

Practica 2 – Obtener la contraseña de Windows de un usuario de nuestra red local.

Teoría:

El equipo atacante coloca un Sniffer a la escucha, de forma que es capaz de capturar todo el tráfico que pasa por su tarjeta de red. Cuando un usuario víctima inicia sesión en el equipo atacante para acceder a sus recursos compartidos, el Sniffer captura el hash desafío-respuesta intercambiado y después de crackearlo por fuerza bruta, se obtiene la contraseña de Windows del usuario víctima que inició sesión en el equipo atacante.

Breve explicación del proceso de Autenticación de Windows en red:

Windows 2000 y XP utilizan de forma predeterminada un mecanismo de autenticación basado en desafío / respuesta para validar. De este modo, ni la contraseña ni el hash aplicado viajan por el cable. El proceso ocurre así:

- El cliente (víctima) solicita el inicio de sesión en el servidor (atacante).
- El servidor emite un desafío al cliente.
- El cliente cifra el desafío con el hash de la contraseña de usuario y la reenvía al servidor.
- El servidor compara la respuesta (desafío hasheado) con el propio hash del desafío y entonces permite o deniega el inicio de sesión.

¿Cómo se obtiene el hash?

Se ha dicho que el verdadero hash y la contraseña no viajan por el cable de conexión, pero sí la respuesta hasheada al desafío. El algoritmo de hash lo divide en dos grupos de 8 Bytes. Los primeros 8 Bytes guardan los 7 primeros caracteres de la contraseña hasheada y los segundos 8 Bytes guardan los caracteres nº 8 y sucesivos.

Una vez obtenidos los hashes, bastará con probar por fuerza bruta todas las combinaciones posibles para cada grupo de Bytes e ir aplicando la función hash hasta encontrar una que coincida con el resultado. Entonces ya tendremos el hash verdadero.

Aplicación práctica:

Sniffado

Escenario:

Atacante: 10.10.0.69

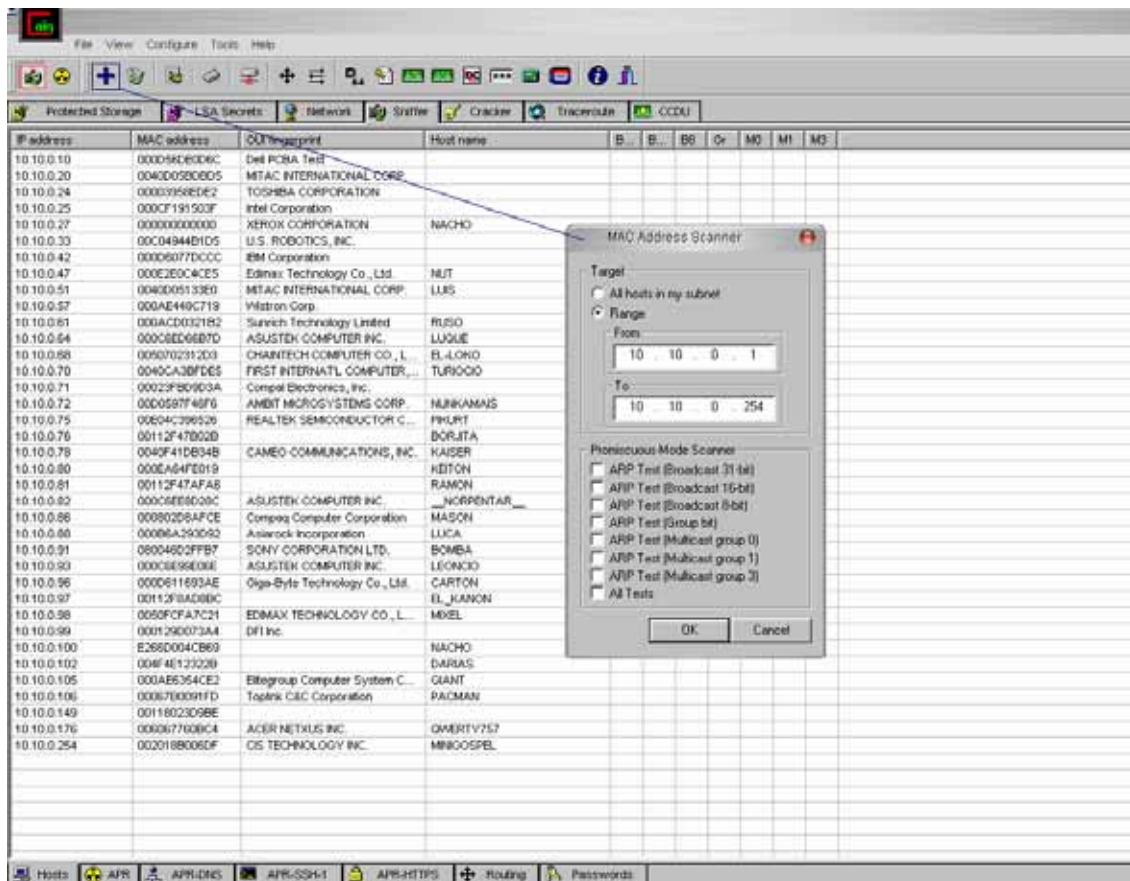
Víctimas: Todos los posibles equipos de la red local que inicien sesión en el equipo atacante.

