

Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red



Módulo Profesional: SAD
Unidad de Trabajo 4.- Seguridad Lógica

*Departamento de Informática y Comunicación
IES San Juan Bosco (Lorca-Murcia)
Profesor: Juan Antonio López Quesada*





Índice de Contenidos

Principios de la Seguridad Lógica

Control de Acceso Lógico

Ataques contra contraseñas en Sistemas Windows

Ataques contra contraseñas en Sistemas Linux

Congeladores

Referencias WEB

Enlaces a Herramientas SW

Prácticas/Actividades



Objetivos de la Unidad de Trabajo:

Profundizar en aspectos de seguridad lógica.

Valorar la importancia del uso de contraseñas seguras.

Restringir el acceso autorizado en el arranque, sistemas operativos, ficheros, carpetas y aplicaciones.

Analizar las ventajas de disponer el sistema y aplicaciones actualizadas.

Garantizar el acceso restringido de los usuarios a datos y aplicaciones, mediante políticas de seguridad.

Abstract/Resumen:

Aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas.

- ◆ *UT4: seguridad de acceso lógico a sistemas y políticas de privilegios a usuarios y grupos.*
- ◆ *UT5: software antimalware.*
- ◆ *UT6: Criptografía.*

slice:\$1\$NLJJ6\$ow5g1I1NgYITqqQQy5D21:14234:0:99999:7:::	
Contraseña	Contraseña encriptada. La forman entre 13 y 24 caracteres (a-z, A-Z, 0-9, \, /). Si comienza por el carácter \$, indica que la contraseña se ha encriptado usando un algoritmo distinto de DES. Si comienza por \$1\$, el algoritmo de cifrado está basado en MD5.
Nombre de usuario	Nombre que identifica al usuario en el sistema. Debe tener entre 1 y 32 caracteres.
Caducidad	Días a los que se deshabilita la cuenta contados desde el 1 de enero de 1970.
Inactivo	Días a los que se deshabilita la cuenta después de que caduque la contraseña.
Aviso	Días a los que el usuario será avisado de que debe cambiar la contraseña antes de que ésta caduque.
Máximo	Días durante los que la contraseña es válida. Al terminar el usuario tiene que cambiar la contraseña.
Mínimo	Días que deben pasar como mínimo para que el usuario pueda cambiar la contraseña.
Último cambio	Días que han pasado desde la última vez que la contraseña fue cambiada contados desde el 1 de enero de 1970.

Principios de la Seguridad Lógica

El activo más importante que se poseen las organizaciones es **la información**, y por lo tanto deben existir técnicas más allá de la seguridad física que la aseguren, estas técnicas las brinda la seguridad lógica.

La seguridad lógica consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo*. A lo largo de los capítulos 4 (seguridad en el acceso lógico a sistemas), 5 (software antimalware), y 6 (criptografía), veremos algunos de los métodos fundamentales.

Algunas de las principales amenazas que tendrán que combatir los administradores de sistemas son el acceso y modificaciones no autorizadas a datos y aplicaciones.

La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

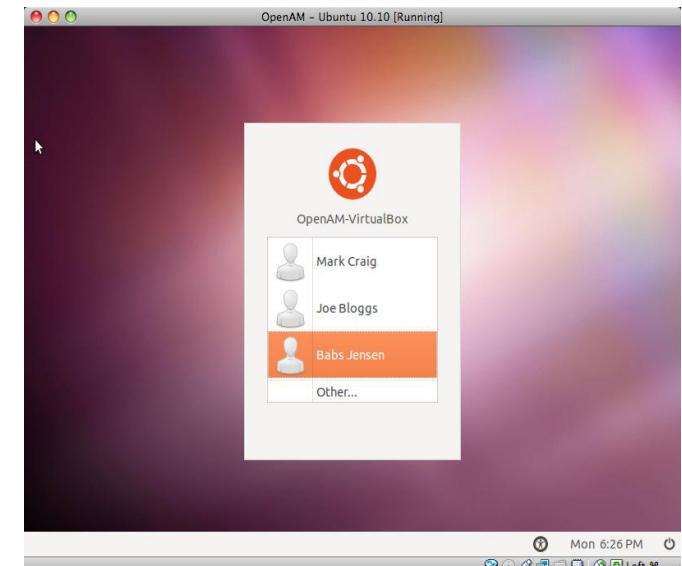
Como principio básico de seguridad lógica en la configuración de sistemas: todo lo que no está permitido debe estar prohibido.

Control de Acceso Lógico

- El control de acceso lógico es la principal línea de defensa para la mayoría de los sistemas, permitiendo prevenir el ingreso de personas no autorizadas a la información de los mismos.
- Para realizar la tarea de controlar el acceso se emplean 2 procesos normalmente: **identificación** y **autenticación**. Se denomina identificación al momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esta identificación.
- Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de ahí a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. *Esto se denomina single login o sincronización de passwords.*

Control de Acceso Lógico

- Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un ***servidor de autenticaciones*** sobre el cual los usuario se identifican y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder.
- Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. ***Es el caso de servidores LDAP en GNU/Linux y Active Directory sobre Windows Server.***



Control de Acceso Lógico

□ Los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, los más comunes son:

Ataque de fuerza bruta: se intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Cuanto más corta, más sencilla de obtener probando combinaciones.

Ataque de diccionario: intentar averiguar una clave probando todas las palabras de un diccionario o conjunto de palabras comunes. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.

Control de Acceso Lógico

Políticas de Contraseñas

- Las contraseñas son las claves que se utilizan para obtener acceso a información personal que se ha almacenado en el equipo y aplicaciones, como en los entornos web (mail, banca online, redes sociales, etc.).

Para que una contraseña sea segura se recomienda:

Longitud mínima: cada carácter en una contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Las contraseñas a ser posible deben contener un mínimo de 8 caracteres, lo ideal es que tenga 14 caracteres o más.

Combinación de caracteres (letras minúsculas y mayúsculas, números y símbolos especiales): cuanto más diversos sean los tipos de caracteres de la contraseña más difícil será adivinarla.

Control de Acceso Lógico

Políticas de Contraseñas

- Para un ataque de fuerza bruta que intenta encontrar contraseñas generando todas las combinaciones posibles, si empleamos una contraseña de 5 caracteres en minúscula para el idioma español que posee 27 caracteres diferentes, tendría que probar $27^5 = 14\ 348\ 907$ combinaciones a probar.
- En caso de emplear mayúsculas y minúsculas el número de combinaciones se multiplicaría siendo $(27 \times 2)^5 = 52^5 = 380\ 204\ 032$ combinaciones a probar.

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar, a fin de evitar contraseñas poco seguras, se recomienda:

No incluir secuencias ni caracteres repetidos. Como "12345678", "222222", "abcdefg"

No utilizar el nombre de inicio de sesión.

No utilizar palabras de diccionario de ningún idioma.

Utilizar varias contraseñas para distintos entornos.

Evitar la opción de contraseña en blanco.

No revelar la contraseña a nadie y no escribirla en equipos que no controlas.

Cambiar las contraseñas con regularidad.

Control de Acceso Lógico

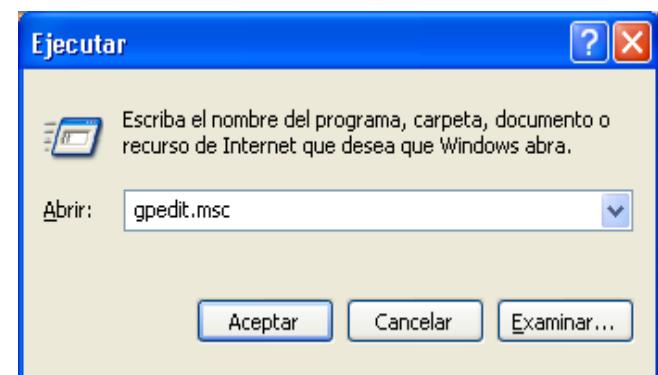
Configuración de Contraseñas Seguras en Windows y Linux

- Todas las recomendaciones anteriormente citadas están muy bien cuando se conocen y se llevan a cabo, pero, ¿no sería mejor opción evitar que los usuarios tengan contraseñas inseguras o débiles y que no se cambien nunca? Veamos que opciones de configuración sobre el control de contraseñas poseen los sistemas operativos.

Windows

Las **directivas de cuentas** nos permiten configurar el comportamiento que van a tener éstas ante una serie de sucesos. La importancia de una correcta configuración de estas directivas radica en que desde ellas vamos a poder controlar de una forma más eficiente la forma de acceder a nuestro ordenador.

En primer lugar, accedemos a la ventana de **Directivas de seguridad de cuentas**, mediante la ejecución del comando **gpedit.msc** o **Herramientas administrativas / Directivas de seguridad local**.



Control de Acceso Lógico

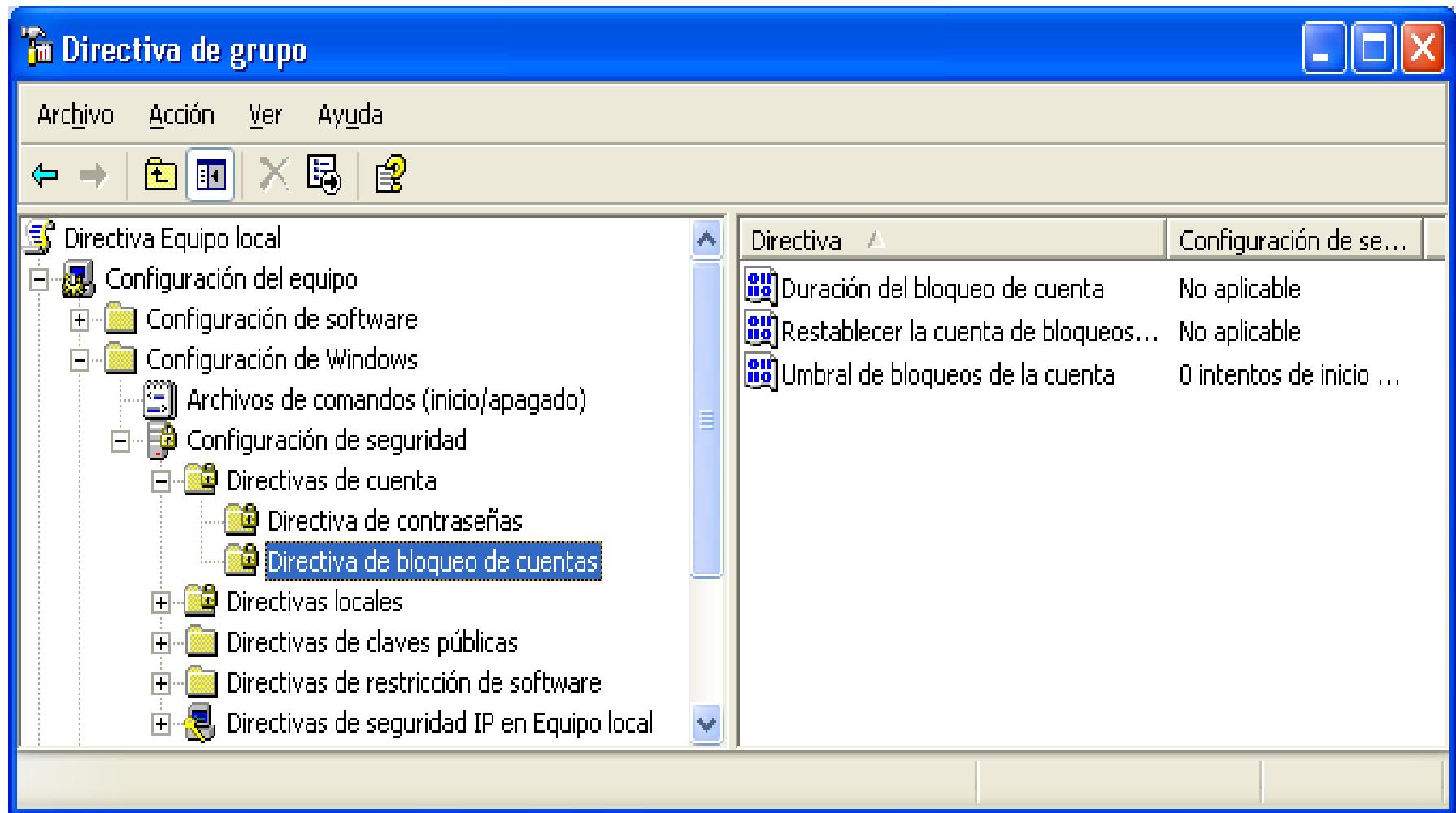
Configuración de Contraseñas Seguras en Windows y Linux

The screenshot shows the Windows Group Policy Management console. The left pane displays a tree structure of policy settings under 'Directiva Equipo local'. The 'Directiva de contraseñas' node under 'Configuración de seguridad' is selected and highlighted in blue. The right pane lists various password-related policies with their current configurations:

Directiva	Configuración de se...
Almacenar contraseña usando cifr...	Deshabilitada
Forzar el historial de contraseñas	0 contraseñas recor...
Las contraseñas deben cumplir los ...	Deshabilitada
Longitud mínima de la contraseña	0 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	0 días

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux



Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

Dentro de las directivas de contraseña nos encontramos con una serie de directivas como:

- Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.
- Forzar el historial de contraseñas: Establece el número de contraseñas a recordar, los usuarios no pueden utilizar la misma contraseña cuando ésta caduca.. Se recomienda un valor mínimo de 1.
- Las contraseñas deben cumplir los requerimientos de complejidad: Se recomienda habilitar esta opción, la cual obliga para nuevas contraseñas:

6 caracteres como mínimo.

Contener caracteres de al menos tres de las cinco clases siguientes: Mayúsculas, minúsculas, dígitos en base 10, caracteres no alfanuméricos (por ejemplo: !, \$, # o %), otros caracteres Unicode.

No contener tres o más caracteres del nombre de cuenta del usuario.

- Longitud mínima de la contraseña.
- Vigencia máxima de la contraseña: Establece el número de días máximo que una contraseña va a estar activa.
- Vigencia mínima de la contraseña: Establece el número de días mínimos que una contraseña va a estar activa.

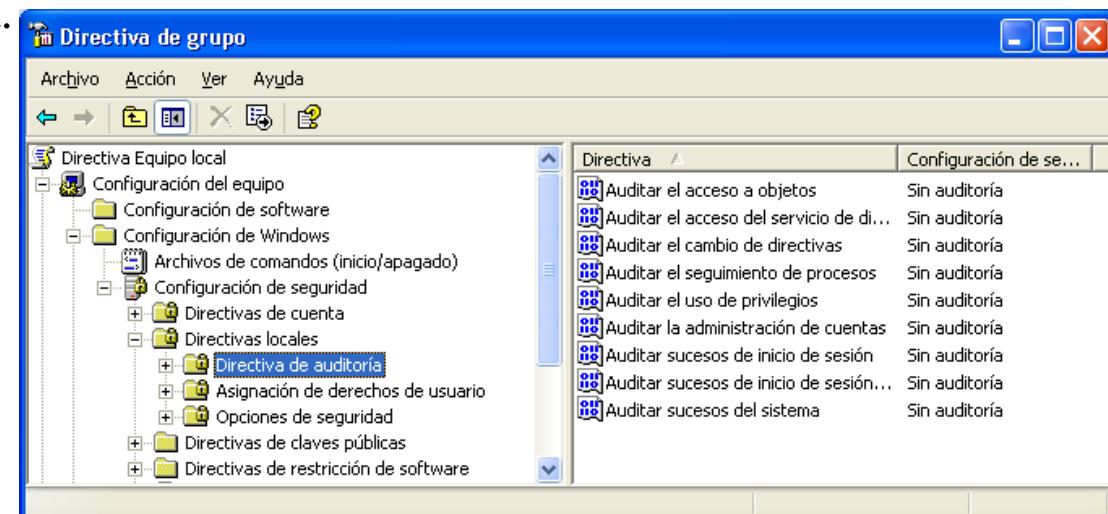
Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

Directiva de bloqueo de cuentas:

- Duración del bloqueo de cuentas: Establece, en minutos, el tiempo que una cuenta debe permanecer bloqueada.
- Restablecer la cuenta de bloqueos después de: Establece, en minutos, el tiempo que ha de pasar para restablecer la cuenta de bloqueos.
- Umbral de bloqueos de la cuenta: Establece el número de intentos fallidos para bloquear el acceso a una cuenta.

Para controlar por parte del administrador los sucesos al sistema habilitaremos las Directivas locales / Directiva de auditoria.. El visor de sucesos nos permitirá analizarlos.



<http://www.microsoft.com/spain/technet/recursos/articulos/secmod49.mspx>

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

GNU/Linux

- El control sobre complejidad y cifrado en contraseñas se realiza en GNU/Linux mediante el servicio PAM (Pluggable Authentication Module).
- El módulo pam-cracklib está hecho específicamente para determinar si es suficientemente fuerte una contraseña que se va a crear o modificar con el comando passwd.

Para instalarlo ejecutaremos: **sudo apt-get install libpam-cracklib**.

- *Uno de los comandos de asignación de contraseñas a usuarios en el acceso a sistemas GNU/Linux suele ser passwd, y su archivo de configuración asociado es /etc/pam.d/passwd. A su vez éste suele referenciar a /etc/pam.d/common-password.*
- *En dicho archivo podremos indicarle las características de los módulos a emplear, en el ejemplo pam-cracklib.so (instalado para el control de la complejidad en contraseñas de usuario) y pam-unix.so (preinstalado y el más empleado por defecto)*

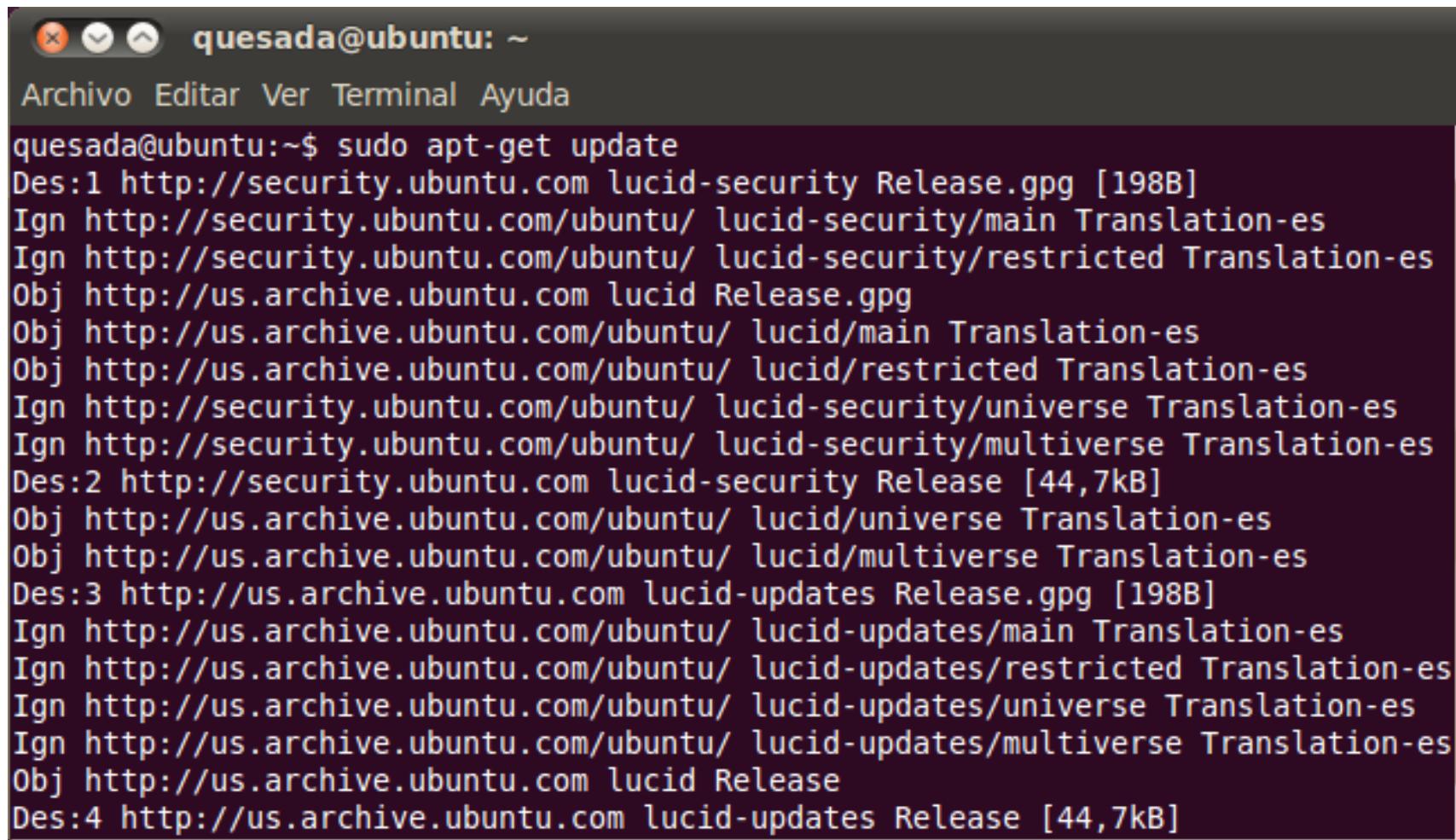
Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

```
quesada@ubuntu: ~
Archivo Editar Ver Terminal Ayuda
quesada@ubuntu:~$ sudo apt-get install libpam-cracklib
[sudo] password for quesada:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalaron de forma automática los siguientes paquetes y ya no son necesarios
.
    linux-headers-2.6.32-33-generic linux-headers-2.6.32-33
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
    cracklib-runtime libcrack2
Se instalarán los siguientes paquetes NUEVOS:
    cracklib-runtime libcrack2 libpam-cracklib
0 actualizados, 3 se instalarán, 0 para eliminar y 14 no actualizados.
Necesito descargar 305kB de archivos.
Se utilizarán 1421kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?
```

Control de Acceso Lógico

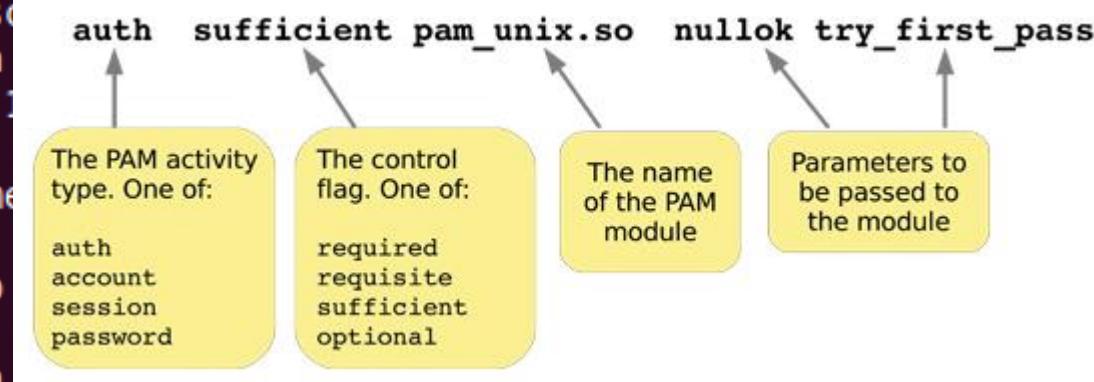
Configuración de Contraseñas Seguras en Windows y Linux



```
quesada@ubuntu: ~
Archivo Editar Ver Terminal Ayuda
quesada@ubuntu:~$ sudo apt-get update
Des:1 http://security.ubuntu.com lucid-security Release.gpg [198B]
Ign http://security.ubuntu.com/ubuntu/ lucid-security/main Translation-es
Ign http://security.ubuntu.com/ubuntu/ lucid-security/restricted Translation-es
Obj http://us.archive.ubuntu.com lucid Release.gpg
Obj http://us.archive.ubuntu.com/ubuntu/ lucid/main Translation-es
Obj http://us.archive.ubuntu.com/ubuntu/ lucid/restricted Translation-es
Ign http://security.ubuntu.com/ubuntu/ lucid-security/universe Translation-es
Ign http://security.ubuntu.com/ubuntu/ lucid-security/multiverse Translation-es
Des:2 http://security.ubuntu.com lucid-security Release [44,7kB]
Obj http://us.archive.ubuntu.com/ubuntu/ lucid/universe Translation-es
Obj http://us.archive.ubuntu.com/ubuntu/ lucid/multiverse Translation-es
Des:3 http://us.archive.ubuntu.com lucid-updates Release.gpg [198B]
Ign http://us.archive.ubuntu.com/ubuntu/ lucid-updates/main Translation-es
Ign http://us.archive.ubuntu.com/ubuntu/ lucid-updates/restricted Translation-es
Ign http://us.archive.ubuntu.com/ubuntu/ lucid-updates/universe Translation-es
Ign http://us.archive.ubuntu.com/ubuntu/ lucid-updates/multiverse Translation-es
Obj http://us.archive.ubuntu.com lucid Release
Des:4 http://us.archive.ubuntu.com lucid-updates Release [44,7kB]
```

