Access

Synopsis

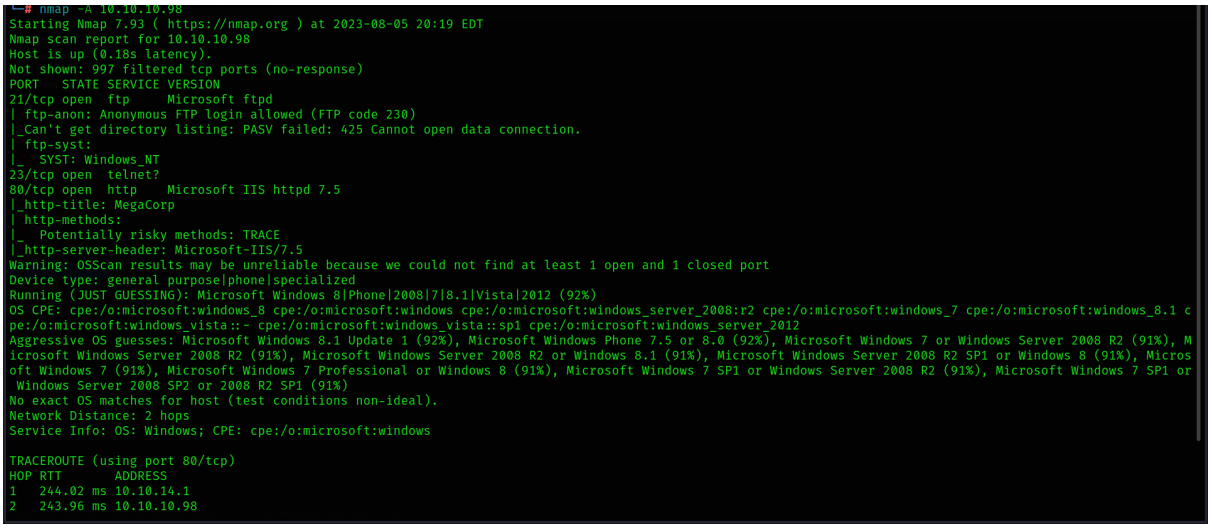
Access highlights how machines associated with the physical security of an environment may not themselves be secure. Also highlighted is how accessible FTP/file shares often lead to getting a foothold or lateral movement. It teaches techniques for identifying and exploiting saved credentials.

Skills

- Knowledge of Windows
- Enumeration of Access databases
- Identification of stored credentials
- DPAPI credentials extraction

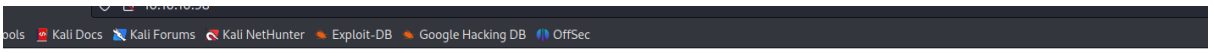
Exploitation

As always we start with the nmap to check what services/ports are open



We see a few ports open, but the most interesting is 23/Telnet

But before digging into that, let's check web port
This gave us only a mock page so we moved from that



