

Hacking ético

Módulo III

Hacking del sistema

Objetivo del módulo

■ Entender lo siguiente:

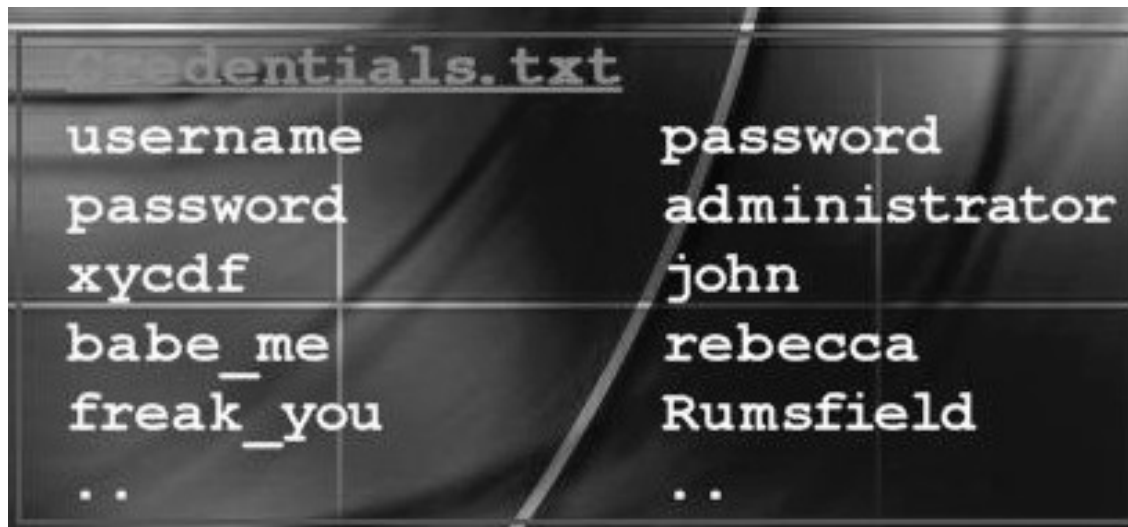
- Adivinación de contraseñas remotas
- Craqueo de contraseñas
- Keyloggers
- Escalada de privilegios
- Denegación de servicio (DoS)
- Buffer overflows
- Sniffers
- Control remoto y puertas traseras
- Redirección de puertos
- Borrado de huellas
- Ocultar ficheros

Adivinación de la password de administrador

- Suponiendo que el puerto TCP139 está abierto, una forma de entrar en un NT/2000 es adivinando la contraseña.
- Intentaremos conectarnos a un recurso compartido (obtenido por enumeración, por ejemplo IPC\$ o C\$) y probar para adivinar username/password.
- Los recursos compartidos por defecto Admin\$, C\$, %Systemdrive% son buenos puntos de partida.

Adivinación por diccionario

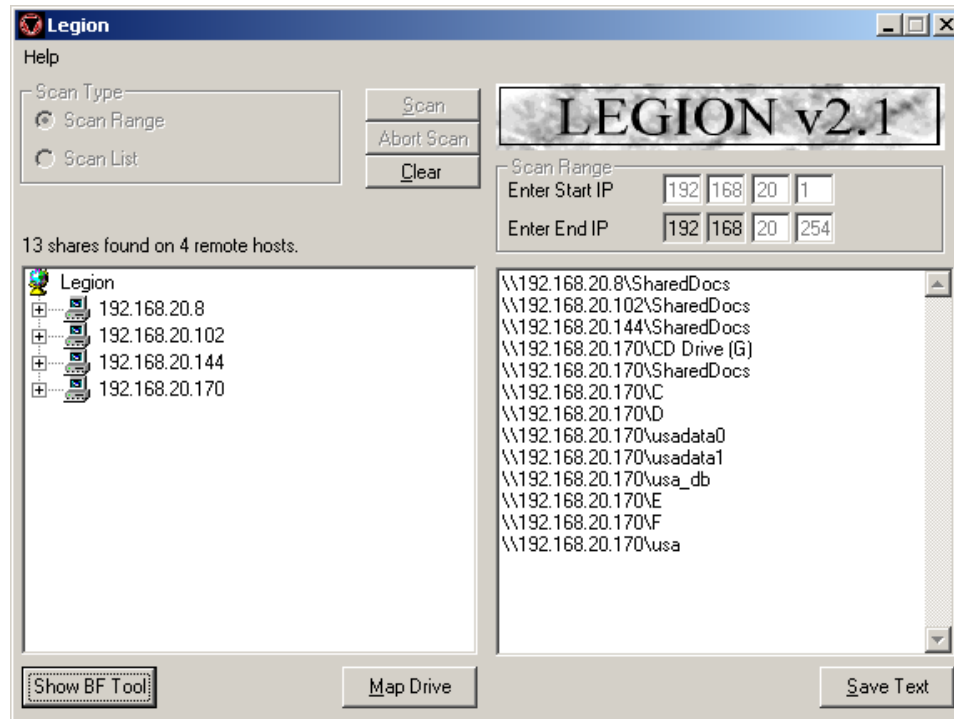
- Realizar una adivinación automática (por diccionario) de contraseñas es relativamente simple usando el shell de NT/2000 y su orden NET USE.
 - 1. Crear un fichero de nombres de usuario y contraseñas simple.
 - 2. Meter este fichero en una estrucuta FOR
 - C:\> FOR /F "token=1, 2*" %i in (credentials.txt) do net use \\target\IPC\$ %i /u: %j



```
credentials.txt
username      password
password      administrator
xycdf         john
babe_me       rebecca
freak_you     Rumsfield
..            ..
```