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux



The diagram shows a PAM configuration line with four yellow callout boxes and arrows pointing to specific words:

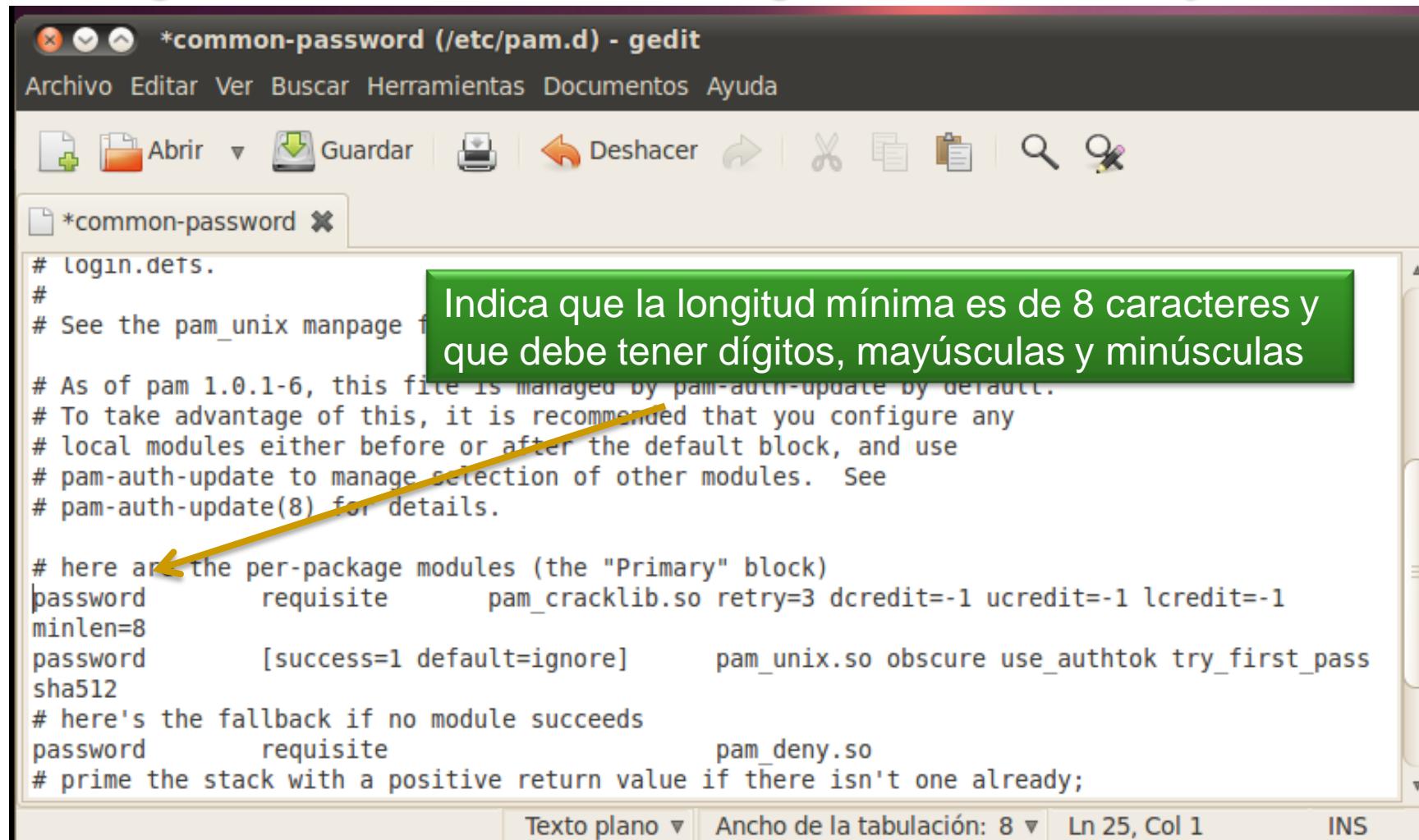
- auth**: The PAM activity type. One of:
auth
account
session
password
- sufficient**: The control flag. One of:
required
requisite
sufficient
optional
- pam_unix.so**: The name of the PAM module
- nullok try_first_pass**: Parameters to be passed to the module

A yellow arrow points from the word "common" in the file listing below to the "common-password" line in the configuration file.

```
quesada@ubuntu: /etc/pam.d
Archivo Editar Ver Terminal Ayuda
Registering documents with so
Procesando disparadores para
Configurando libcrack2 (2.8.1)
Configurando cracklib-runtime
Configurando libpam-cracklib
Procesando disparadores para
ldconfig deferred processing now taking place
quesada@ubuntu:~$ cd /etc/pam.d/
quesada@ubuntu:/etc/pam.d$ ls
atd           common-password
chfn          common-session
chpasswd      common-session-noninteractive
chsh          cron
common-account cups
common-auth   gdm
common-auth   gdm-autologin
common-auth   gnome-screensaver
common-auth   login
common-auth   newusers
common-auth   other
common-auth   passwd
quesada@ubuntu:/etc/pam.d$
```

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux



The screenshot shows the gedit text editor displaying the contents of the `/etc/pam.d/common-password` file. The file contains configuration for password authentication modules. A yellow arrow points from the text "Indica que la longitud mínima es de 8 caracteres y que debe tener dígitos, mayúsculas y minúsculas" to the line `minlen=8`.

```
# login.dets.
#
# See the pam_unix manpage for details.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite      pam_cracklib.so retry=3 dcredit=-1 ucredit=-1 lcredit=-1
minlen=8
password      [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass
sha512
# here's the fallback if no module succeeds
password      requisite      pam_deny.so
# prime the stack with a positive return value if there isn't one already;
```

Indica que la longitud mínima es de 8 caracteres y que debe tener dígitos, mayúsculas y minúsculas

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

Cuando empleemos de nuevo el comando `passwd` para renovación de contraseñas de un usuario, dicho comando verificará que se cumplen las reglas descritas en el archivo de configuración `common-password`.

Para visualizar los accesos al sistema y otros sucesos del sistema o logs, estos se guardan en archivos ubicados en el directorio `/var/log`, aunque muchos programas manejan sus propios logs y los guardan en `/var/log/<programa>`.

Con respecto al acceso e identificación de usuarios encontramos:

- `/var/log/auth.log`: se registran los login en el sistema. Los intentos fallidos se registran en líneas con información del tipo `invalid password` o `authentication failure`.

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

The screenshot shows the 'auth.log - Visor de sucesos del sistema' window. The left pane lists log files: Xorg.0.log, auth.log (selected), auth.log.1, boot, boot.log, bootstrap.log, daemon.log, daemon.log.1, debug, debug.1, dmesg, dmesg.0, dpkg.log, dpkg.log.1, and fontconfig.log. The right pane displays log entries from the auth.log file. The entries show multiple password changes (passwd[2095], passwd[2101], passwd[2181], passwd[2186], passwd[2191], passwd[2196], passwd[2201], passwd[2206], passwd[2211]) for the user 'ubuntu' on November 5, 2011, between 11:50:22 and 12:02:20.

Fecha/Hora	Usuario	Acción	Detalles
Nov 5 11:50:22	ubuntu	sudo:	quesada : TTY=pts,
Nov 5 11:52:09	ubuntu	sudo:	quesada : TTY=pts,
Nov 5 11:57:42	ubuntu	sudo:	quesada : TTY=pts,
Nov 5 11:58:13	ubuntu	sudo:	quesada : TTY=pts,
Nov 5 12:02:02	ubuntu	polkitd(authority=local)	
Nov 5 12:02:18	ubuntu	groupadd[2068]:	group add
Nov 5 12:02:18	ubuntu	groupadd[2068]:	group add
Nov 5 12:02:18	ubuntu	groupadd[2068]:	new group
Nov 5 12:02:18	ubuntu	useradd[2072]:	new user:
Nov 5 12:02:18	ubuntu	usermod[2079]:	change user
Nov 5 12:02:18	ubuntu	chfn[2084]:	changed user
Nov 5 12:02:19	ubuntu	passwd[2095]:	password fo
Nov 5 12:02:19	ubuntu	passwd[2101]:	password fo
Nov 5 12:02:19	ubuntu	gpasswd[2181]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2186]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2191]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2196]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2201]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2206]:	user pruel
Nov 5 12:02:20	ubuntu	gpasswd[2211]:	user pruel

6 líneas (876 bytes) - última actualización: sáb nov 5 11:42:53 2011

Control de Acceso Lógico

Configuración de Contraseñas Seguras en Windows y Linux

PAM (Pluggable Authentication Modules) Face
Authentication: Install/Configure for SUDO



PAM (Pluggable Authentication Modules) Face
Authentication: Install/Configure for LOGIN

Control de Acceso Lógico

Peligros de las Distribuciones LIVE!



Son innumerables los sistemas operativos arrancables desde unidades extraíbles USB, CD o DVD en modo Live sin necesidad de formatear e instalarlos en disco duro. Incluye gran cantidad de aplicaciones de recuperación de datos y contraseñas de usuario.

Desde las opciones de SETUP o configuración de la BIOS (sigla en inglés de *basic input/output system*; en español "sistema básico de entrada y salida") , podemos hacer que arranque en primer lugar desde cualquiera de las mencionadas unidades.

Vulnerabilidades:

A modo de ejemplo mencionaremos algunas distribuciones arrancables en modo Live:

Control de Acceso Lógico

Peligros de las Distribuciones LIVE!

- **Ultimate Boot CD (UBCD)**: posee en un entorno simulado Windows con aplicaciones como antivirus, recuperación de datos, aplicaciones de recuperación y borrado de contraseñas de la BIOS (cmos_pwd), borrado y restitución de nuevas contraseñas de usuarios de sistema Windows instalados en disco, incluso creación de nuevas cuentas de usuario administrador.



<http://www.ultimatebootcd.com/>

- **Backtrack**: distribución específica con un conjunto de herramientas de auditoria informática, entre otras algunas que permiten escalada de en sistemas Windows (ophcrack) y GNU/Linux (John the ripper)

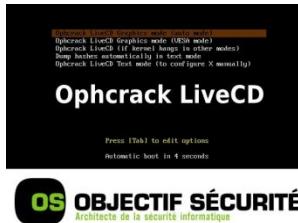
<http://www.backtrack-linux.org/>



Control de Acceso Lógico

Peligros de las Distribuciones LIVE!

- **Ophcrack:** distribución específica que contiene la aplicación de mismo nombre con capacidad de extraer contraseñas de usuarios en sistemas Windows. *Veremos más adelante un ejemplo de aplicación.*



<http://ophcrack.sourceforge.net/>

- **Slax:** distribución basada en Slackware, muy ligera y arrancable desde USB. Permite el montaje y acceso a los sistemas de ficheros instalados en disco.

<http://www.slax.org/>



- **Wifiway y Wifislax:** distribuciones orientadas a realizar auditorías wireless, como recuperación de contraseñas.



www.wifiway.org



<http://www.wifislax.com/>

Control de Acceso Lógico

Peligros de las Distribuciones LIVE!

- En la mayoría de las ocasiones desde estas distribuciones es posible acceder a las particiones y sistemas de ficheros de forma transparente, es decir, sin restricciones del sistema operativo, por lo que puede comprometer la seguridad de los datos y ficheros.

Comprobación:

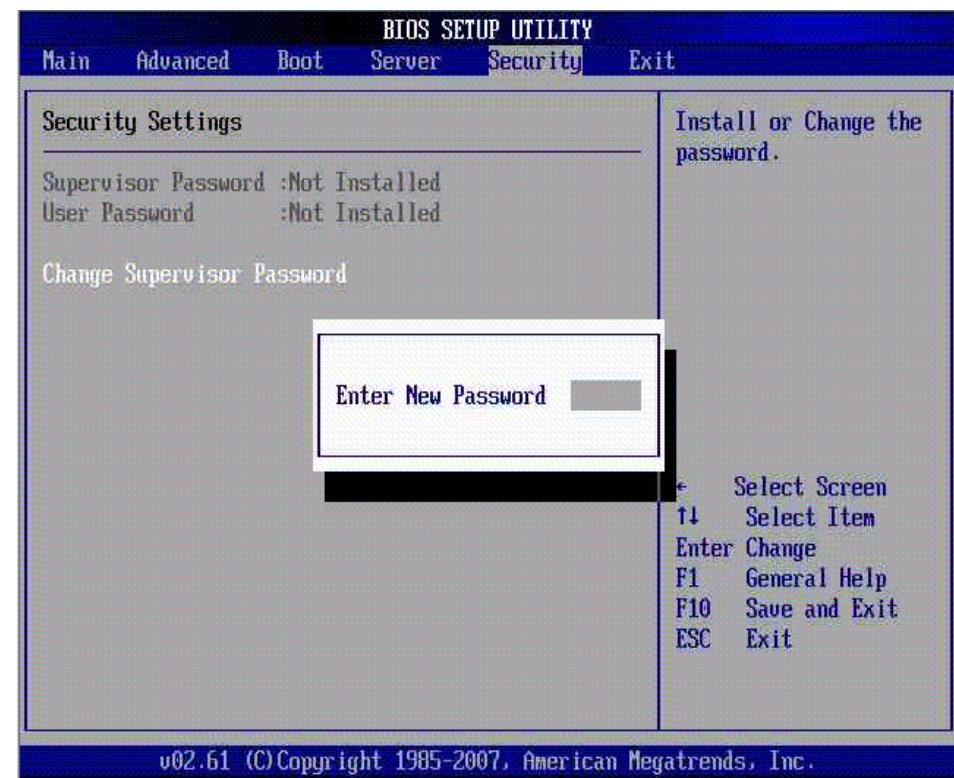
A modo de ejemplo podemos comprobar después de arrancar con un DVD Live de Backtrack el listado de particiones disponibles en el disco duro mediante el comando ejecutado como root: `fdisk -l`.

Tras analizar las particiones disponibles, montaremos por ejemplo en una carpeta creada por ejemplo `/mnt/win`, la partición de formato NTFS de Windows `/dev/sda2`, con el comando: `mount -t ntfs /dev/sda2 /mnt/win`. La opción `-t` nos permite indicar el formato de la partición. De esta forma podemos acceder a través de la carpeta `/mnt/win` a todos los ficheros de dicha partición.

Control de Acceso Lógico

Control de Acceso en la BIOS

- **BIOS (Basic Input/Output System):** es el nivel más bajo de software que configura o manipula el hardware de un ordenador de manera que cada vez que iniciamos el ordenador este se encarga de reconocer todo el hardware que contiene el ordenador y controlar el estado de los mismos.
- En la BIOS podemos configurar cualquier parámetro referente al hardware, de qué dispositivo arrancará en primer lugar o parámetros más comprometidos como el voltaje que se le suministra al núcleo del microprocesador.
- Por este motivo tendremos que proteger nuestra BIOS de manera que solo un Administrador o un usuario responsable puedan cambiar los valores de la configuración.



Control de Acceso Lógico

Control de Acceso en la BIOS

- Según la versión y la marca de la BIOS podemos configurar la seguridad del mismo de distintas formas. Estableceremos una clasificación sobre los niveles de seguridad que suele tener:

Seguridad del sistema (system): en cada arranque de la máquina nos pedirá que introduzcamos una contraseña que previamente se ha configurado en el BIOS. En caso de no introducirla o introducirla incorrectamente, el sistema no arrancará-

Seguridad de configuración de la BIOS (setup): en este apartado se suelen distinguir dos roles aplicables: Usuario (solo lectura) y Administrador (lectura/modificaciones).

Recomendaciones:

- Cabe destacar que la seguridad de la BIOS es muy vulnerable ya que existen varias formas de restear la BIOS:
 - Quitar la pila de la placa base.
 - Conexión del jumper CLR_CMOS que suele traer junto a la pila.
 - Reseteando mediante la distribución LIVE como Ultimate Boot CD for Windows, o arrancando bajo windows y ejecutando cmos_pwd, que encuentra y borra contraseñas.

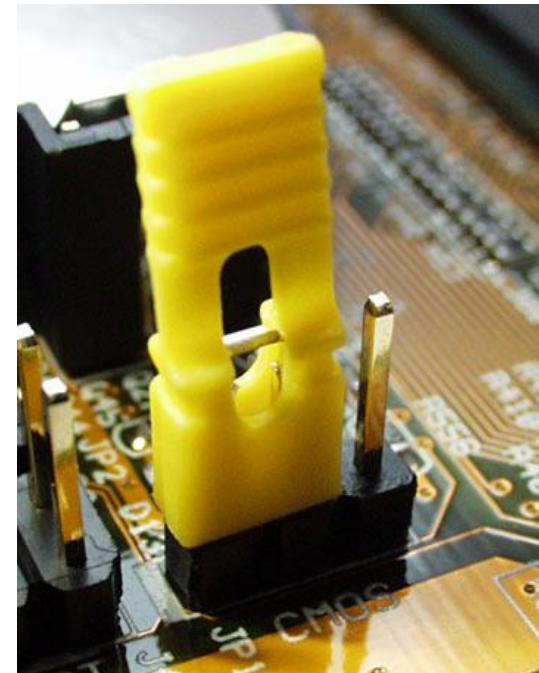
Control de Acceso Lógico

Control de Acceso en la BIOS

Recomendaciones:

- Cabe destacar que la seguridad de la BIOS es muy vulnerables ya que existen varias formas de restear la BIOS:
 1. Quitar la pila de la placa base.
 2. Conexión del jumper CLR_CMOS que suele traer junto a la pila.

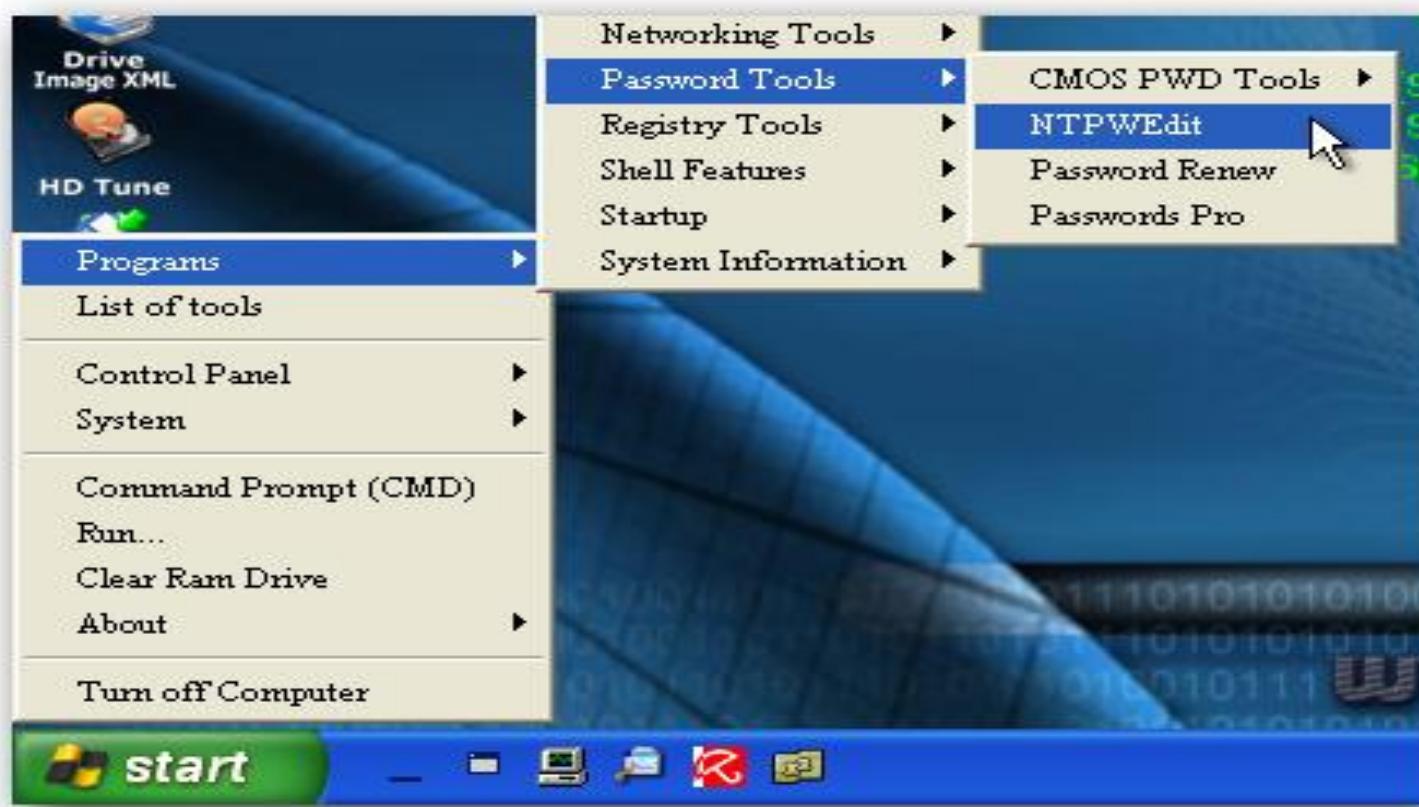
Jumper cubre 2 pines que técnicamente son el 1 y 2 y deja al descubierto uno que seria el 3,, es en esa posición en la que el Jumper se encuentra en todas las placas. Ponemos el jumper en los pines 2 y 3, es en este momento en el cual la bios esta siendo reseteada a sus valores de fábrica. Y lo colocamos en la posición original ósea sobre los pines 1 y 2 .



