap -sn 10.0.2.0/24.*



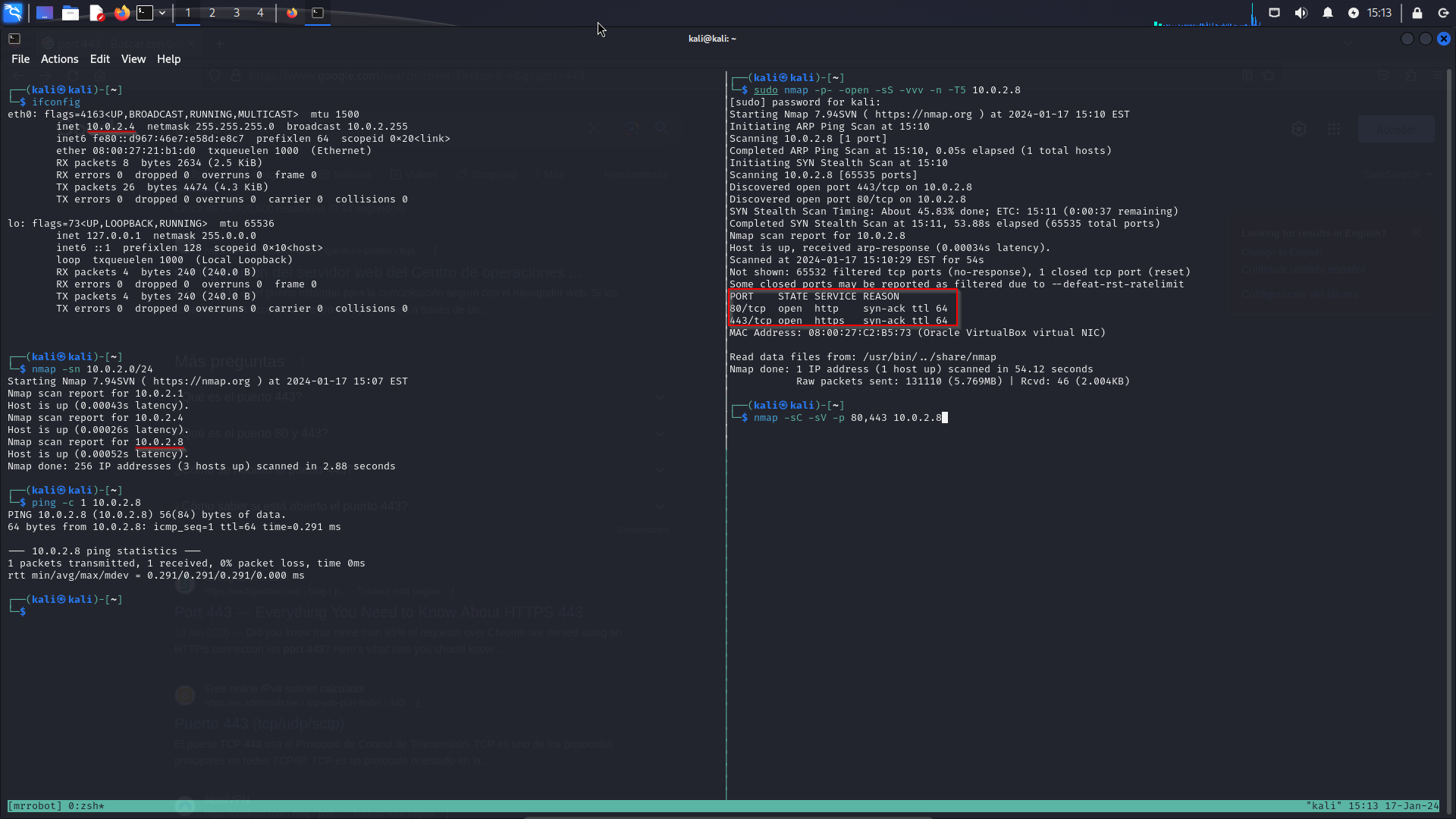
A través de la descripción de la MAC identificamos la máquina víctima (Mr Robot), envío un *ping* con un paquete icmp para ver si obtengo comunicación.

Texto

Descripción generada automáticamente

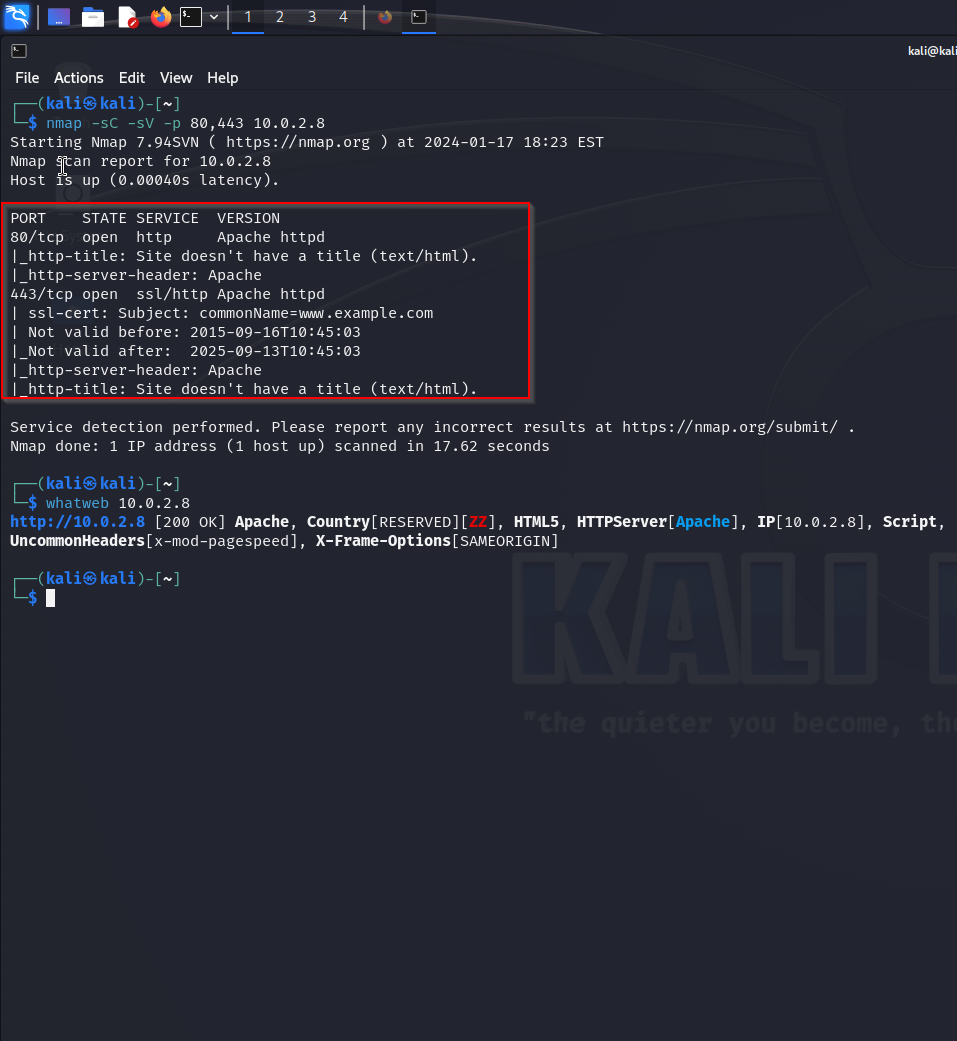
# Escaneo

En esta instancia, ejecuto nuevamete la herramienta nmap para hacer un escaneo de puertos abiertos dentro de la ip 10.0.2.8.

