Contraseñas en Windows NT

[Artículo publicado en Raregazz 19 - http://www.raregazz.org]

Hernán Marcelo Racciatti
paper@hernanracciatti.com.ar
10/01/2002

Indice

00. Introducción

A menudo sucede que escuchamos algunas frases que por su naturaleza podrían aplicarse a un sin numero de situaciones.

Al momento de decidir cual de ellas utilizaría para ilustrar esta nota, inmediatamente vino a mi mente aquella que reza “Hay que volver a las fuentes”

Desde los inicios de la humanidad hubo cosas que mantener en secreto. Esta absolutamente comprobado que desde edades remotas la inventiva humana trabajo afanoSAMente por encontrar formas de comunicarse en forma segura.

Mas de una persona se sorprenderá al revisar la historia y descubrir lo antiguo del concepto de “contraseña”

De aquellos primeros días hasta hoy ha corrido mucha agua bajo el puente y sin embargo, las “Contraseñas reutilizables” siguen siendo un eslabón fundamental en la seguridad de sistemas.

01. Conceptos Generales

El concepto de contraseña reutilizable se encuentra presente en un sin numero de dispositivos y sistemas. Agendas electrónicas, teléfonos celulares, contestadores telefónicos, alarmas de incendio y por supuesto la mayoría de los sistemas informáticos sumado a un largo etcétera forman parte de este universo.

Como suele suceder en estos casos, si bien existen diferencias sustanciales en su Implementación hay algunos conceptos propios de la autentificación por Contraseñas que parecen mantenerse inalterables en los sistemas informáticos, mas allá de la implementación que cada uno de ellos desarrolle en sus productos.

A continuación mencionaremos dos de los puntos mas importantes:

- Conjunto de pares
Esto es sencillamente lo que conocemos como el conjunto de USUARIO / CONTRASEÑA.
Este punto de seguro le resultara conocido puesto que es la forma que habitualmente utilizan los sistemas informáticos para reconocer un usuario legitimo.

- Almacenamiento de las credenciales
Aquí otro de los puntos en común entre las diferentes Implementaciones. Todas ellas en algún punto necesitan almacenar físicamente las credenciales contra las cuales se validaran los datos correctos.

02. Debilidades en la Implementación de Contraseñas

Antes de entrar de lleno al tema al que atiende este articulo, me gustaría mencionar algunos aspectos por los cuales el ataque sistemático a Contraseñas sigue siendo con el correr de los tiempos uno de los riesgos mas importantes a tener en cuenta a la hora de asegurar un sistema.

A pesar del relativo esfuerzo que los proveedores principales han enfocado en las diferentes Implementaciones existe un denominador común que bajo ningún aspecto debe pasarse por alto a la hora de verificar la seguridad de un sistema: “El Factor Humano”.

Nombres de Usuario
Si bien existen unas cuantas buenas herramientas, sean libres o comerciales, utilizadas en la fase de “enumeración” (Se denomina comúnmente de esta forma a una de las instancias iniciales en los ciclos de un ataque a sistemas informáticos) que nos permiten conocer los nombres de usuarios del sistema objetivo, muchas veces siquiera es necesario hacer uso de las mismas para obtener un nombre de usuario valido.

La mayoría de las veces bastara con conocer el nombre y apellido de algún empleado o usuario del sistema a atacar (Ver articulo de Ingeniería Social en RareGazz 18) y probar las típicas combinaciones utilizadas al momento de nombrar usuarios en un sistema.

Esto es, si la persona identificada por el atacante como empleado / usuario del sistema objetivo se llama Juan Pérez, lo mas habitual será encontrar que alguna de las siguientes denominaciones es en definitiva la utilizada por el administrador para nombrar sus usuarios:

jperez@objetivo.com

perezj@objetivo.com
juanp@objetivo.com
pjuan@objetivo.com

Es muy común encontrar que los administradores no prestan atención a la hora de seleccionar la metodología al momento de nombrar a sus usuarios, pero lo cierto es que en entornos de "Seguridad Media" se debería dedicar un esfuerzo mayor a la hora de resolver este dilema.

Después de todo... acaso obteniendo un nombre de usuario valido... el atacante no tiene el cincuenta por ciento de su trabajo culminado ????

Contraseñas
Y aquí es donde mas interviene tal como mencionara en los párrafos anteriores, "el factor humano".

En principio es sumamente habitual al realizar una auditoria de Contraseñas, encontrarse con palabras triviales y absolutamente adivinables. Nombres propios, nombres de mascotas, nombres de astros y otra vez un largo etcétera... hacen de la selección de passwords por parte de los usuarios un mero tramite.

En el otro extremo tenemos aquellos gerentes o directores a los cuales se suele "asignar" un password con algún grado de complejidad los cuales terminan siendo anotados en un taco, estampados mediante un autoadhesivo en el monitor o teclado de su pc personal y por supuesto conocido por su secretaria y colaboradores, perdiendo de esta forma su estatus de "palabra secreta".

Si bien a lo largo de este documento intentare poner de manifiesto unas cuantas vulnerabilidades propias de las Implementaciones de user / pass en Windows NT, me pareció sumamente importante mencionar en este apartado aquellas características que trascienden lo "particular" de estos sistemas.

