



Universidad
Francisco de Vitoria
UFV Madrid

Contraseñas

1



Universidad
Francisco de Vitoria
UFV Madrid

Contraseñas

Craquear contraseñas

2



Contraseñas

Craquear contraseñas



Contraseñas

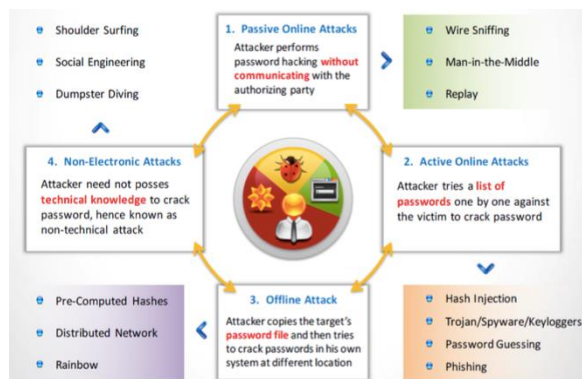
AUDITAR contraseñas

Indice

- Proceso general de obtención de contraseñas
- Tipos de ataques
- Ejemplo práctico

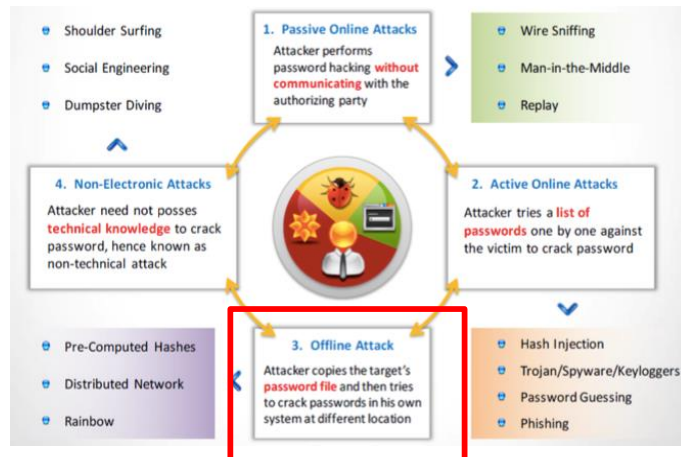
5

Tipos de ataques



6

Tipos de ataques



7

Offline attack

- **Ataque offline** – debo hacerme con el fichero donde se almacenan las contraseñas
- Y luego en casa con tiempo ya intento descifrarla
- El problema: normalmente las contraseñas se almacenan en el disco duro del equipo cifradas