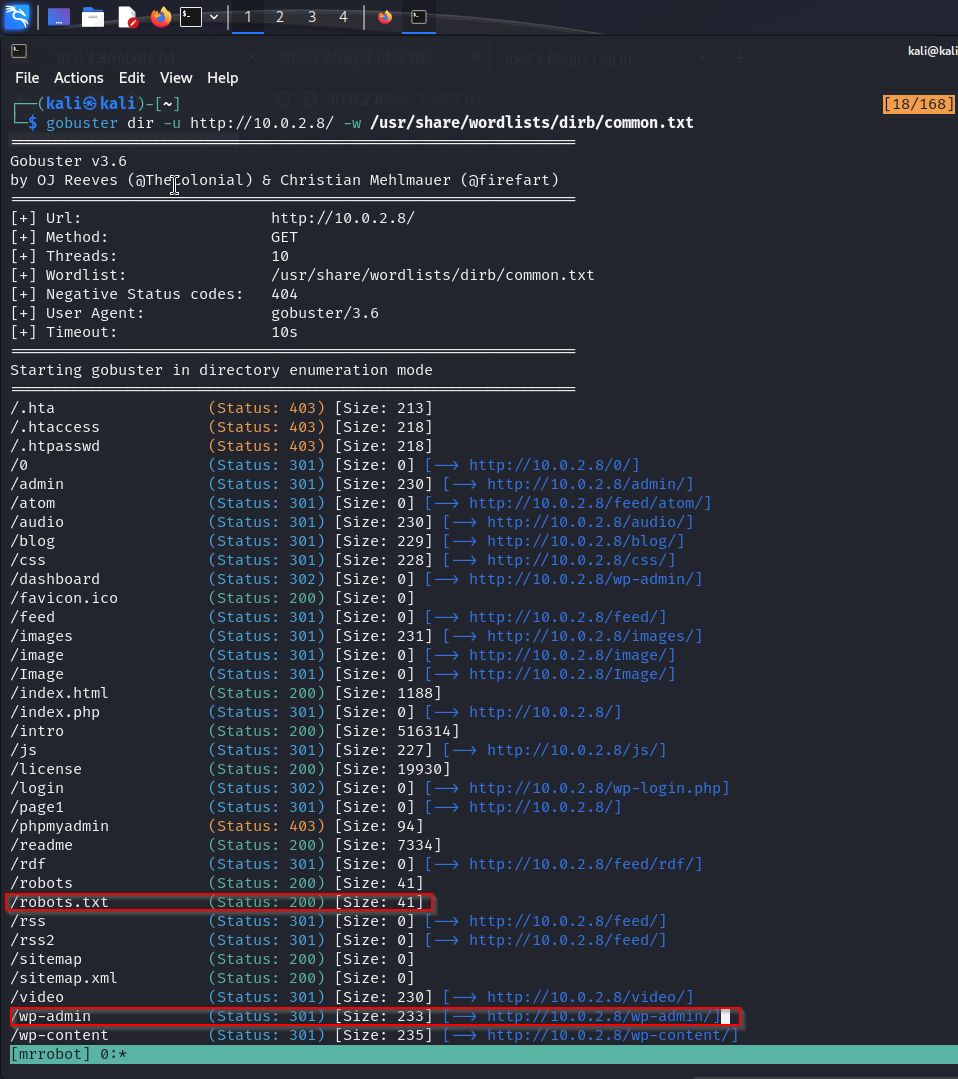


**Puertos encontrados**

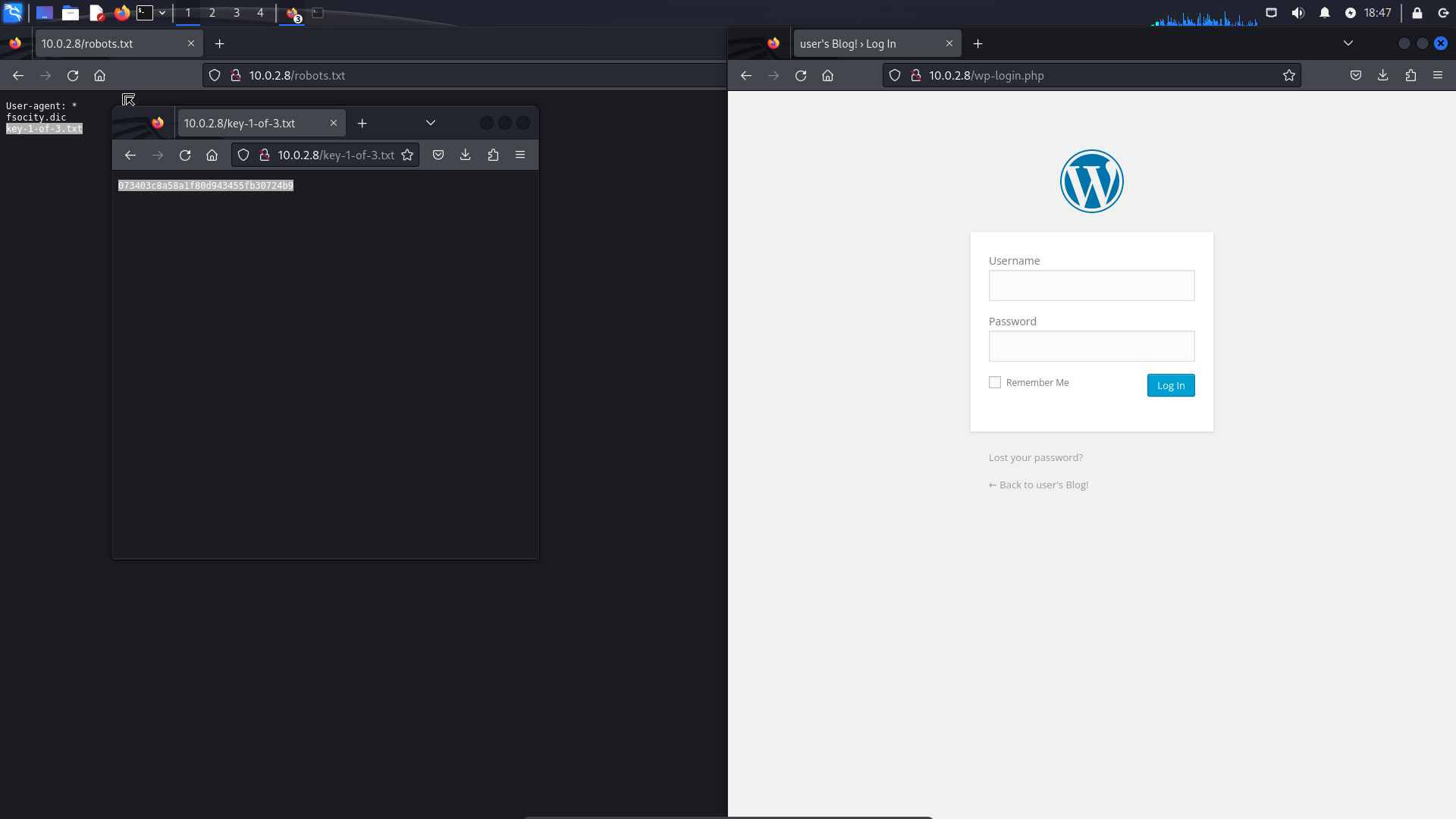
|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **State** | **Service** | **Version** |
| 80/tcp | Open | http | Apache httpd |
| 443/tcp | Open | ssl | Apache httpd |