LON-MC6

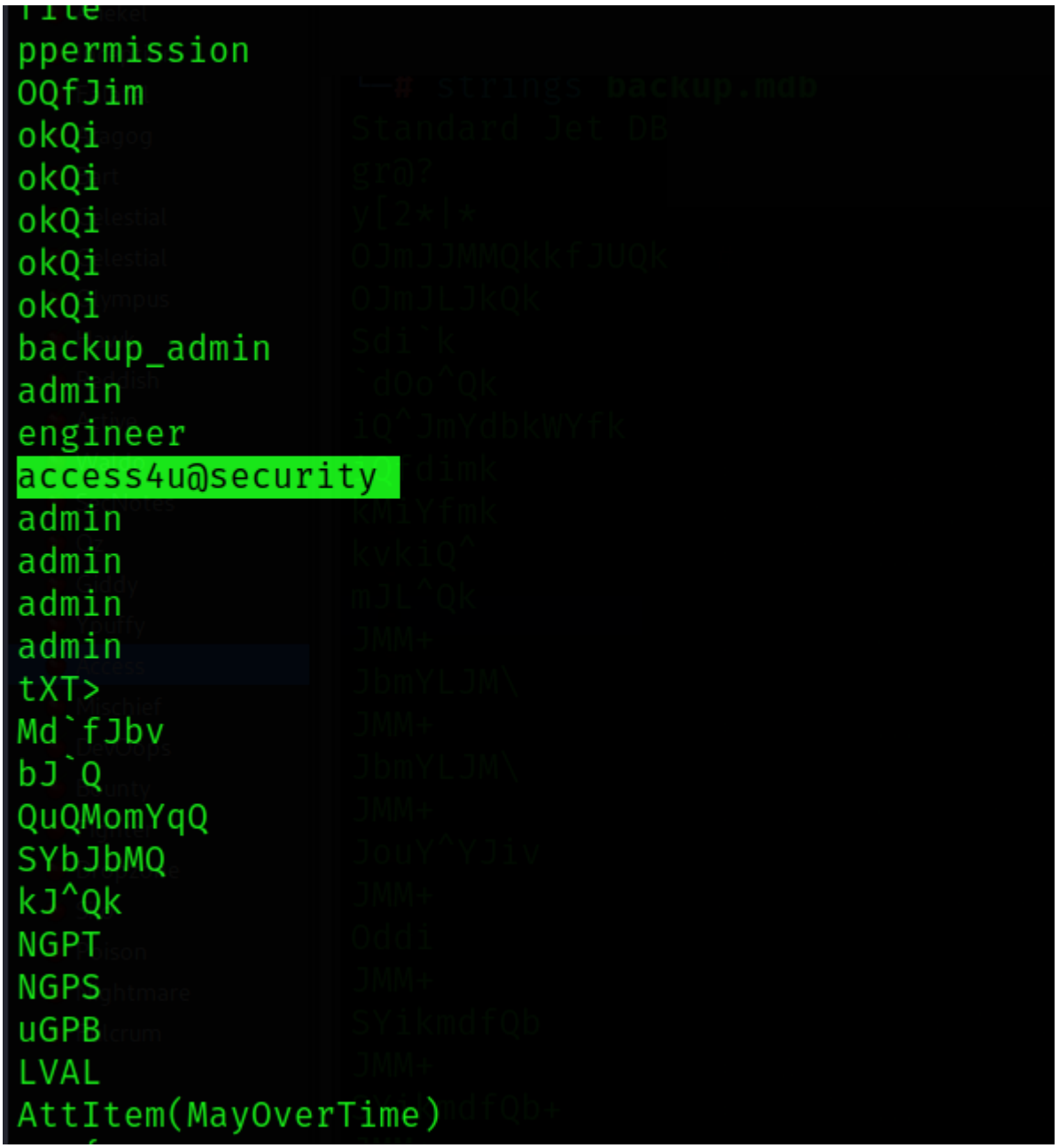
Next we check the FTP service, especially that anonymous access is allowed

```
└─# wget -m --no-passive-ftp ftp://anonymous:anonymous@10.10.10.98
--2023-08-05 20:27:51--  ftp://anonymous:*password*@10.10.10.98/
           => '10.10.10.98/.listing'
Connecting to 10.10.10.98:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PORT ... done.    ==> LIST ... done.

10.10.10.98/.listing                    [ <=>                                ]      97  --.-KB/s    in 0s

==> PORT ... done.    ==> LIST ... done.

10.10.10.98/.listing                    [ <=>                                ]      97  --.-KB/s    in 0s

2023-08-05 20:27:52 (1.15 MB/s) - '10.10.10.98/.listing' saved [194]

--2023-08-05 20:27:52--  ftp://anonymous:*password*@10.10.10.98/Backups/
           => '10.10.10.98/Backups/.listing'
==> CWD (1) /Backups ... done.
==> PORT ... done.    ==> LIST ... done.

10.10.10.98/Backups/.listing            [ <=>                                ]      51  --.-KB/s    in 0s

2023-08-05 20:27:52 (1.01 MB/s) - '10.10.10.98/Backups/.listing' saved [51]

--2023-08-05 20:27:52--  ftp://anonymous:*password*@10.10.10.98/Backups/backup.mdb
           => '10.10.10.98/Backups/backup.mdb'
==> CWD not required.
==> PORT ... done.    ==> RETR backup.mdb ... done.
Length: 5652480 (5.4M)

10.10.10.98/Backups/backup.mdb          94%[=================================================>    ]   5.07M  1.10MB/s    eta 1s
```