username	password
password	administrator
xycdf	john
babe_me	rebecca
freak_you	Rumsfield
..	..

Tool: Legion



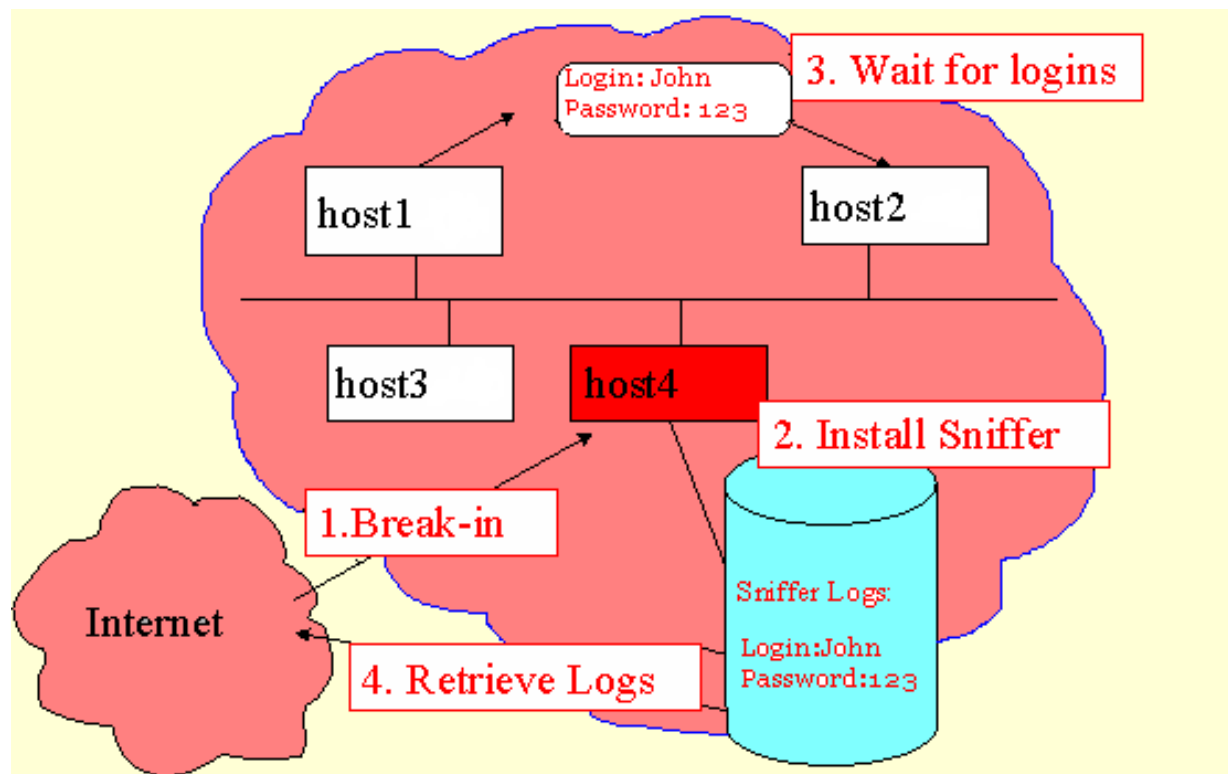
- Legion automatiza la adivinación de contraseñas en sesiones NetBIOS. Legion puede escanear un rango de IPs de equipos Windows con recursos compartidos y permite un ataque por diccionario.

Prevenir adivinación de contraseñas

- Bloquear el acceso a los puertos TCP y UDP 135-139..
- Usar passwords complejas.
- Registrar (auditar) intentos de inicio de sesión fallidos en el visor de sucesos y auditoría
- Visión general de las auditorías y los logs en windows.