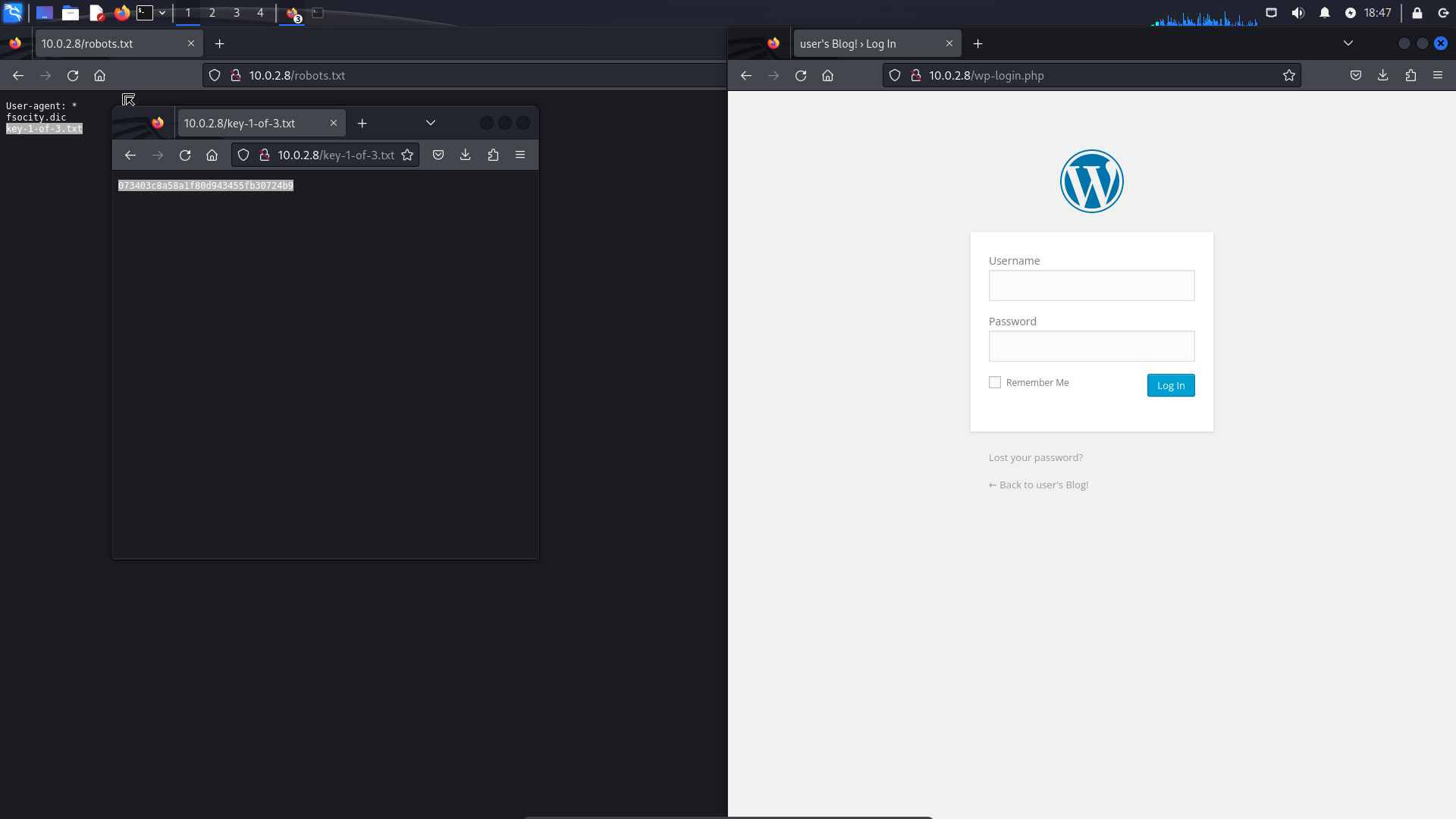
Busqué directorios ocultos que me puedan llegar a interesar con la ayuda de ***gobuster***.



Ingreso al directorio /robots.txt donde encontré otro directorio que me llevó a encontrarme con la primer flag.



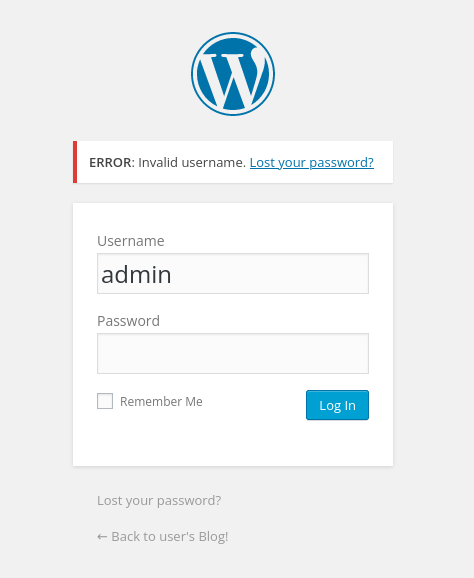
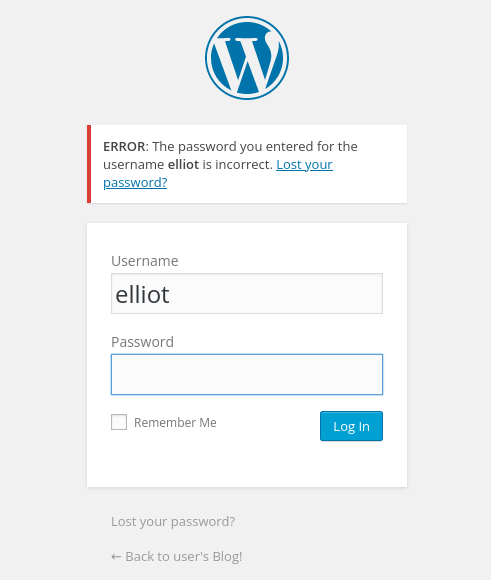
Los directorios que comenzaban con “wp-“ me dieron indicios que la web estaba corriendo sobre WordPress, a lo que decidí ingresar al directorio /wp-login, encontrándome con un una página de ingreso de WordPress.



