

Alumno: Christian Valdespin Bautista

Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Materia: Servicios de Seguridad en Sistemas Operativos Multiusuario.

Profesor: M. en C. Marcos Arturo Rosales García.

Actividad: Cracking de Contraseñas en offline.

Reporte de Actividades:

1. A través del programa Ophcrack romper las contraseñas de cuentas de usuario y almacenadas en la base de datos de la SAM.
 - Otro programa similar Johntheripper
2. Ver como deshabilitar en Windows XP un hash de administrador de LM y dejar solo el hash de NT.

Introducción:

El sistema operativo Windows no almacena la contraseña de la cuenta de usuario en texto claro, genera dos representaciones de contraseña distinta, denominada normalmente "hash". Estos hash se almacenan en la base de datos del SAM.

Nota: Cuando se establece o cambia la contraseña de una cuenta de usuario por otra que contiene menos de 15 caracteres, Windows genera un hash de LM y un hash de NT de la contraseña.

Diferencias:

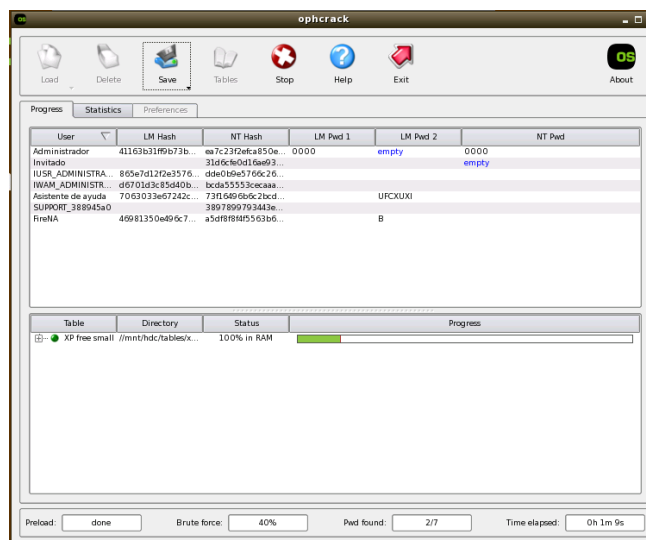
LM

- Manda todos los caracteres a mayúsculas
- La contraseña la divide en 2 partes de 7 caracteres

- A cada cadena de 7 caracteres le aplica hash MD5.
- Solo cifra los 14 caracteres si tiene mas no los cifra los guarda en claro
-

NT

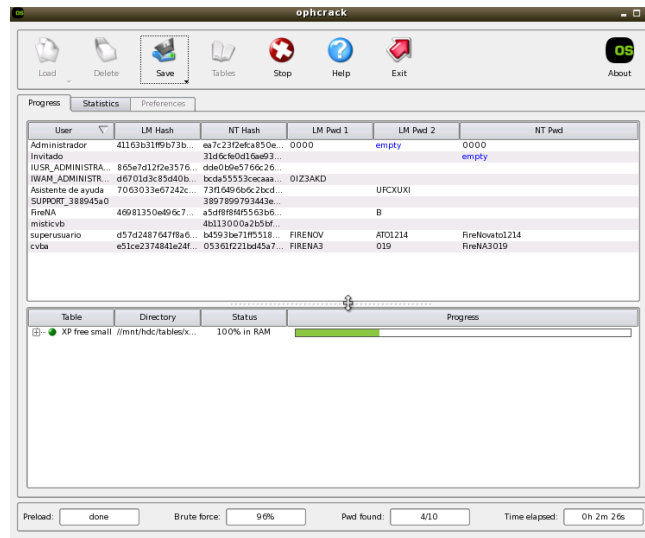
- También las manda a mayúsculas
- Para el ataque ocupamos un Live CD
 - Este Live CD hace un ataque hibrido.
 - Tiene un kernel de Linux (por lo tanto actúa con una partición de disco duro EXT3 por que no existen permisos de NTFS)
 - Hace un ataque a la contraseña que se encuentra System32/config/SAM



- Creamos los siguientes usuarios de Windows XP:

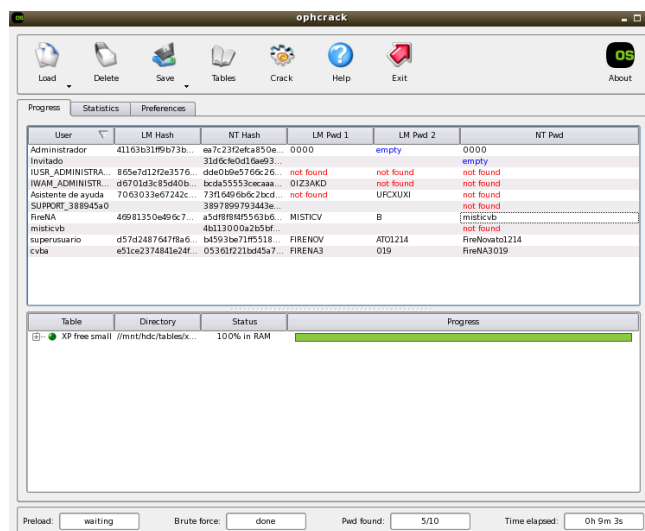
Nombre	Password	Encontrado
FireNA	misticvb	si
misticvb	taviut021Kegr7ypf	no
superusuario	FireNovato1214	si
cvba	FireNA3019	si

- En la siguiente figura boteamos el sistema para iniciar el ataque por fuerza bruta.



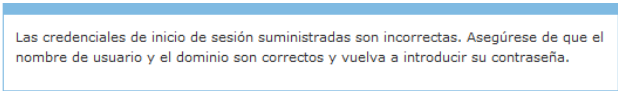
- Al final del análisis podemos observar que de todos los usuarios el único que no encontró su contraseña es:

Nombre	Password
Misticvb	taviut021Kegr7ypf



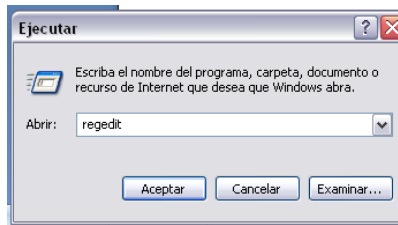
2. Ver como deshabilitar en Windows XP un hash de administrador de LM y dejar solo el hash de NT.

- En caso de deshabilitar el hash LM se pueden producir los siguientes problemas
 - Los usuarios sin un hash de LM no podrán conectarse a un equipo basado en Windows 95 o en Windows 98 que actúe de servidor a menos que el cliente de servicios de directorio para Windows 95 y Windows 98 esté instalado en el servidor.
 - Los usuarios de equipos basados en Windows 95 o en Windows 98 no podrán autenticarse en los servidores con su cuenta de dominio a menos que tengan instalado el cliente de servicios de directorio en sus equipos.
 - Los usuarios de equipos basados en Windows 95 o en Windows 98 no podrán autenticarse con una cuenta local en un servidor si éste ha deshabilitado los hash de LM a menos que tengan instalado el cliente de servicios de directorio en sus equipos.
 - Es posible que los usuarios no puedan cambiar sus contraseñas de dominio desde un equipo basado en Windows 95 o en Windows 98, o que tengan problemas de bloqueo de cuenta cuando intenten cambiarlas desde estos clientes anteriores.
 - Es posible que los usuarios de los clientes de Macintosh Outlook 2001 no puedan tener acceso a sus buzones en servidores de Microsoft Exchange Server. Es posible que vean el siguiente error en Outlook:



Las credenciales de inicio de sesión suministradas son incorrectas. Asegúrese de que el nombre de usuario y el dominio son correctos y vuelva a introducir su contraseña.

- **Windows XP y Windows Server 2003**
 - Para agregar este valor DWORD mediante el Editor del Registro, siga estos pasos:
 1. Haga clic en **Inicio** y en **Ejecutar**, escriba **regedit** y haga clic en **Aceptar**.



2. Busque la siguiente clave del Registro y haga clic en ella:
3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa (Figura 1 y 1.1)
4. En el menú **Edición**, seleccione **Nuevo** y haga clic en **Valor DWORD**. (Figura 2)
5. Escriba **NoLMHash** y presione Entrar.
6. En el menú **Edición**, haga clic en **Modificar**.
7. Escriba **1** y, a continuación, haga clic en **Aceptar**.
8. Reinicie el equipo y, a continuación, cambie la contraseña.

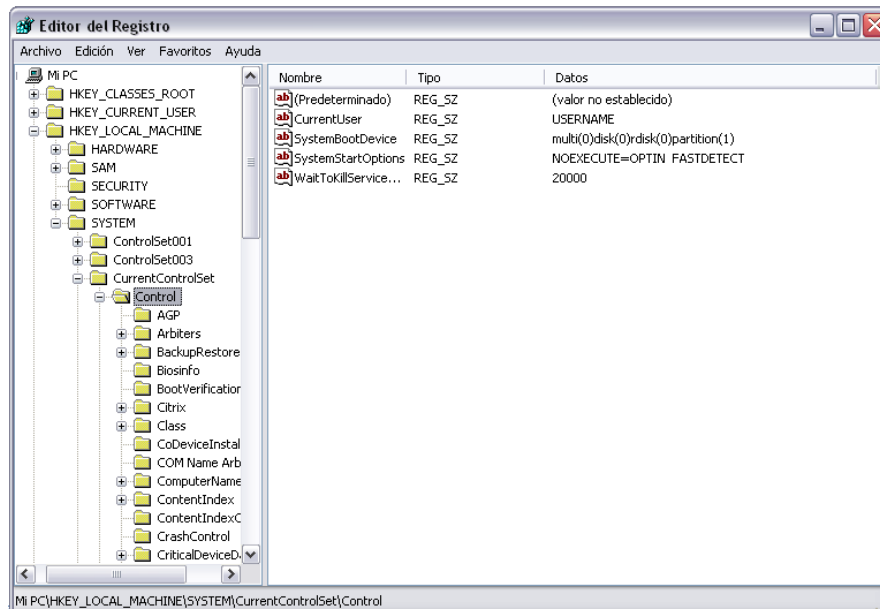


Figura 1

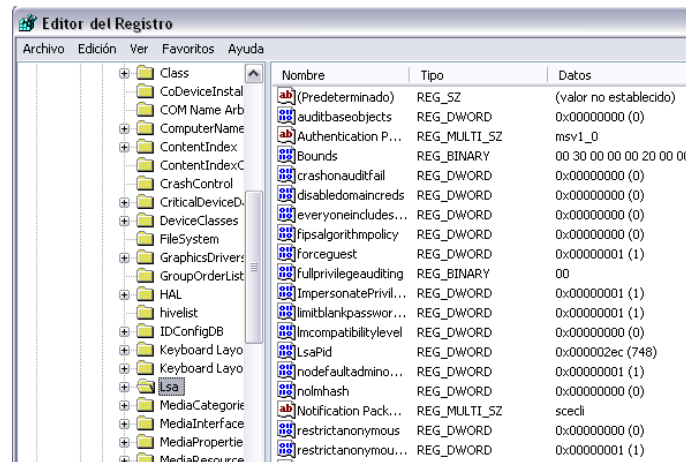


Figura 1.1

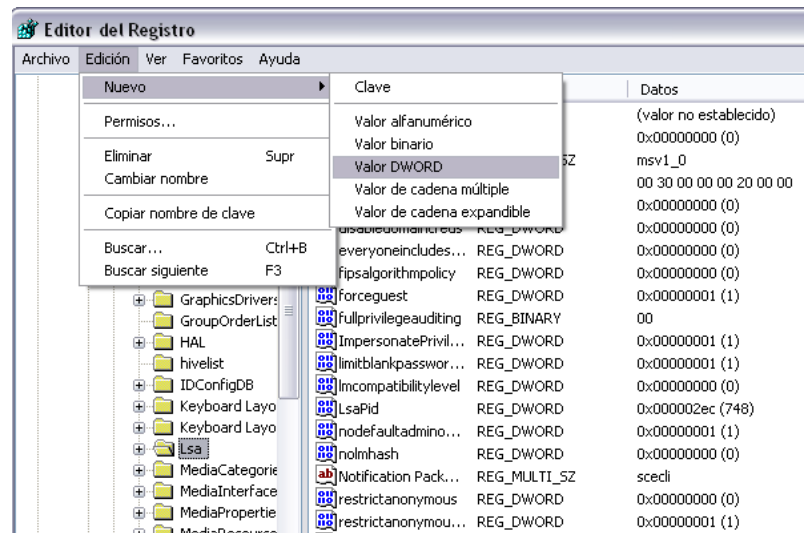
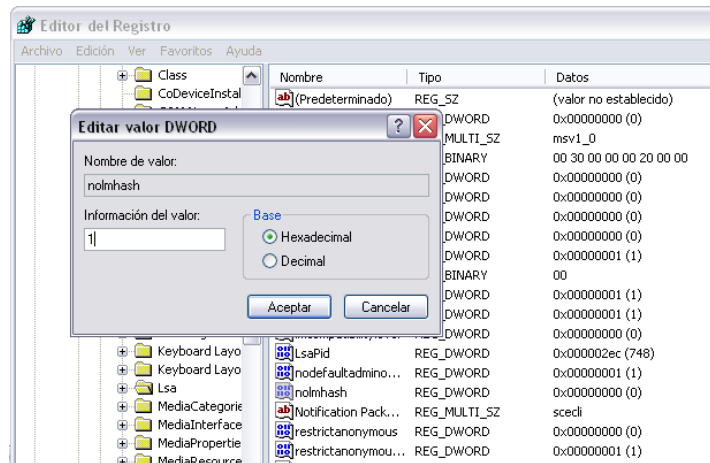


Figura 2

- Este valor DWORD impide que se creen hash de LM nuevos en los equipos basados en Windows XP y en Windows Server 2003. El historial de todos los hash de LM anteriores se borra al completar estos pasos.



Conclusión:

- Para el primer ataque podemos observar que en base a la memoria asignada al equipo es el tiempo en que tarda hacer el ataque de fuerza bruta.
- Los diccionarios de la herramienta puede hacer que no se encuentre la contraseña.

- Si colocan contraseñas con longitud mínima de 15 caracteres, en este caso, Windows almacena un valor de hash de LM que no se puede usar para autenticar al usuario.