8

Offline attack

- ¿Cómo se llama la contraseña cifrada?
- Hash

9

HASH

- ¿Y qué es un hash?

```
lqarwed -> 4259cc34599c530b28a6a8f225d668590  
hh021da -> c744b1716cbf8d4dd0ff4ce31a177151  
9da8dasf -> 3cd696a8571a843cda453a229d741843  
sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

10

HASH

- Básicamente es el resultado de aplicar una función matemática a una contraseña
- Pero es una función unívoca (one-way hash)
- Es decir, dado el hash obtenido aplicando una función f , no hay una función inversa f^{-1} que devuelva la contraseña original a partir del hash

11

HASH

- Los hashes se crean cuando yo hago login (logon en Windows)
- Se usa un algoritmo de cifrado, se aplica y se crea el hash

12

Autenticación en Windows y en Linux

- Vamos a ver:
- Contraseñas y proceso de autenticación en Windows
 - LM
 - NTLM
 - Kerberos
- Herramientas para craquear contraseñas

13

Autenticación en Windows y en Linux

- Conceptos previos:
- Grupo de trabajo vs dominio
- Cuentas locales vs cuentas de dominio

14

Autenticación en Linux

- Cuentas locales
- ¿Dónde está la SAM en Linux?
 - /etc/passwd
 - /etc/shadow

15

Autenticación en Windows

- ¿Y las cuentas locales en Windows?
- En System32 → SAM y system

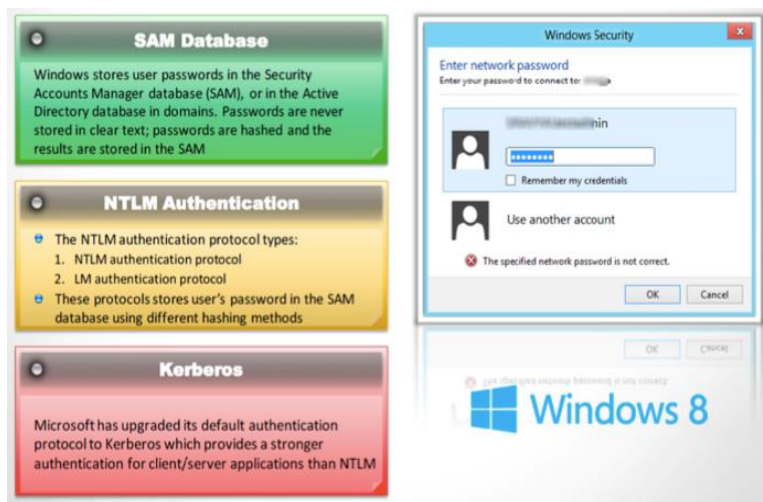
16

Autenticación en Windows

- Hay tres métodos de autenticación en sistemas Windows
 - LAN Manager
 - NTLM – a partir de Windows XP
 - Kerberos – a partir de Windows 2000 trabajando en un dominio
- Kerberos es el método más difícil de crackear

17

Contraseñas en Windows



18

Contraseñas en Windows

Diagram illustrating password hashing in Windows:

1. User (Martin/magician) logs in.

2. Password hash using LM/NTLM:

- Martin: 1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::

3. SAM File is located at: c:\windows\system32\config\SAM

4. SAM File contents (User name, User ID, LM Hash, NTLM Hash):

User name	User ID	LM Hash	NTLM Hash
Administrator	500	598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::	
Guest	501	NO PASSWORD	
HelpAssistant	1000	B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::	
SUPPORT_388945a0	1002	NO	
PASSWORD		F5C1D381495948F434C42AEE04DE990C:::	
Hackers	1003	37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::	