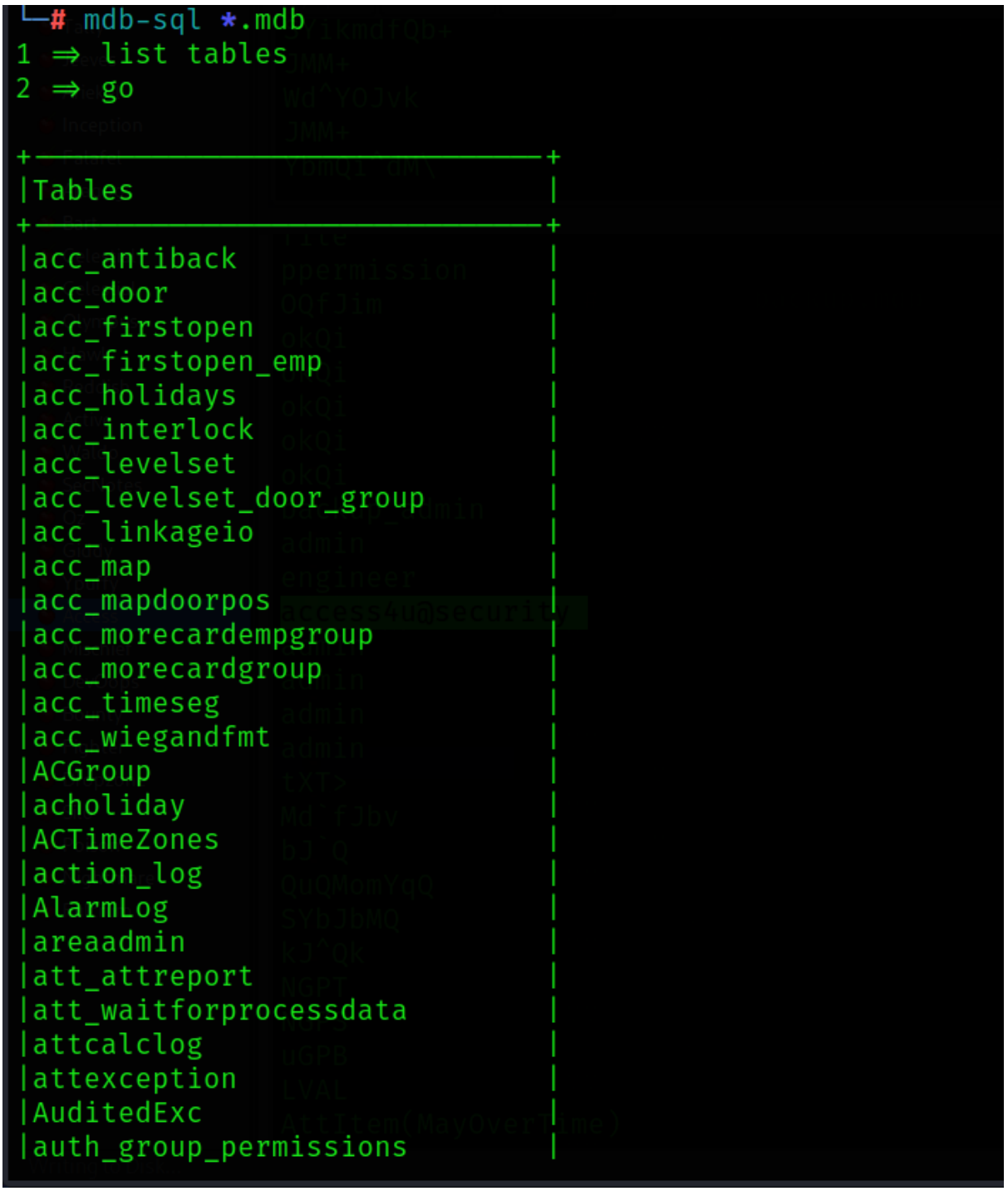
We download files from the service, and we found MDB database file