Control de Acceso Lógico

Control de Acceso en la BIOS

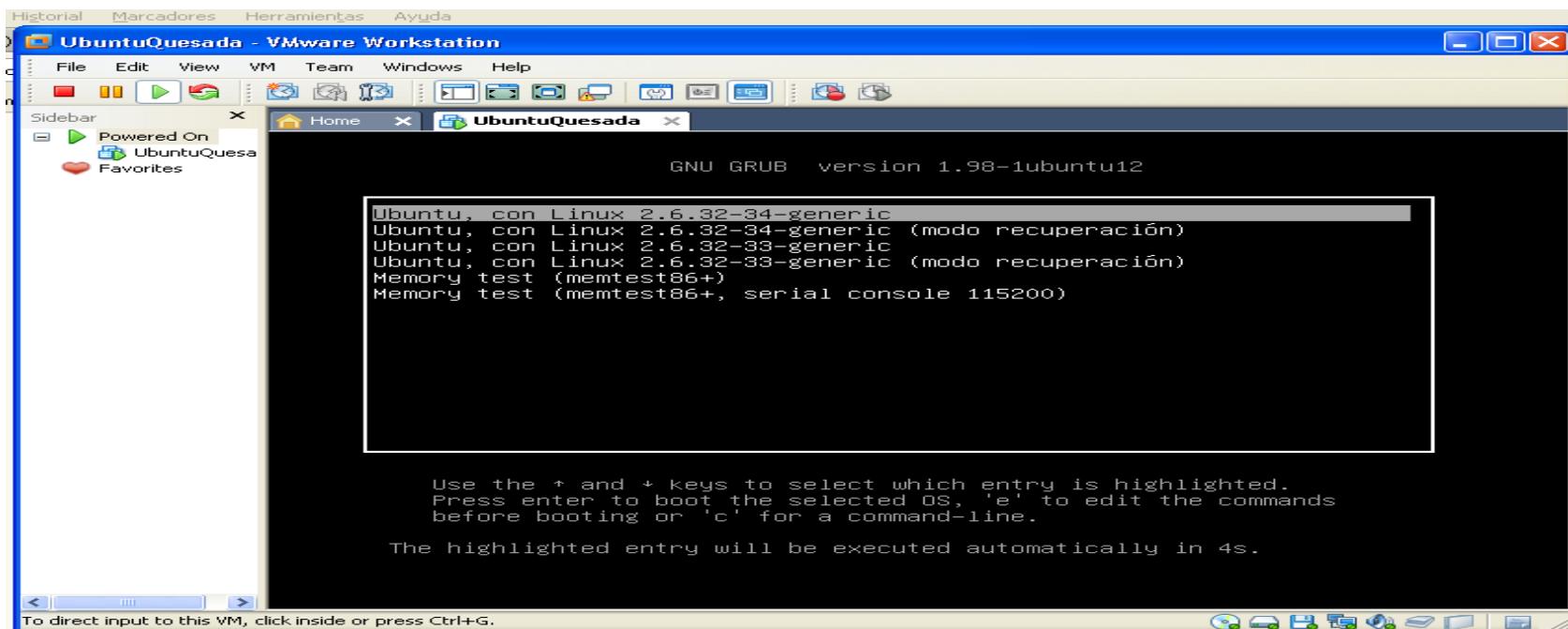
3. Reseteando mediante la distribución LIVE como *Ultimate Boot CD for Windows*, o arrancando bajo windows y ejecutando *cmos_pwd*, que encuentra y borra contraseñas.



Control de Acceso Lógico

Gestor de Arranque

GRUB (GRand Unifier Bootloader) es un gestor de arranque (*Grub 2.0 es el gestor de arranque predeterminado de algunas de las últimas versiones de linux.*): es lo primero que se carga cuando se inicia la computadora. Permite tener diferentes sistemas operativos, y diferentes versiones de ellos, en el mismo disco duro. Por ejemplo podemos tener Windows y GNU/Linux en la misma computadora, GRUB se cargará antes que cualquiera de éstos permitiéndonos elegir cuál iniciar.



Control de Acceso Lógico

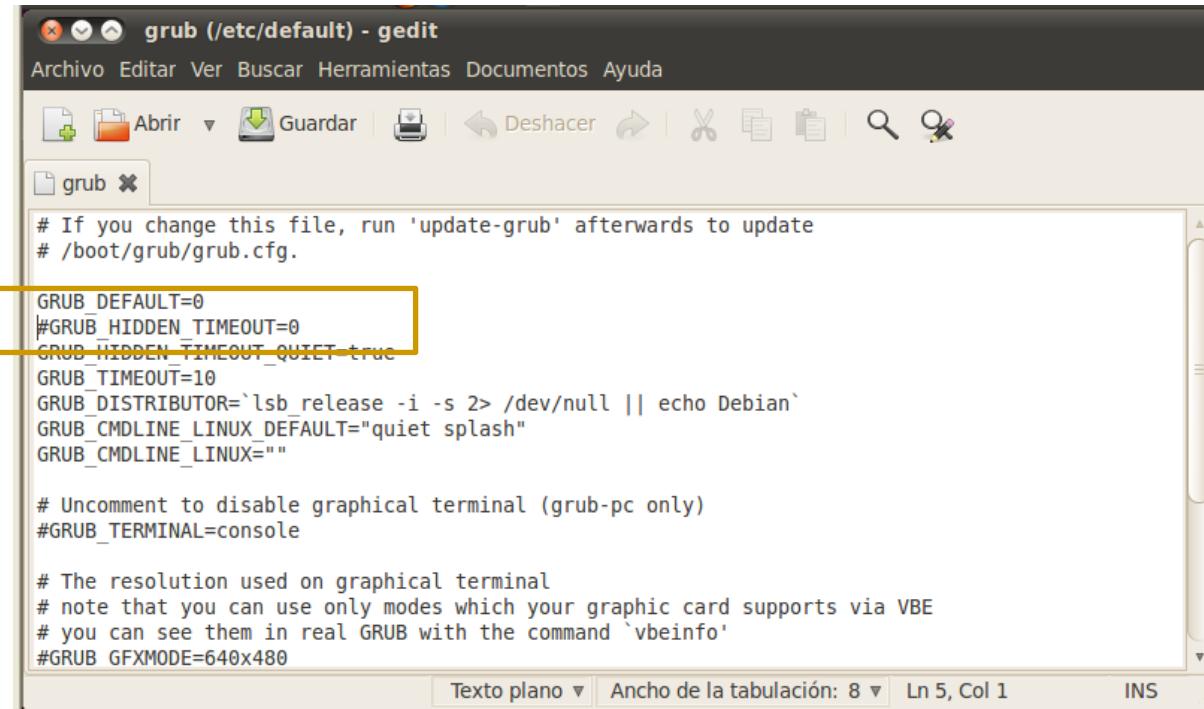
Gestor de Arranque

http://www.guias-ubuntu.org/index.php?title=GRUB#Grub_2

usuario:~\$: sudo apt-get install grub2

...

usuario:~\$: sudo gedit /etc/default/grub



```
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg

GRUB_DEFAULT=0
#GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
GRUB_CMDLINE_LINUX=""

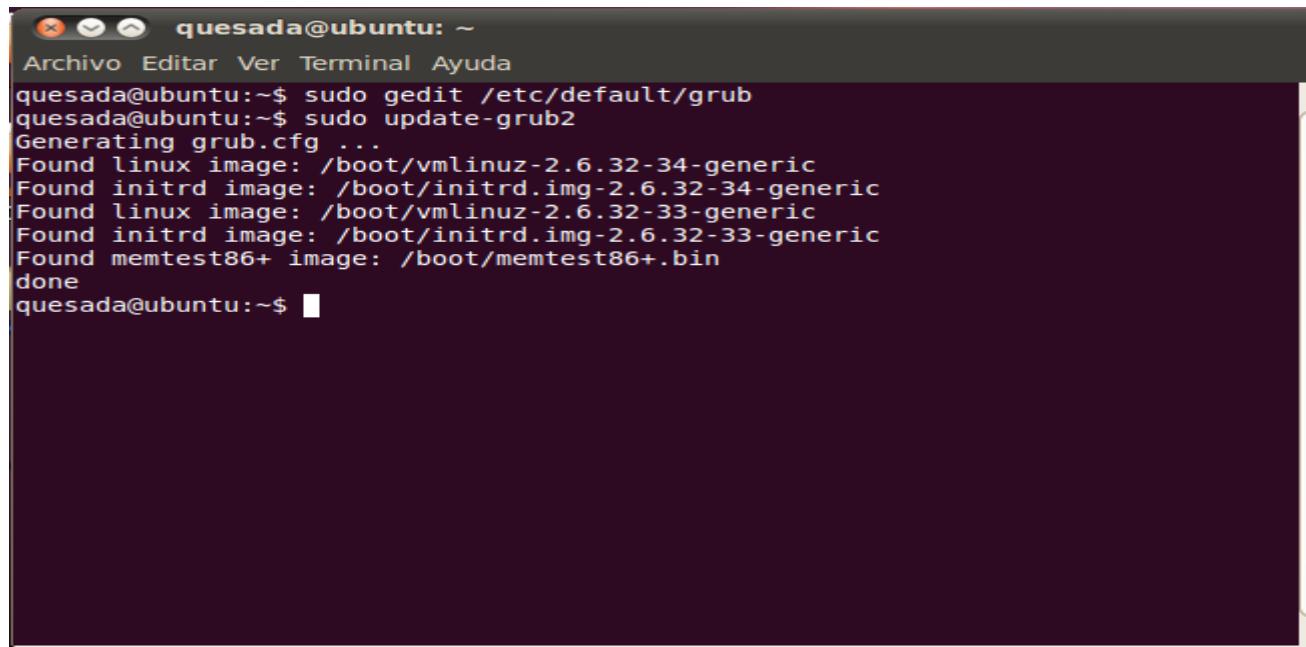
# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo'
#GRUB_GFXMODE=640x480
```

Control de Acceso Lógico

Gestor de Arranque

Para modificar el tiempo de espera, sistema operativo por defecto, el nombre de los sistemas operativos y toda la información del arranque de cada uno de ellos (igual que se hacía antes en /boot/grub/menu.lst –grub1) se puede hacer mediante el archivo /boot/grub/grub.cfg. No es recomendable hacerlo de este modo, ya que este archivo es un archivo creado automáticamente por el sistema utilizando otros archivos que son los que se deben modificar para cambiar los ajustes de Grub2 (archivos que están en la carpeta /etc/grub.d/ y el archivo /etc/default/grub). El archivo grub.cfg se genera/actualiza escribiendo en terminal: sudo update-grub2



```
quesada@ubuntu: ~
Archivo Editar Ver Terminal Ayuda
quesada@ubuntu:~$ sudo gedit /etc/default/grub
quesada@ubuntu:~$ sudo update-grub2
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-2.6.32-34-generic
Found initrd image: /boot/initrd.img-2.6.32-34-generic
Found linux image: /boot/vmlinuz-2.6.32-33-generic
Found initrd image: /boot/initrd.img-2.6.32-33-generic
Found memtest86+ image: /boot/memtest86+.bin
done
quesada@ubuntu:~$
```

Control de Acceso Lógico

Gestor de Arranque

The screenshot shows a window titled "grub.cfg [Sólo lectura] (/boot/grub) - gedit". The window contains the GRUB configuration file "grub.cfg". A portion of the file is highlighted with a yellow box, specifically the section starting with "# It is automatically generated by /usr/sbin/grub-mkconfig using templates". The file includes comments like "# DO NOT EDIT THIS FILE" and "#". Below this, there is code for setting the default boot entry and saving previous entries.

```
#  
# DO NOT EDIT THIS FILE  
#  
# It is automatically generated by /usr/sbin/grub-mkconfig using templates  
# from /etc/grub.d and settings from /etc/default/grub  
#  
### BEGIN /etc/grub.d/00_header ###  
if [ -s $prefix/grubenv ]; then  
    load_env  
fi  
set default="0"  
if [ ${prev_saved_entry} ]; then  
    set saved_entry=${prev_saved_entry}  
    save_env saved_entry  
    set prev_saved_entry=  
    save_env prev_saved_entry  
    set boot_once=true  
fi  
  
function savedefault {  
    if [ -z $boot_once ]; then  
        saved_entry=$boot_device  
        save_env boot_device  
        boot_once=true  
    fi  
}
```

Control de Acceso Lógico

Gestor de Arranque

Amenazas o vulnerabilidades:

Después de realizar la BIOS las comprobaciones de hw y dar paso al arranque de los dispositivos configurados, puede aparecer el menú de GRUB. La opción de recovery mode bajo sistemas GNU/Linux tiene un propósito en caso de fallo del sistema, pero puede ser utilizada entre otras acciones para recuperar y modificar contraseñas de administrador (root) o incluso acceder a información del disco duro.



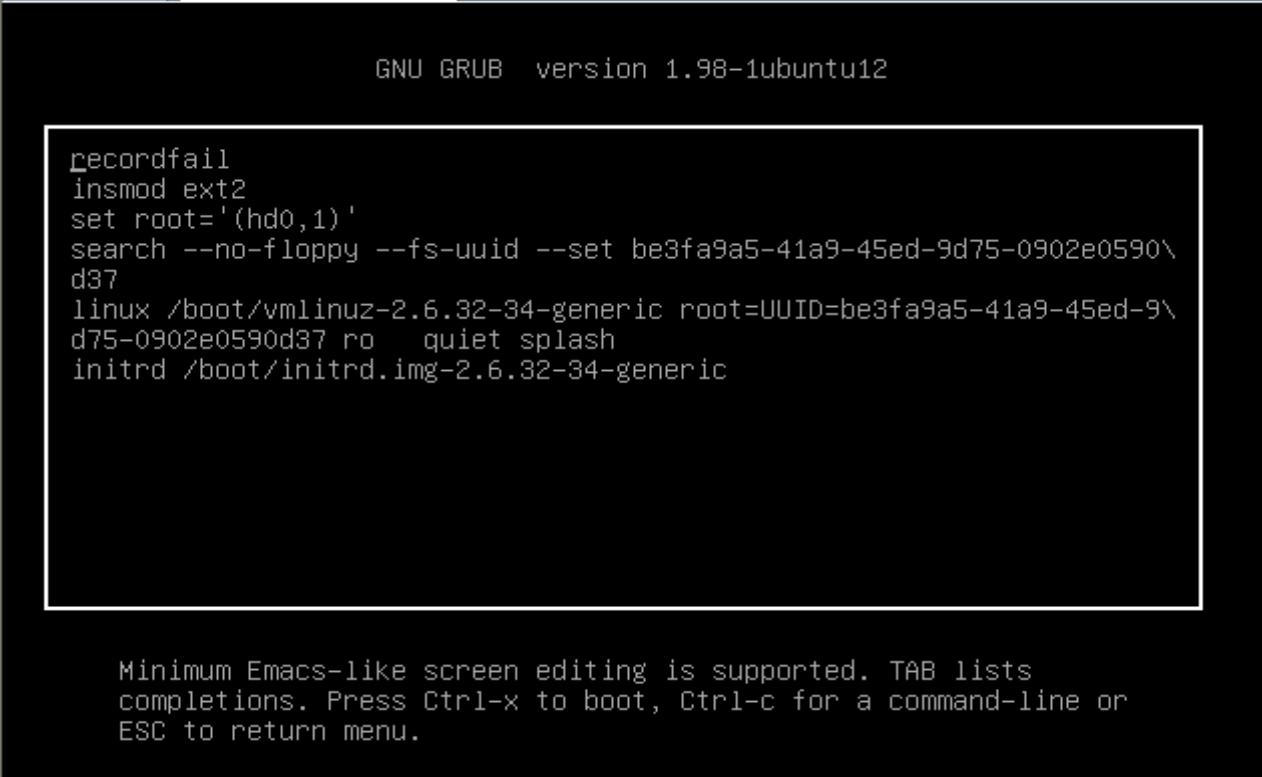
```
Home X UbuntuQuesada X
root@ubuntu:~# passwd root
Contraseña: -
```

Control de Acceso Lógico

Gestor de Arranque

Amenazas o vulnerabilidades:

Otra posibilidad si tuviéramos restringida la opción de recuperación, sería editando – pulsando la tecla e- alguna de las entradas del menú:



The screenshot shows a GRUB menu with a single entry highlighted. The entry is a modified version of the default boot command. The modified part is shown in red:

```
recordfail
insmod ext2
set root='(hd0,1)'
search --no-floppy --fs-uuid --set be3fa9a5-41a9-45ed-9d75-0902e0590\
d37
linux /boot/vmlinuz-2.6.32-34-generic root=UUID=be3fa9a5-41a9-45ed-9\
d75-0902e0590d37 ro quiet splash
initrd /boot/initrd.img-2.6.32-34-generic
```

Below the menu, there is a message about screen editing:

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x to boot, Ctrl-c for a command-line or ESC to return menu.

Control de Acceso Lógico

Gestor de Arranque

```
GNU GRUB version 1.98-1ubuntu12
```

```
recordfail
insmod ext2
set root='(hd0,1)'
search --no-floppy --fs-uuid --set be3fa9a5-41a9-45ed-9d75-0902e0590\
d37
linux /boot/vmlinuz-2.6.32-34-generic root=UUID=be3fa9a5-41a9-45ed-9\
d75-0902e0590d37 ro quiet splash
initrd /boot/initrd.img-2.6.32-34-generic
```

```
GNU GRUB version 1.98-1ubuntu12
```

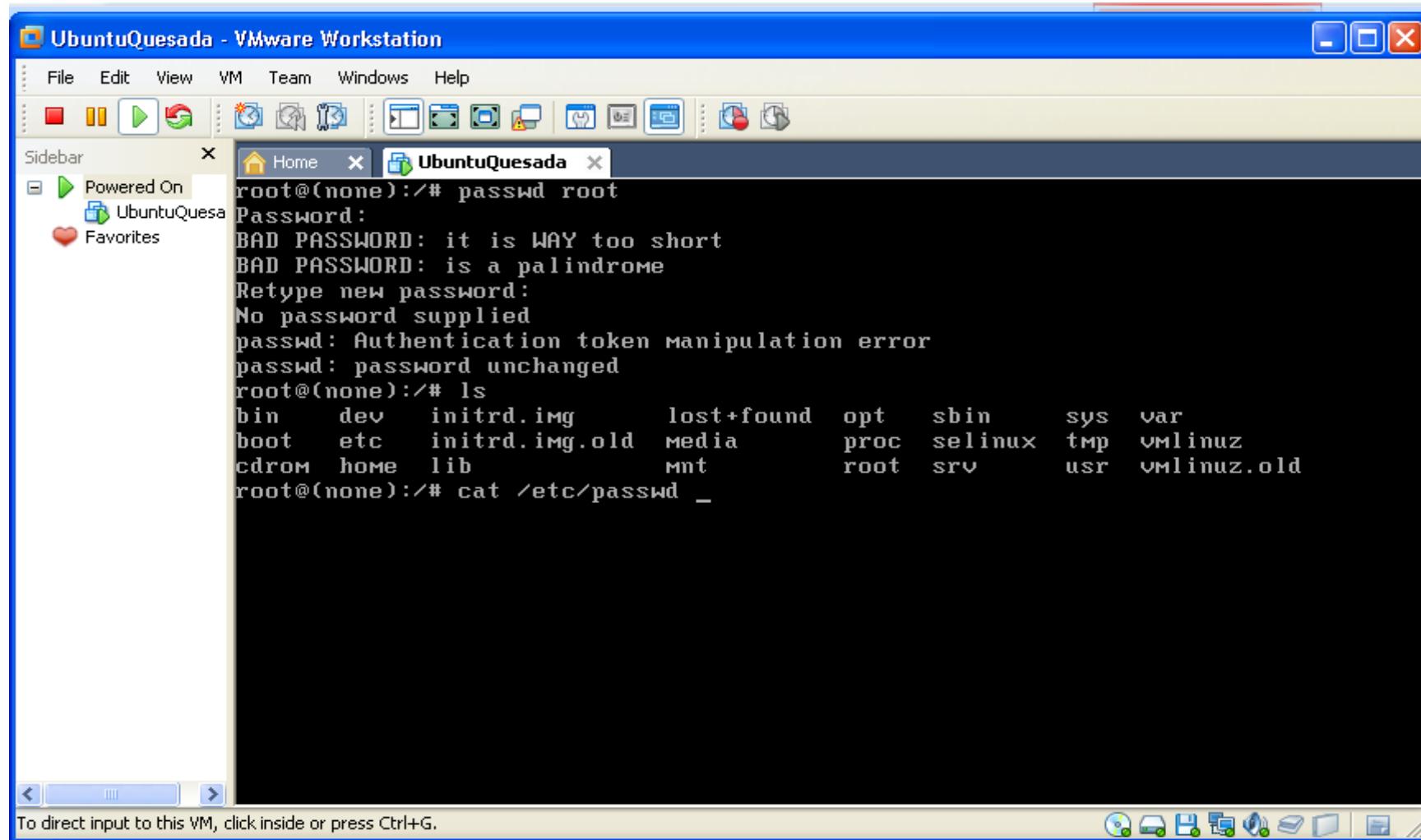
```
recordfail
insmod ext2
set root='(hd0,1)'
search --no-floppy --fs-uuid --set be3fa9a5-41a9-45ed-9d75-0902e0590\
d37
linux /boot/vmlinuz-2.6.32-34-generic root=UUID=be3fa9a5-41a9-45ed-9\
d75-0902e0590d37 ro quiet splash rw init=/bin/bash_
initrd /boot/initrd.img-2.6.32-34-generic
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x to boot, Ctrl-c for a command-line or ESC to return menu.

Si arrancamos después de la edición, desde esta opción este cambio ejecutará en el arranque un shell con permisos de root, teniendo el control total sobre el sistema. (para añadir el carácter = -ALT+61-) A continuación CTRL+X para realizar el boot

Control de Acceso Lógico

Gestor de Arranque



Control de Acceso Lógico

Gestor de Arranque

CASO 1.- Proceso de asignación de contraseña a GRUB

usuario:~\$ sudo grub

```
[root@redlinux ~]# grub-md5-crypt  
Password:  
Retype password:
```

```
$1$vFKrk/$jve/iE82AMCyZPT09yT/D0
```

The screenshot shows a terminal window with a purple border. The title bar says "Terminal". The menu bar includes "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main area of the terminal shows the following text:

```
File Edit View Terminal Tabs Help  
jon@ubuntu: ~  
[ Minimal BASH-like line editing is supported. For  
the first word, TAB lists possible command  
completions. Anywhere else TAB lists the possible  
completions of a device/filename. ]  
grub> md5crypt  
Password: *****  
Encrypted: $1$xcLi0$4czPGUKIdo5e8Vi3nIpme0  
grub> █
```

A large, semi-transparent gray box is overlaid on the right side of the terminal window, containing the following explanatory text:

[Minimal BASH-like line editing is supported. For
the first word, TAB lists possible command
completions. Anywhere else TAB lists the possible
completions of a device/filename.]

Control de Acceso Lógico

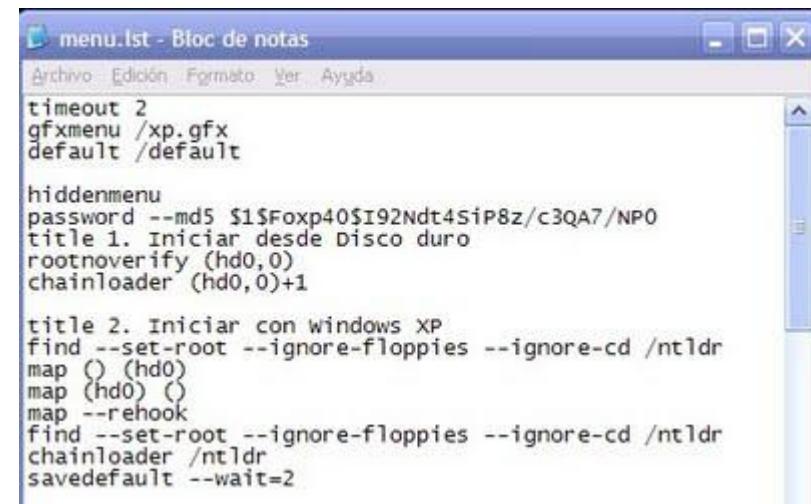
Gestor de Arranque

usuario:~\$: sudo gedit /boot/grub/menu.lst