Admin	1004	NO	
Martin	1005	624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::	
John	1006	624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::	
Jason	1007	624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::	
Smith	1008	624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::	

5. Legend:

- User name
- User ID
- LM Hash
- NTLM Hash

6. Note: "LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems."

19

LAN Manager Hash (LM)

- Hasta Windows Vista, se seguían almacenando los hashes creados con el protocolo de autenticación LAN Manager (LM)
- 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

20

¿Qué es un hash LanManager (LM)?

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_'

21

¿Qué es un hash LanManager (LM)?

- 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 ens concatenado:
'123456Q' = 6BF11E04AFAB197F
'WERTY_' = F1E9FFDCC75575B15
- El hash es
6BF11E04AFAB197FF1E9FFDCC75575B15

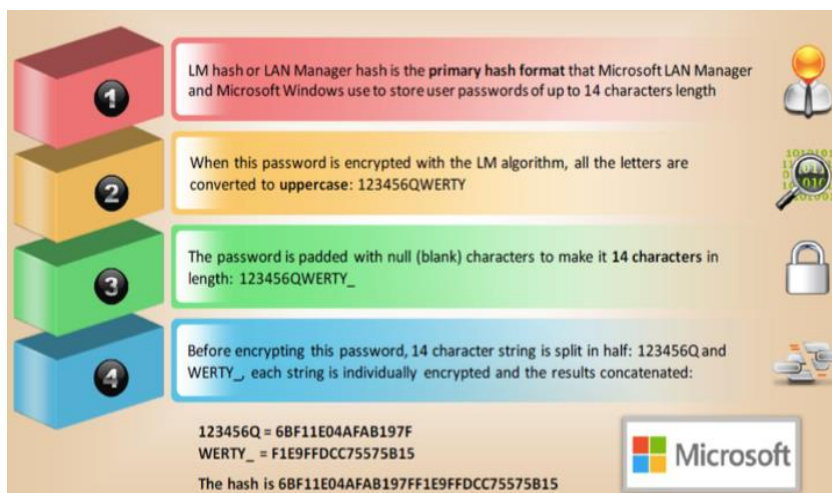
22

¿Qué es un hash LanManager (LM)?

Nota: La primera mitad del hash contiene caracteres alfanuméricos, por lo que nos llevará horas descifrarlo con Lophtrcrack (ya lo veremos), mientras que la segunda apenas un minuto.

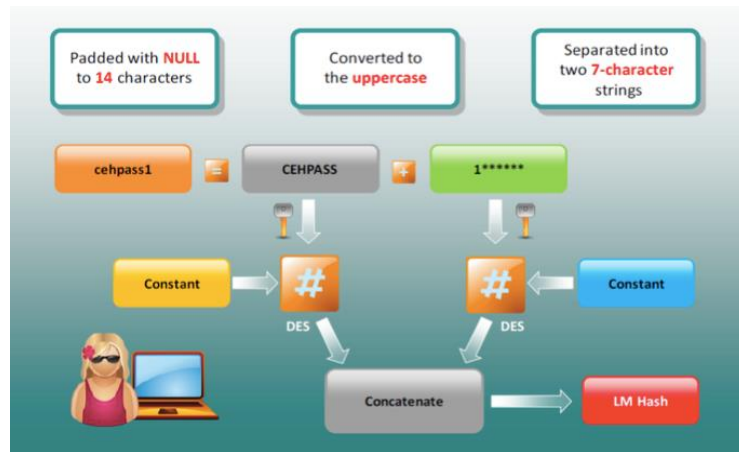
23

LAN Manager Hash (LM)



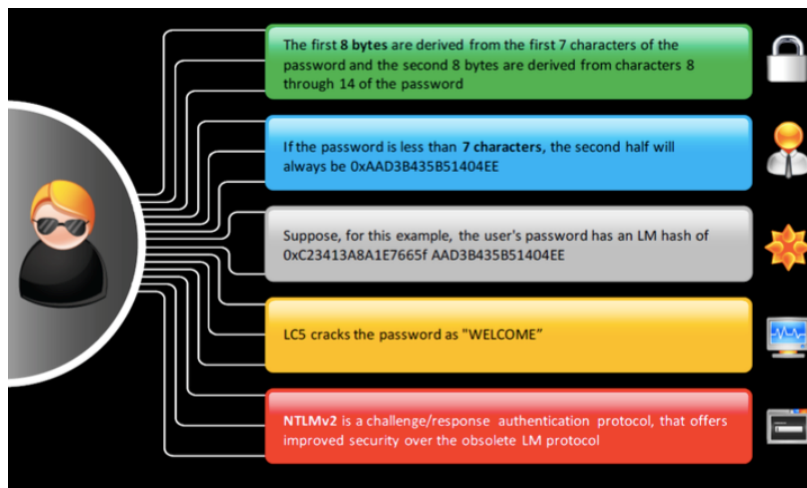
24

¿Qué es un hash LanManager (LM)?



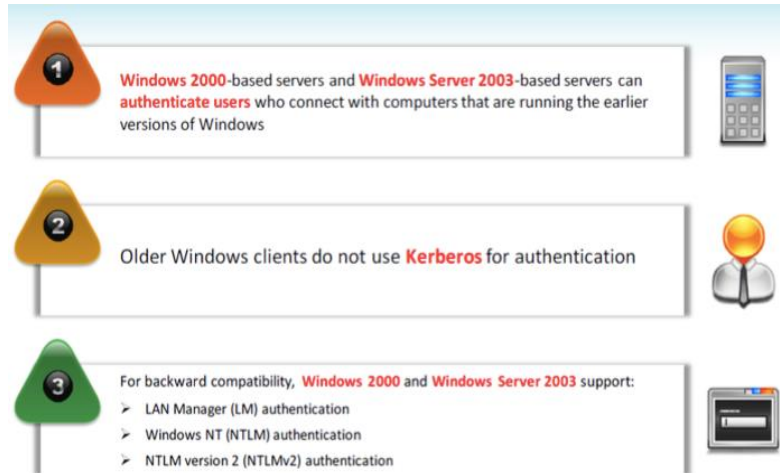
25

¿Qué es un hash LanManager (LM)?



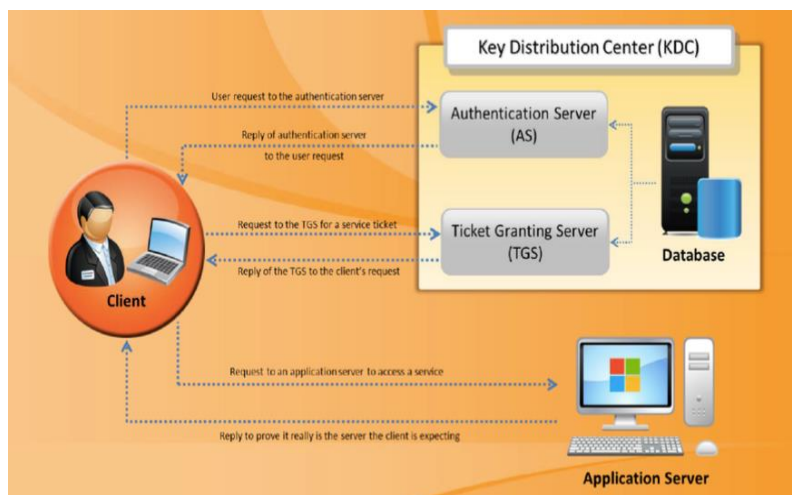
26

Compatibilidad clientes antiguos



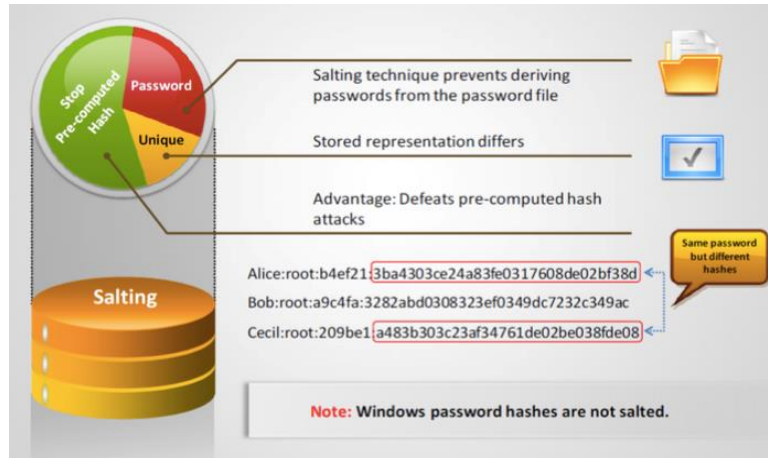
27

Kerberos



31

Salting



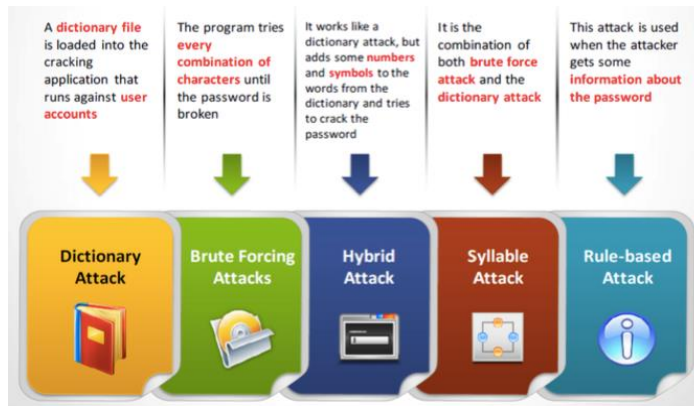
32

Ataques a contraseñas (offline)

- Hay cinco tipos de ataques
- Ataque por diccionario
- Ataque por fuerza bruta
- Ataque híbrido
- Syllable attack
- Ataque basado en reglas (rule-based attack)

33

Cracking passwords



34

Cracking passwords

- **Ataque por diccionario** – Existen en Internet diccionarios con millones de contraseñas conocidas o usadas
- <https://wiki.skullsecurity.org/Passwords>
- <http://www.openwall.com/passwords/wordlists/>

35

Cracking passwords

- **Ataque por fuerza bruta** – Se intenta la adivinación de la contraseña, carácter a carácter.
