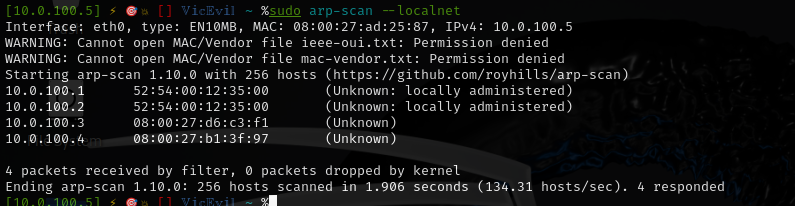
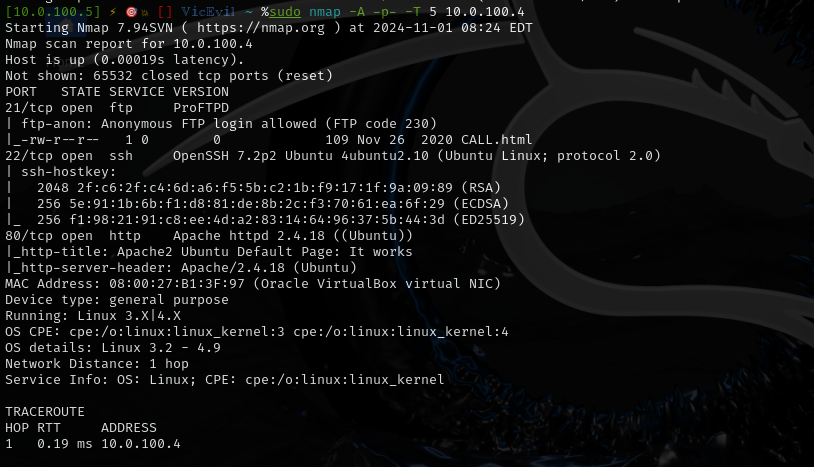


**SPRINGO 18**

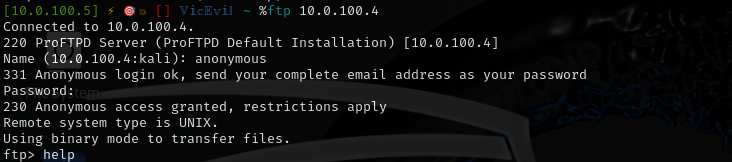
**TEAM CHALLENGE**

**RETO SSH - PIVOTING**

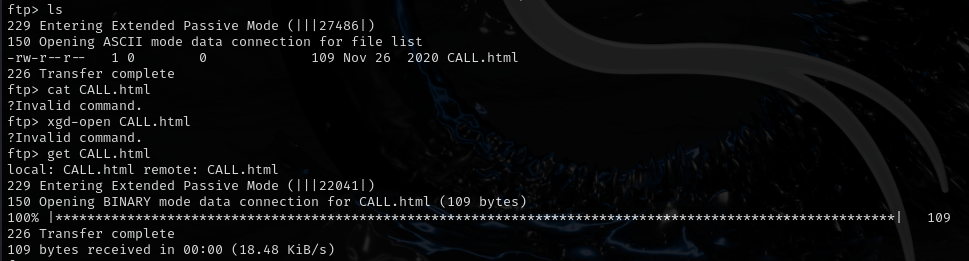


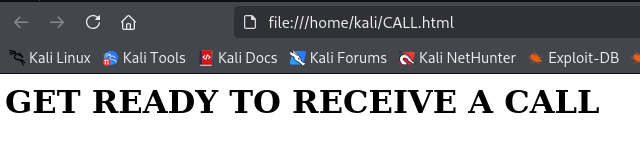


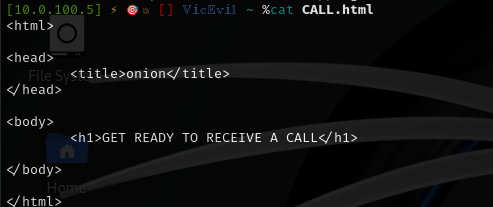
ftp - anonymous - code:230



hay un archvo CALL.html pero no se permite abrir desde FTP, lo llevo a mi kali:

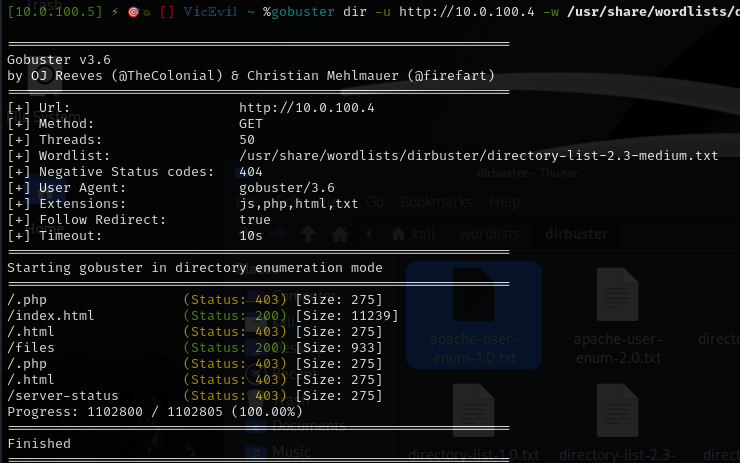






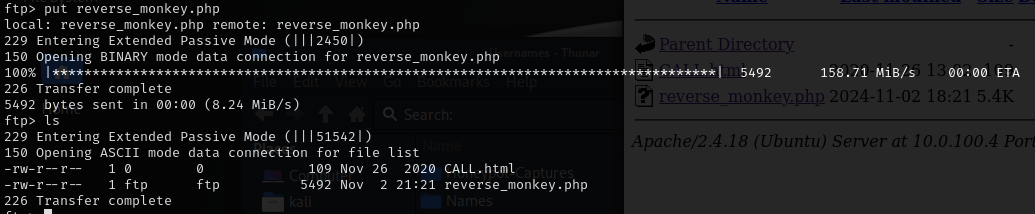
intrsantes onion ty la frase

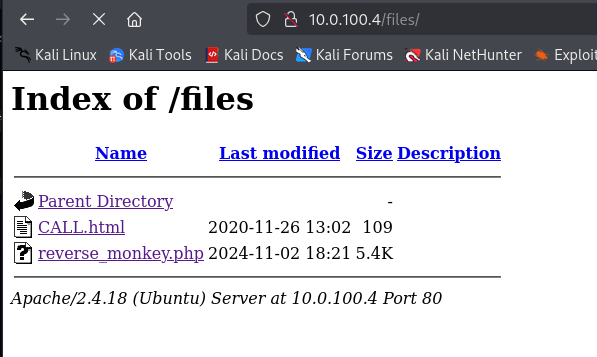
se revisa con dirsearch y otrs programas, el servidor web y nada mas

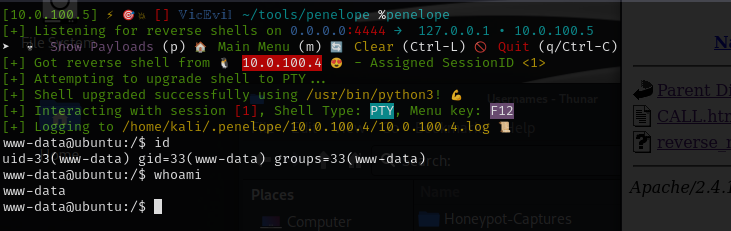


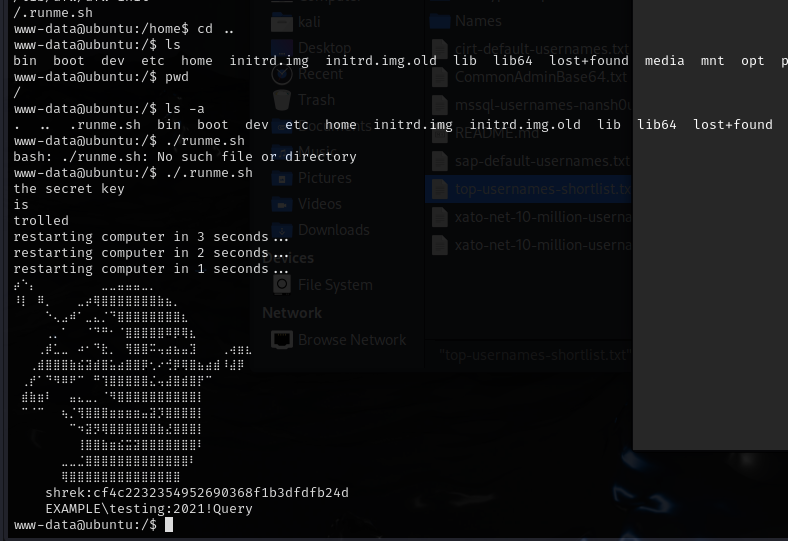
se comprueba que si subo archivos al ftp con user anonymous, salen en el directorio de la web /files

Por lo que se subo un shell reverse en .php y se ejecuta desde el navegador con resultado positivo:





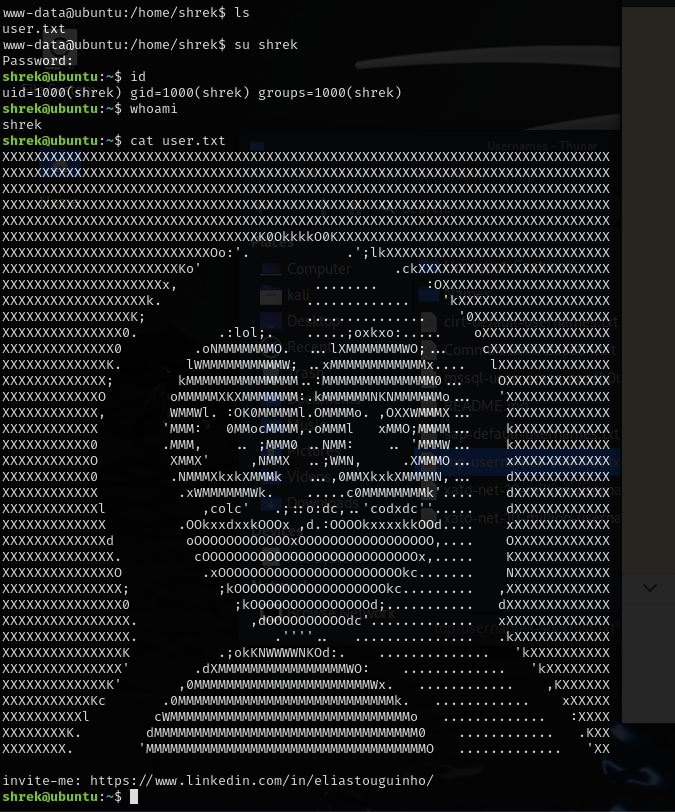


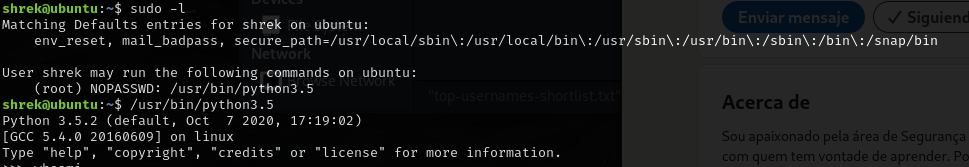
ejecutando find y dando como resusta una larga lista, al final de la misma se encuntra el archvio el cual esta oculto siendo ejecutado.

se descifra el hash MD5 shrek:cf4c2232354952690368f1b3dfdfb24d correspondiendo a “onion”, igual que el titulo de la web donde sali el mensaje de la llamada,

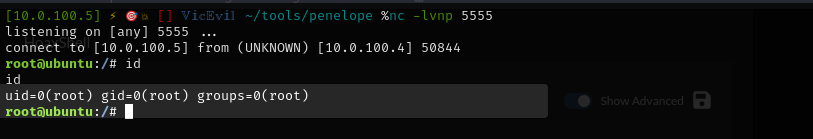
con shrek y onion iniciamos cuanta en sistema usuraio shrek, y abribo un archivo user.txt:



pulsando el enlace:  

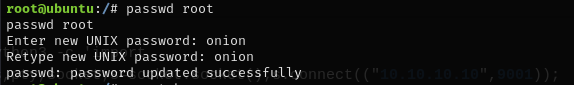





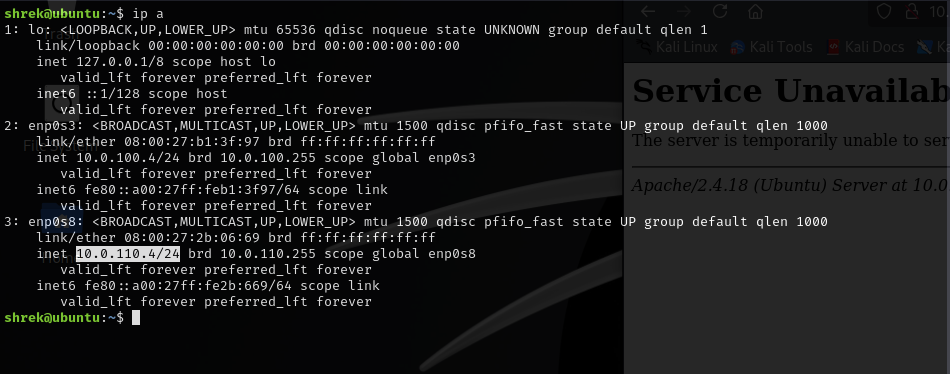


soy root de lña maquina linux User Reto AD.

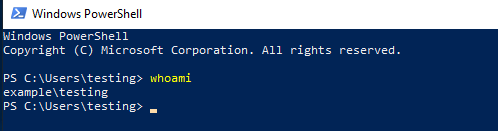
\*\*\*\*\*\*+++ ahora voy a cambiar la contraseña de root para poder acceder al servicio SSH y hacer un tunel dinamico para llegar a la maquina windows



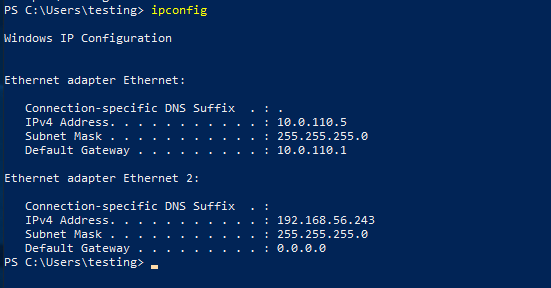
Conexion por ssh en tuenl dinamico por el usuario shrek, consiguiendo la Ip de la otra interfaz de la maquina Linux User reto Ad:



Con la contraseña extraida anteriormente ejecuntado el archivo ./runme.sh, accedemos a la maquina winbdows user:

consultamos las IPs de esta maquina siendo las siguienmtes:



para poder usar de pivoting esta maquina para pasar a la que hay q explotar, vamos usar chiell estableciendo un tunel entre la kali y la maquina windows:

