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:

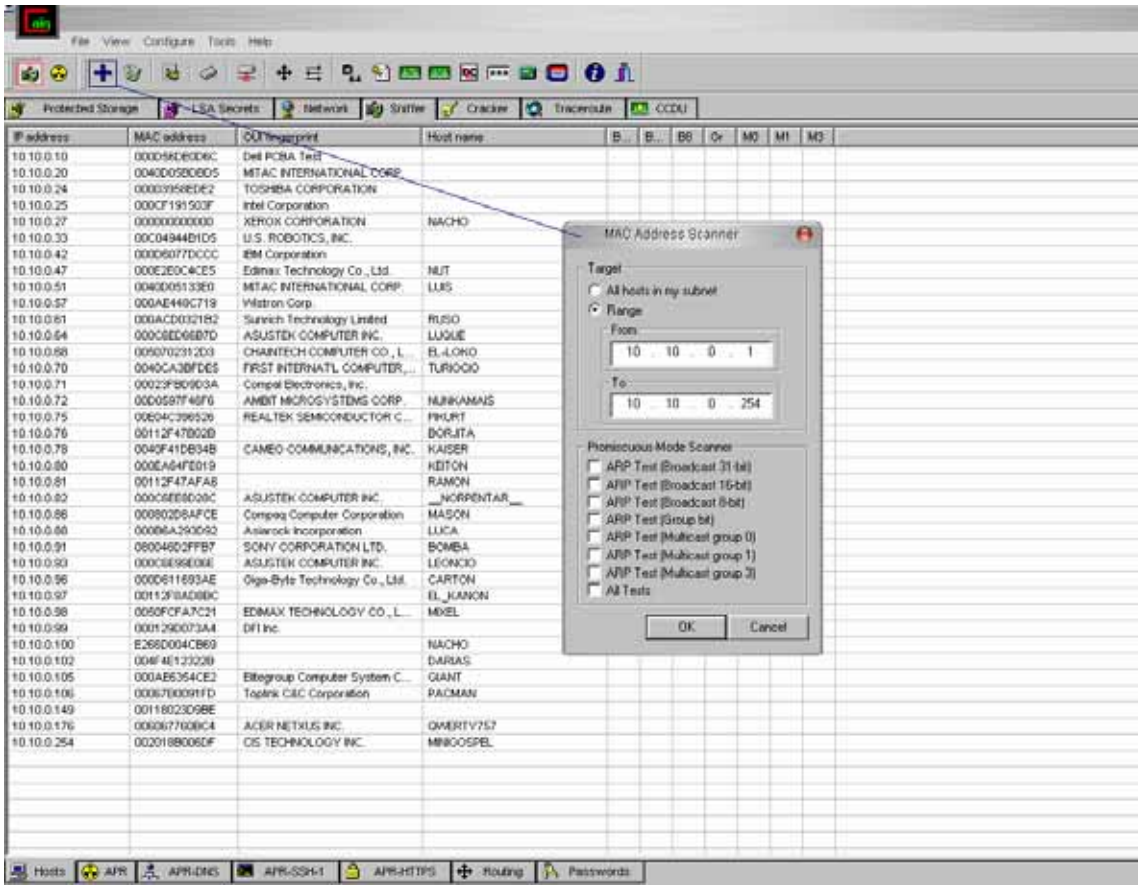
Atacante: 10.10.0.69
Víctimas: Todos los posibles equipos de la red local que inicien sesión en el equipo atacante.

Herramientas:

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

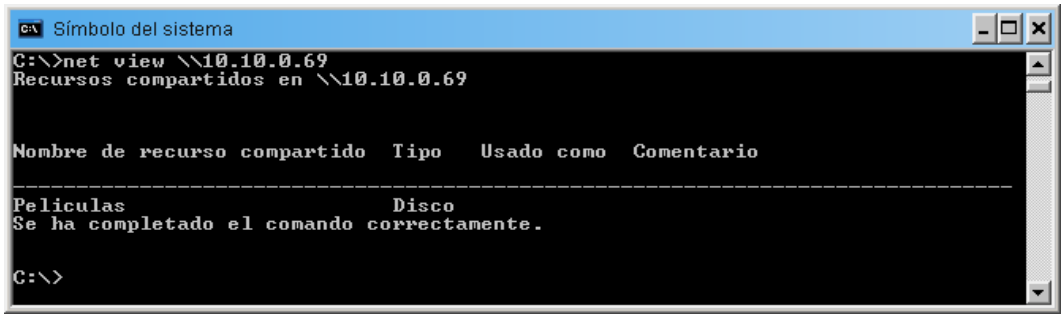
Procedimiento:

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*:



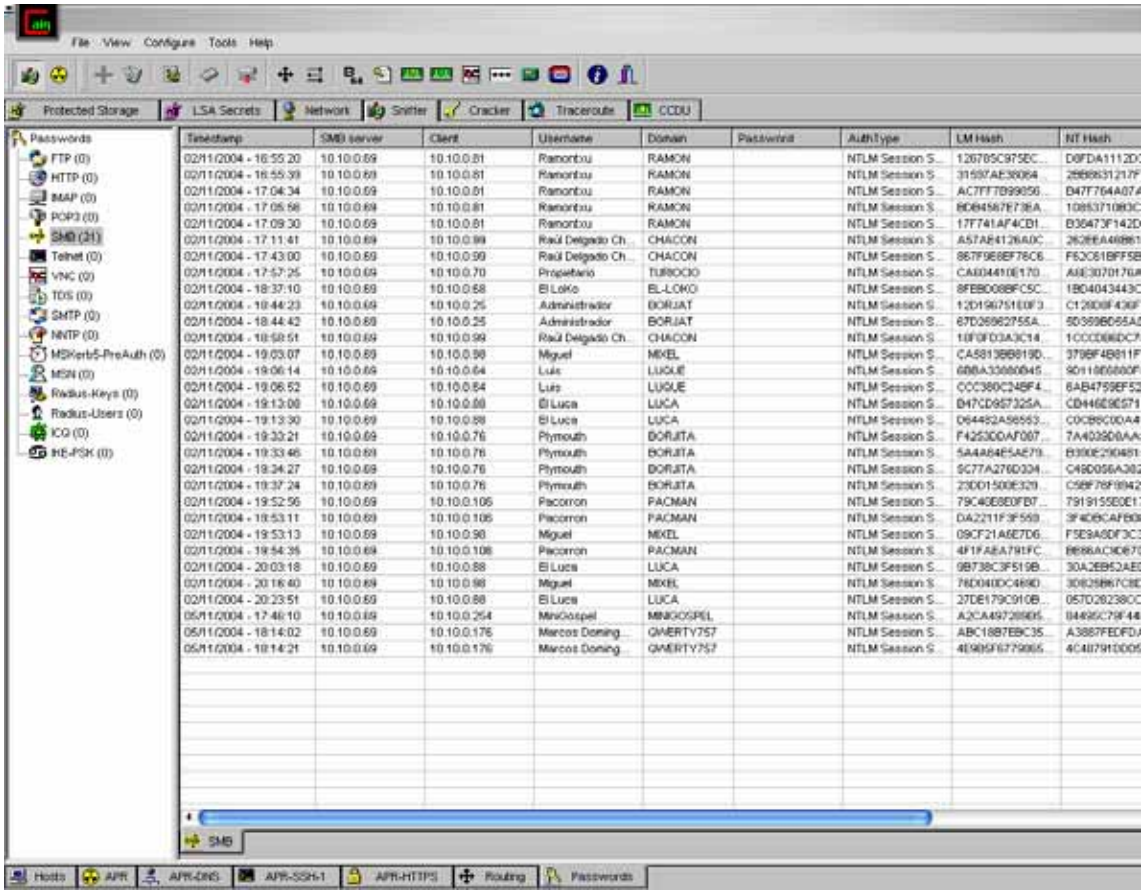
Según la imagen, pulsando el botón + recuadrado con marco azul, podremos scannear todo el rango de IPs de nuestra red local para descubrir a los Hosts conectados a la misma. Para mayor comodidad, Caín también permite resolver los nombres de equipos (Hostnames)
Ahora ya podemos comenzar a Sniffar, pulsando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

2. Lo siguiente es atraer a estas víctimas potenciales. Para ello, nada mejor q 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!

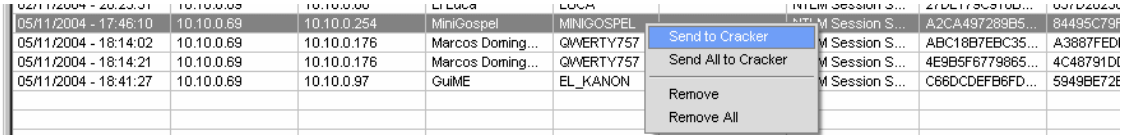
4. Uno por uno, todos esos usuarios que iniciaron sesión en el equipo atacante para acceder al recurso compartido serán logueados en la pestaña *Sniffer*, subpestaña *Passwords*, Protocolo *SMB*:



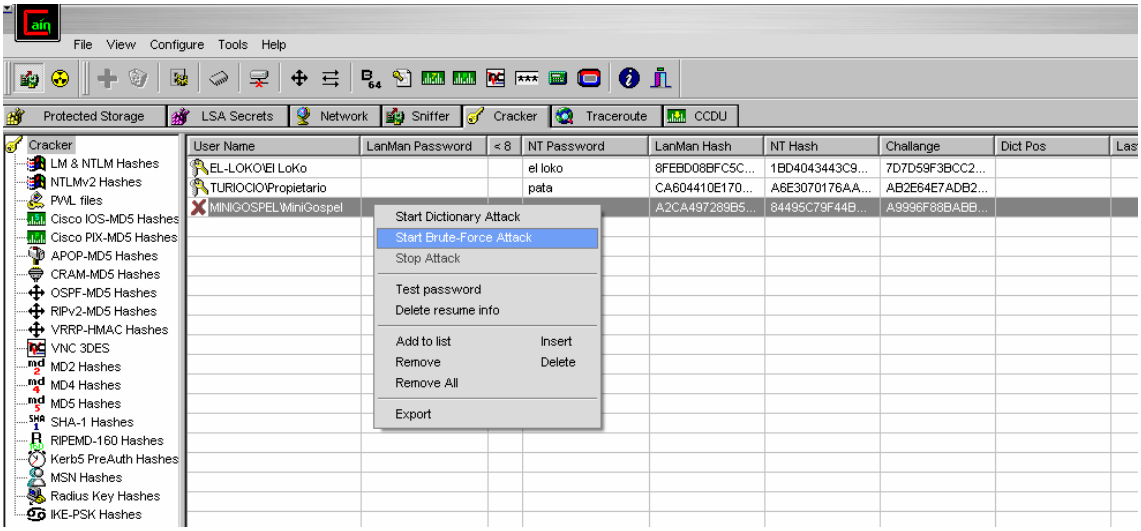
El Log del Sniffer guardará el TimeStamp, Servidor Local SMB (atacante), Cliente Origen (víctima), Nombre del Usuario víctima, el Tipo de Autenticación utilizado durante el inicio de sesión, el Hash LM, el Hash NT, etc.

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:



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	Challange
EL-LOKO\El LoKo			el loko	8FEBD08BFC5C...	1BD4043443C9...	7D7D59F3BCC2...
TURIOCIO\Propietario			pata	CA604410E170...	A6E3070176AA...	AB2E64E7ADB2...
MINIGOSPEL\MiniGospel			xxxxxxxx	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/victhor/hxc/FAQ/faq2.pdf

Gospel @ unrayodesoul[at]hotmail[dot]com