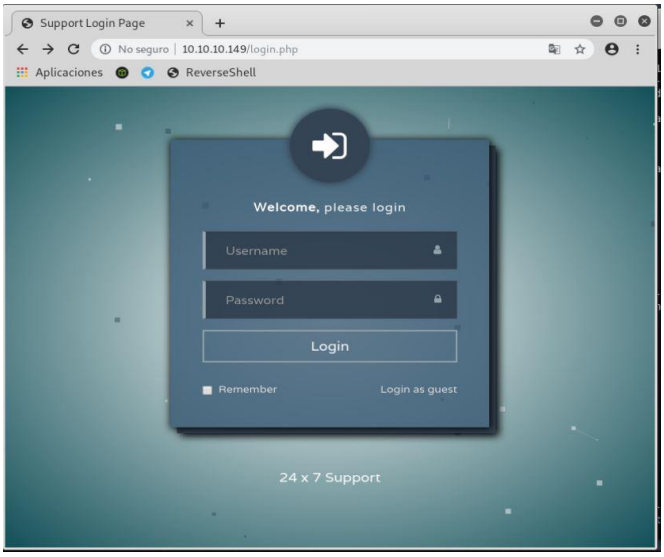
HTB MÁQUINA HEIST

Veamos las características de la Maquina, vemos que tiene una puntuación 4.4, se debe hacer una buena enumeración, vemos que es Windows, entre otras cosas.

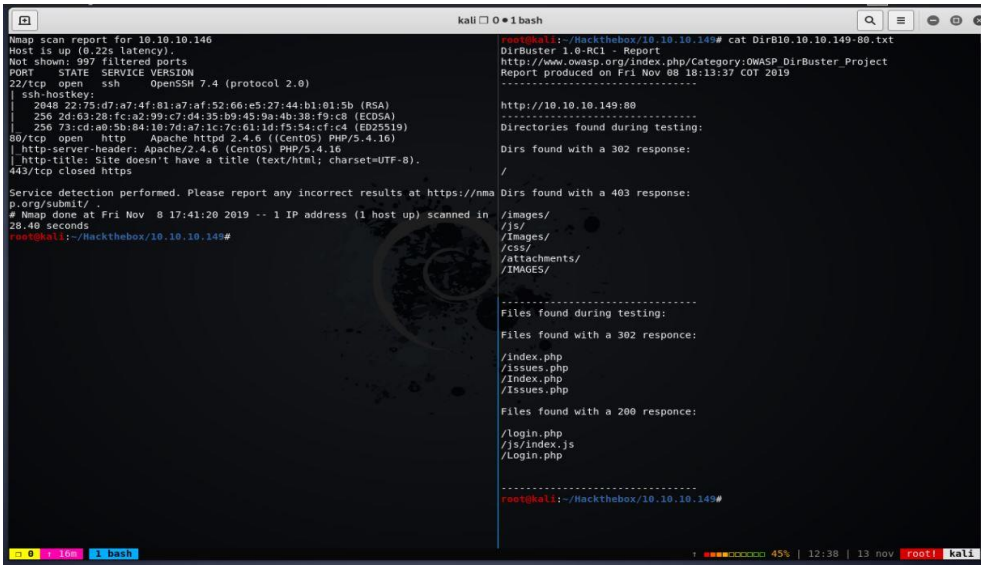
- ***User:***

En la pantalla principal vemos un Login, que nos permite entrar como invitado.