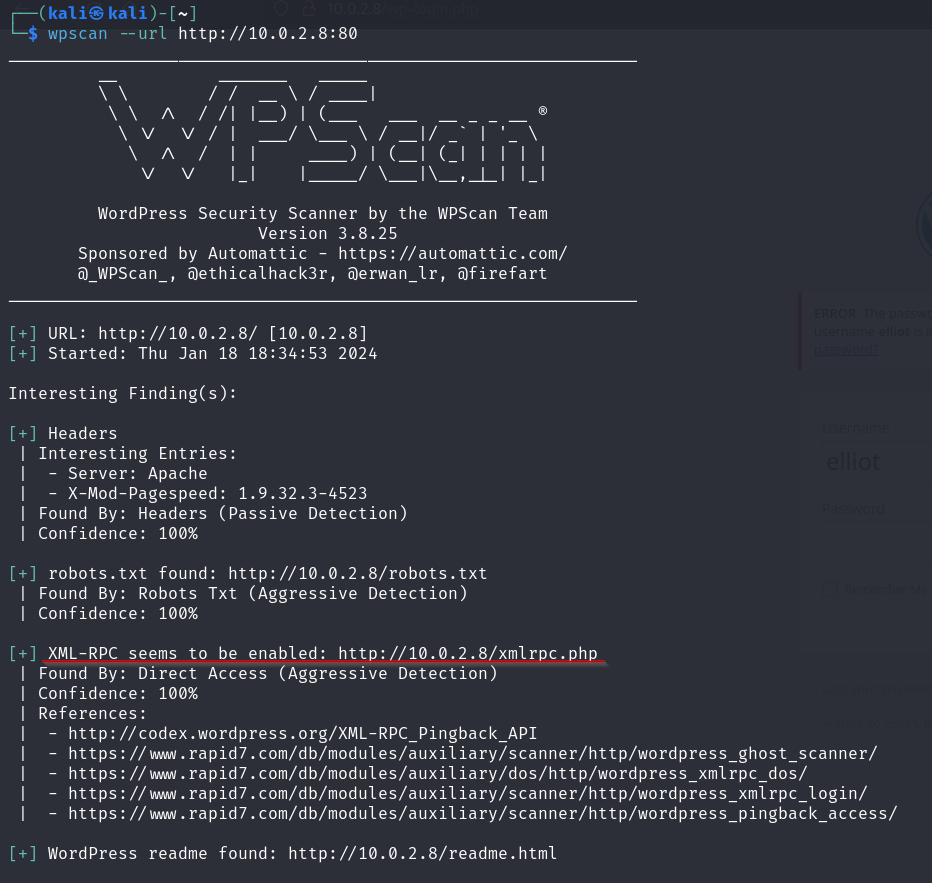
Teniendo en cuenta que la máquina virtual está basada en la serie de Mr Robot, comencé a probar ingresando los nombres de los protagonistas en el campo de username para ver el comportamiento del login.

A lo que me llevó a descubrir los siguientes errores:

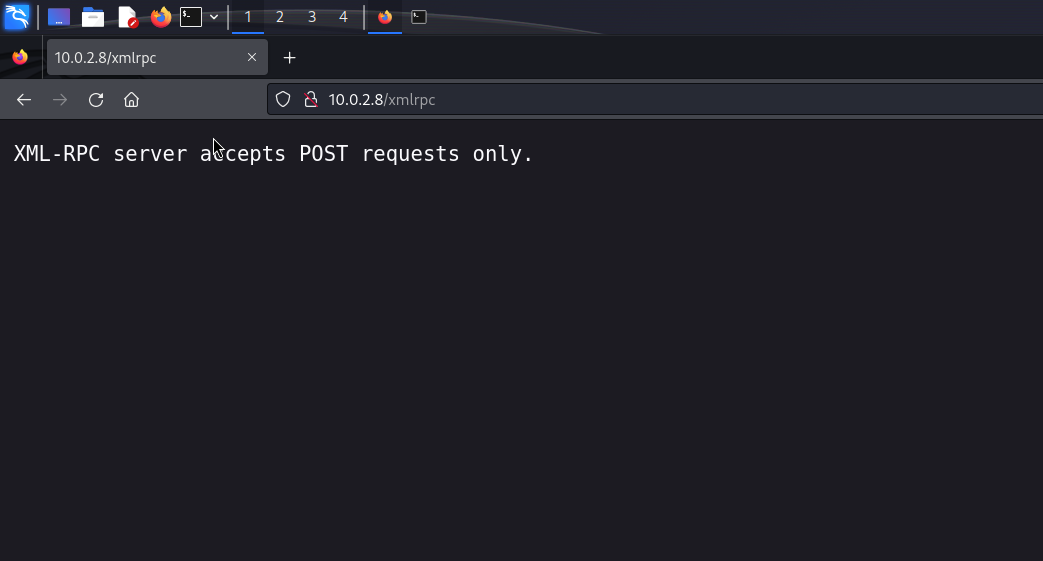
* Error: The password you entered for the username <username> is incorrect. (cuando un usuario es correcto).
* Error: Invalid username. (cuando un usuario NO es correcto).



Hago uso de la herramienta **wpscan** para ver la información importante que me podría devolver. De esta manera me doy cuenta que tiene servidor XML-RPC visible (con XML-RPC busco obtener acceso a las credenciales del panel WordPress).



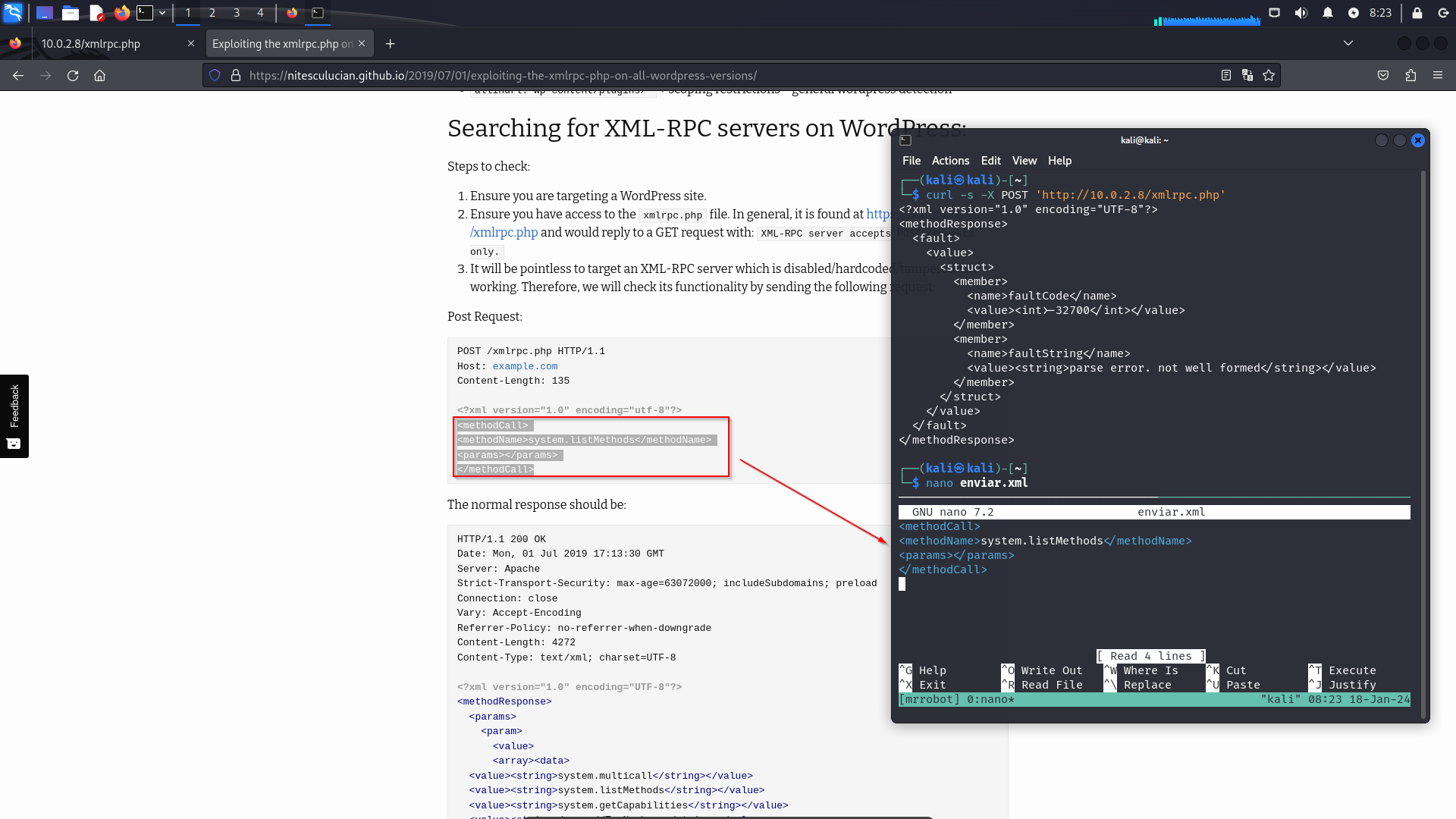
Pruebo ingresar al directorio /xmlrpc.php. A lo que me pongo a investigar en internet formas de vulnerar esto a través de peticiones POST.



