**Hacking**

**ético**

# Crackear claves

# Índice

[**Crackear claves 1**](#_ncqwc238sads)

[**Índice 2**](#_hr2t6nva06zg)

[**Linux 3**](#_hdzes8ia1b37)

[Archivos: 3](#_z3vpcclh5z0x)

[passwd.txt: 3](#_u24n7ebxps73)

[shadow: 3](#_9ntub7z9xqr)

[Pasos 3](#_u0zsj3mmzdie)

[Formatear los ficheros passwd y shadow con unshadow: 3](#_hcvbjnb4ecu3)

[Crackeo de hashes 4](#_d8q00dnngm1x)

[**Windows 4**](#_7daw6ddh5g53)

[Archivos: 4](#_7w8b99x818yk)

[SAM (Security Account Manager): 4](#_j5tl6h607eyq)

[SYSTEM: 5](#_wxbhkj2i6gvn)

[Pasos 5](#_qmaz1sdlsfrq)

[Formateo de ficheros SAM y SYSTEM con SAMdump2: 5](#_v1915b9p7i3l)

[Crackeo de hashes 5](#_l1tdo97qi6d1)

| Linux |
| --- |
| Archivos: |
| passwd.txt Definición: passwd.txt es un archivo en sistemas basados en Unix que almacena información básica de cuentas de usuario.  Función principal: Contiene detalles como nombres de usuario, identificadores de usuario (UID), identificadores de grupo (GID), nombres completos, directorios de inicio y rutas de shell. Sin embargo, no almacena las contraseñas directamente; estas suelen estar cifradas y almacenadas en el archivo shadow. shadow Definición: shadow es un archivo en sistemas basados en Unix que almacena información sensible de cuentas de usuario, especialmente las contraseñas cifradas.  Función principal: Contiene datos críticos de seguridad, como las contraseñas cifradas, políticas de contraseñas, fechas de expiración, entre otros. Este archivo está diseñado para ser más seguro que passwd.txt y generalmente tiene permisos de lectura restringidos. |
| Pasos |
| Formatear los ficheros passwd y shadow con unshadow: |
| Utilizamos el comando unshadow para combinar la información de los archivos passwd.txt y shadow.txt. Este comando toma como entrada ambos archivos y genera un nuevo archivo con la información combinada en un formato fácilmente por herramienta de crackeo de hashes. |
| unshadow passwd.txt shadow.txt > claves.txt |
| Este comando se encarga de fusionar la información de ambos archivos y redirige el resultado al archivo claves.txt. Ahora, claves.txt contendrá la información combinada de passwd.txt y shadow.txt |
|  |
| Crackeo de hashes |
| El formato es reconocible por por john the ripper |
| john claves.txt |
|  |

| Windows |
| --- |
| Archivos: |
| SAM (Security Account Manager): Definición: SAM es una base de datos en el sistema operativo Windows que almacena información de cuentas de usuario y contraseñas en entornos locales.  Función principal: Contiene datos de seguridad, como contraseñas cifradas y perfiles de usuario. El archivo SAM está ubicado en el directorio %SystemRoot%\system32\config y es esencial para el inicio de sesión y la autenticación de usuarios locales en un sistema Windows. |
| SYSTEM: Definición: SYSTEM es otro archivo en el sistema operativo Windows que almacena información importante del registro del sistema.  Función principal: Contiene configuraciones y parámetros del sistema, como la configuración del hardware, configuración del sistema operativo y detalles de seguridad. El archivo SYSTEM también está ubicado en el directorio %SystemRoot%\system32\config |
| Pasos |
| Formateo de ficheros SAM y SYSTEM con SAMdump2: |
| samdump2 SAM SYSTEM > claves.txt |
| Crackeo de hashes |
| John —format=NT –wordlist=/usr/share/wordlist/rockyou.txt.gz claves |
|  |