- Puede llevar muchísimo tiempo, dependiendo del algoritmo de cifrado.

36

Cracking passwords

- **Ataque híbrido** – Se usan variaciones del diccionario.
- Por ejemplo, si en el diccionario está la posible contraseña system, se prueba también con system1, system2,...

37

Cracking passwords

- **Syllable attack** – Combinación de ataque por diccionario y fuerza bruta.
- Por ejemplo, usando la combinación de todas las palabras presentes en el diccionario, o con partes de ellas (sílabas)

38

Cracking passwords

- **Ataque basado en reglas** – conocemos cierta información de la contraseña
- Por ejemplo, es más fácil si sabemos que la contraseña tiene 2 o 3 números
- O si sabemos la longitud de la contraseña

39

Offline attack: Rainbow attacks

- Estas técnicas necesitan de mucho tiempo de procesador
- ¿Qué puedo hacer para minimizar esto?
- La respuesta en el siguiente ataque

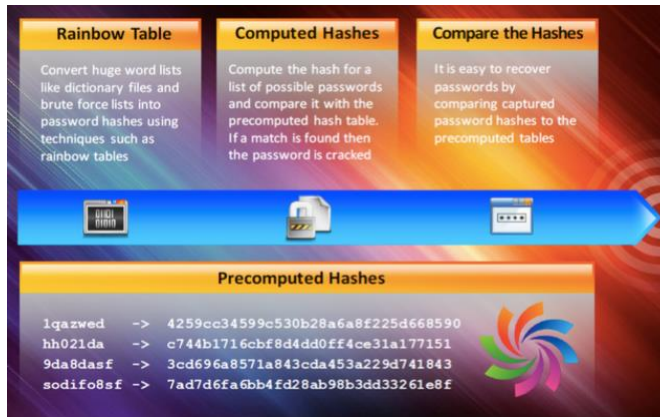
40

Offline attack: Rainbow attacks

- La idea es crear los hashes de un montón de contraseñas según un algoritmo concreto de cifrado (**precomputed hashes**) y las comparo con el que tengo

41

Offline attack: Rainbow attacks



42

La búsqueda: rainbow table

- Una **tabla rainbow** es una tabla y un algoritmo de búsqueda que permite recuperar una contraseña a partir de su hash (contraseña cifrada)

43

Rainbow table

- ¿Cómo me creo una rainbow table?
- Hay programas para ello: rtgen (www.project-rainbowcrack.com) o Winrtgen (www.oxid.it)

44

Matching: comparar y encontrar

- Comparo el hash capturado y el creado por mí mismo, y si coinciden, ya lo tengo ☺



45

SAM

- Pero claro, para ello debo hacerme con el fichero donde están almacenadas las contraseñas
- Porque recordemos que esto es un craqueo offline
- Lo veremos en la segunda parte

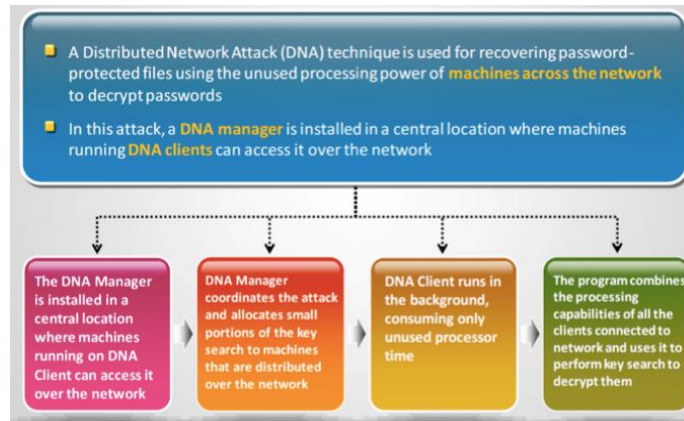
46

Distributed network attack (DNA)

- La herramienta: Elcomsoft Distributed Password Recovery (www.elcomsoft.com)

47

Distributed network attack (DNA)



48

Distributed network attack (DNA)