Herramientas:

Vamos a utilizar el sniffer Caín @ <http://www.oxid.it/>

Procedimiento:

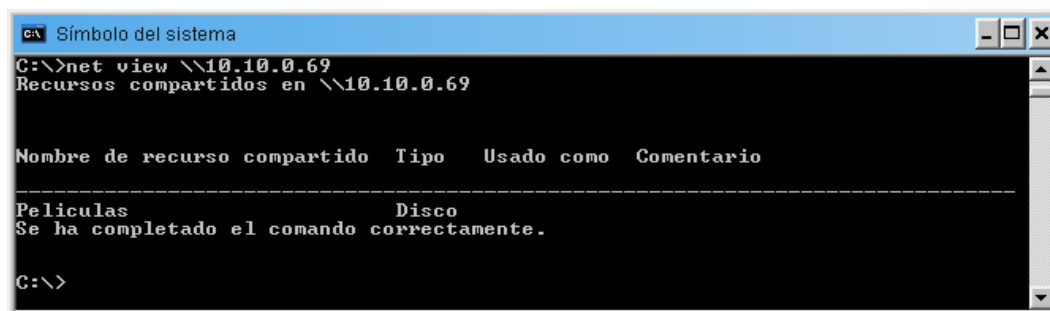
1. Instalar, configurar y poner en funcionamiento el Sniffer Caín en el equipo atacante. Lo siguiente es scannear la red en busca de Hosts. Nos vamos a la pestaña *Sniffer*, subpestaña *Hosts*:



Según la imagen, pulsando el botón **+** recuadrado con marco azul, podremos scannear todo el rango de IPs de nuestra red local para descubrir a los Hosts conectados a la misma. Para mayor comodidad, Caín también permite resolver los nombres de equipos (Hostnames)