Sauna

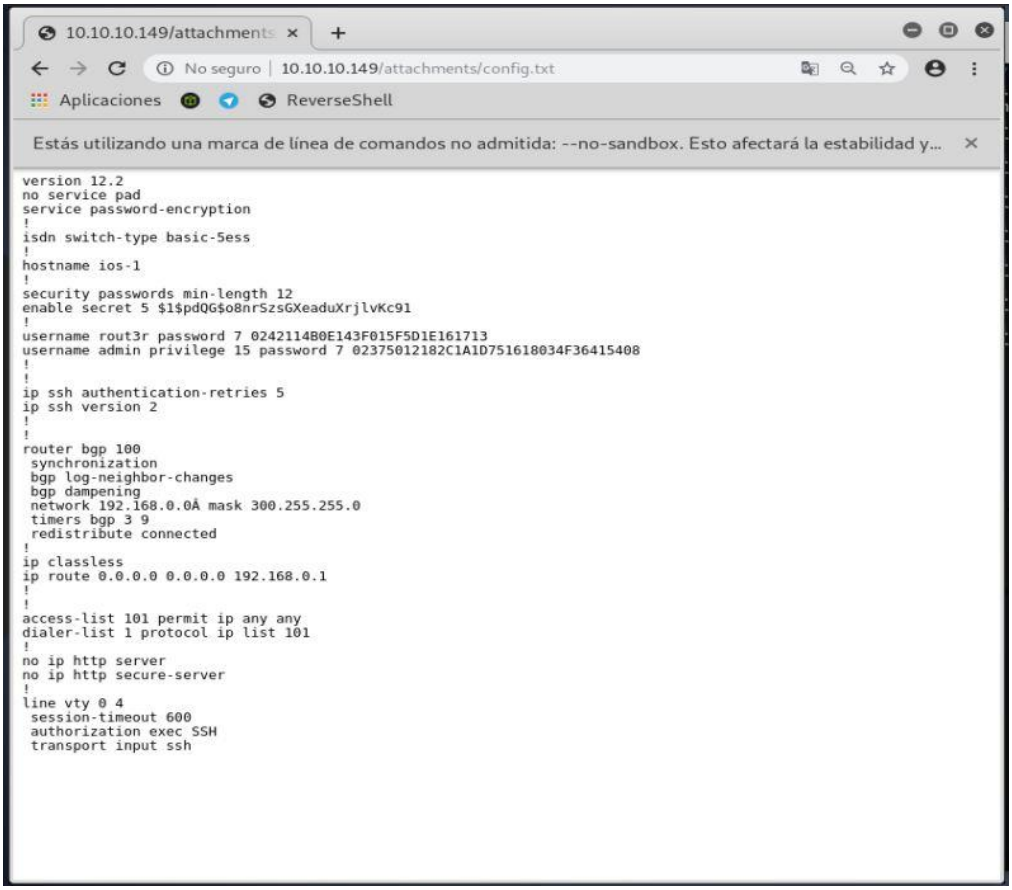
En el primer escaneo no vemos mucho que nos ayude en la explotación.