First we run strings tool to find any human readable information e.g passwords, and after a bit of search we found a string that looks like a password

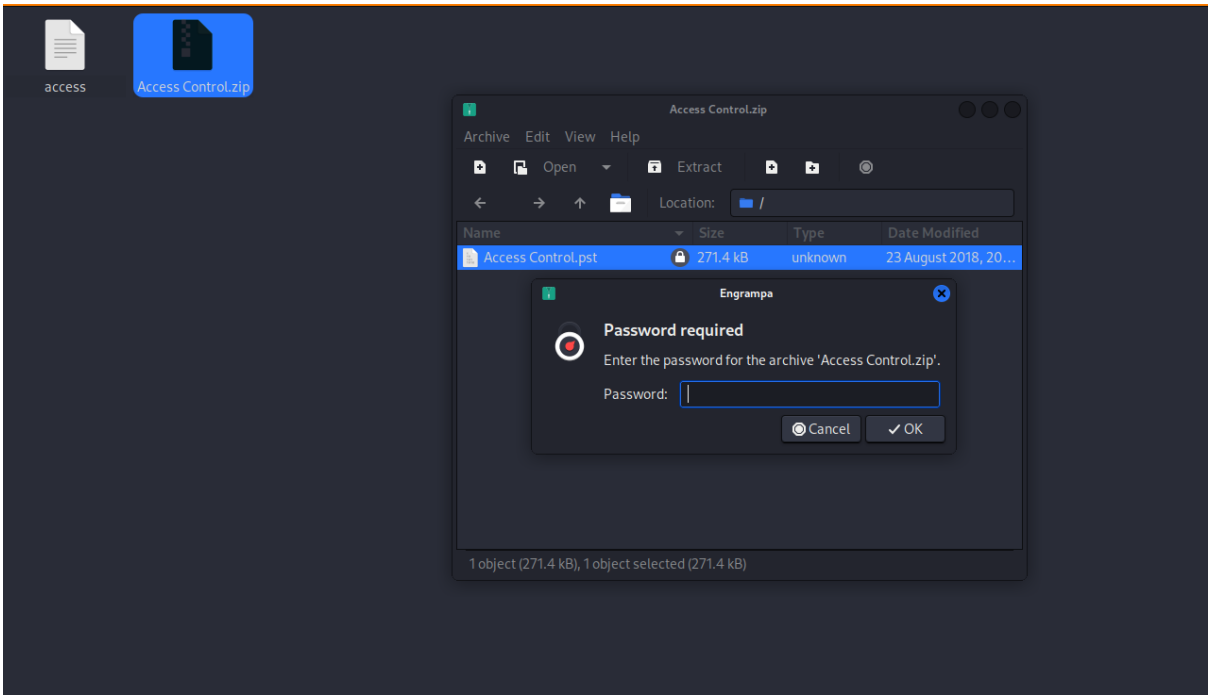

└─# strings backup.mdb
Standard Jet DB
gr@?
y[2*|*
OJmJJMMQkkfJUQk
OJmJLJkQk
Sdi^k
^dOo^Qk
iQ^JmYdbkWYfk
iQfdimk
kMiYfmk
kvkiQ^
mJL^Qk
JMM+
JbmYLJM\
JMM+
JbmYLJM\
JMM+
JouY^YJiv
JMM+
Oddi
JMM+
SYikmdfQb
JMM+
SYikmdfQb+
JMM+
Wd^YOJvk
JMM+
YbmQi^dM\