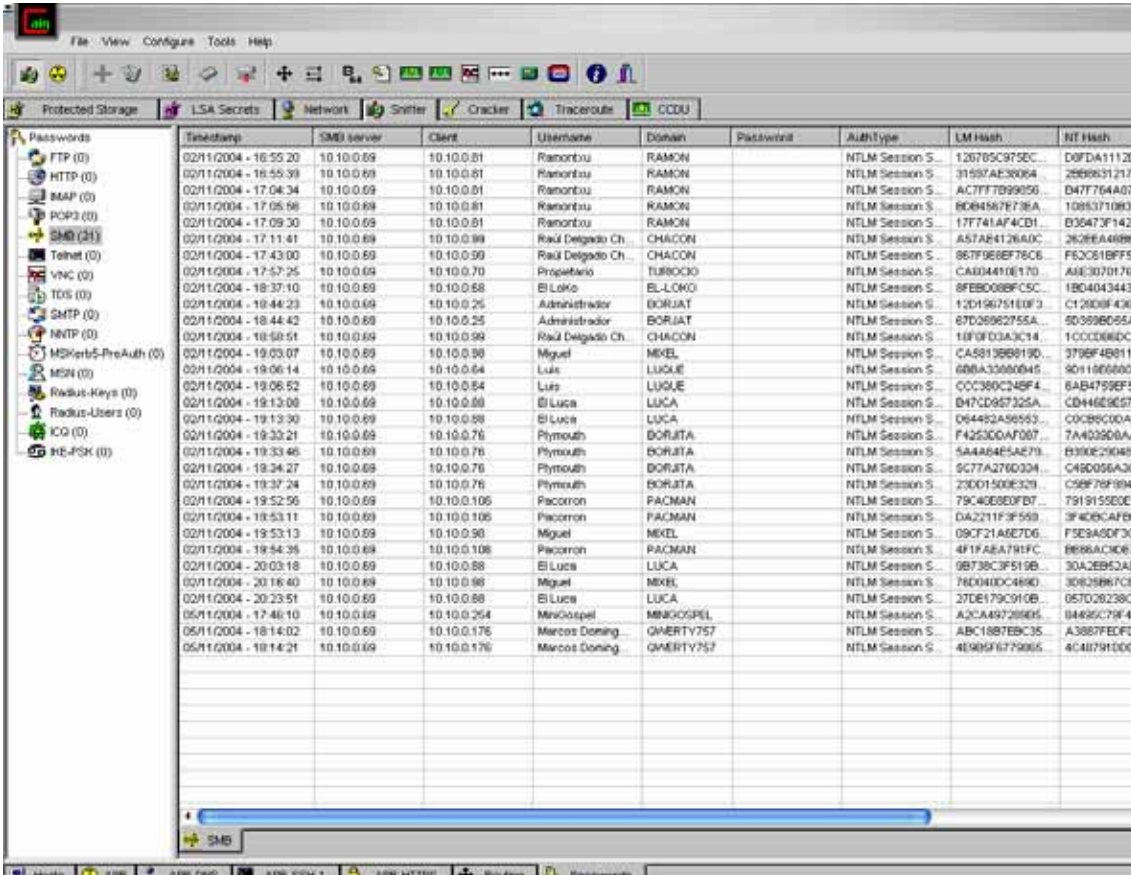
Ahora ya podemos comenzar a Sniffar, pulsando el botón recuadrado en rojo.

2. Lo siguiente es atraer a estas víctimas potenciales. Para ello, nada mejor que ofrecerles una carpeta compartida con un nombre sugerente: “Películas”. Lo dicho, compartimos en red una carpeta llamada “Películas”.



3. Al cabo de un rato, ciertos usuarios de la red local accederán a Mis Sitios de Red desde sus respectivos equipos y encontrarán que el equipo atacante comparte una carpeta llamada “Películas”. Atraídos por la curiosidad, intentarán acceder a esta carpeta para ver su contenido. Es en este momento cuando nuestro Sniffer Caín entra en acción!

4. Uno por uno, todos esos usuarios que iniciaron sesión en el equipo atacante para acceder al recurso compartido serán logueados en la pestaña *Sniffer*, subpestaña *Passwords*, Protocolo *SMB*:



Protocol	Timestamp	SMB server	Client	Username	Domain	Password	AuthType	LM Hash	NT Hash
FTP (0)	02/11/2004 - 16:55:20	10.10.0.69	10.10.0.81	RamonXu	RAMON		NtLm Session S:	126795C975EC	D9FDA1112D
HTTP (0)	02/11/2004 - 16:55:39	10.10.0.69	10.10.0.81	RamonXu	RAMON		NtLm Session S:	31597AE39004	266993121F
IMAP (0)	02/11/2004 - 17:04:34	10.10.0.69	10.10.0.81	RamonXu	RAMON		NtLm Session S:	AC7777D99050	D47776A074
POP3 (0)	02/11/2004 - 17:05:56	10.10.0.69	10.10.0.81	RamonXu	RAMON		NtLm Session S:	96945676736A	108937109C
SMB (21)	02/11/2004 - 17:09:30	10.10.0.69	10.10.0.81	RamonXu	RAMON		NtLm Session S:	177741AF4CD1	D36473F142D
Telex (0)	02/11/2004 - 17:11:41	10.10.0.69	10.10.0.89	Raul Delgado Ch.	CHALCON		NtLm Session S:	A57A8126A0C1	2626EA489B1
VNC (0)	02/11/2004 - 17:43:00	10.10.0.69	10.10.0.99	Raul Delgado Ch.	CHALCON		NtLm Session S:	867F9E8F76C6	F52C518FF5E
MSRDP (0)	02/11/2004 - 17:57:25	10.10.0.69	10.10.0.70	Proprietario	TURCOJO		NtLm Session S:	C4004410E170	A6E3070170A
TDS (0)	02/11/2004 - 18:37:10	10.10.0.69	10.10.0.88	El Loko	EL-LOKO		NtLm Session S:	8FEB0D8FC5C	18C4043443C
SMTP (0)	02/11/2004 - 18:44:23	10.10.0.69	10.10.0.25	Administrador	BORJAT		NtLm Session S:	12D196751E0F3	C12008F436F
NNTP (0)	02/11/2004 - 18:44:42	10.10.0.69	10.10.0.25	Administrador	BORJAT		NtLm Session S:	67D26862755A	5D3596D55A2
MSKerB5-PreAuth (0)	02/11/2004 - 18:58:51	10.10.0.69	10.10.0.99	Raul Delgado Ch.	CHALCON		NtLm Session S:	18F0F03A3C14	1CCDD86DC7
MSN (0)	02/11/2004 - 19:03:07	10.10.0.69	10.10.0.90	Miguel	MXEL		NtLm Session S:	CA58136B819D	3796F48811F
Radius-Keys (0)	02/11/2004 - 19:06:14	10.10.0.69	10.10.0.64	Luca	LUQUE		NtLm Session S:	688A33880945	8011806000F
Radius-Users (0)	02/11/2004 - 19:06:52	10.10.0.69	10.10.0.84	Luca	LUQUE		NtLm Session S:	C0C380C248F4	6AB47598F52
ICQ (0)	02/11/2004 - 19:13:06	10.10.0.69	10.10.0.88	El Luca	LUCA		NtLm Session S:	B47CD667325A	CD446E8E571
HE-P2K (0)	02/11/2004 - 19:13:30	10.10.0.69	10.10.0.88	El Luca	LUCA		NtLm Session S:	D64482A56553	C0CB9C00A4
	02/11/2004 - 19:33:21	10.10.0.69	10.10.0.76	Plymouth	BORJATA		NtLm Session S:	F425300AF007	7A038D0AA
	02/11/2004 - 19:33:46	10.10.0.69	10.10.0.76	Plymouth	BORJATA		NtLm Session S:	5A4484E5AE79	E930E290491
	02/11/2004 - 19:34:27	10.10.0.69	10.10.0.76	Plymouth	BORJATA		NtLm Session S:	5C77A2760304	C48D056A383
	02/11/2004 - 19:37:24	10.10.0.69	10.10.0.76	Plymouth	BORJATA		NtLm Session S:	23D01500E320	C58F78F8942
	02/11/2004 - 19:52:56	10.10.0.69	10.10.0.106	Pacorrion	PACMAN		NtLm Session S:	79C40E8E3FB7	7919155E0E1
	02/11/2004 - 19:53:11	10.10.0.69	10.10.0.106	Pacorrion	PACMAN		NtLm Session S:	DA2211F3F599	3F409CAF808
	02/11/2004 - 19:53:13	10.10.0.69	10.10.0.90	Miguel	MXEL		NtLm Session S:	09CF21A6E7D6	F5E9A8DF3C3
	02/11/2004 - 19:54:35	10.10.0.69	10.10.0.106	Pacorrion	PACMAN		NtLm Session S:	4F1FAEA791FC	8E86AC0E71
	02/11/2004 - 20:03:18	10.10.0.69	10.10.0.88	El Luca	LUCA		NtLm Session S:	9B738C3F519B	30A2EB52AE1
	02/11/2004 - 20:16:40	10.10.0.69	10.10.0.98	Miguel	MXEL		NtLm Session S:	76D040DC4880	30E29867C8E
	02/11/2004 - 20:23:51	10.10.0.69	10.10.0.88	El Luca	LUCA		NtLm Session S:	27DE179C910B	057D082380C
	06/11/2004 - 17:46:10	10.10.0.69	10.10.0.254	Mnigospel	MNIGOSPIL		NtLm Session S:	A2CA48728865	04496C79F44
	06/11/2004 - 18:14:02	10.10.0.69	10.10.0.176	Mircos Doming	QWERTY757		NtLm Session S:	ABC1887EBC35	A3887EBCD0D
	06/11/2004 - 18:14:21	10.10.0.69	10.10.0.176	Mircos Doming	QWERTY757		NtLm Session S:	4E905F675905	4C41791D0D5