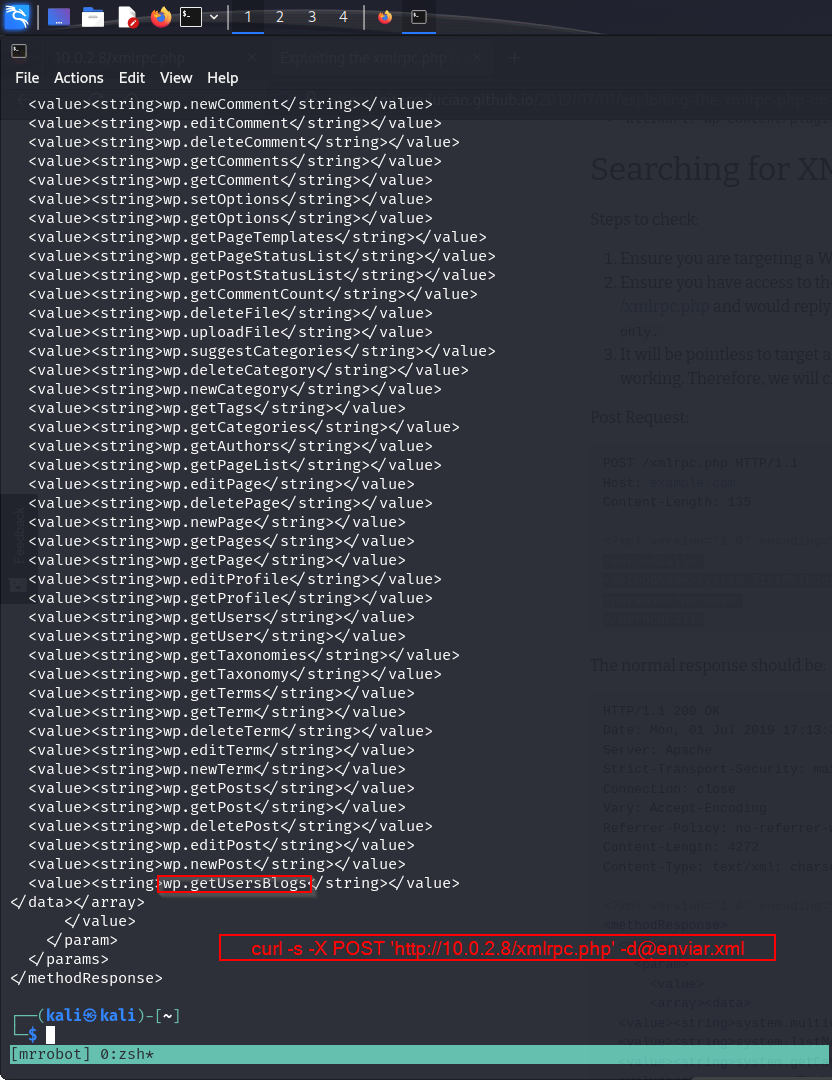
# Explotación

Encontré el siguiente [blog](https://nitesculucian.github.io/2019/07/01/exploiting-the-xmlrpc-php-on-all-wordpress-versions/) donde seguí los siguientes pasos para explotar el xmlrpc.php de WordPress.

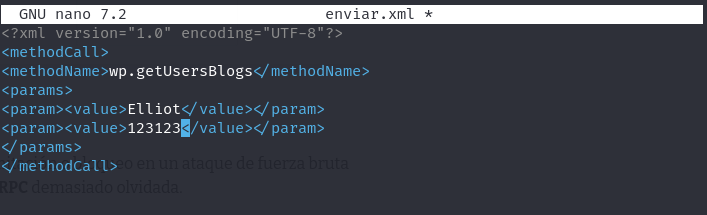
- Comprobé la funcionalidad del servidor XML-RPC enviando mediante ***curl*** un archivo .xml con el contenido resaltado.



Respuesta

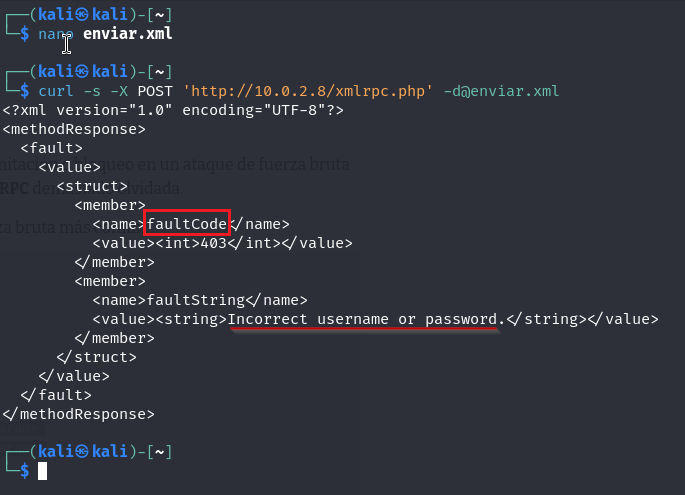


- Como obtuve de respuesta “wp.getUsersBlogs” me confirma que puedo hacer fuerza bruta. Por lo que modifico el archivo enviar.xml.