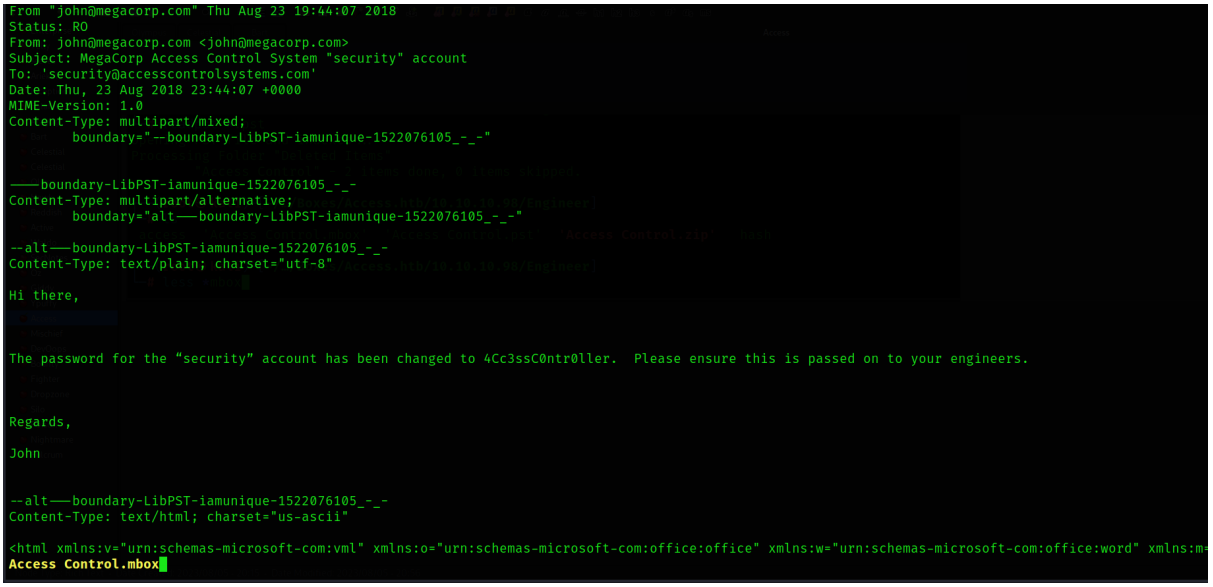
Next we enumerate a content of the database, yet we didn't find anything interesting there



In another directory downloaded from the FTP we found zip file that request password for extraction, so we used the password obtained from analysing MDB file and it worked

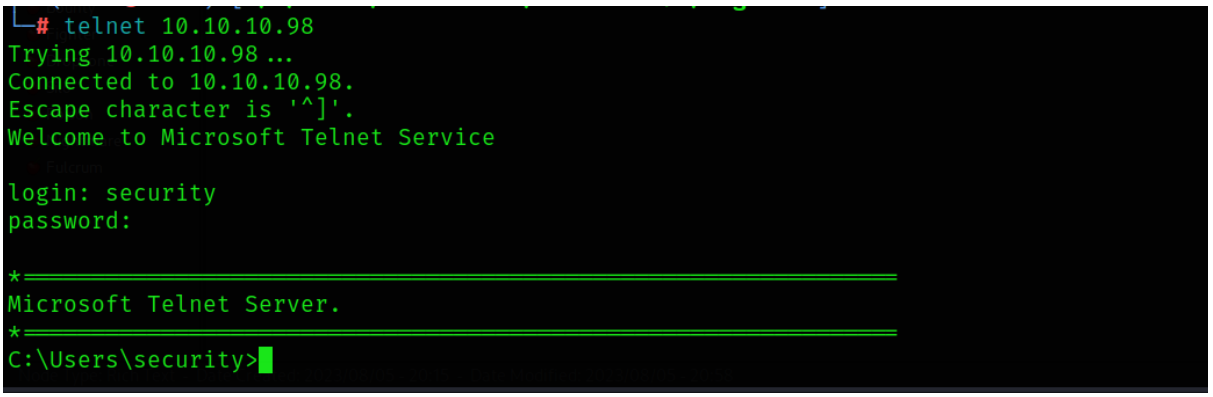


We got .pst file what is an email file format



Reading the email gave us credential to a security account

At this point, it was time to check out the telnet service



We logged into the telnet using credential from the email what provided us with a shell on the box