Password Sniffing

Adivinar passwords es un trabajo muy duro. ¿Por qué no mejor intentamos capturarlas cuando un usuario inicie sesión con un sniffer?



Types of Password Attacks



- Ataque por diccionario
- Ataque por fuerza bruta
- Ataque híbrido
- Ingeniería Social
- Shoulder surfing

Tipos Password

- Passwords que contienen solo letras
- Passwords que contienen solo números.
- Passwords que contienen sólo caracteres especiales.
- Passwords que contienen letras y números.
- Passwords que contienen letras y caracteres especiales.
- Y cualquier variación

Autenticación en Windows

- Windows siguen almacenando los hashes creados con el protocolo de autenticación LAN Manager (NTLM) por la compatibilidad con pre-windows 2000
- Este es un punto débil, porque son fáciles de craquear (por diccionario o fuerza bruta).
- Estos hashes se guardan en la SAM (<C:/windows/system32/config/sam>), aunque esto se puede deshabilitar en el registro (si no tengo equipos pre-windows 2000)

Qué es un hash LanManager (NTLM)?

Ejemplo: Supongamos la contraseña siguiente: '123456qwerty'

- Cuando la password se cifra con el algoritmo LM (NT y Windows sin dominio) primero se convierte todo a mayúsculas :
'123456QWERTY'
- La contraseña se rellena con _ hasta completar los 14 caracteres de longitud: '123456QWERTY_'
- Antes de cifrarlo se divide por la mitad, resultando dos cadenas de 7 caracteres: '123456Q and WERTY_'
- Cada cadena se cifra individualmente y el resultado es concatenado:
 - '123456Q' = 6BF11E04AFAB197F
 - 'WERTY_' = F1E9FFDCC75575B15
- El hash es 6BF11E04AFAB197FF1E9FFDCC75575B15

Nota: La primera mitad del hash contiene caracteres alfanuméricos, por los que llevará horas descifrarlo con Lophtrcrack, mientras que la segunda apenas un minuto.

Medidas de prevención para evitar el craqueo de contraseñas

- Obligar a una long. mínima de 7-12 caracteres alfa-numéricos.
- Fijar un apolítica de cambio de contraseñas cada 30 días.
- Proteger y aislar físicamente el DC.
- Usar la utilidad SYSKEY para guardar cifrados los hashes en disco (por defecto en 2000).
- Monitorizar los intentos erróneos de inicio de sesión.



Hacking tools: cracking offline

- Pwdump – primera versión que sólo funciona para windows NT 4.0 y sin SP2 (se introdujo el programa de cifrado syskey de 128b).
 - Permite volcar una SAM y descifrarla

Hacking tools: cracking offline

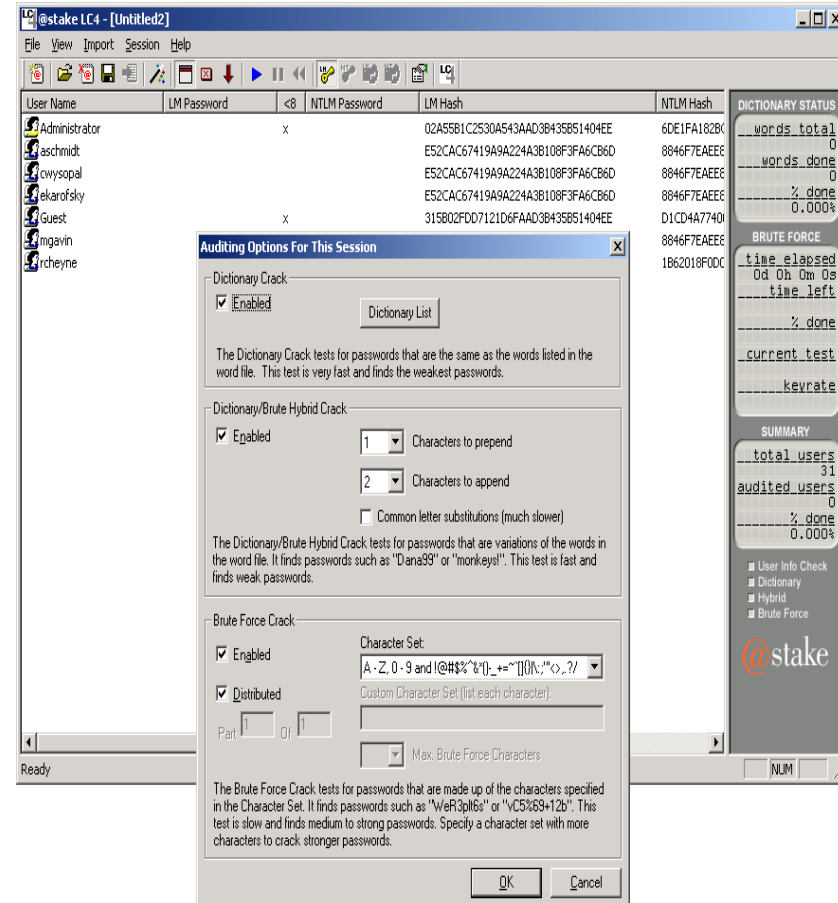
- Pwdump2 – Ya funciona con NT SP2 (syskey), e incluso W2000 y XP.
 - Se basa en un ataque llamado “DLL injection”, que necesita de una aplicación ejecutada como administrador para ejecutar el código malicioso.
 - La aplicación que se utiliza es lsass.exe (sassser)
 - Se necesita ejecutarlo de forma local y como administrador
 - Podría servir para detectar passwords débiles en mi sistema