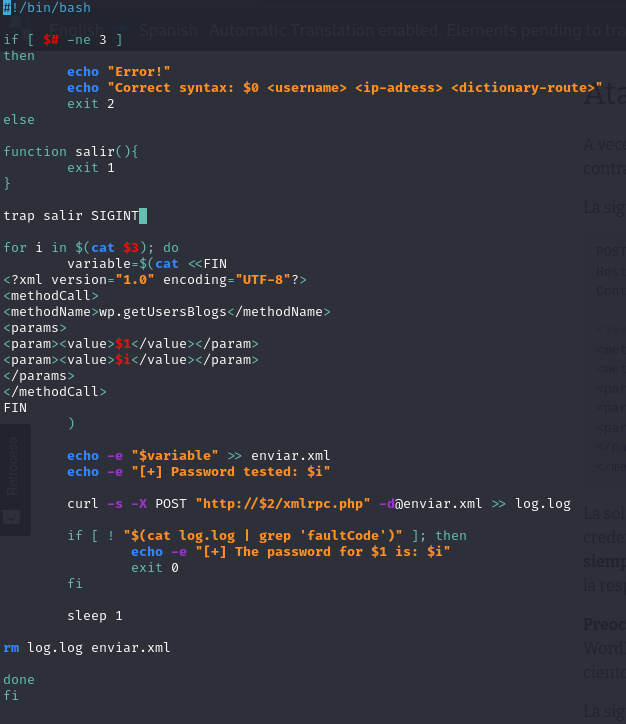


- Lo envío con curl -s -X POST ‘http://10.0.2.8/xmlrpc.php’ -d@enviar.xml

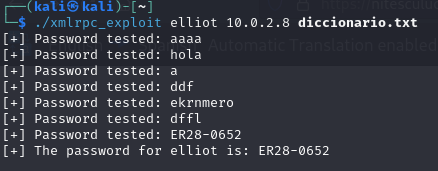
Respuesta, “faultCode” me indica que ubo un error, por lo que la contraseña que forzamos en el archivo enviar.xml no era correcta.



- Para ahorrar tiempo a la hora de probar contraseña por contraseña y andar modificando el archivo enviar.xml, realicé un script en bash que lo automatiza todo.



- Lo ejecuto enviándole como argumentos el usuario, la dirección ip y el diccionario para realizar fuerza bruta.



**Credenciales** Username: Elliot – Password: ER28-0652.

Obtengo acceso al panel de administración de WordPress.

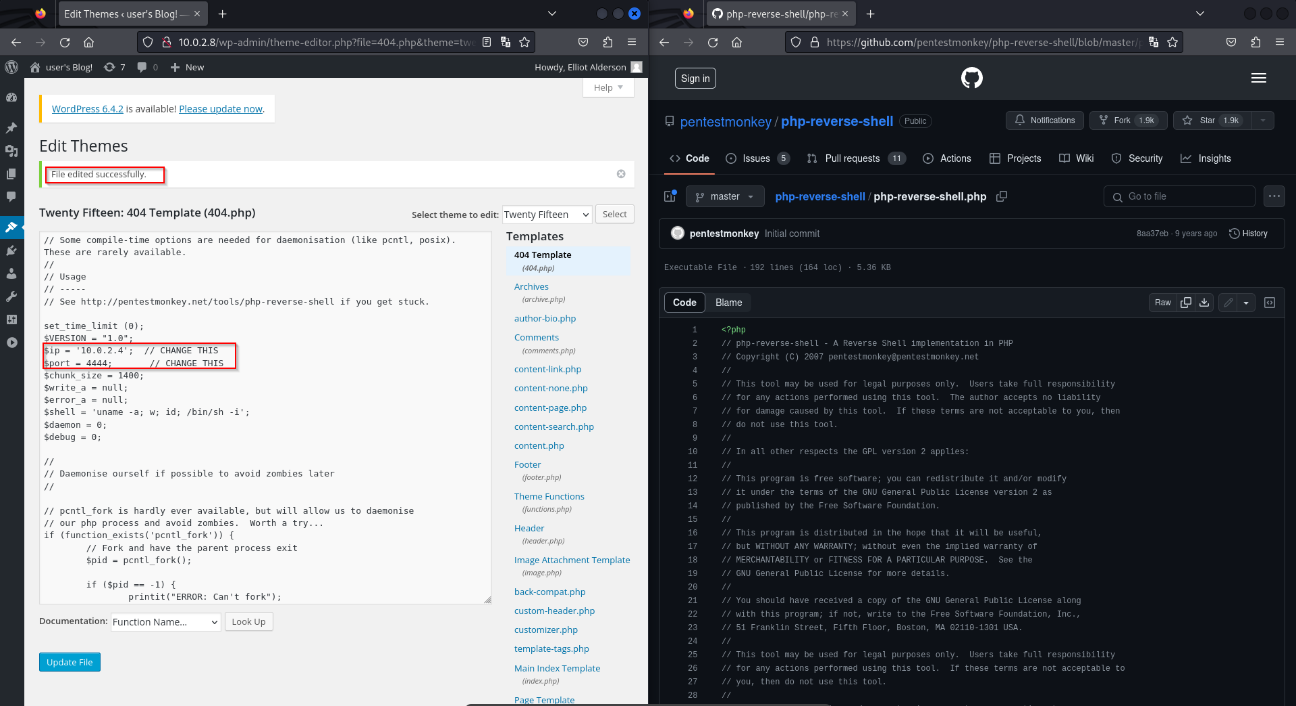
Me dirijo a la sección de apariencia – editor.