```
## password ['--md5'] passwd
# If used in the first section of a menu file, disable all interactive editing
# control (menu entry editor and command-line) and entries protected by the
# command 'lock'
# e.g. password topsecret
#       password --md5 $1$gLhU0/$aW78kHK1QfV3P2b2znUoe/
# password topsecret
```

Añadir contraseña encriptada al menú de edición es decir imposibilitar la edición por cualquier usuario no autorizado.

Añadir encriptada contraseña en modo recuperación



```
menu.lst - Bloc de notas
Archivo Edición Formato Ver Ayuda
timeout 2
gfxmenu /xp gfx
default /default

hiddenmenu
password --md5 $1$Foxp40$192Ndt4SiP8z/c3QA7/NPO
title 1. Iniciar desde Disco duro
rootnoverify (hd0,0)
chainloader (hd0,0)+1

title 2. Iniciar con Windows XP
find --set-root --ignore-floppies --ignore-cd /ntldr
map () (hd0)
map (hd0) {}
map --rehook
find --set-root --ignore-floppies --ignore-cd /ntldr
chainloader /ntldr
savedefault --wait=2
```

Control de Acceso Lógico

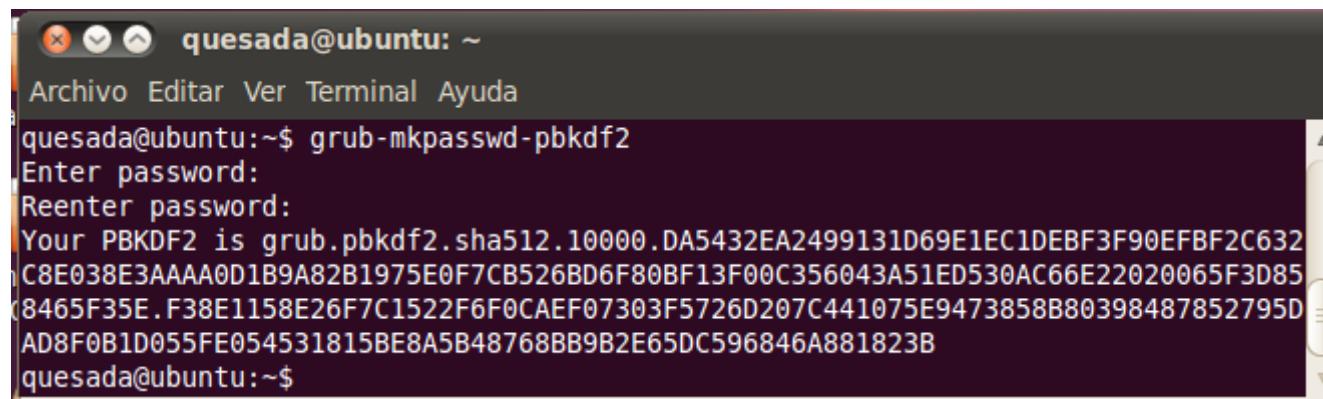
Gestor de Arranque

CASO 2.- Proceso de asignación de contraseña a GRUB2

Al poner contraseña en el grub podemos evitar que se puedan introducir líneas de comandos a través de grub para administrar el equipo, también podemos restringir el arranque de un sistema operativo.

La contraseña que le pondremos al grub2 esta encriptada en SHA512 por lo tanto deberemos utilizar un comando que nos proporciona el grub para sacar la cadena encriptada de la contraseña, este comando es: grub-mkpasswd-pbkdf2

Pasos:



```
quesada@ubuntu: ~
Archivo Editar Ver Terminal Ayuda
quesada@ubuntu:~$ grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
Your PBKDF2 is grub.pbkdf2.sha512.10000.DA5432EA2499131D69E1EC1DEBF3F90EFBF2C632
1C8E038E3AAAA0D1B9A82B1975E0F7CB526BD6F80BF13F00C356043A51ED530AC66E22020065F3D85
08465F35E.F38E1158E26F7C1522F6F0CAEF07303F5726D207C441075E9473858B80398487852795D
AD8F0B1D055FE054531815BE8A5B48768BB9B2E65DC596846A881823B
quesada@ubuntu:~$
```

Control de Acceso Lógico

Gestor de Arranque

Una vez que tenemos en un terminal la contraseña generada en SHA512 abrimos otro terminal y tecleamos **sudo gedit /boot/grub/grub.cfg** para abrir el fichero de configuración del grub.



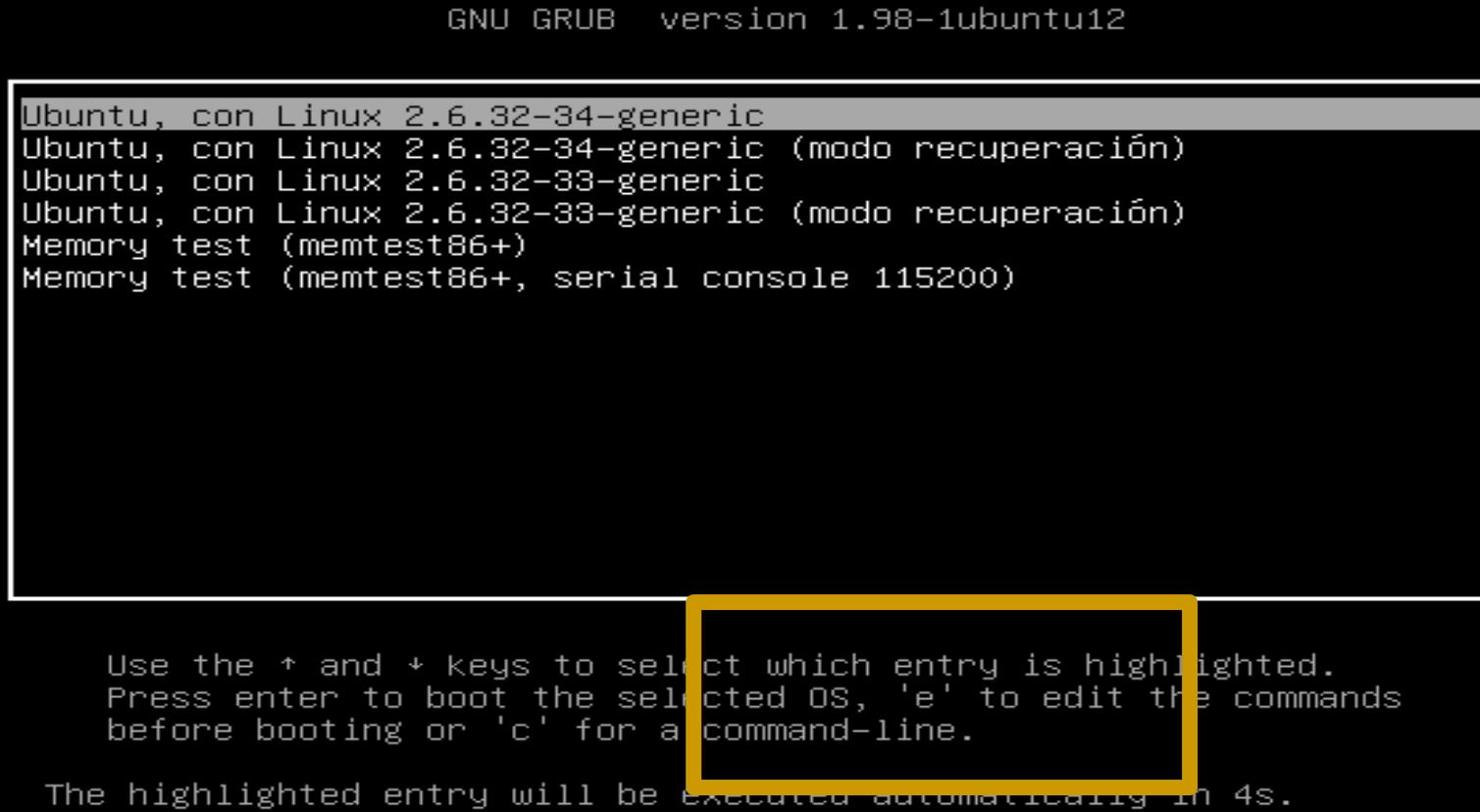
```
grub.cfg ✘
set superusers="usuario"
password_pbkdf2 usuario
grub.pbkdf2.sha512.10000.DA5432EA2499131D69E1EC1DEBF3F90EFBF2C632C8E038E3AAAA0D1B9A82B1975E0F7CB
```

Una vez abierto el fichero debemos crear un usuario como mínimo y asignarle la contraseña generada en SHA512 de la siguiente forma mostrada a continuación. Este contenido debe ir al empezar el fichero.

- set superusers="..." - con esto creamos el usuario.*
- password_pbkdf2 - indicamos la contraseña en SHA512*
- grub.pbkdf2.....E - es la clave encriptada que debe sustituirse por la que hemos generado*

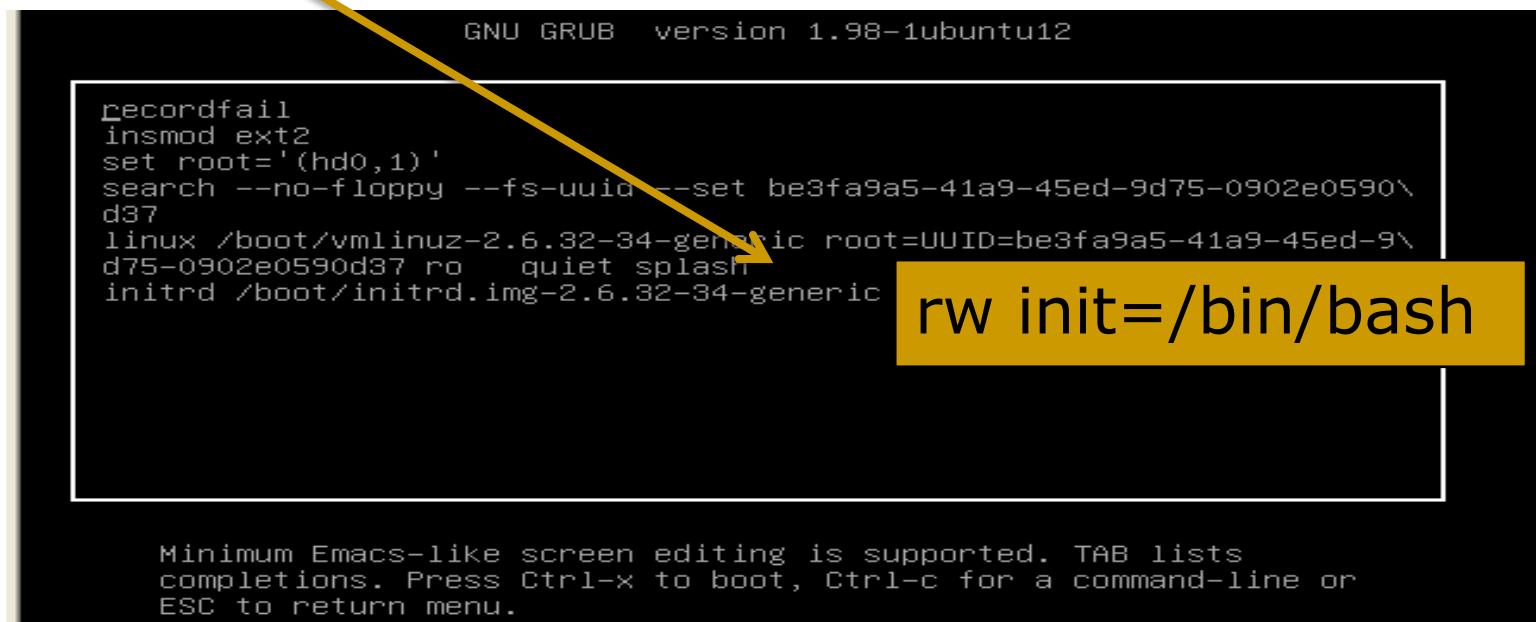
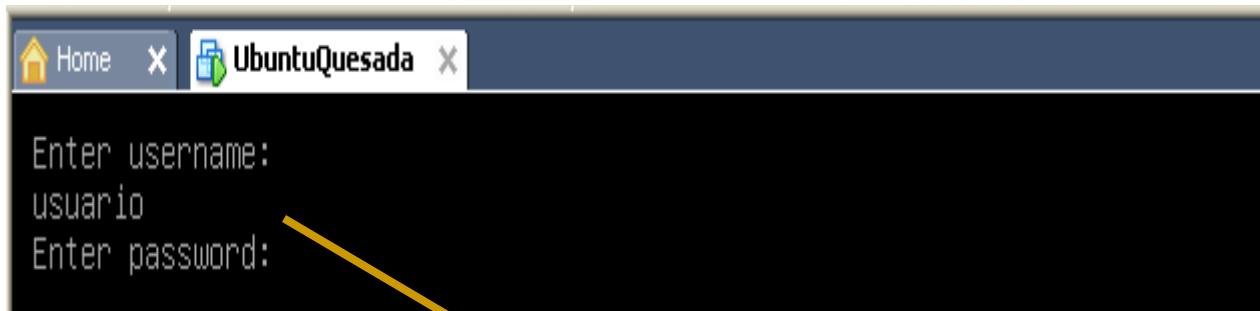
Control de Acceso Lógico

Gestor de Arranque



Control de Acceso Lógico

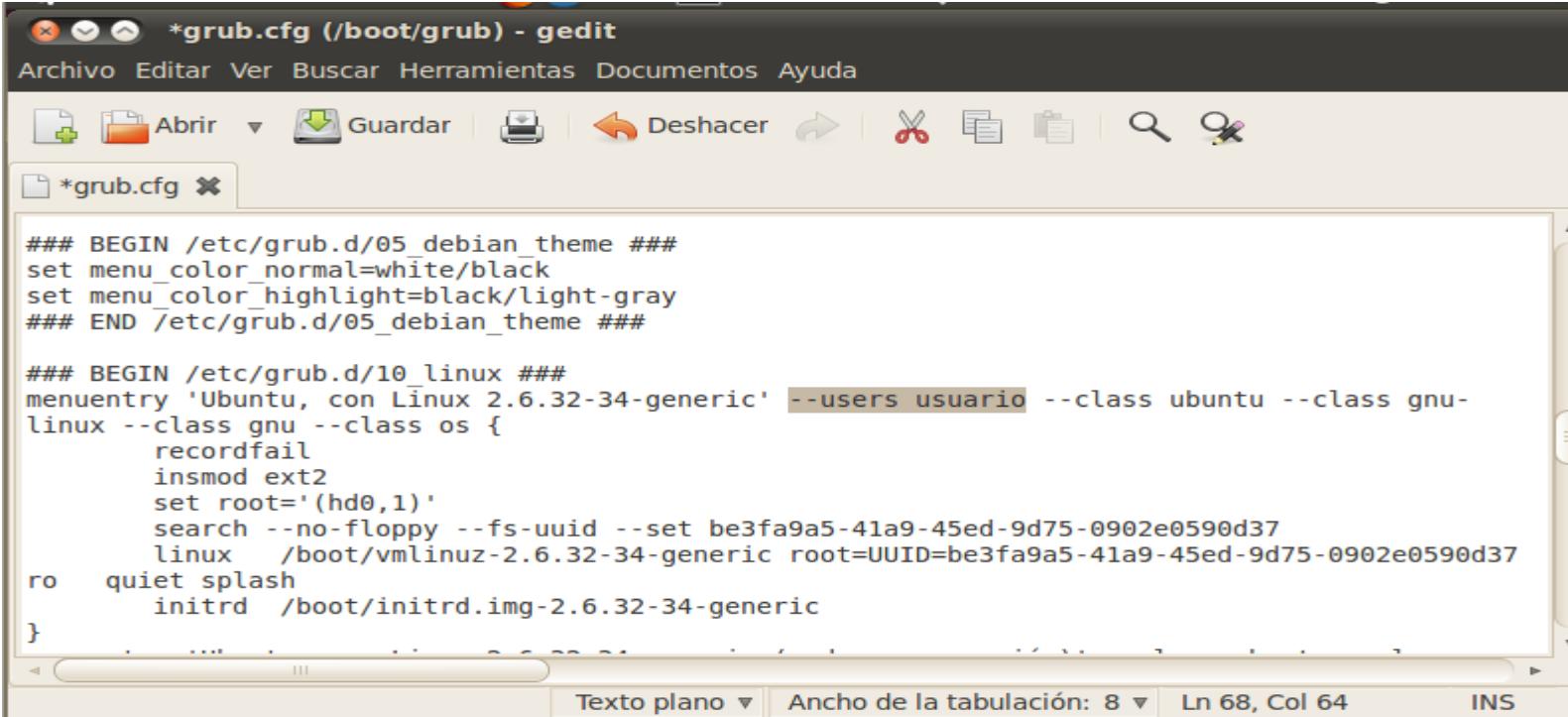
Gestor de Arranque



Control de Acceso Lógico

Gestor de Arranque

Para que también nos pida el usuario y la contraseña para el arranque de la opciones que nos da el grub debemos indicárselo añadiéndole --users usuario en la opciones de arranque (cada opcion de arranque se nos muestra el grub la línea empieza por menunentry) editando de nuevo el fichero.



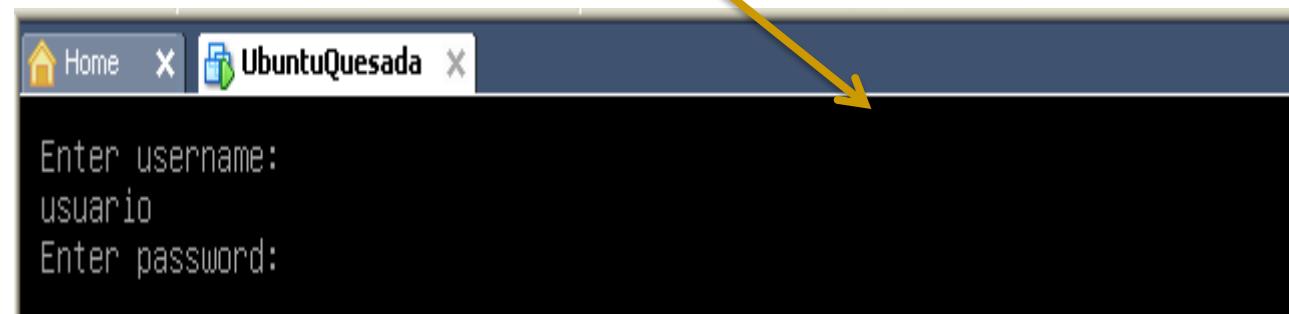
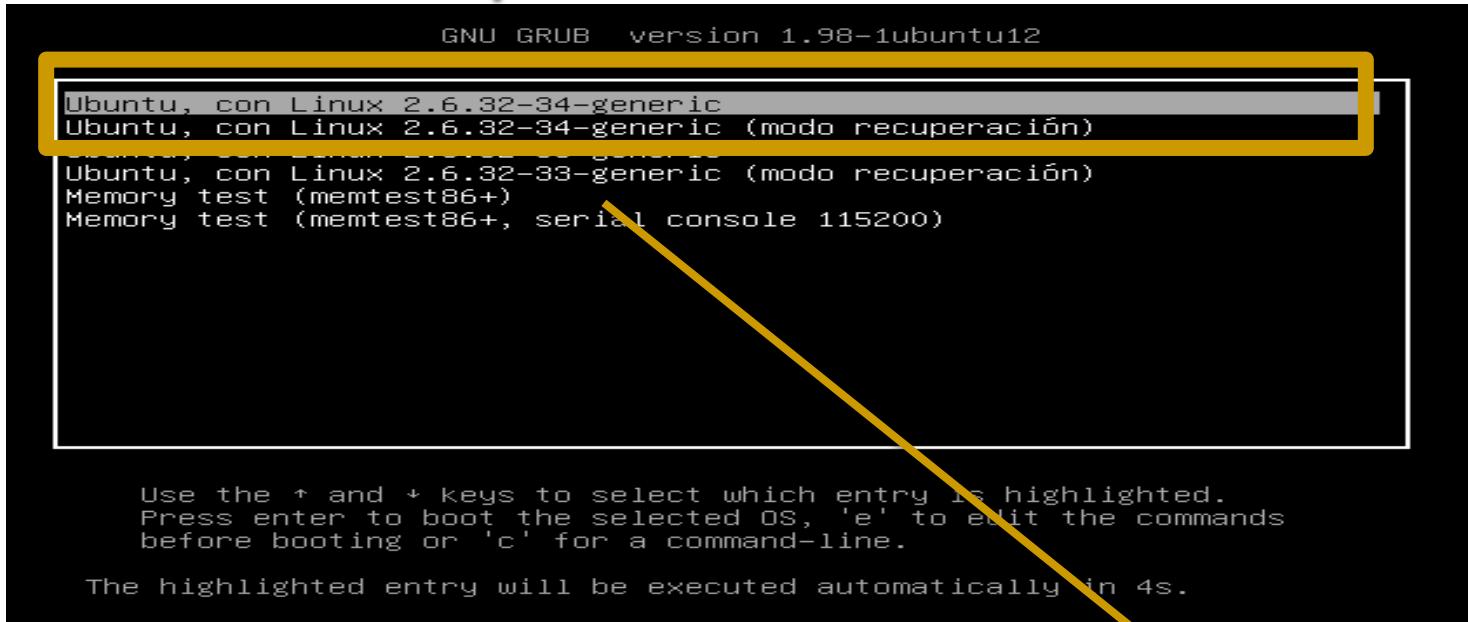
The screenshot shows the gedit text editor with the file `*grub.cfg (/boot/grub)` open. The code in the editor is as follows:

```
### BEGIN /etc/grub.d/05_debian_theme ###
set menu_color_normal=white/black
set menu_color_highlight=black/light-gray
### END /etc/grub.d/05_debian_theme ###

### BEGIN /etc/grub.d/10_linux ###
menuentry 'Ubuntu, con Linux 2.6.32-34-generic' --users usuario --class ubuntu --class gnu-linux --class gnu --class os {
    recordfail
    insmod ext2
    set root='(hd0,1)'
    search --no-floppy --fs-uuid --set be3fa9a5-41a9-45ed-9d75-0902e0590d37
    linux /boot/vmlinuz-2.6.32-34-generic root=UUID=be3fa9a5-41a9-45ed-9d75-0902e0590d37
    ro quiet splash
    initrd /boot/initrd.img-2.6.32-34-generic
}
```

Control de Acceso Lógico

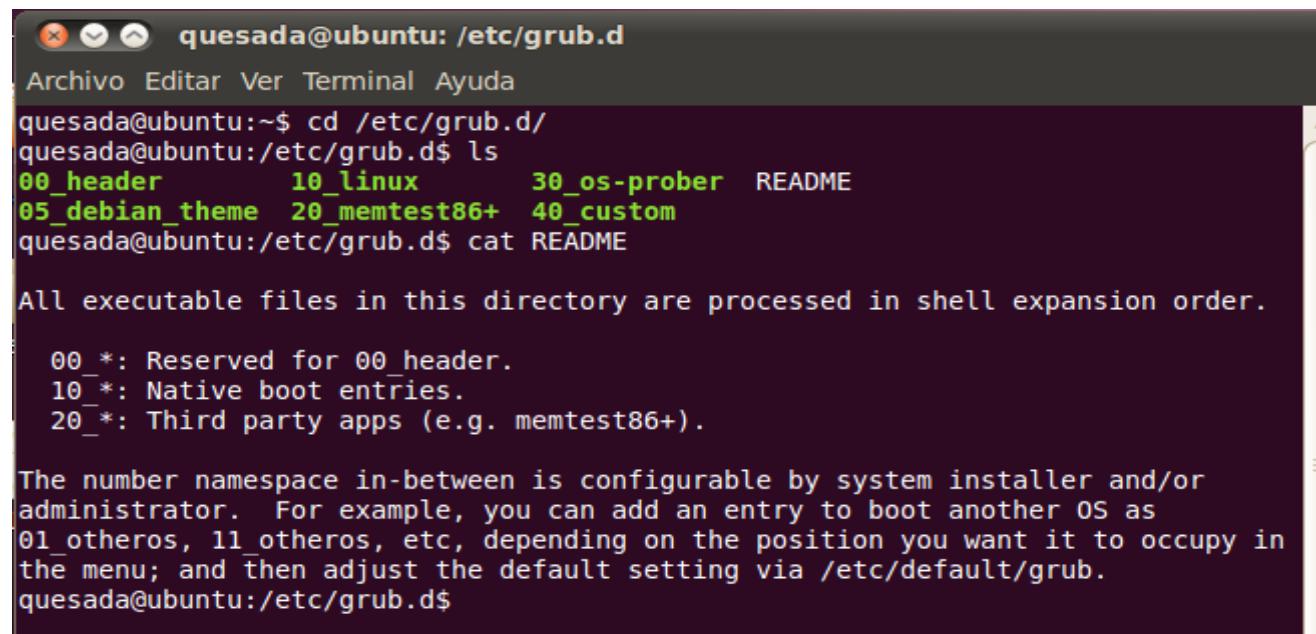
Gestor de Arranque



Control de Acceso Lógico

Gestor de Arranque

Como se ha indicado anteriormente no es recomendable hacerlo de este modo, ya que este archivo es un archivo creado automáticamente por el sistema -update-grub2- utilizando otros archivos que son los que se deben modificar para cambiar los ajustes de Grub2 (archivos que están en la carpeta /etc/grub.d/ y el archivo /etc/default/grub)



The screenshot shows a terminal window titled "quesada@ubuntu: /etc/grub.d". The terminal displays the following command-line session:

```
Archivo Editar Ver Terminal Ayuda  
quesada@ubuntu:~$ cd /etc/grub.d/  
quesada@ubuntu:/etc/grub.d$ ls  
00_header      10_linux      30_os-prober  README  
05_debian_theme  20_memtest86+  40_custom  
quesada@ubuntu:/etc/grub.d$ cat README  
  
All executable files in this directory are processed in shell expansion order.  
  