The screenshot shows the Elicomsoft Distributed Password Recovery software interface. It features a main window with a file explorer on the left, a central pane showing a list of files and folders with columns for Name, Progress, Remaining Time, Expected Time, Current Speed, Average Speed, and Status. Below this, there are sections for 'Backup' and 'Recovery' with various options and checkboxes. A smaller window in the bottom right corner shows a detailed view of the recovery process, including a progress bar and a list of recovered files. The URL <http://www.elicomsoft.com> is visible in the bottom right corner of the interface.

Features:

- Distributed password recovery over LAN, Internet, or both
- Plug-in architecture allows for additional file formats
- Schedule support for flexible load balancing
- Install and remove password recovery clients remotely
- Encrypted network communications

Elicomsoft Distributed Password Recovery breaks complex passwords, recovers strong encryption keys, and unlocks documents in a production environment

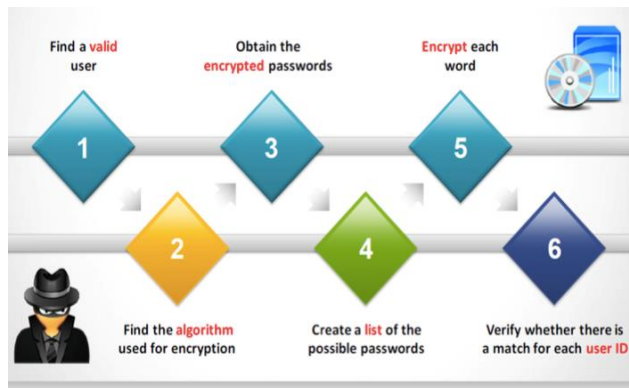
49

Distributed network attack (DNA)

- Esto suena a troyano, ¿verdad?

50

En resumen



51

Otros métodos

52

Contraseñas por defecto

- Hay passwords que utilizan los fabricantes por defecto (el famoso admin/admin de telefónica)
- Y hay bases de datos con estas contraseñas conocidas, y herramientas online para buscar en ellas

53

Contraseñas por defecto

- A default password is a password supplied by the **manufacturer** with new equipment that is password protected



Online tools to search default passwords:

- <http://cirt.net>
- <http://default-password.info>
- <http://www.defaultpassword.us>
- <http://www.passwordsdatabase.com>
- <https://w3dt.net>
- <http://www.virus.org>
- <http://open-sez.me>
- <http://securityoverride.org>
- <http://www.routerpasswords.com>
- <http://www.fortypoundhead.com>

The table displays a list of all default passwords.

Vendor/Model	Model/Type	Model	Version	Username	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Debug	Synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Tech	Tech
3COM	HiPerARC	v4.1.x	Telnet	Adm	(none)
3COM	LANplex	2500	Telnet	Debug	Synnet
3COM	LANplex	2500	Telnet	Tech	Tech
3COM	LinkSwitch	2000/2700	Telnet	Tech	Tech
Huawei	E960			Admin	Admin
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	Admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	Synnet