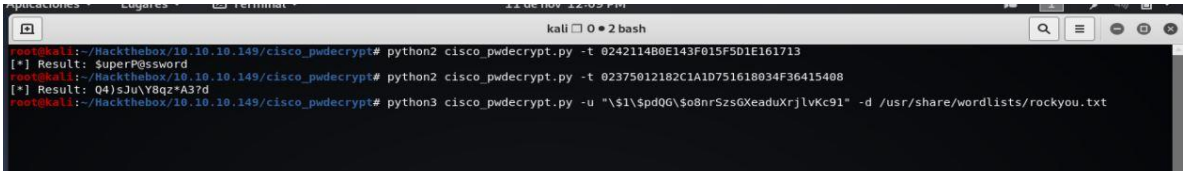


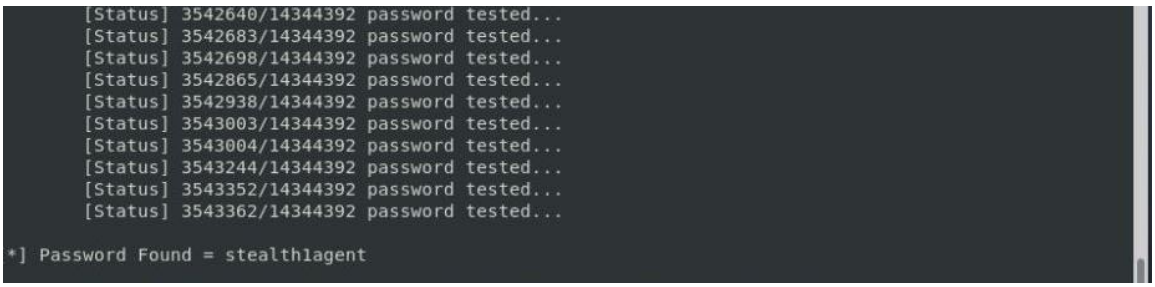
Así que realizamos un escaneo un poco más completo, donde observamos el puerto 5985 Abierto no nos queda muy claro, los servicios que nos encontramos así que realizamos otro scan con nmap en este caso con –script=msrpc-enum, donde vemos que el servicio 5985, está corriendo el servicio wisman, buscamos un poco sobre este servicio y vemos que es un complemento de WinRM. (https://docs.microsoft.com/es-es/powershell/scripting/learn/remoting/wsman-remoting-in-powershell-core?view=powershell-6).

Sauna

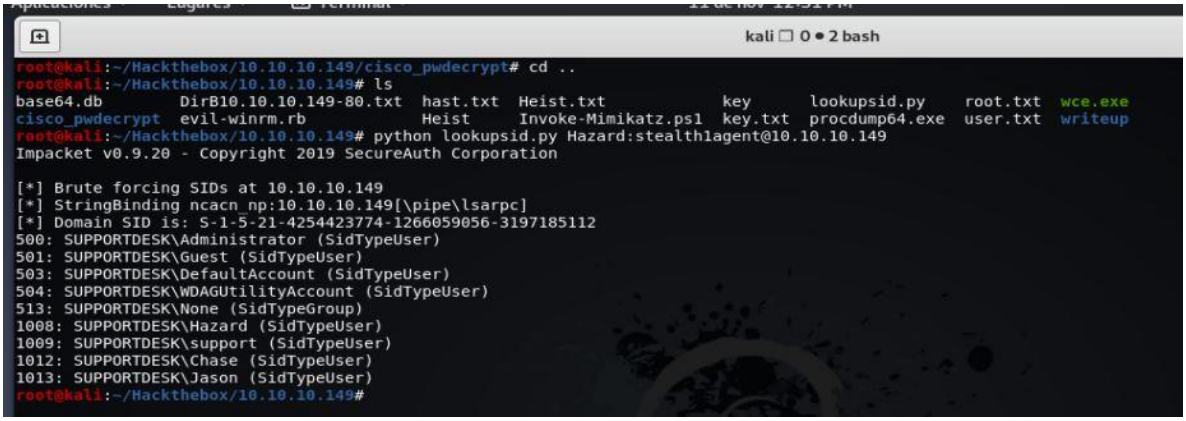
Ingresando como invitado en la página principal encontramos un link que nos lleva a un archivo de configuración Http://10.10.10.149/attachments/config.txt el cual nos muestra unos usuarios y unos hast de cisco Nivel 7 y Nivel 5. Googleando un poco nos encontramos con el script cisco_pwdecrypt.py (https://github.com/axcheron/cisco_pwdecrypt) el cual nos permite decodificar contraseñas tipo 7 y tipo 5 de Cisco, las contraseñas tipo 7 fueron muy rápidas de conseguir, pero la tipo 5, tiene un tiempo considerado de Decodificación.