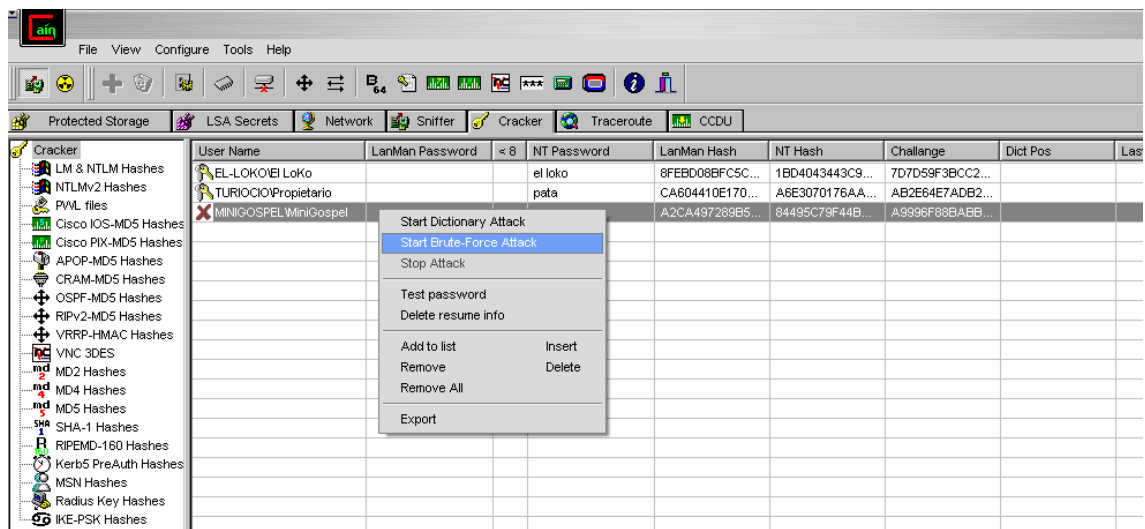
El Log del Sniffer guardará el TimeStamp, Servidor Local SMB (atacante), Cliente Origen (víctima), Nombre del Usuario víctima, el Tipo de Autenticación utilizado durante el inicio de sesión, el Hash LM, el Hash NT, etc.

Podéis comprobar que el campo Password aparece en blanco, ohh!!! Pero es que no iba a ser tan fácil...