Interfaz de usuario gráfica, Texto, Aplicación

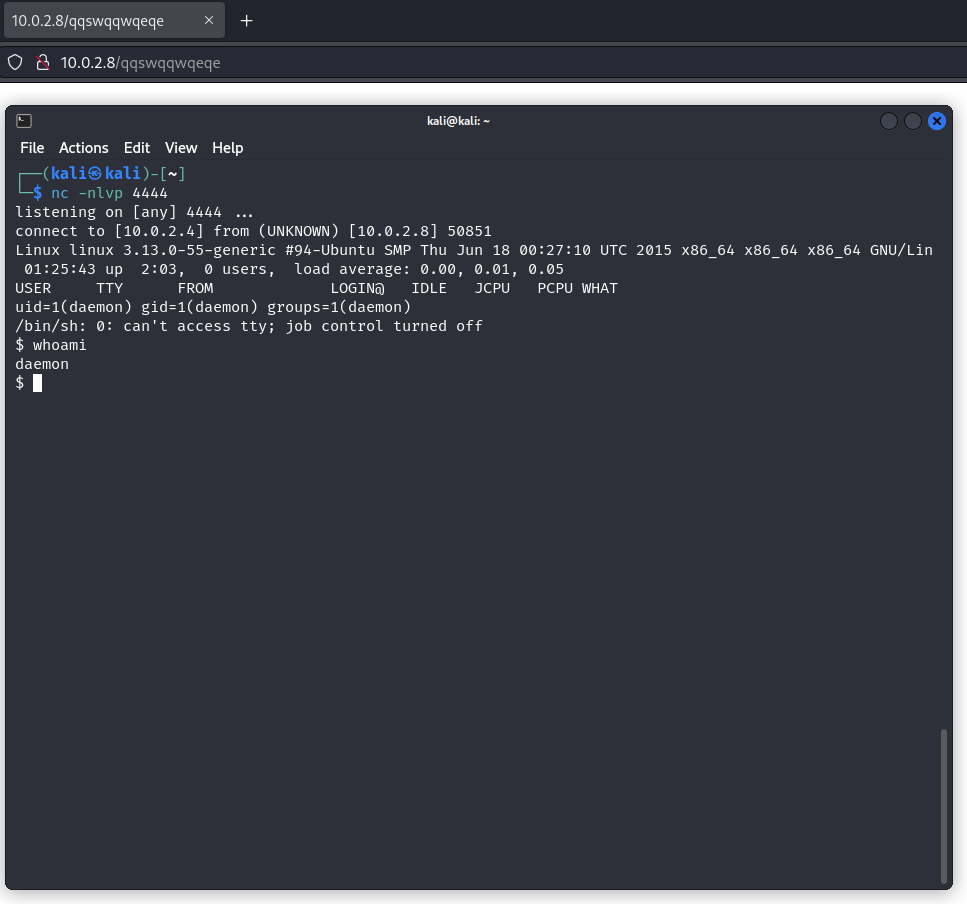
Descripción generada automáticamente

Reemplazo código del template 404.php por código malicioso del siguiente repositorio: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>.

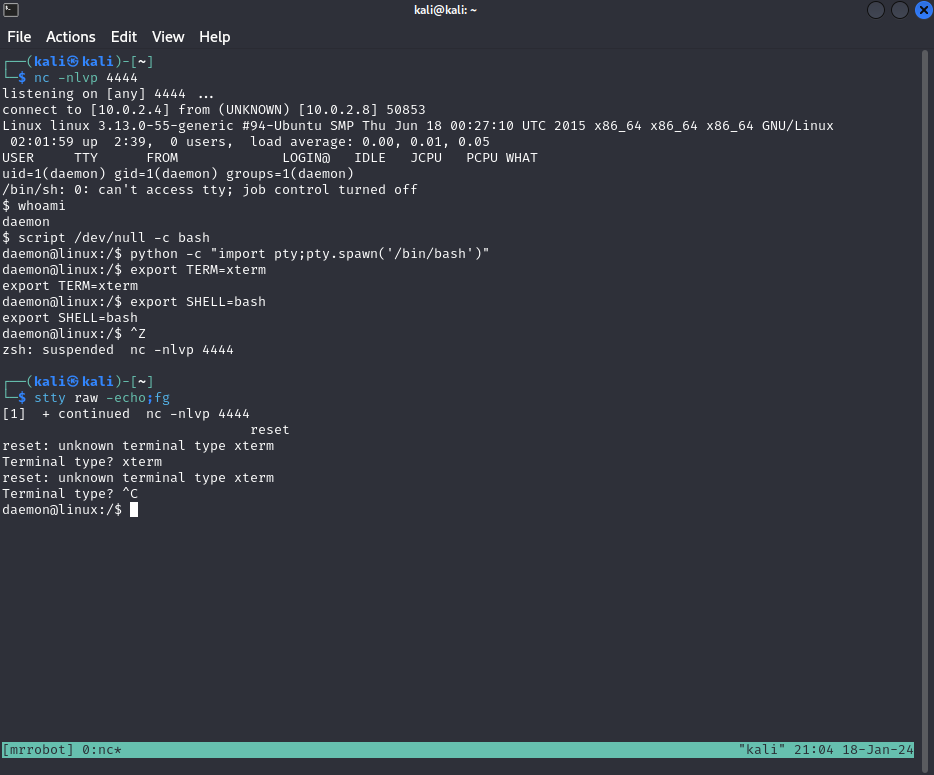
Modifiqué la IP y puerto, tal como me lo indicaba las instrucciones del repositorio.



Me puse en escucha en la terminal con netcat y modifiqué la url para forzar la redirección a una ruta que no existe (obtener el código de respuesta 404).



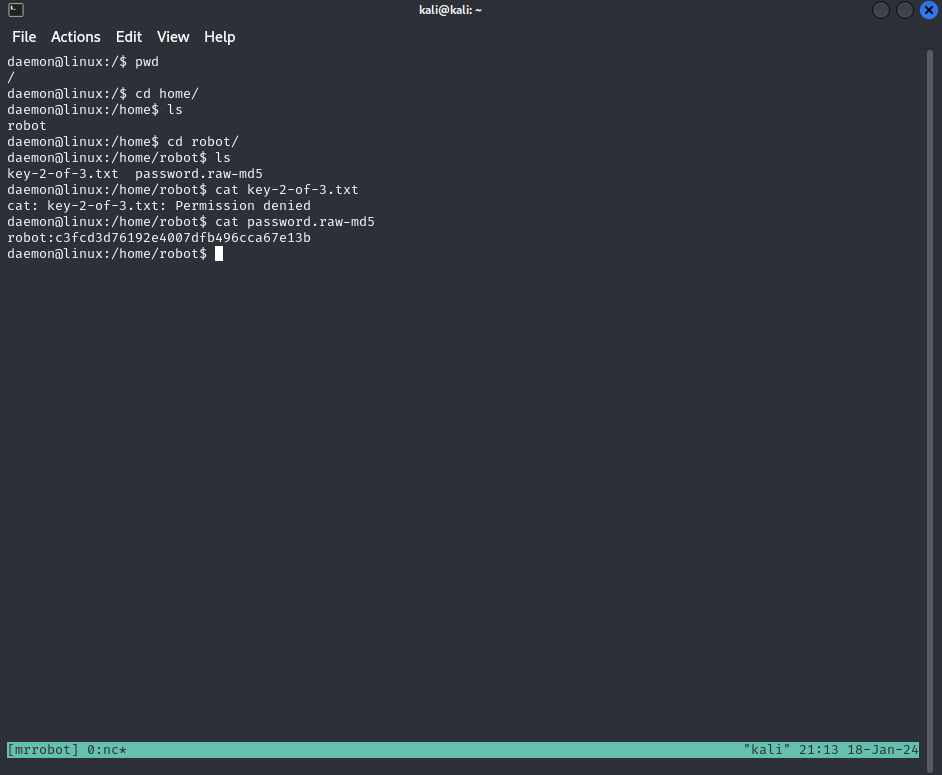
De esta manera el payload almacenado en dicha ruta se ejecuta y obtengo acceso a la máquina víctima (como usuario daemon). Configuré tty operativa.