00_*: Reserved for 00_header.  
10_*: Native boot entries.  
20_*: Third party apps (e.g. memtest86+).  
  
The number namespace in-between is configurable by system installer and/or administrator. For example, you can add an entry to boot another OS as 01_otheros, 11_otheros, etc, depending on the position you want it to occupy in the menu; and then adjust the default setting via /etc/default/grub.  
quesada@ubuntu:/etc/grub.d$
```

Control de Acceso Lógico

Gestor de Arranque

```
00_header * grub.cfg *

echo "insmod $i"
done

if [ "x${GRUB_DEFAULT}" = "x" ] ; then GRUB_DEFAULT=0 ; fi
if [ "x${GRUB_DEFAULT}" = "xsaved" ] ; then GRUB_DEFAULT='${saved_entry}' ; fi
if [ "x${GRUB_TIMEOUT}" = "x" ] ; then GRUB_TIMEOUT=5 ; fi
if [ "x${GRUB_GFXMODE}" = "x" ] ; then GRUB_GFXMODE=640x480 ; fi

cat << EOF

#Aqui situo la clave para evitar modificar los comando de inicio

if [ -s \$prefix/grubenv ] ; then
    load_env
fi

quesada@ubuntu:/etc/grub.d$ sudo update-grub2
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-2.6.32-34-generic
Found initrd image: /boot/initrd.img-2.6.32-34-generic
Found linux image: /boot/vmlinuz-2.6.32-33-generic
Found initrd image: /boot/initrd.img-2.6.32
Found memtest86+ image: /boot/memtest86+.bin
done
quesada@ubuntu:/etc/grub.d$ 
```

```
# DO NOT EDIT THIS FILE
#
# It is automatically generated by /usr/sbin/grub-mkconfig using templates
# from /etc/grub.d and settings from /etc/default/grub
#
### BEGIN /etc/grub.d/00_header ###
#Aqui situo la clave para evitar modificar los comando de inicio

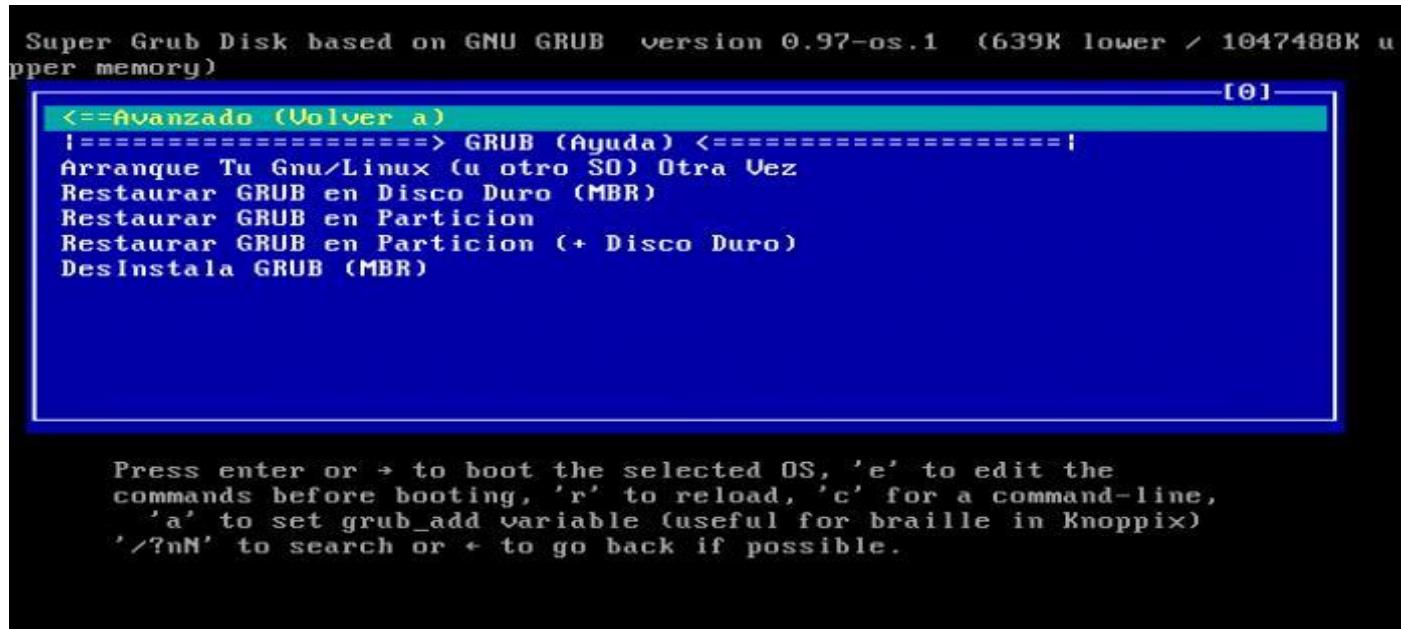
if [ -s $prefix/grubenv ] ; then
    load_env
fi
```

Control de Acceso Lógico

Gestor de Arranque

Super Grub Disk: www.supergrubdisk.org/

Super Grub Disk (SGD) es un herramienta distribuida bajo licencia GPL orientada a la recuperación y restauración del arranque de nuestro sistema en MBR automáticamente.



Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

- Existen métodos de acceso al sistema operativo muy seguros como por ejemplo mediante huella dactilar, pero el más utilizado sigue siendo a través de una contraseña asociada a una cuenta de usuario.
- Como hemos visto anteriormente existen métodos para poder acceder a los sistemas operativos sin control de contraseña, en el caso de GNU/Linux mediante el modo de recuperación. En el caso de Windows para versiones como XP mediante el modo prueba de fallos o pulsando 2 veces en la ventana de inicio de usuarios Ctrl + Alt + Supr e intentando acceder a la cuenta del usuario Administrador sin contraseña, ya que en la instalación no se le asigna ninguna, por tanto por defecto suele estar vacía.
- Pero existen otros métodos, normalmente asociados a poder arrancar con una distribución Live para poder recuperar o conocer las contraseñas de cualquier usuario, así como borrarlas o modificarlas.
- Como recomendación, estas herramientas empleadas nos servirán para auditar nuestros sistemas de credenciales de acceso a sistemas operativos y ver el nivel de fortaleza de las mismas, ya que dependiendo del nivel de nuestras contraseñas no siempre será posible recuperarlas.

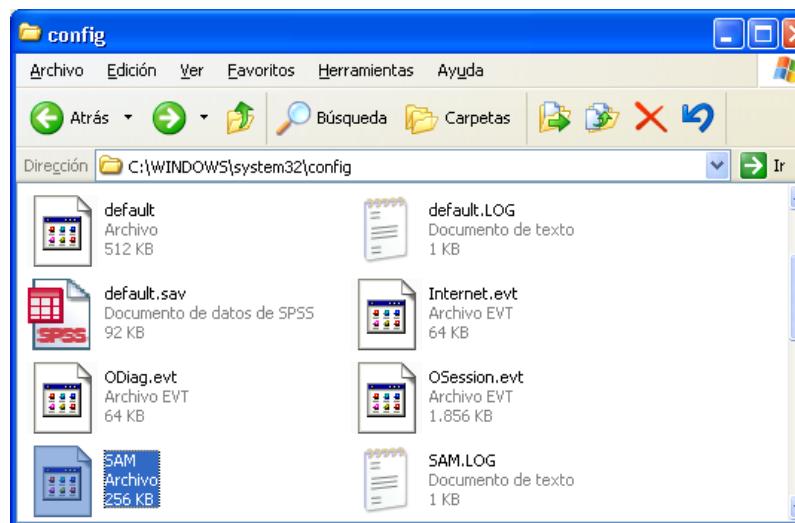
A continuación veremos algunos ejemplos de craqueo del sistema operativo wx y ubuntu.

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP

Ophcrack es una aplicación que permite recuperar contraseñas de Windows. También se encuentra disponible en distribuciones como Backtrack, o incluso posee su propia distribución Live. Se basa en el conocimiento de cómo almacena Windows sus contraseñas de usuario (*normalmente en windows/system32/config/SAM*, accesible sin arrancar el sistema operativo, por ejemplo desde una distribución Live), y emplea una comprobación mediante fuerza bruta y diccionarios que habrá que cargar dependiendo de la versión y el idioma.



Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP

- Debemos indicar en primer lugar la ruta del directorio donde se almacenan las contraseñas, normalmente Windows/system32/config. Previamente habremos montado la partición correspondiente.
- Por otro lado, mediante el botón Tables, indicaremos la ruta donde podrá encontrar la tabla rainbow con la que queremos probar; en este caso, hemos cargado XP -free-fast.
- Una vez cargadas las tablas de diccionario, ejecutaremos el comienzo de pruebas, y como vemos en la siguiente imagen de ejemplo, para los usuarios de la partición de Windows seleccionada ha encontrado:

The screenshot shows the ophcrack website interface. At the top, there's a navigation bar with links like 'Home', 'Project page', 'Download', 'Tables' (which is circled in yellow), and 'Support'. Below the navigation, there's a heading 'XP Rainbow tables'. A text block states: 'These tables can be used to crack Windows XP passwords (LM hashes). They CANNOT crack Windows Vista passwords (NT hashes.)'. Below this, there's a table with three rows: 'german' (red background), 'special' (yellow background), and 'mixedalphanum' (green background). Each row has a 'brute force' column and a corresponding file name: 'xp_german(7.4GB)', 'xp_special(7.5GB)', and 'xp_free_small(380MB) and xp_free_fast(703MB)'. At the bottom of the table, there's a 'length' column with options from 1-4 to 16.

	brute force	xp_german(7.4GB)
german		
special		xp_special(7.5GB)
mixedalphanum		xp_free_small(380MB) and xp_free_fast(703MB)

length 1-4 5 6 7 8 9 10 11 12 13 14 15 16



About

Progress Statistics Preferences

User	LM Hash	NT Hash	LM Pad 1	LM Pad 2	NT Pad
Administrador	cacf7c00ea45	4f37	1111111111111111	1111111111111111	1111111111111111
Invitado		31d6			empty
Residente de ayuda	5bf1a6e5dc9...	8fff	not found	8H6FEZZ	not found
SUPERUSUARIO	222222222222	8777			not found
root		31d6			empty

Table	Directory	Status	Progress
XP free small	/mnt/l1live/mnt/hdc/ophcrack//tables	35% in RAM	<div style="width: 70%;"></div>
table0		on disk	<div style="width: 100%;"></div>
table1		100% in RAM	<div style="width: 100%;"></div>
table2		on disk	<div style="width: 100%;"></div>
table3		38% in RAM	<div style="width: 38%;"></div>

Preload: waiting Brute force: done Pwd found: 3/5 Time elapsed: 0h 26m 1s

one > > launch.sh

ophcrack

19:33

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP

¿Qué son las Rainbow Tables?

- Cuando un usuario asigna su contraseña, el sistema operativo necesita guardar esa contraseña. Para no hacerlo en texto plano (sería muy simple encontrarla), lo que hace es aplicar una función Hash y almacenar el resultado de dicha función en un archivo (en el caso de Windows en C:\Windows\System32\config\SAM).
- Una función Hash es una función que devuelve un valor casi único por cualquier cadena de texto (o incluso archivos, directorios, etc.). Es decir, si yo le aplico un Hash MD5 (un tipo de Hash) a la palabra "Sebastián", el resultado será "c2d628ba98ed491776c9335e988e2e3b". Y si hago lo mismo con "unmundobinario.com", el resultado será "373e838e5050faca627b0433768aedef". Claramente el resultado de una función Hash dista bastante de almacenar el texto plano.

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP

- Sin embargo, las funciones Hash tienen un inconveniente. Siempre que yo ponga la misma cadena obtendré el mismo resultado. Y aquí aparecen las tablas rainbow.
- Básicamente a alguien se le ocurrió lo siguiente: no necesito hacer un ataque de fuerza bruta (prueba-error) para obtener la contraseña. Si conozco la función Hash, conozco la contraseña.
- Las tablas rainbow son una estructura de datos (mapas o arrays asociativos) que proveen información acerca de la recuperación de contraseñas en texto plano generadas con ciertas funciones hash conocidas. De esta forma, lo que antes era un ataque de fuerza bruta ahora es una búsqueda en unas tablas gigantes. Obviamente el gran problema de estas técnicas es el espacio. De hecho, aunque aquí fue explicado de forma resumida, se utilizan funciones de reducción para no tener que ocupar tanto espacio de almacenamiento.

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP – Modificación de Contraseñas

- En caso de olvidar la contraseña o querer modificarla sin conocerla, podemos recurrir a herramientas en modo Live que permiten resetearlas o cambiarlas sin autorización.

Podemos considerar entre otras opciones:

1. Mediante la distribución UBCD podemos ejecutar la aplicación Password Renew. Le indicamos en qué directorio se encuentra la carpeta y a continuación nos mostrará un listado de usuarios disponibles, pudiendo realizar acciones como renovar una contraseña, crear un administrador...
2. Otro procedimiento o vulnerabilidad que presentan los sistemas Windows es a través de herramientas que pueden verse modificadas o sustituidas por la consola de comandos. Por ejemplo la utilidad StickyKeys sw de ayuda y accesibilidad.

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en WXP – Modificación de Contraseñas

- ❑ El fichero que ejecuta es sethc.exe ubicado en c:\windows\system32. La vulnerabilidad consiste en sustituir este programa por cmd.exe, de forma que al pulsar la tecla SHIFT 5 veces seguidas se nos abrirá el shell de comandos, desde el cual podemos ejecutar los comandos que queramos como root del sistema.
- ❑ Desde una distribución LIVE accedemos a la partición de Windows montada y realizamos las acciones indicadas anteriormente.
- ❑ La reiniciar el sistema y al mostrarse la página de inicio de sesión pulsamos 5 veces seguidas la tecla SHIFT y nos ejecutará la consola de comandos. Podremos ejecutar por ejemplo **control userpasswords2** que nos abrirá la utilidad de configuración de contraseñas de usuarios, pudiendo renovarlas sin conocerlas previamente.

```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>control userpasswords2
C:\WINDOWS\system32>
```



Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en GNU/LINUX

- En los sistemas GNU/Linux el archivo que controla los usuarios y sus contraseñas encriptadas es /etc/shadow visible tan solo por el usuario root, aunque en caso de poder acceder a una partición GNU/Linux y a su sistema de ficheros, tenemos el fichero visible.
- La estructura del mismo es un listado con una línea por cada usuario en la que la segunda columna separada por : es la contraseña encriptada según algún algoritmo de cifrado, habitualmente MD5 si comienza por \$1\$, o SHA si comienza por \$6\$, opción más segura e incluida por defecto en las versiones de distribuciones actuales.

slice:\$1\$NLJJ6\$ow5g1I1NgYITqqQQy5D21:14234:0:99999:7:::	
Contraseña	Contraseña encriptada. La forman entre 13 y 24 caracteres (a-z, A-Z, 0-9, \, /). Si comienza por el carácter \$, indica que la contraseña se ha encriptado usando un algoritmo distinto de DES. Si comienza por \$1\$, el algoritmo de cifrado está basado en MD5.
Nombre de usuario	Nombre que identifica al usuario en el sistema. Debe tener entre 1 y 32 caracteres.
Caducidad	Días a los que se deshabilita la cuenta contados desde el 1 de enero de 1970.
Inactivo	Días a los que se deshabilita la cuenta después de que caduque la contraseña.
Aviso	Días a los que el usuario será avisado de que debe cambiar la contraseña antes de que ésta caduque.
Máximo	Días durante los que la contraseña es válida. Al terminar el usuario tiene que cambiar la contraseña.
Mínimo	Días que deben pasar como mínimo para que el usuario pueda cambiar la contraseña.
Último cambio	Días que han pasado desde la última vez que la contraseña fue cambiada contados desde el 1 de enero de 1970.

Control de Acceso Lógico

Control de Acceso en el Sistema Operativo

Usuarios/Contraseñas en GNU/LINUX

Arrancando desde una distribución Backtrack accedemos al contenido del archivo /etc/shadow de una partición GNU/Linux instalada en disco duro y previamente montada.

Mediante la aplicación John the Ripper, podemos efectuar distintos tipos de ataques contra este archivo (deberemos indicarle la ruta del archivo-shadow) para descubrir contraseñas encriptadas, por ejemplo:

```
john --single archivo_shadow
```



Ataques contra contraseñas en Sistemas Windows

- ❑ En los sistema windows las contraseñas no se almacenan en texto plano, sino que se almacenan cifradas con una función hash en una zona llamada Administración de las Cuentas de Seguridad (SAM).
- ❑ Para obtener la contraseña de un sistema, primero hay que obtener los valores hash del sistema ejecutando el comando `pwdump3`, y después hay que utilizar las Rainbow Tables para obtener las contraseñas que representan dichos valores. Las tablas Rainbow son tablas que se generan previamente para obtener una contraseña con una longitud y un determinado conjunto de caracteres.
- ❑ El problemas y la dificultas para obtener las contraseñas de un sistema, es el de disponer de las tablas suficientemente grandes para romper cualquier tipo de contraseña. Para hacerse una idea del problema, a continuación puede verse, para diferentes conjunto de caracteres, el tamaño en disco que ocupa y el tiempo de ejecución necesario para generar cada tabla. Lógicamente, cuanto mayor sea el conjunto de caracteres mayor será la probabilidad de acierto para obtener la contraseña.
- ❑ Los conjunto de caracteres tan sólo utilizan caracteres en mayúsculas porque un paso previo es convertir la contraseñas a mayúsculas por que el ataque es mucho más simple.

Ataques contra contraseñas en Sistemas Windows

Conjunto de caracteres	Tamaño en disco	Tiempo ejecución para generar tabla*
0123456789	125 MB	4 horas
ABCDEFGHIJKLMNPQRSTUVWXYZ	610 MB	2 días
ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789	3 GB	15 días
ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789	18.3 GB	224 días
!@#\$%^&*()_-+=		
ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789	119 GB	2354 días
!@#\$%^&*()_-+=~`[]{} \:;";<>,?/		

* El tiempo ha sido calculado con un Pentium 666MHz

- Además de poder generar nuestras propias tablas, puede utilizar las servicios proporcionados por diferentes portales: para descargar las tablas:

<http://www.freerainbowtables.com/>



Free Rainbow Tables
Distributed Rainbow Table Project

Ataques contra contraseñas en Sistemas Windows

- Y las tablas de otros sistemas previo pago:

<http://ophcrack.sourceforge.net/tables.php>

 **XP free small (380MB)**
formerly known as SSTIC04-10k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
md5sum: 17cfa3fc613e275236c1f23eb241bc86

 **XP free fast (703MB)**
formerly known as SSTIC04-5k

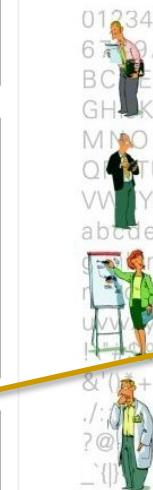
Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
md5sum: f6f5536975b57c891ed5f2de702a02bd

 **XP special (7.5GB)**
formerly known as WS-20k

Success rate: 96%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!#\$%&(')+,-./;<=>?@[|^`{|}`^] (including the space character)



OS OBJECTIF SÉCURITÉ [Audits](#) [Consulting](#) [Training](#) [Products](#) [OS Labs](#) [Contact](#)



Products

Following products have been developed by Objectif Sécurité, the inventors of rainbow tables. All products can be downloaded as soon as we receive your payment. If needed a DVD can be sent by post.

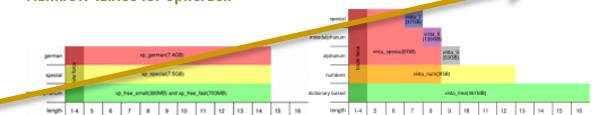
Ophcrack_office

This unique program cracks Word and Excel documents using rainbow tables. It cracks the default encryption technique (the one compatible with Office '97) of these documents within a few minutes. The use of ophcrack_office is very simple and its success rate is 99.6%.

[details >](#)

[buy \\$249](#)

Rainbow tables for ophcrack



Ophcrack is the most efficient Windows password cracker on the market. It is based on rainbow tables which speed up the cracking process consequently.

[details >](#)

[buy \\$99](#)

Professional rainbow tables for ophcrack

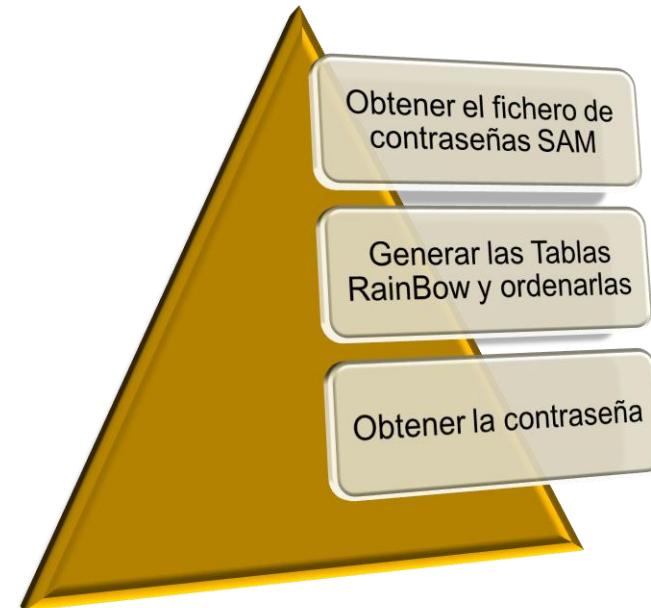
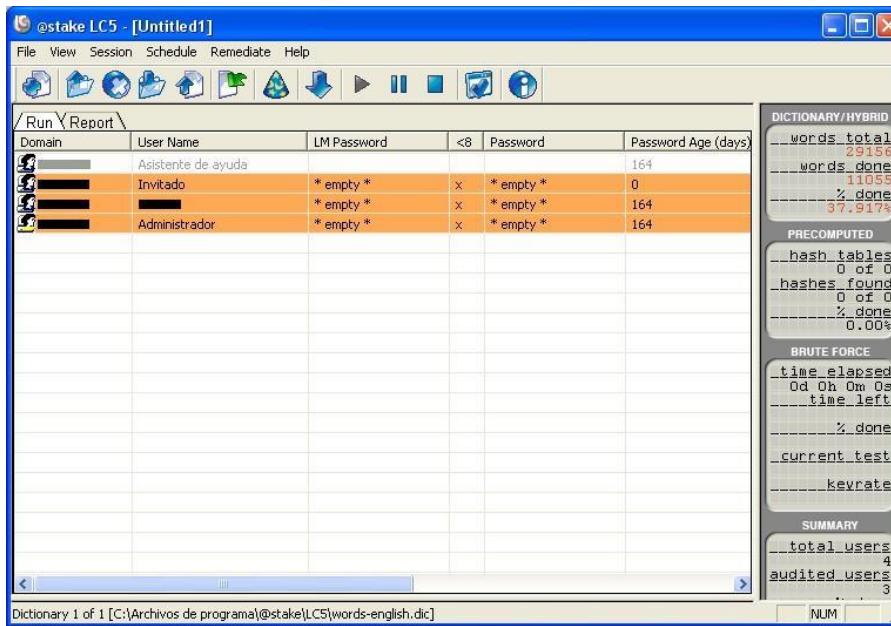
These large rainbow tables are intended especially for security professionals and enterprises. Higher resources are needed in order to get an efficient cracking.

[details >](#)

[buy \\$999](#)

Ataques contra contraseñas en Sistemas Windows

- ❑ Además de poder obtener la contraseña con rcarck, también puede utilizarse otras herramientas como Cain y @stack LC4 que resulta más fácil cuando las contraseñas se pueden romper con un ataque de diccionario.
- ❑ A continuación se expone ejemplos/pasos que complementa al punto “Control de Acceso Lógico” para obtener las contraseñas de los usuarios de un sistema.



Ataques contra contraseñas en Sistemas Windows

Obtención del fichero SAM

- ❑ El fichero SAM se encuentra en el directorio %windir%\system32\config donde se puede encontrar un fichero llamado "SAM", que está formado por la representación de los bytes pertenecientes a la clave del registro HKEY_LOCAL_MACHINE\SAM. Si intenta acceder desde el sistema de ficheros o desde el registro de Windows cuando el sistema está en funcionamiento se niega el acceso tanto en modo lectura como escritura.
- ❑ Existen varias maneras de conseguir los datos almacenados en el fichero SAM que dependen de la situación en la que acceda a la máquina objetivo del ataque y de las herramientas que utilice. A continuación se van a ver algunas maneras de obtener el fichero SAM.

Extraer SAM con discos de arranque

- ❑ Puesto que el sistema operativo bloquea los accesos al fichero SAM cuando está en funcionamiento, puede utilizar un disco de arranque y acceder a los ficheros; como el sistema operativo no se está ejecutando no tendrá ningún problema para copiar el fichero SAM.

Ataques contra contraseñas en Sistemas Windows

CIA COMMANDER

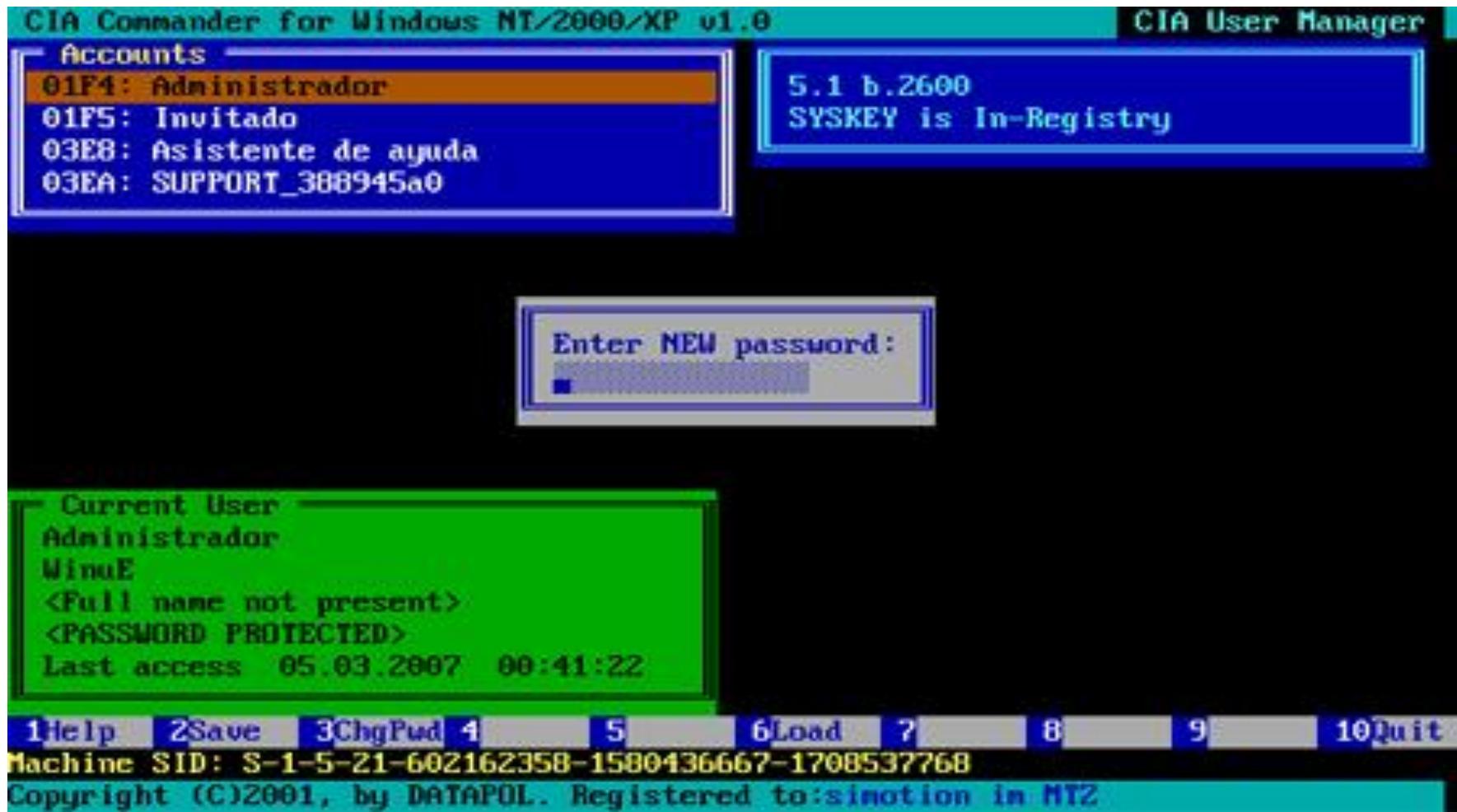
- Existen discos de arranque que permiten realizar copias de seguridad, restaurar y modificar directamente el fichero SAM. Un ejemplo de estos programas es CIA (Commander for windows) que permiten modificar la contraseña de un usuario del sistema:

El funcionamiento de CIA es sencillo:

- Arrancar el equipo con el disco de inicio.
- Selección del disco duro y la partición donde se encuentra instalado el SO.
- Selección de *USER MANAGER* y en la pantalla que aparece se selecciona el directorio, donde se encuentra instalado windows, pulsando a continuación la barra espaciadora.
- Finalmente, en la pantalla aparece el listado de usuarios del equipo, donde se podrá actuar sobre el valor de las contraseñas.

Lógicamente, al ser un disco de arranque la gran desventaja es que se necesita tener acceso físico

Ataques contra contraseñas en Sistemas Windows



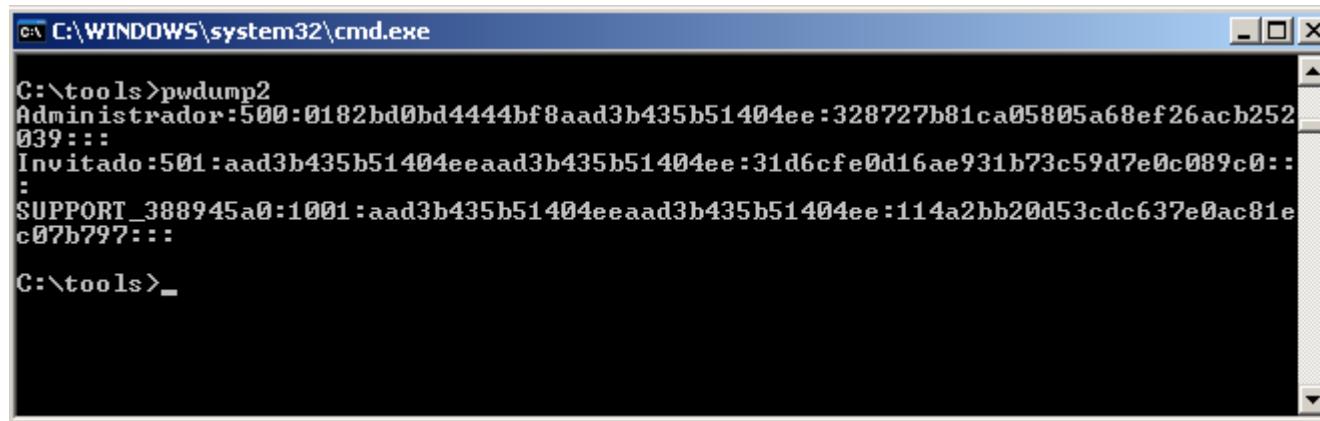
Ataques contra contraseñas en Sistemas Windows

Extraer SAM con pwdump

- ❑ Pwdump es una herramienta creada con el fin de extraer el contenido del SAM en un fichero de texto. Para poder realizar esta función necesita tener privilegios de administrador. Para obtener los valores hash de las contraseñas de un sistema debe ejecutar el comando `pwdump3` (`pwdump`, hasta el `pwdump7`) como administrador del sistema.

La sintaxis del comando es:

```
C:\>pwdump3 <nombre_máquina> <fichero a generar>
C:\>pwdump3 localhost >> claves.txt
```



The screenshot shows a Windows Command Prompt window titled 'cmd C:\WINDOWS\system32\cmd.exe'. The command entered was 'C:\>pwdump3 localhost >> claves.txt'. The output displays several user hashes in the format 'User:Hash'. The output is as follows:

```
C:\>tools>pwdump2
Administrador:500:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252
039:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0:::
:
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:114a2bb20d53cdc637e0ac81e
c07b797:::
C:\>tools>_
```

Ataques contra contraseñas en Sistemas Windows

Ejemplo de uso *pwdump*:

Adivinar las contraseñas de usuarios de un equipo remoto, en este caso voy a sacar las contraseñas de los usuarios de un controlador de dominio Windows 2003, sería igual para un Windows 2000, y no tiene por que ser controlador de dominio, puede ser un Windows XP y tampoco tendría por que ser un PC o servidor remoto, si no local.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>cd\
C:\>net use \\srvdc1\admin$ /u:*****\administrador *****
Se ha completado el comando correctamente.

C:\>
```

Ataques contra contraseñas en Sistemas Windows

Lo primero es validarnos contra el servidor remoto como un administrador, sí, nos tenemos que saber la contraseña de un usuario con privilegios de administrador en el host remoto, por eso en este documento se explica cómo sacar las demás passwords de los usuarios sabiéndose la de un administrador. Desde MSDOS, nos autenticamos con privilegios de administrador en el host remoto, en mi caso es un controlador de dominio:

"net use \\SERVIDOR_DESTINIO\admin\$ /u:DOMINIO\USUARIO CONTRASEÑA"

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>cd "C:\pwdump6\PwDumpRelease"
C:\pwdump6\PwDumpRelease>PwDump svrdci > C:\claves.txt

pwdump6 Version 1.5.0-BETA by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2006 foofus.net

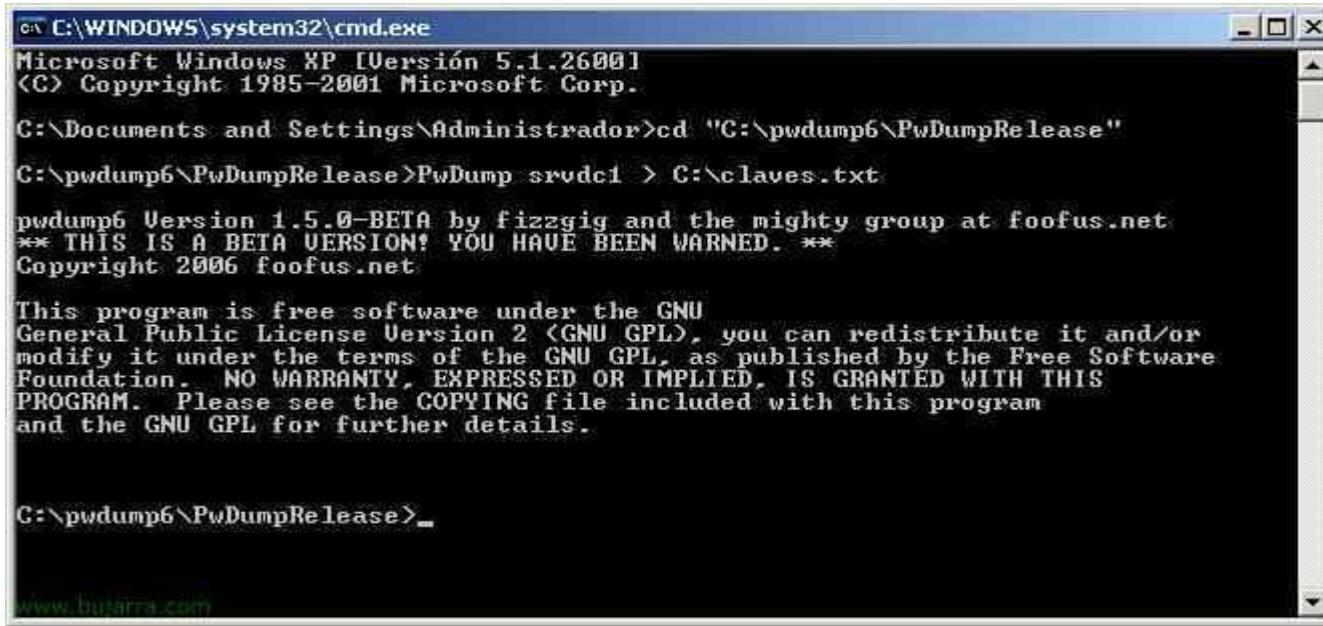
This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program
and the GNU GPL for further details.

C:\pwdump6\PwDumpRelease>_
```

Ataques contra contraseñas en Sistemas Windows

Ahora, nos bajamos a nuestro PC el PWDUMP, lo descomprimimos por ejemplo en C:\pwdump\, entramos por MSDOS hasta ese directorio, ejecutamos el programa para que nos exporte los usuarios y los hashes de sus contraseñas a un fichero:

"pwdump SERVIDOR_DESTINO > FICHERO_DE_CLAVES"



```
on C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>cd "C:\pwdump6\PwDumpRelease"
C:\pwdump6\PwDumpRelease>PwDump svadc1 > C:\claves.txt

pwdump6 Version 1.5.0-BETA by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2006 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program
and the GNU GPL for further details.

C:\pwdump6\PwDumpRelease>_
```

Ataques contra contraseñas en Sistemas Windows

```
Administrador:500:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FCD3D759941E45C490F143D5F:::  
ana:1013:75F4E8AEB411340CAAD3B435B51404EE:4A527F798ADC0342BB254A61DC2B35C1:::  
ASPNET:1010:86016426E8CB617C8A01DD24A5CE1FE9:BD2D649BE7B052A223A079A9432ED671:::  
Invitado:501:NO PASSWORD*****:NO  
PASSWORD*****:  
IUSR_SERVIDOR:1006:2B8791BF3216C99E7FA00745DD85F9C0:5831FD008A01008B3AA5AB9C7818DB9A:::  
IWAM_SERVIDOR:1007:750316ABC3FB42D232BBB9C26A173DFA:784D894EE7702A8CF0157CF557697276:::  
javier:1014:F1ECE1368017F367AAD3B435B51404EE:25CC6B6415740F1E08B1AA92EA84480A:::  
maria:1012:0B1D44C6C4139530AAD3B435B51404EE:483D9BAAAF3104161C3AD1B34553D374:::  
pepe:1011:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FCD3D759941E45C490F143D5F:::  
SUPPORT_388945a0:1001:NO  
PASSWORD*****:B90CBD7BE7496C050D641A32F25E0B93:::
```

La sección delimitada por los (:), que comienza con AEBD y termina con 04EE es el hash LANMAN. La sección entre 7A21 y 3D5F es el hash contraseña. Ambos hash tienen 32 caracteres de longitud y representan la misma contraseña, pero el primero resulta mucho más fácil de craquear y de recuperar la contraseña en texto plano.

Ataques contra contraseñas en Sistemas Windows

Extraer SAM utilizando el programa Cain & Abel

- Lo primero que debe hacerse es instalar el servicio Abel en la máquina remota donde se quiere extraer las contraseñas; esto se puede hacer de dos maneras: enviando los ficheros Abel.exe y Abel.dll a dicha máquina y ejecutando el primero, o utilizar Cain y realizar los siguientes pasos:

- *En la pestaña Network se selecciona la raíz del árbol Microsoft Windows Network.*
- *Se despliega el subárbol All computers y seleccionando el equipo remoto objetivo.*
- *Del subárbol de accede a services.*
- *Y con el botón derecho del ratón se selecciona la opción install Abel*



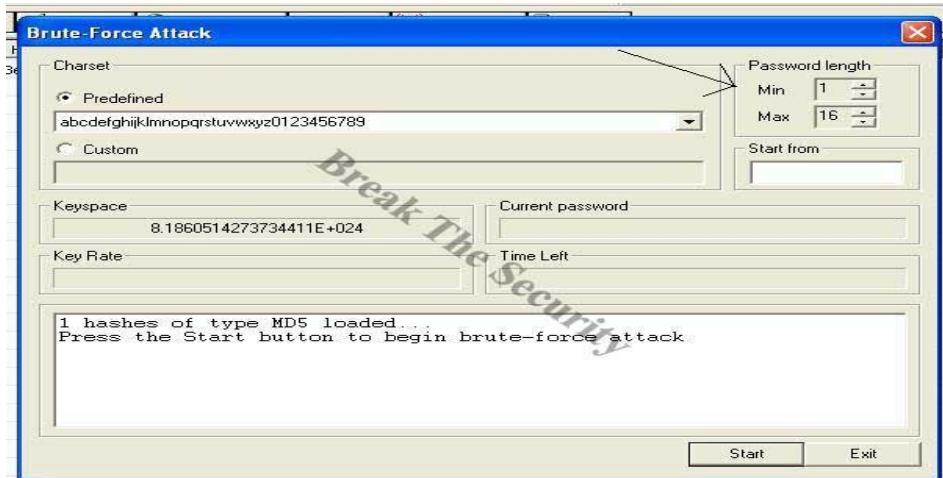
- Una vez instalado el servicio Abel aparece un nuevo subárbol de opciones cuya raíz se denomina Abel. Entre las diferentes posibilidades que permite realizar este servicio existe una que se llama Hashes. Si se selecciona la opción Hashes se muestran las contraseñas encriptadas pertenecientes al sistema remoto. Si se selecciona las claves con Abel y se hace clic con el botón derecho, se desplegará un submenú desde el que puede exportar los hashes a un fichero con formato *.lc (L0phtcrack) o enviar las contraseñas encriptadas al propio cracker que Cain incorpora.

Ataques contra contraseñas en Sistemas Windows

- Para obtener las contraseñas hay que realizar los siguientes pasos:



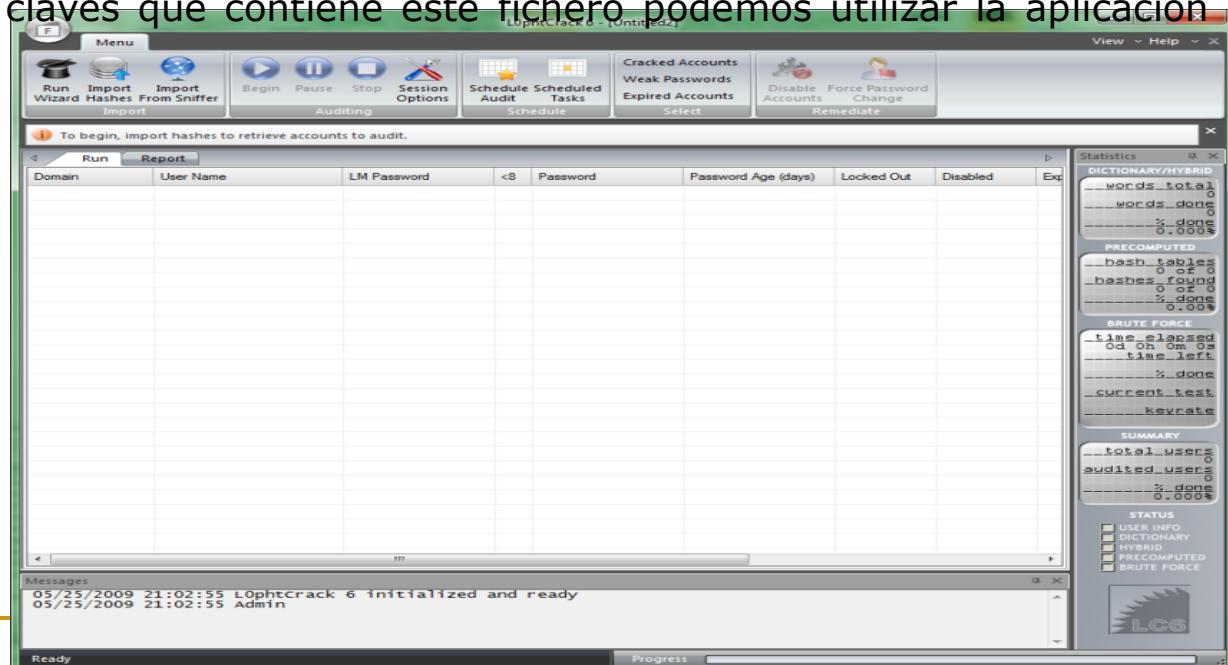
- Se selecciona los hashes, se pulsa el botón derecho y se elige la opción "Send to cracker" o "Send all to cracker".
- En la pestaña Cracker, se selecciona el subárbol LM & NTLM hashes
- Se selecciona la cuenta de usuario de la que quiere la contraseña, se pulsa el botón derecho, se selecciona el tipo de ataque que se desea realizar y Cain iniciará el ataque.
- Una vez finaliza el ataque, Cain muestra la contraseña del usuario seleccionado.



Ataques contra contraseñas en Sistemas Windows

Extraer SAM del directorio Repair

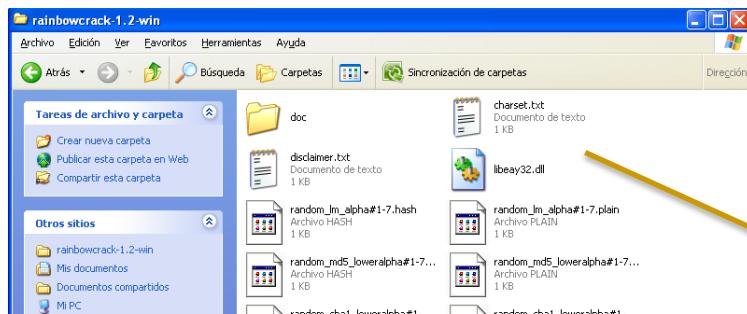
- En los sistemas operativos Windows existe una utilidad denominada rdisk, la cual permite recuperar fallos en el SO gracias a que guarda en el directorio %WindowsRoot%\Repair una copia de seguridad de los datos más importantes. Entre la información que almacena se encuentra un fichero denominado SAM, donde se guarda de forma comprimida el fichero SAM. Este fichero puede copiarse y modificarse. Para descomprimir podemos utilizar el comando expand. Para craquear las claves que contiene este fichero podemos utilizar la aplicación **L0phCrack**.



Ataques contra contraseñas en Sistemas Windows

Craqueando el fichero SAM

- El paso más importante que tenemos que realizar es generar las tablas rainbow. Si utilizamos herramientas como LiveCD ophcrack,, Cain & Abel, @stake LC4 .. etc ya tienen creadas una serie de tablas. En este apartado vamos a crear nuestras tablas con el fin de atacar el fichero claves.txt obtenido previamente.. Para realizar esto último necesitamos ejecutar el comando rtgen que va incluido en rainbowcrack1.2-win.



Para generar la tabla hay que indicar la longitud máxima de la contraseña y el conjunto de caracteres que puede tener la contraseña que se desea romper. Los conjuntos de caracteres están definidos en el fichero charset.txt

A screenshot of a Windows Notepad window titled 'charset.txt - Bloc de notas'. The text in the window is as follows:

```
# charset configuration file for rainbowcrack 1.1 and later
# by zhu shuanglei <shuanglei@hotmail.com>

alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+=~`[]{}|\:;''<>,._?/]
all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+=~`[]{}|\:;''<>,._?/]

numeric = [0123456789]
loweralpha = [abcdefghijklmnopqrstuvwxyz]
loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]
```

Ataques contra contraseñas en Sistemas Windows

Craqueando el fichero SAM

- Por ejemplo, si deseamos generar una tabla con el conjunto de caracteres numérico debemos ejecutar el siguiente comando:

The screenshot shows a Windows desktop environment. In the foreground, there are two command-line windows (CMD.exe) and a file explorer window.

The left CMD window (C:\WINDOWS\system32\cmd.exe) displays the output of the command: rainbowcrack-1.2-win>rtgen.exe lm numeric 1 7 0 2100 8000000 all. The output shows the progress of generating rainbow tables for the LM hash routine, specifying a charset of numeric characters (0-9), a length of 8 characters, and a space total of 11111110. It also shows the reduction offset and the generation of 8000000 chains.

The right CMD window (C:\WINDOWS\system32\cmd.exe) displays the output of the command: C:\WINDOWS\system32\cmd.exe. This shows the current directory path and the results of the previous command, including the generated rainbow table file (lm_numeric#1-7_0_2100x8000000_all.rt).

The file explorer window (Seleccionar C:\WINDOWS\system32\cmd.exe) shows the contents of the directory C:\WINDOWS\system32\cmd.exe. It lists various files and subdirectories, including charset.txt, disclaimer.txt, doc, ejemplo, FicheroHashWindows.txt, libeay32.dll, random_lm_alpha#1-7.hash, random_lm_alpha#1-7.plain, random_md5_loweralpha#1-7.hash, random_md5_loweralpha#1-7.plain, random_sha1_loweralpha#1-7.hash, random_sha1_loweralpha#1-7.plain, rcrack.exe, readme.txt, rtdump.exe, rtgen.exe, and rtsort.exe. It also shows statistics for the folder: 16 archivos, 13.988.223 bytes, 4 dirs, and 8.683.708.416 bytes libres.

Ataques contra contraseñas en Sistemas Windows

Craqueando el fichero SAM

- Los parámetros más importantes:

- lm es el tipo de firma digital. Los tipos de firma digital son lm, ntlm, md5 y shal.
- numeric es el conjunto de caracteres definido en el fichero charset.txt:

```
# charset configuration file for rainbowcrack 1.1 and later
# by Zhu ShuangLei <shuanglei@hotmail.com>
alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+=~`[]{}|\;\"<>,.?/]
all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+=~`[]{}|\;\"<>,.?/]

numeric = [0123456789]
loweralpha = [abcdefghijklmnopqrstuvwxyz]
loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]
```

- 1 es la longitud mínima de la contraseña, y 7 es la máxima.
- 0 es el índice de la tabla rainbow.
- all es el sufijo que tendrá el fichero.

- La probabilidad de obtener la contraseña teniendo una tabla es del 60,05%. Si se quiere aumentar la probabilidad de acierto puede añadirse más tablas rainbow. Para calcular la probabilidad de acierto teniendo varias tablas hay que seguir la siguiente ecuación: rtgen.exe lm numeric 1 7 0 2100 800000 all

$$P(n) = 1 - (1 - 0.6055)^n$$

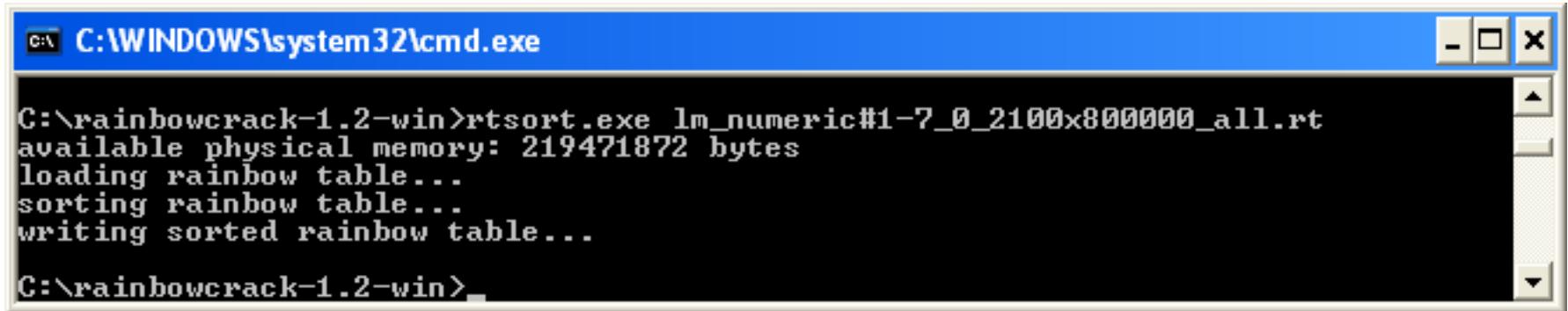
Ataques contra contraseñas en Sistemas Windows

Craqueando el fichero SAM

- Para generar 5 tablas numéricas y así aumentar la probabilidad de éxito:

```
rtgen.exe lm numeric 1 7 0 2100 800000 all  
rtgen.exe lm numeric 1 7 1 2100 800000 all  
rtgen.exe lm numeric 1 7 2 2100 800000 all  
rtgen.exe lm numeric 1 7 3 2100 800000 all  
rtgen.exe lm numeric 1 7 4 2100 800000 all
```

- Una vez generadas las tablas, el siguiente paso que debe realizarse es ordenarlas. Para ello debe ejecutarse el comando rsort <nombre de la tabla>:



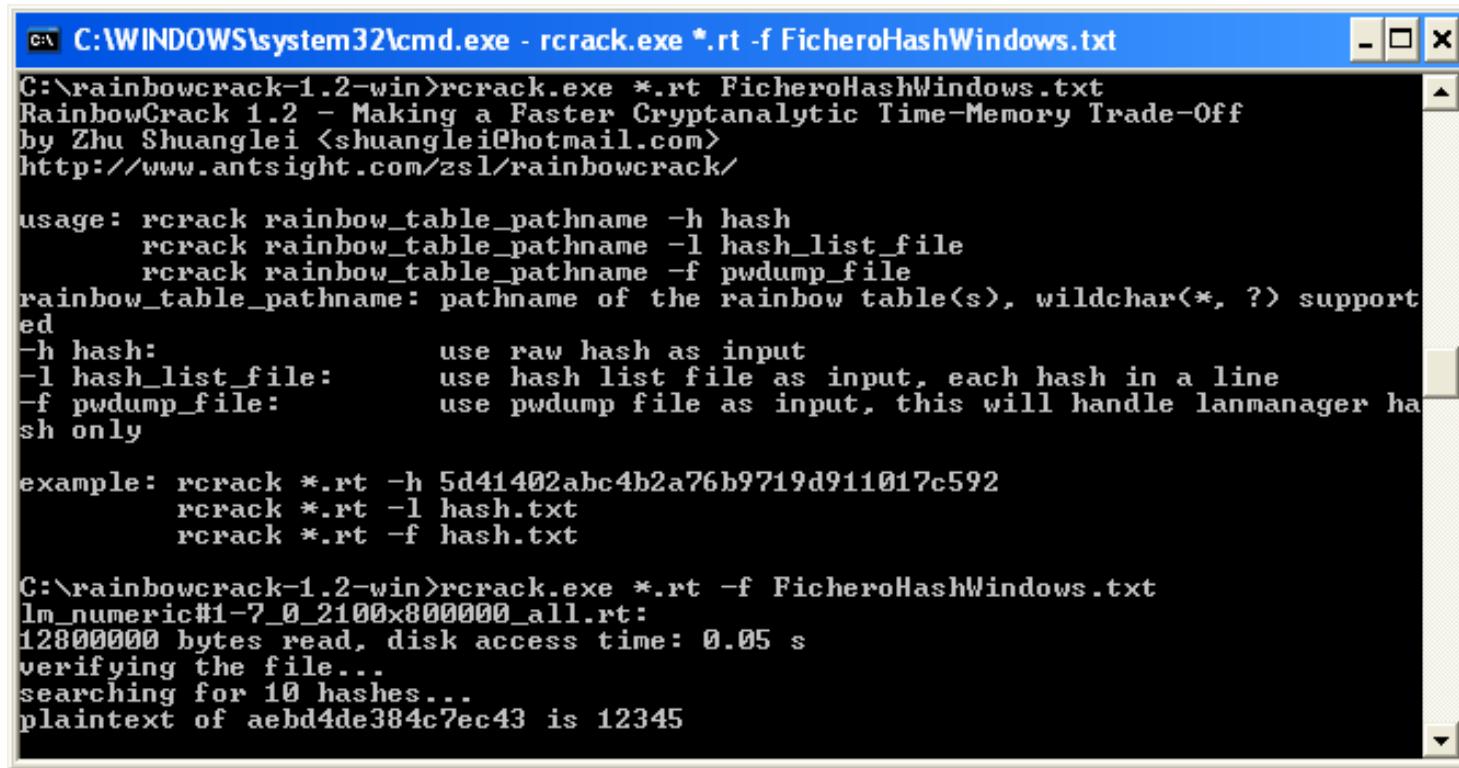
The screenshot shows a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd.exe'. The command entered is 'C:\rainbowcrack-1.2-win>rtsort.exe lm_numeric#1-7_0_2100x800000_all.rt'. The output shows the process of loading, sorting, and writing a rainbow table. The window has standard Windows controls (minimize, maximize, close) and scroll bars.

```
C:\rainbowcrack-1.2-win>rtsort.exe lm_numeric#1-7_0_2100x800000_all.rt  
available physical memory: 219471872 bytes  
loading rainbow table...  
sorting rainbow table...  
writing sorted rainbow table...  
C:\rainbowcrack-1.2-win>
```

Ataques contra contraseñas en Sistemas Windows

Obtención de las contraseñas

- Una vez guardados los valores hash en el fichero claves.txt para obtener las contraseñas debemos ejecutar el comando rcrack:



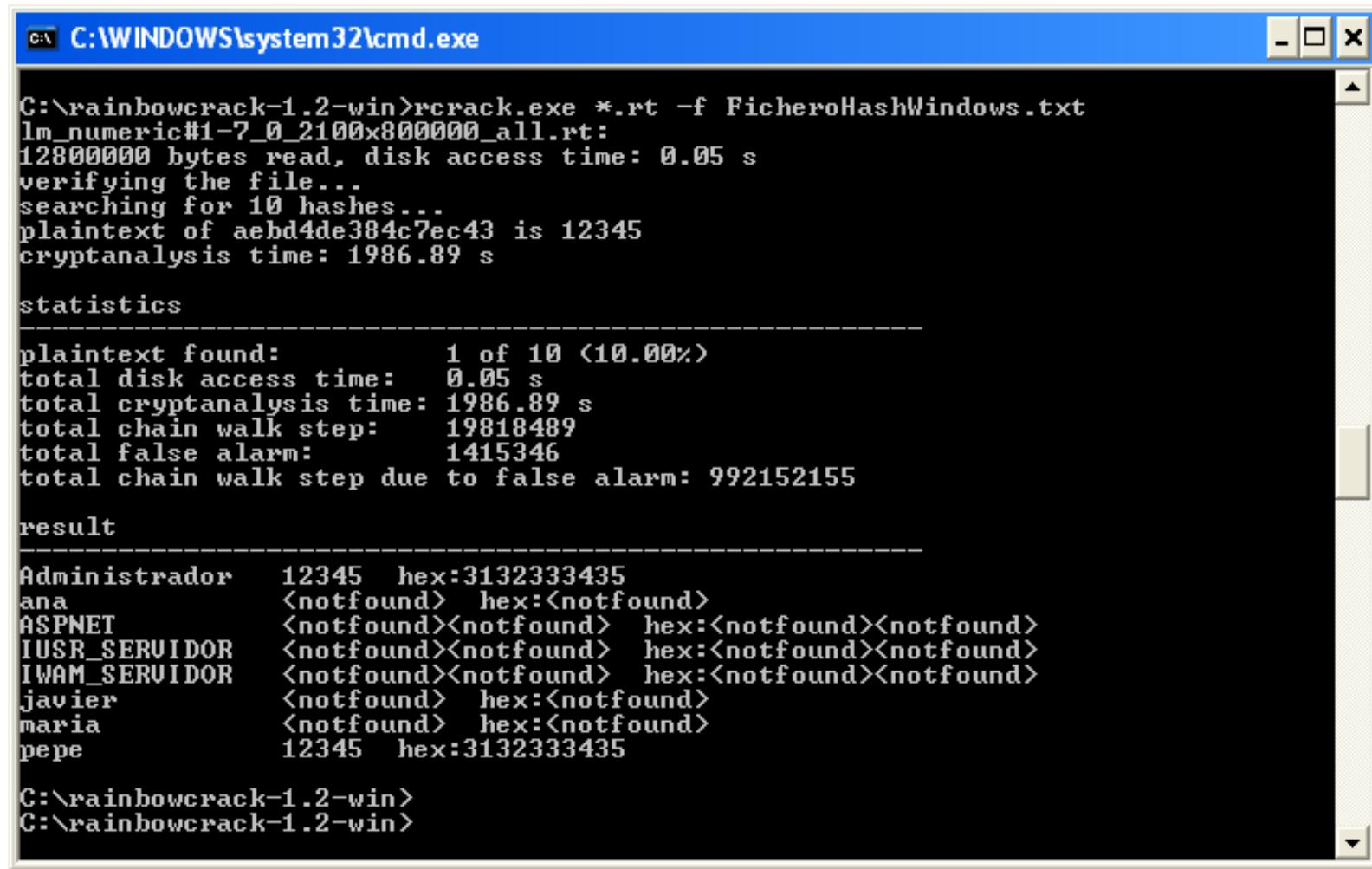
```
C:\WINDOWS\system32\cmd.exe - rcrack.exe *.rt -f FicheroHashWindows.txt
C:\rainbowcrack-1.2-win>rcrack.exe *.rt FicheroHashWindows.txt
RainbowCrack 1.2 - Making a Faster Cryptanalytic Time-Memory Trade-Off
by Zhu Shuanglei <shuanglei@hotmail.com>
http://www.antsight.com/zsl/rainbowcrack/

usage: rcrack rainbow_table.pathname -h hash
       rcrack rainbow_table.pathname -l hash_list_file
       rcrack rainbow_table.pathname -f pwdump_file
rainbow_table.pathname: pathname of the rainbow table(s), wildchar(*, ?) supported
-h hash:           use raw hash as input
-l hash_list_file: use hash list file as input, each hash in a line
-f pwdump_file:   use pwdump file as input, this will handle lanmanager hash only

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
          rcrack *.rt -l hash.txt
          rcrack *.rt -f hash.txt

C:\rainbowcrack-1.2-win>rcrack.exe *.rt -f FicheroHashWindows.txt
lm_numeric#1-7_0_2100x800000_all.rt:
12800000 bytes read, disk access time: 0.05 s
verifying the file...
searching for 10 hashes...
plaintext of aebd4de384c7ec43 is 12345
```

Ataques contra contraseñas en Sistemas Windows



```
C:\WINDOWS\system32\cmd.exe
C:\rainbowcrack-1.2-win>rrcrack.exe *.rt -f FicheroHashWindows.txt
lm_numeric#1-7_0_2100x800000_all.rt:
12800000 bytes read, disk access time: 0.05 s
verifying the file...
searching for 10 hashes...
plaintext of aebd4de384c7ec43 is 12345
cryptanalysis time: 1986.89 s

statistics
-----
plaintext found:      1 of 10 <10.00%>
total disk access time:  0.05 s
total cryptanalysis time: 1986.89 s
total chain walk step: 19818489
total false alarm: 1415346
total chain walk step due to false alarm: 992152155

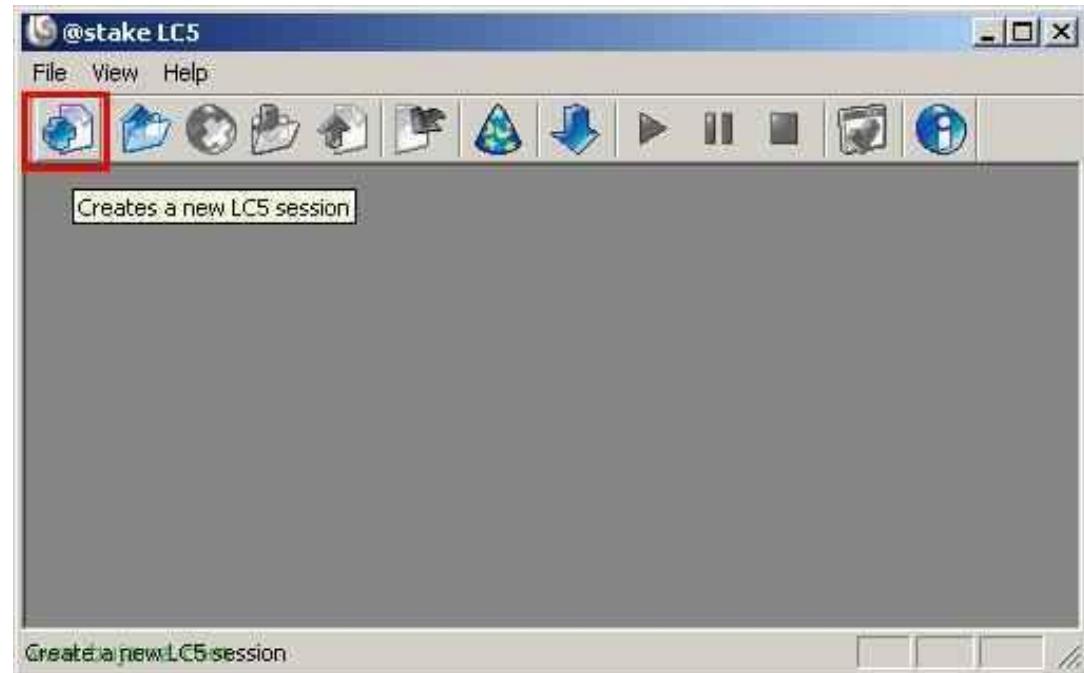
result
-----
Administrador    12345  hex:3132333435
ana              <notfound>  hex:<notfound>
ASPNET           <notfound><notfound>  hex:<notfound><notfound>
IUSR_SERVIDOR   <notfound><notfound>  hex:<notfound><notfound>
IWAM_SERVIDOR   <notfound><notfound>  hex:<notfound><notfound>
javier           <notfound>  hex:<notfound>
maria            <notfound>  hex:<notfound>
pepe             12345  hex:3132333435