Hacking tools: cracking offline

- Pwdump3e – permite acceder a una SAM remota, pero tiene que ejecutarse como administrador de la máquina remota.
 - Se conecta al admin\$, se instalan la librería samdump.dll y el servicio pwservice.exe en la máquina remota que permitirán extraer los hash de la SAM.
 - Todo esto a través de SMB (TCP 139 y 445)
- Pwdump4 ,5 y 6 – sucesivas mejoras del 3e.
- Todos estos y más se pueden obtener de Openwall (*bringing security into open environments*):<http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003>

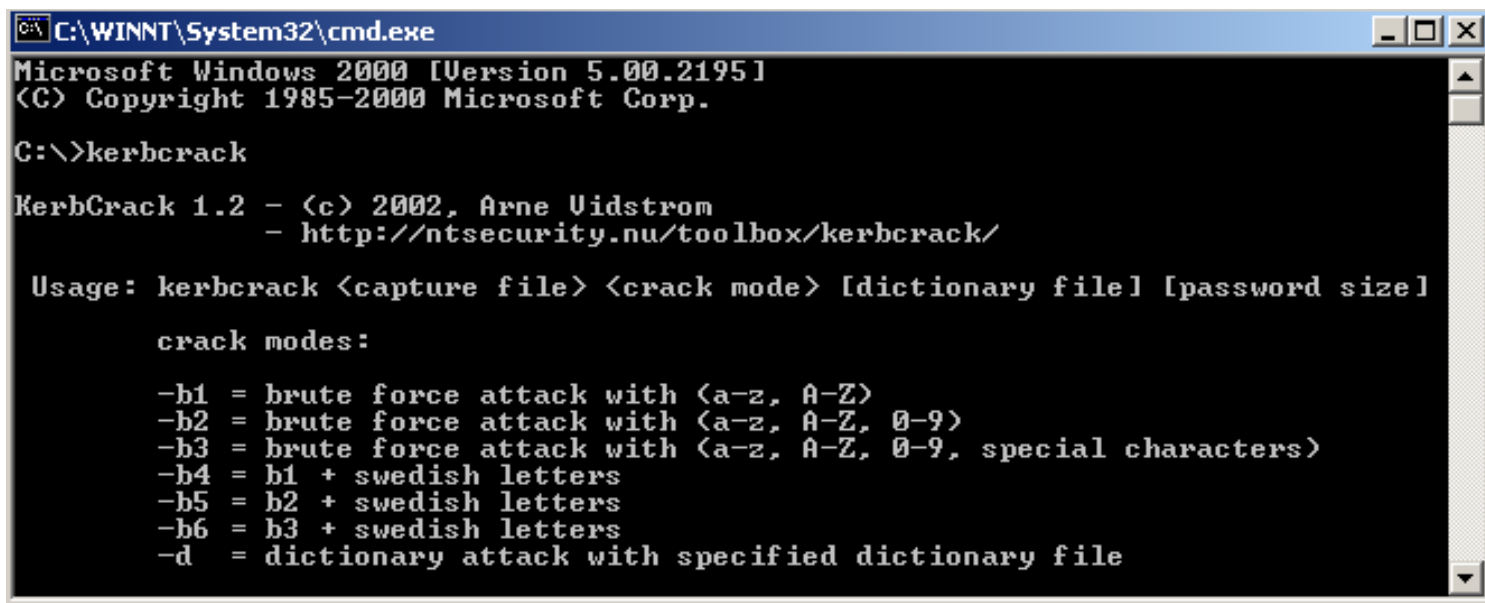
Hacking Tool: Lophtrcrack

- LC4 es un sistema de auditorías y recuperación de passwords distribuido por @stake software. Se capturan los paquetes SMB de un segmento de la red local y se capturan los credenciales (cuentas de usuario)
- Podemos dejar Lophtrcrack un periodo de tiempo extenso (días) para obtener la password de administrador.
- También craquea passwords de la SAM local o de una remota. Pero para eso debo ejecutarlo como administrador.



Hacking Tool: KerbCrack

- KerbCrack consta de dos programas: un sniffer, kerbsniff, que captura de la red logins basados en kerberos de Windows 2000/XP, y kerbcrack. Este último puede ser usado para craquear las passwords capturadas mediante diccionario, híbrido (variaciones de diccionario) y fuerza bruta.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>kerbcrack

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

crack modes:

-b1 = brute force attack with <a-z, A-Z>
-b2 = brute force attack with <a-z, A-Z, 0-9>
-b3 = brute force attack with <a-z, A-Z, 0-9, special characters>
-b4 = b1 + swedish letters
-b5 = b2 + swedish letters
-b6 = b3 + swedish letters
-d  = dictionary attack with specified dictionary file
```

Hacking Tool: John the Ripper

- Es un programa en línea de comandos diseñada para craquear passwords en Unix y Windows. Es una herramienta gratuita y muy rápida.

```
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/MD5/BF/AFS/LM)
-savemem:LEVEL        enable memory saving, at LEVEL 1..3
```

Hacking Tool: John the Ripper

- Craquear passwords de Linux/UNIX/MacOSX
 - `sudo apt-get install john` (o desde <http://www.openwall.com/john/>)
 - `umask 077` (haré que la copia generada sea accesible a cualquiera y no tengo que ser root para usar john)
 - `unshadow /etc/passwd /etc/shadow > mypasswd`
 - `john mypasswd`

Hacking Tool: John the Ripper

- Tipos de ataque:
- Single crack - passwords obvias como que sea igual al nombre de usuario:
 - `john --single mypasswd`
- Ataque híbrido diccionario y variaciones
Ver uso de diccionarios :
 - `john -wordfile=/usr/share/john/password.lst --rules mypasswd`
 - `john -wordfile=/usr/share/john/all.lst --rules mypasswd`
- Fuerza bruta o incremental:
 - `john --incremental mypasswd`

Hacking Tool: John the Ripper

■ Uso de diccionarios:

<http://www.openwall.com/wordlists/>

- Gratis:
`ftp://ftp.ibiblio.org/pub/linux/distributions/openwall/wordlists/all.gz`
- Editar `/etc/john/john.config` para que use el diccionario all
 - `Wordfile = /usr/share/john/all.lst`
- O copiarlo con ese nombre:
 - `cp /usr/share/john/password.lst.bkp /usr/share/john/password.lst.bkp`
 - `cp all /usr/share/john/password.lst`

■ Ver las passwords craqueadas:

- `john --show mypasswd`

Hacking Tool: John the Ripper

■ Consejos:

■ Sólo craquear ciertas cuentas:

- La de root: `john --wordlist=all.lst --rules --users=0 *passwd*`
- O todas menos las mías que sé que son difíciles: `john --wordlist=all.lst --rules --users=-root,solar *passwd*`

■ Usar background (&)

- Ver el estado: `john -status`
- Restaurar sesiones: `john -restore`

■ No quitar tiempo de CPU: editar `john.conf` y poner `Iddle=YES`

Hacking Tool: Cain & Abel

■ Herramienta que permite:

- Obtener las passwords de una SAM local o remota
- Obtener cualquier contraseña almacenada (IEexplorer, Outlook, MSN, ...)
- Sniffer de contraseñas.
 - En redes conmutadas utiliza un envenenamiento de la caché ARP y un ataque man-in-the-middle.
- Herramienta de hacking para redes wireless.
- [Ejercicio de uso de Cain & Abel](#)

Hacking tools: cracking offline

- Como hemos visto ya, la SAM en Windows NT/2000 contiene los usuarios del sistema y sus contraseñas cifradas. La SAM se encuentra en %systemroot%\system32\config
- Password offline reset: se trata de arrancar con un linux en un disquete (o CD) y eliminar la password de administrador.
- Este fichero está bloqueado cuando el SO está arrancado.
- Así que debemos hacer lo siguiente...

Hacking tools: cracking offline

- Se necesita acceso físico y arranque desde el CD (o disquete)
- O extraer la SAM (los hashes) y usar por ejemplo Lophtrcrack (que veremos después) para obtener las contraseñas.