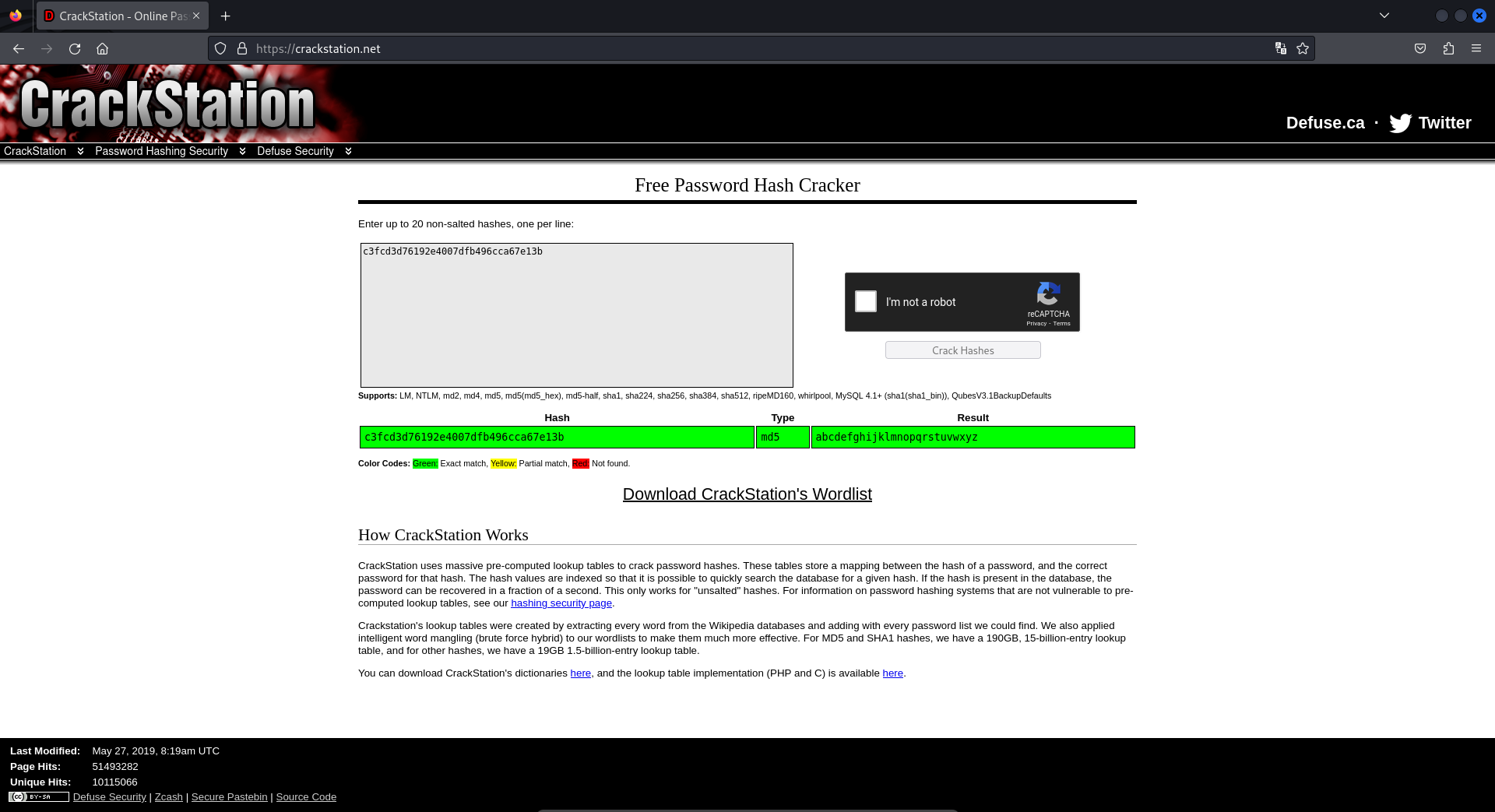
# Escalada de privilegios

Busco contenido en la ruta home, me encuentro con directorio del usuario robot que en su contenido tenía un 2 ficheros.

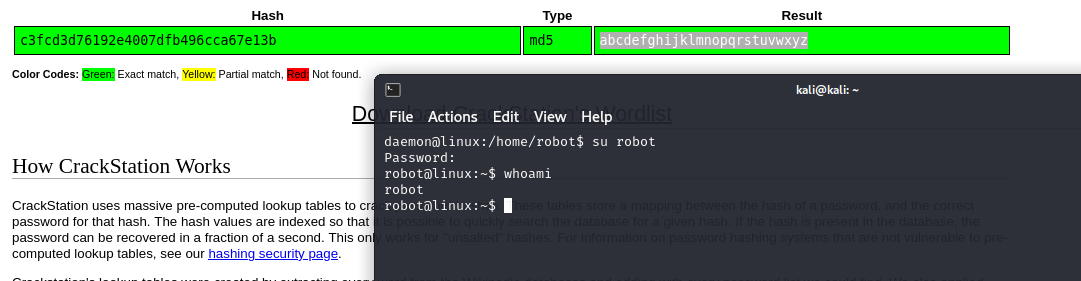
* key-2-of-3.txt -> No me permitió ingresar.
* password.raw-md5.



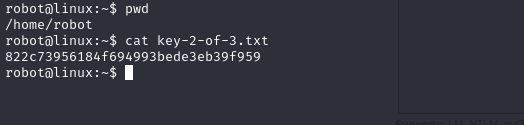
Procedo a decodificar la cadena de texto del fichero password.raw-md5, con la ayuda de la herramienta [crackstation](https://crackstation.net/).



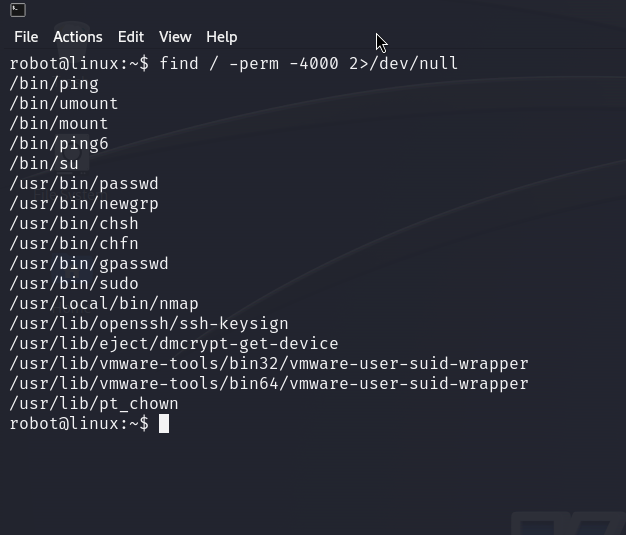
Utilizo el resultado para escalar privilegios al usuario robot.



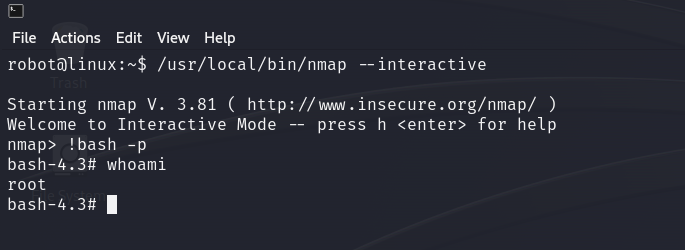
Acceso al contenido encontrado en /home/robot que me había sido denegado el acceso con el usuario daemon. (2da flag).



Busco binarios que puedo correr como usuario root.



Veo que está instalado nmap. Procedo a ejecutarlo de forma interactiva y abuso de esto para escalar privilegios a root.



Encuentro la tercer flag en el directorio root.