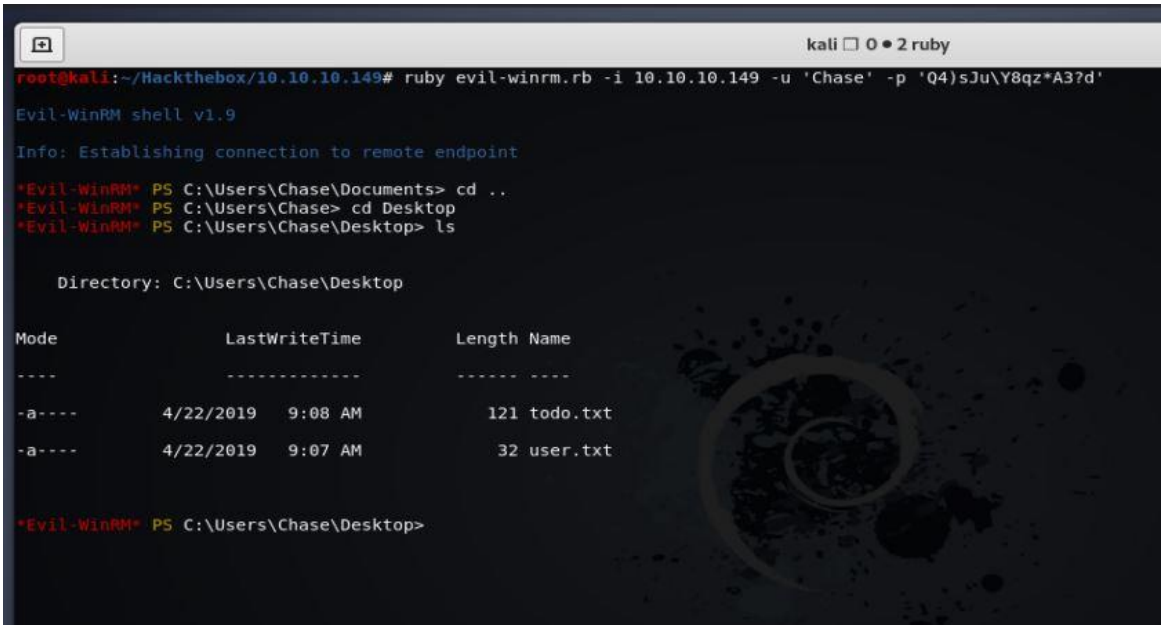


Utilizamos el script Lookupsid.py que nos permite realizar una búsqueda de los usuarios, teniendo ya un Usuario y una contraseña conocida, el cual nos da varios usuarios y ya tenemos unas contraseñas que debemos probar en estos usuarios, El script lo encontramos como parte de la colección de
impacket(https://github.com/SecureAuthCorp/impacket/blob/master/examples/lookupsid.py)



Paro esto vamos a hacer uso del Script de evil-winrm realizado en Ruby que encontramos en: (https://github.com/Hackplayers/evil-winrm) el cual nos permite tener acceso remoto a una máquina, que corre el servicio de winrm, y como hemos visto anteriormente el servicio del puerto 5985 está corriendo winman, que forma parte de este servicio

Con el parámetro -u para el Usuario y -p para el Password, después de probar distintos usuarios, que nos tiró el script lookupid.py con las contraseñas decodificadas de cisco, vemos que podemos tener permisos de usuario con Chase.