3COM	SuperStack II Switch	2700	Telnet	tech	Tech
3COM	OfficeConnect 812 ADSL		Multi	adminnttd	adminnttd

<http://securityoverride.org>

54


Contraseñas por defecto

Vendor	Model	Version	Access Type	User-name	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Debug	Synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Tech	Tech
3COM	HiPerARC	v4.1.x	Telnet	Adm	(none)
3COM	LANplex	2500	Telnet	Debug	Synnet
3COM	LANplex	2500	Telnet	Tech	Tech
3COM	LinkSwitch	2000/2700	Telnet	Tech	Tech
Huawei	E960			Admin	Admin
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	Admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	Synnet
3COM	SuperStack II Switch	2700	Telnet	tech	Tech
3COM	OfficeConnect 812 ADSL		Multi	adminnttd	adminnttd


TABLE 5.1: Online Tools To Search Default Password


55

Troyanos, spyware y keyloggers





1 Spyware is a type of malware that allows attackers to **secretly** gather information about a person or organization






2 With the help of a Trojan, an attacker gets access to the **stored passwords** in the attacked computer and is able to read personal documents, delete files, and display pictures





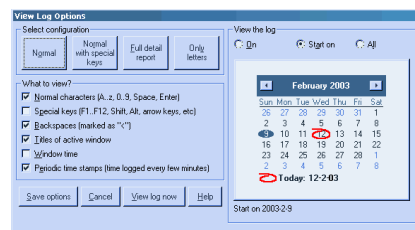
3 A Keylogger is a program that runs in the background and allows remote attackers to **record every keystroke**



56

Keystroke Loggers

- Si todos los intentos anteriores fallan, entonces un *keystroke logger* es la solución.
- Keyloggers son programas que registran cada pulsación de teclas en el teclado.
- Hay dos tipos:
 - 1. Basados en Software
 - 2. Basados en Hardware



57

Hacking Tool: Hardware Key Logger (www.keyghost.com)

- Un Key Logger por hardware se debe conectar entre el teclado y el equipo.



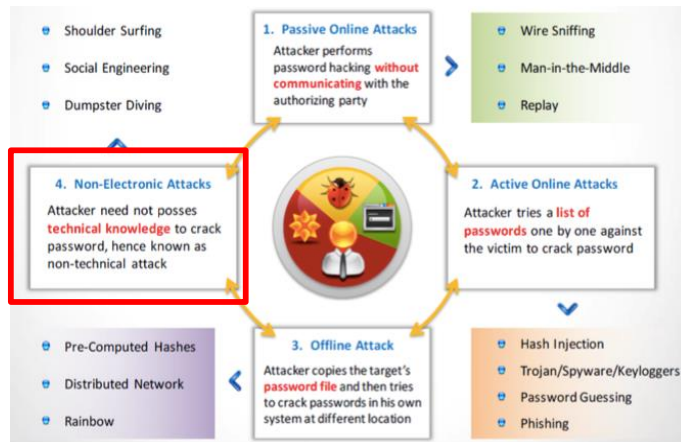
58

Otros ataques

- Pero resulta que al final lo más fácil es usar la ingeniería social

59

Tipos de ataques



60

Non-electronic attacks: ingeniería social



61

Herramientas

62

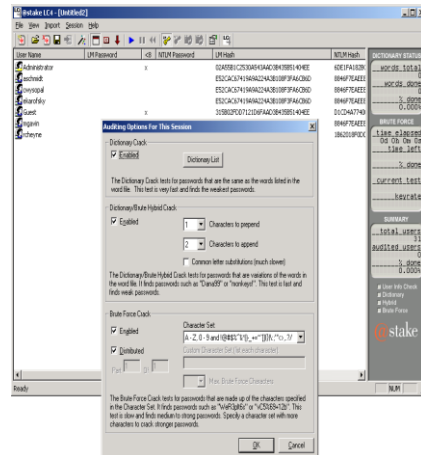
Herramientas

- Ranking en nmap: password audit
<http://sectools.org/tag/pass-audit/>
- Ver también:
- <http://www.openwall.com/>

63

Hacking Tool: Lophtrcrack

- LC6 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.



64

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
```

65

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`

66

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`

67

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`

68

Hacking Tool: John the Ripper

■ Consejos:

■ Sólo craquear ciertas cuentas:

- La de root: `john --wordlist=all.lst --rules --users=o *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`

69

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.

70

Hacking Tool: Cain & Abel

■ Ejercicio de uso de Cain & Abel




71

Otras herramientas

 Password Unlocker Bundle http://www.passwordunlocker.com	 Passware Kit Enterprise http://www.top-password.com
 Proactive System Password Recovery http://www.ekomsoft.com	 PasswordsPro http://www.insidepro.com
 John the Ripper http://www.openwall.com	 LSASecretsView http://www.nirsoft.net
 Windows Password Cracker http://www.windows-password-cracker.com	 LCP http://www.kpssoft.com
 WinPassword http://lastbit.com	 Password Cracker http://www.amlpages.com

72

Otras herramientas

 Kon-Boot http://www.thelead82.com	 Password Recovery Bundle http://www.top-password.com
 Windows Password Recovery Tool http://www.windowspasswordsrecovery.com	 krbpguess http://www.cqire.net
 Hash Suite http://hashsuite.openwall.net	 THC Hydra http://www.thc.org
 SAMInside http://www.insidepro.com	 Windows Password Breaker Enterprise http://www.recoverwindowspassword.com
 Windows Password Recovery http://www.passcape.com	 Rekeysoft Windows Password Recovery Enterprise http://www.rekeysoft.com

73