5. Para obtener la contraseña tenemos que crackear los hashes obtenidos. Nada más fácil que utilizar para ello el propio Crackeador que incorpora Caín. Así pues, elegimos el usuario víctima cuyo hash queremos crackear y lo enviamos al Crackeador:

Time	Source IP	Destination IP	Source User	Source Hash	Action	Destination Hash	Destination User
05/11/2004 - 17:46:10	10.10.0.69	10.10.0.254	MiniGospel	MINIGOSPEL	Send to Cracker	A2CA497289B5...	84495C79F...
05/11/2004 - 18:14:02	10.10.0.69	10.10.0.176	Marcos Doming...	QWERTY757	Send All to Cracker	ABC18B7EBC35...	A3887FEDI...
05/11/2004 - 18:14:21	10.10.0.69	10.10.0.176	Marcos Doming...	QWERTY757		4E9B5F6779865...	4C48791DI...
05/11/2004 - 18:41:27	10.10.0.69	10.10.0.97	GuiME	EL_KANON	Remove	C66DCDEFB6FD...	5949BE72E...

En la pestaña *Cracker*, encontraremos aquellos usuarios cuyos hashes vamos a proceder a crackear. Podemos crackear estos hashes a través de Ataque por Diccionario o bien por Fuerza Bruta.



Después de un tiempo indefinido, el Crackeador habrá encontrado la cadena de caracteres tal que, al utilizarla como clave de cifrado para el desafío conocido y comparando el resultado con el hash cifrado por el cliente víctima, da éxito. Obtenemos, pues, el password del usuario víctima:

User Name	LanMan Password	< 8	NT Password	LanMan Hash	NT Hash	Challenge
EL-LOKO\El LoKo			el loko	8FEBD08BFC5C...	1BD4043443C9...	7D7D59F3BCC2...
TURIOCIO\Propietario			pata	CA604410E170...	A6E3070176AA...	AB2E64E7ADB2...
MINIGOSPEL\MiniGospel			xxxxxxx	A2CA497289B5...	84495C79F44B...	A9996F88BABB...

6. ¿Y qué podemos hacer con la contraseña del Usuario víctima? Muchos de vosotros ya os estaréis frotando las manos pensando en la cantidad de maldades que podéis llevar a cabo conociendo la contraseña de un usuario víctima de vuestra red local. Menos mal que estoy yo aquí para decepcionaros y deciros que con esta contraseña podréis hacer más bien poco... Hey, ¿pero y si la contraseña es de un usuario con privilegios de Administrador? Pues lo mismo, más bien poco...

Si la víctima utiliza:

- Windows 2000 con privilegios de Administrador
- Windows XP con privilegios de Administrador y, además, este Windows XP pertenece a un dominio.

a) Conectar como unidad de red local sus particiones lógicas que todos los Windows basados en tecnología NT comparten de manera administrativa. Es decir, podéis conectaros a su C\$, D\$... de forma remota, con privilegios de Administrador: leer, escribir, mover, etc.

El comando para agregar como unidad de red local una unidad remota compartida es el siguiente:

```
C:\>net use x: \\10.10.0.254\C$ xxxxxxxx /user:MINIGOSPEL\Minigospel
```

b) Conseguir una shell remota con la utilidad **PSEXEC**.

Para más información, consultar el excelente artículo de Vic_Thor:

¿Queréis una Shell? pues TOMAD UNA SHELL

@ <http://www.hackxcrack.com/phpBB2/viewtopic.php?t=5026>

c) Conseguir un control gráfico con la utilidad **ATELIER WEB REMOTE COMMANDER**.

Para más información, consultar el excelente artículo de Vic_Thor:

¿Queréis Control Remoto? Pues Tomad CONTROL REMOTO

@ <http://www.hackxcrack.com/phpBB2/viewtopic.php?t=6250>

Si la víctima utiliza:

- Windows XP sin pertenecer a un dominio.

No podréis conseguir nada. Ya que Windows XP no acepta conexiones remotas utilizando cuentas de usuario.

Documentación

La mayor parte del contenido de este escrito está basado en:

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR
Documento creado por Vic_Thor.

@ <http://www.freewebs.com/victor/hxc/FAQ/faq2.pdf>

Gospel @ unrayodesoul[at]hotmail[dot]com