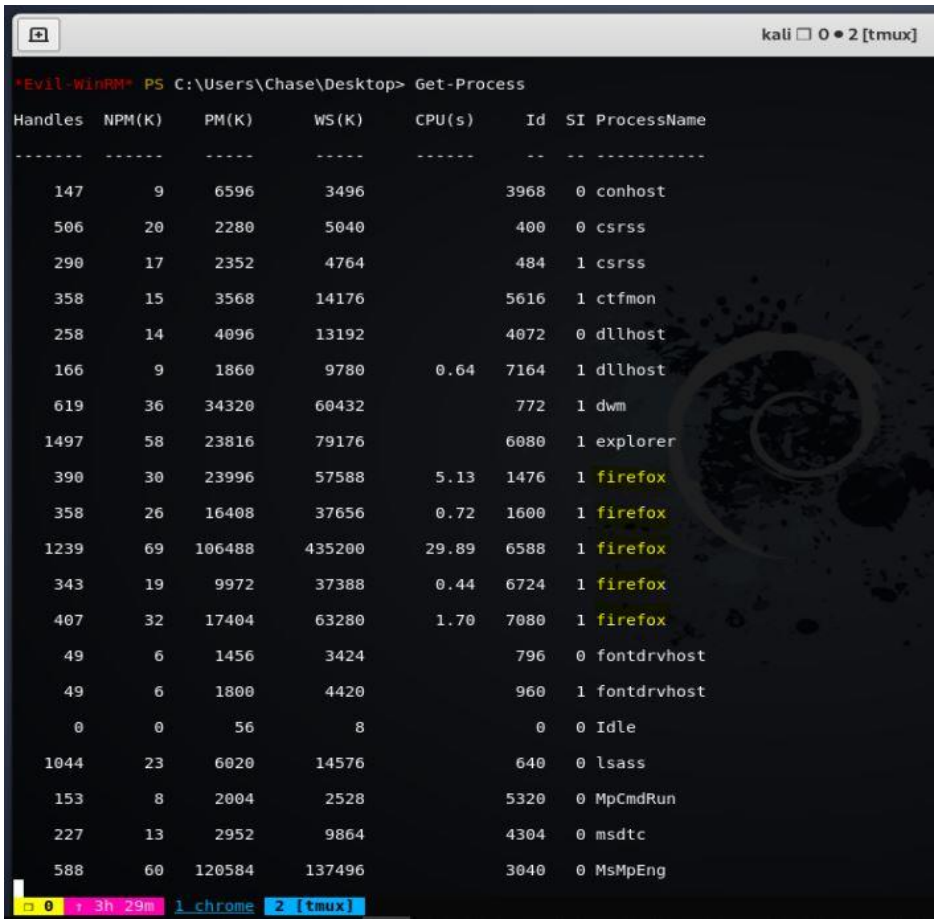


De esta manera encontramos la flag del User.

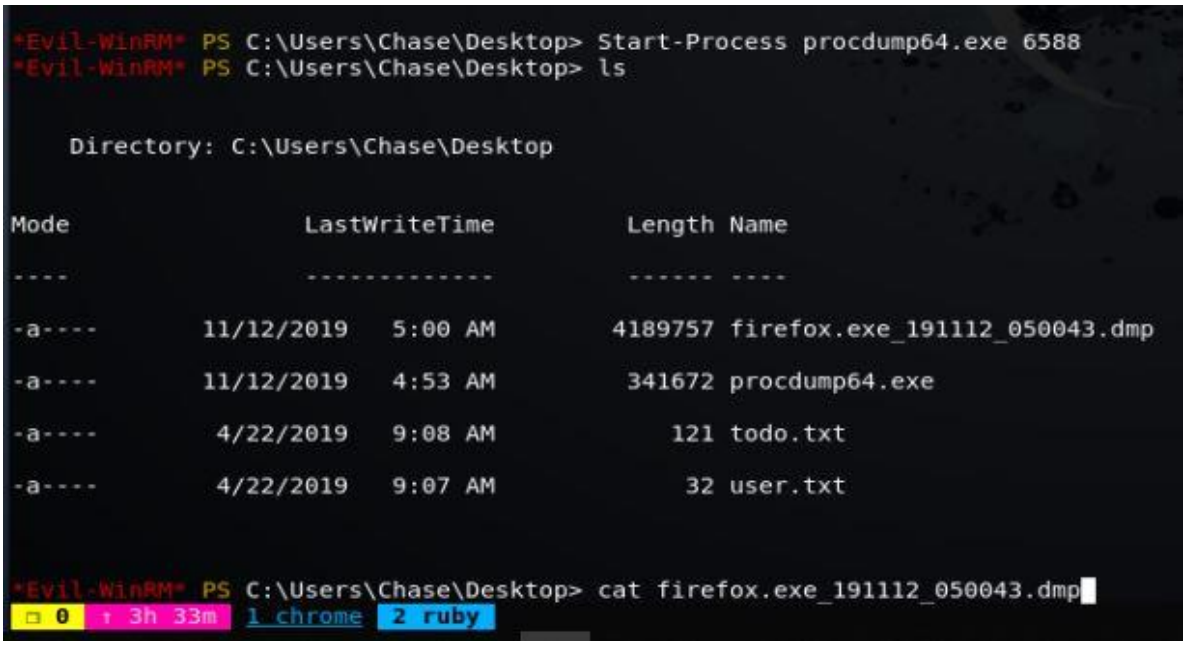
Escalada de Privilegios:

Realizamos un Get-process, pare revisar los procesos que está corriendo la máquina el único proceso que está corriendo es Firefox, así que entendemos que dentro de Firefox encontraremos algún tipo de información, por lo que tendremos que buscar la forma de volcar la memoria de ese proceso, para más tarde ver si encontramos algo de información interesante.

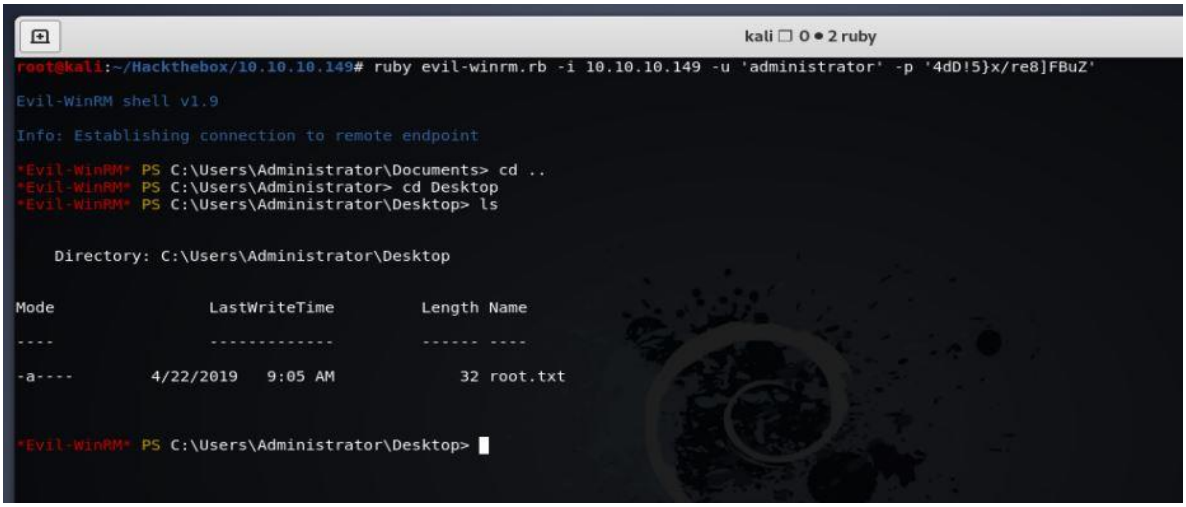
Para hacer esto nos fijamos en el proceso que más uso del procesador está haciendo y con la herramienta procdump64.exe que sirve precisamente para el objetivo que tenemos, monitorizar una aplicación de la cpu y así poder volcar su memoria en un archivo para luego estudiarlo por strings (https://docs.microsoft.com/en-us/sysinternals/downloads/procdump).
El ejecutable nos lo descargamos desde GitHub, en esta colección (https://github.com/phackt/pentest/tree/master/privesc/windows).
Aunque lo podemos encontrar en varios repositorios, Vamos a hacer uso de Procdump.exe



Ejecutamos en procdump64.exe en el ID 6588, para obtener el fiefox.exe_191112_050043.dpm



Realizamos un cat fiefox.exe_191112_050043.dpm para ver que nos arroja al archivo y realizamos una búsqueda con palabras claves como user, username, login en este caso vemos una contraseña de administrador, así que muy posiblemente se pueda escalar privilegios con este Passsword, probaremos en evil-winrm con el usuario administrador conseguido anteriormente y la contraseña encontrada.



De esta manera encontramos la flag del Root.

Saludos de parte de **Fr13ndS**