C:\rainbowcrack-1.2-win>
C:\rainbowcrack-1.2-win>
```

Ataques contra contraseñas en Sistemas Windows

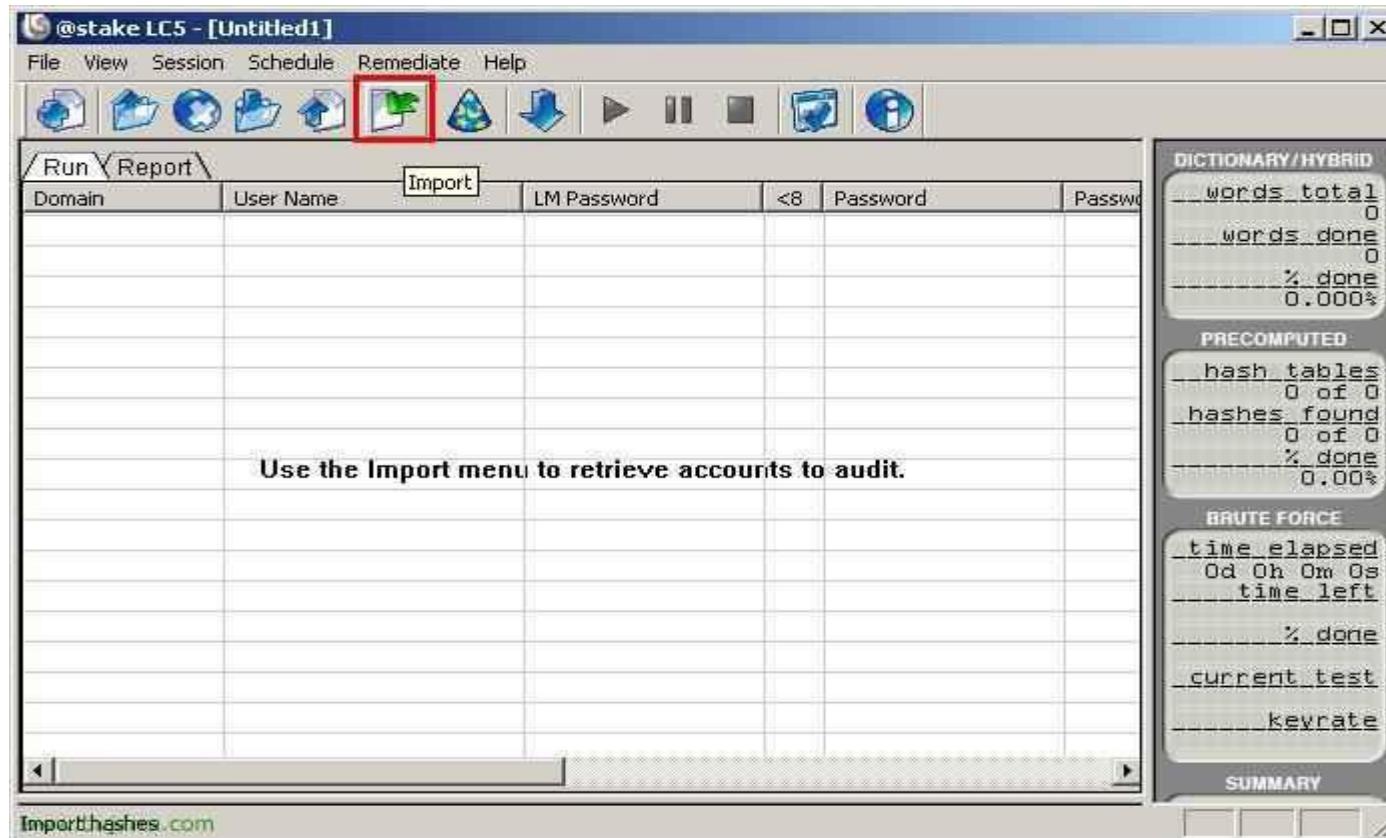
Obtener las contraseñas

- Supongamos que hemos obtenido el fichero de claves partiendo del comando: `pwdump SERVIDOR_DESTINO > FICHERO_DE_CLAVES`. Utilizamos la aplicación @stake LC5 importando el fichero obtenido.



Ataques contra contraseñas en Sistemas Windows

- Ahora abrimos el L0phcrack o LC, en mi caso, usaré la versión LC5 o L0phcrack 5. Lo primero de todo es crearnos una nueva sesión para poder importar luego el fichero de las claves y reventarlo.



Ataques contra contraseñas en Sistemas Windows

- Una vez que tenemos una sesión, tenemos que importar el fichero que hemos generado con el pwdump, para ello pulsamos sobre "Import". Y en "Import from file" indicamos "From PWDUMP file" y en "Filename" buscamos el fichero generado anteriormente, pulsamos sobre "OK". Veremos el listado de usuarios, ahora tenemos que personalizar un poco esta sesión con las opciones que nos interese. Veremos que usuarios tienen un password menor de 8 caracteres y quieren no tienen contraseña. Bueno personalizamos la sesión desde "Session" > "Session Options..."

The screenshot shows the @stake LC5 interface. On the left, a modal dialog titled 'Import' is open, showing options to import from Local machine, Remote machine, or From PWDUMP file (which is selected). The 'Filename' field is set to 'C:\claves.txt'. On the right, the main window displays a table of user accounts with columns for Domain, User Name, LM Password, <8, Password, Password Age (days), Locked Out, Disabled, and Expired. Several accounts have '???????' in the LM Password column. A status bar at the bottom indicates 'Dictionary 1 of 1 [C:\Archivos de programa\@stake\LC5\words-english.dic]'. The right side of the window contains various performance metrics and progress bars for dictionary attacks.

Ataques contra contraseñas en Sistemas Linux

- En los sistemas GNU/Linux se puede utilizar el algoritmo md5 de firma digital para guardar el hash de las contraseñas en el fichero /etc/password o en el fichero /etc/shadows.
- Antiguamente las hash se guardan siempre en el fichero /etc/password y como todos los usuarios tienen permiso de lectura en ese fichero, lo copiaban y realizaban un ataque de fuerza bruta para obtener las contraseñas del sistema.
- Posteriormente se tomó como opción guardar el hash de las contraseñas en el fichero /etc/shadow y en teoría ese fichero no lo pueden copiar los usuarios porque tan sólo tiene permiso de lectura el root del sistema.
- Para obtener las contraseñas de un sistema GNU/Linux se realiza un ataque de fuerza bruta utilizando John the Ripper o @stack LC5

John the Ripper

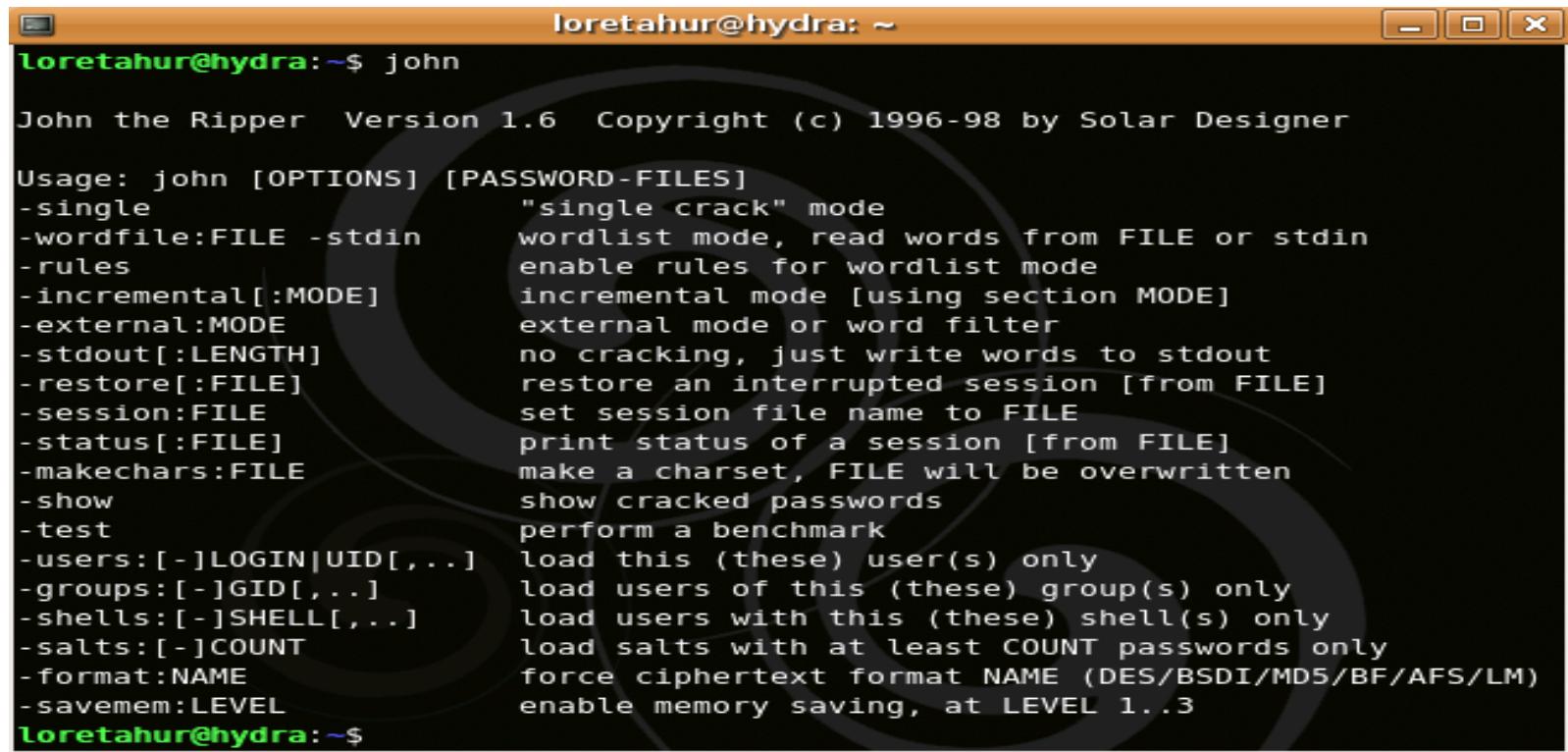
- Permite realizar un ataque de fuerza bruta a un fichero de contraseñas de un sistema GNU/LINUX. Para realizar esta operación primero hay que obtener las contraseñas del fichero passwd y/o shadow

```
unshadow passwd shadow > nuevo_passwd.txt
```

Ataques contra contraseñas en Sistemas Linux

- Una vez que se tiene el fichero de contraseñas para iniciar el ataque tan solo hay que ejecutar el comando:

```
john nuevo_passwd.txt
```



The screenshot shows a terminal window titled "loretahur@hydra: ~". The command "john" is entered, and the output is as follows:

```
John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single          "single crack" mode
-wordfile:FILE -stdin      wordlist mode, read words from FILE or stdin
-rules           enable rules for wordlist mode
-incremental[:MODE]    incremental mode [using section MODE]
-external:MODE      external mode or word filter
-stdout[:LENGTH]    no cracking, just write words to stdout
-restore[:FILE]     restore an interrupted session [from FILE]
-session:FILE       set session file name to FILE
-status[:FILE]      print status of a session [from FILE]
-makechars:FILE    make a charset, FILE will be overwritten
-show             show cracked passwords
-test              perform a benchmark
-users:[-]LOGIN|UID[...] load this (these) user(s) only
-groups:[-]GID[...]  load users of this (these) group(s) only
-shells:[-]SHELL[...] load users with this (these) shell(s) only
-salts:[-]COUNT     load salts with at least COUNT passwords only
-format:NAME        force ciphertext format NAME (DES/BSDI/MDS/BF/AFS/LM)
-savemem:LEVEL      enable memory saving, at LEVEL 1..3
```

Ataques contra contraseñas en Sistemas Linux

- Existen tres formas de aplicar el John:

WordList (archivo de palabras): Este es el modo más simple, todo lo que necesitas hacer es especificar un archivo que contenga una palabra por línea.

```
John -wordfile:NOMBRE_FICHERO FICHERO_PASSWORD
```

o bien puedes añadirle -rules para que "juegue" con las palabras del diccionario

```
john -w:FICHERO_DICCIONARIO -rules FICHERO_PASSWORD
```

SingleCrack: Este es el modo con el que deberías comenzar a crackear. Este modo intentará usar la información de login/GECOS

```
john -single FICHERO_PASSWORD
```

Ataques contra contraseñas en Sistemas Linux

Incremental (fuerza bruta): El más potente, ya que probará todas las combinaciones de caracteres posibles. Necesitas indicar la longitud de la clave y los juegos de caracteres.

```
john -i FICHERO_PASSWORD
```

puedes especificar que caracteres usará con este método y la longitud, las configuraciones están en el fichero john.conf en la sección [incremental:MODO]

```
john -i:alpha FICHERO_PASSWORD (a..z - 26 caracteres)
john -i:all FICHERO_PASSWORD (todo - 95 caracteres)
john -i:digits FICHERO_PASSWORD (0..9 - 10caracteres)
```

@stack LC5

- ❑ Es un programa muy sencillo que permite realizar ataques de fuerza bruta a las contraseñas de los sistemas Windows y GNU/LINUX. Para utilizarlo tan solo hay que importar el fichero passwd y pulsar el Play para iniciar el ataque.

Congeladores

- Es un software del tipo "reinicie y restaure" (Reboot and Restore), el cual hace que al instalar este SW el PC queda en un estado de congelación, con todas las características que tenia en ese momento y se regrese a ese punto cada vez que se reinicie la pc.
- Mientras esté encendido el equipo se podrá hacer todo tipo de cambios instalar programas crear archivos etc. Indicar que hay congeladores que permiten un nivel de administración tal que se puede definir restricciones en las acciones que el usuario puede realizar.
- Cuando se reinicie el equipo se perderá todos os cambios realizados volviendo al momento en que instalaste el congelador.
- Suele congelarse solo la partición del SO (C:) o al disco duro donde esta el sistema operativo, teniendo la otra unidad libre para guardar lo que deseas sin que se pierda (D:)



Referencias WEB:

- Sitio web sobre seguridad informática de Microsoft:
 - <http://www.microsoft.com/spain/protect/>
- Manual de administración segura de GNU/Linux:
 - <http://es.tldp.org/Manuales-LuCAS/GSAL/gsal-19991128.pdf>
- Seguridad en GNU/Linux:
 - http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEG_LIN00.html
- Administración de aspectos de seguridad en GNU/Linux y Windows:
 - <http://www.adminso.es/wiki/index.php/>
- Cómo de fuerte es tu contraseña:
 - <http://howsecureismypassword.net/>
- Comprobador de contraseñas de Microsoft:
 - <http://www.microsoft.com/latam/protect/yourself/password/checker.mspx>
- Administración de usuarios en GNU/Linux:
 - http://www.linuxtotal.com.mx/index.php?cont=info_admon_008
- Comprueba la fortaleza y generador de claves. Password tools bund. Disponible en Sourceforge:
 - <http://sourceforge.net/projects/pwdstr/>
- Recomendaciones para la creación y uso de contraseñas seguras de Inteco.
 - http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas

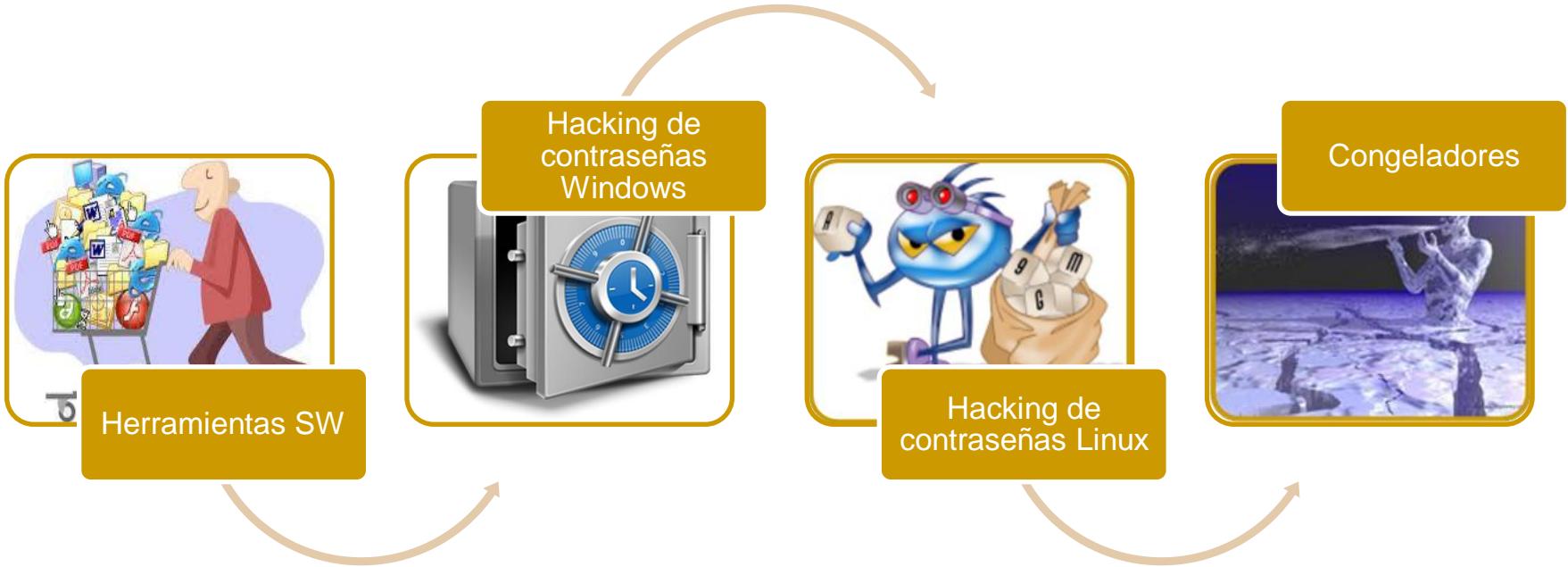
Enlaces a Herramientas SW:

- Pam cracklib: Módulo PAM de control de autenticación de usuarios en sistemas GNU/Linux.
 - <http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/ch11.html>
- Algunas distribuciones arrancables en modo **Live**, con aplicaciones de recuperación y modificación de contraseñas de sistemas:
 - Ultimate Boot CD (UBCD): distribución entorno simulado Windows aplicaciones como antivirus, recuperación de datos, aplicaciones de recuperación y borrado de contraseñas de la BIOS (cmos pwd), borrado y restitución de nuevas contraseñas de usuarios de sistemas Windows instalados en disco, incluso creación de nuevas cuentas de usuario administrador.
 - <http://www.ultimatebootcd.com/>
 - Backtrack: distribución específica con un conjunto de herramientas de auditorías de seguridad, entre otras algunas que permiten escalada de privilegios en sistemas Windows (ophcrack) y GNU/Linux (John the ripper).
 - <http://www.backtrack-linux.org/>
 - Ophcrack: Distribución específica que contiene la aplicación de mismo nombre con capacidad de extraer contraseñas de usuarios en sistemas Windows.
 - <http://ophcrack.sourceforge.net/>
 - Slax: Distribución basada en Slackware, muy ligera y arrancable desde USB. Permite el montaje y acceso a los sistemas de ficheros instalados en disco.
 - <http://www.slax.org/>
 - Wifiway y Wifislax: distribuciones orientadas a realizar auditorías wireless, como recuperación de contraseñas.
 - www.wifiway.org/ y <http://www.wifislax.com/>

Enlaces a Herramientas SW:

- **John the ripper**: software de recuperación de contraseñas. Especializado en contraseñas de sistemas GNU/Linux.
□ <http://www.openwall.com/john>
- **Generador de funciones hash-resumen**: Cifrado de texto plano mediante diversos algoritmos como MD5 o SHA.
□ <http://www.hashgenerator.de/>
- **Windows SteadyState**: control y administración de usuarios y seguridad de sistemas Windows de forma centralizada y sencilla.
□ <http://www.microsoft.com/spain/protect/products/family/steadystate.mspx>
- **Keepass Password Safe**: administrador de contraseñas de diversas cuentas como mail, bancos, etc.
□ keepass.info/
- **DeepFreeze**: congelador de sistemas operativos. Permite arrancar el sistema siempre con una configuración predeterminada.
□ www.faronics.com/

Prácticas/Actividades



Prácticas/Actividades

Actividad 1.- Búsqueda de Información



Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, y de aquellos que resulten de la búsqueda de información, en el que se describan los siguientes elementos: descripción, http de descarga y http de tutorial/manual de uso, http de ejemplo de aplicación/uso, otros aspectos.

slice:\$1\$NLJJ6\$ow5g1l1NgYlTqqQQy5D21:14234:0:99999:7: :						
Contraseña	Contraseña encriptada. La forman entre 13 y 24 caracteres (a-z, A-Z, 0-9, _). Si comienza por el carácter \$, indica que la contraseña se ha encriptado usando un algoritmo distinto de DES. Si comienza por \$1\$, el algoritmo de cifrado está basado en MD5.		Caducidad	Días a los que se deshabilita la cuenta contados desde el 1 de enero de 1970.		
			Inactivo	Días a los que se deshabilita la cuenta después de que caduque la contraseña.		
			Aviso	Días a los que el usuario será avisado de que debe cambiar la contraseña antes de que ésta caduque.		
			Máximo	Días durante los que la contraseña es válida. Al terminar el usuario tiene que cambiar la contraseña.		
			Mínimo	Días que deben pasar como mínimo para que el usuario pueda cambiar la contraseña.		
			Último cambio	Días que han pasado desde la última vez que la contraseña fue cambiada contados desde el 1 de enero de 1970.		

Prácticas/Actividades

Actividad 2.- Tipos de Ataques



En base a los contenidos que se han desarrollado en el tema enumera/describe las distintas posibilidades de acceso no permitido a un sistema Windows y GNU/Linux, mediante reseteo de contraseña, borrado de contraseña, creación de cuentas, craqueo de contraseña, acceso no permitido mediante gestor de arranque o utilización de distribuciones CD LIVE.



Prácticas/Actividades



Actividad 3.1- Ataques contra contraseñas en Sistemas Windows

El objetivo de la práctica es obtener las contraseñas de los usuarios del siguiente fichero hash y que puedes descargar dentro de los recursos de la unidad. *Utiliza rainbowcrack1.2-win*

```
Administrador:500:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FCD3D759941E45C490F143
D5F:::
ana:1013:75F4E8AEB411340CAAD3B435B51404EE:4A527F798ADC0342BB254A61DC2B35C1:::
ASPNET:1010:86016426E8CB617C8A01DD24A5CE1FE9:BD2D649BE7B052A223A079A9432ED671:::
Invitado:501:NO PASSWORD*****:NO
PASSWORD*****:::
IUSR_SERVIDOR:1006:2B8791BF3216C99E7FA00745DD85F9C0:5831FD008A01008B3AA5AB9C7818
DB9A:::
IWAM_SERVIDOR:1007:750316ABC3FB42D232BBB9C26A173DFA:784D894EE7702A8CF0157CF55769
7276:::
javier:1014:F1ECE1368017F367AAD3B435B51404EE:25CC6B6415740F1E08B1AA92EA84480A:::
maria:1012:0B1D44C6C4139530AAD3B435B51404EE:483D9BAAAF3104161C3AD1B34553D374:::
pepe:1011:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FCD3D759941E45C490F143D5F:::
SUPPORT_388945a0:1001:NO
PASSWORD*****:B90CBD7BE7496C050D641A32F25E0B93:::
```

Prácticas/Actividades



Actividad 3.2- Ataques contra contraseñas en Sistemas Windows

- Caso 1.-** Utilizar Ophcrack para obtener las claves del fichero SAM de los usuarios de un WXP
- Caso 2.-** Analiza otras distribución CD-LIVE para la obtención, borrado o resteo de las claves de un usuario de un SO WXP.
- Caso 3.-** Utilizar la herramienta Cain & Abel para obtener las claves de los usuarios de un WXP
- Caso 4.-** Utilizar Backtrack (MetaExploits) para acceder a un Windows Server 2003 y obtener el fichero SAM. A continuación utilizando una aplicación como L0phtCrack craqueamos las contraseñas.
- Caso 5.-** Utiliza el comando pwdump y @stake LC5 para craquear las claves de los usuarios de un sistema Windows



Prácticas/Actividades

Actividad 3.3- Ataques contra contraseñas en Sistemas Linux



Hemos obtenido el fichero /etc/passwd de la máquina virtual de Linux y el objetivo de la práctica es obtener las contraseñas de la máquina. A continuación se muestra un resumen del fichero de contraseñas que también puedes descargar de los recursos asociados a la práctica.

```
root:$1$jm4I4yf$tE/CNDDbPcn68qifD1rfA::0:0:root:/root:/bin/bash
usuario:$1$CVRtQoXNShx0c8zWjZC81P4dA.4Ph:/500:500::/home/usuario:/bi
```



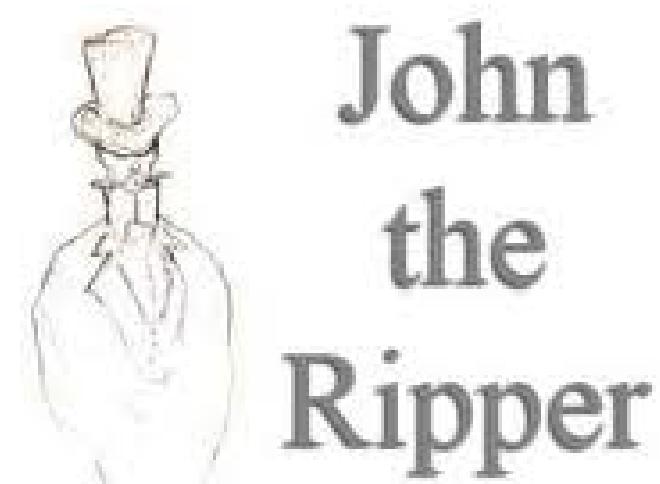
John
the
Ripper

Prácticas/Actividades



Actividad 3.3- Ataques contra contraseñas en Sistemas Linux

Utiliza BackTrack y John The Ripper para descubrir las contraseñas encriptadas de un equipo Ubuntu.



Prácticas/Actividades



DEEP FREEZE
STANDARD



Congeladores

Actividad 4- Analiza la instalación y configuración de los 2 congeladores indicados en el tema.



Prácticas/Actividades

Formato de entrega:

Documento en formato XHTML 1.0, por grupos, con enlaces a elementos multimedia, que resuelvan las cuestiones planteadas. El grupo deberá realizar la actividad...