03. Debilidades en la Implementación de Contraseñas en Windows NT 4.0

Quienes hayan seguido de cerca la evolución de los sistemas operativos de Microsoft habrán notado su esfuerzo continuo por mantener la compatibilidad con sus desarrollos anteriores.

Si bien este atributo suele ser en principio bienvenido y en muchos casos hasta necesario, lo cierto es que lamentablemente también ha sido el causante principal de alguna de las mas terribles vulnerabilidades conocidas hasta la fecha de los sistemas Windows NT.

Un claro ejemplo de lo expuesto en el párrafo anterior es el que se da respecto de las formas en que NT maneja los hash de Contraseñas en virtud de mantener la compatibilidad con los clientes Windows for Workgroups y Windows 95/98.

Para entenderlo un poco mejor les propongo revisar al menos superficialmente algunos de los puntos principales en el proceso de administración de credenciales en Windows NT:

a. Que es una función hash? Que es un hash?

Recogiendo la definición publicada por RSA en su Website podríamos decir que una función hash H, es una transformación que sucede al tomar un valor de entrada m y retornar un string de extensión fija, el cual recibe el nombre de "valor hash" h (Esto es igual que decir h=(H(m))

Las funciones hash H son también llamadas *de una sola dirección, esto significa que: dado un valor h, es computacionalmente impracticable el encontrar alguna entrada x tal como H(x)=h.

Nota: *Para obtener una definición completa acerca de funciones y valores Hash, puede dirigir su explorador a:*

http://www.rsasecurity.com/rsalabs/faq/2-1-6.html

b. Como trabaja NT con valores hash?

Como la mayoría de los sistemas basados en Contraseñas los sistemas Windows requieren algún mecanismo para almacenar en forma segura las credenciales que se utilizaran para realizar los chequeos necesarios al momento de autentificar un usuario.

Windows NT encripta las Contraseñas antes de almacenarlas en lo que se denomina SAM, por "Security Account Manager".

La SAM es en definitiva una base de datos que alberga los nombres de usuarios y Contraseñas del sistema local o del "Controlador de Dominio", en caso que esta sea la función asignada al equipo en cuestión, previa codificación de los datos a almacenar.

Este proceso de codificación no es mas que un proceso de hashing como el que se describiera en párrafos anteriores.

De esta forma entonces NT toma el valor de longitud variable ingresado al registrar una contraseña (El cual según el ejemplo precedente seria m) y lo procesa mediante su función de hash (H) para finalmente almacenar el *valor hash* (h, en su caracter de string de tamaño fijo y generación Impredecible) de la contraseña ingresada.

En definitiva, como consecuencia de este proceso, cada vez que un usuario inicia una sesion e introduce una contraseña, NT procede a codificar la contraseña y compararla con el hash legitimo del usuario almacenado en la SAM. En caso de que estos valores coincidan, NT autentifica al usuario.

Nota: *NT realiza dos encriptaciones siendo el calculo de valor hash la primera de estas. A los efectos de no complicar la explicación, tanto esta segunda fase como*

algunos procesos adicionales incluidos al momento del logon, se han obviado en forma intencional (Ejemplo algoritmo MD4, circuito LSA, token's, etc).

Podrá obtener una explicación detallada de este proceso en la Knowledge Database de Microsoft bajo el ID=102716.

Como seguramente habrán imaginado a estas alturas, el objetivo de manejarse con valores hash apunta principalmente a los siguientes puntos:

- Que lo que se transmita por la red sean "valores hash" y no Contraseñas.
- Que en caso de que se consiga acceder a la SAM lo que se logre solo (¿?) sea obtener valores hash, no Contraseñas.

c. Tipos básicos de autentificación en Windows

Inicialmente Microsoft comenzó a incluir conectividad en sus sistemas operativos aproximadamente a partir de su versión de Windows for Workgroups.

Si bien de aquel momento hasta nuestros días se ha recorrido mucho camino, la realidad es que aun hoy en día es mas que frecuente encontrar que muchas empresas que poseen sistemas centrales montados sobre Windows NT o Windows 2000 aun conservan gran cantidad de clientes Windows 95/98 y Workstation.

Conforme las tecnologías fueron avanzando, los tipos de autentificación se fueron reforzando llegando hasta le Implementación Kerberos en Windows 2000.

El siguiente cuadro muestra los tipos de autentificación implementados en los entornos Windows y los clientes soportados:

Tipos de Clientes	
Autentificación	**Compatibles**
LANMan	Todos (95/98/NT/2000)
NTLM	NT4, 2000
NTLM v2	NT4 Pos SP4, 2000
Kerberos	2000

d. El verdadero problema: LAN Manager

Algún tiempo atrás, una debilidad en la vieja hash de LAN Manager fue divulgada y desde aquel momento muchas cosas han cambiado respecto de la mentada seguridad de el esquema de autentificación en sistemas Windows NT/2000.

NT maneja dos versiones encriptadas totalmente independientes una de la otra. Por un lado la versión LanMan (Hash LANMan) y por otro la versión NT (Hash de NT). El objetivo de este procedimiento, es preciSAMente mantener la compatibilidad con las versiones de Windows que utilizan el sistema LAN Manager al momento de autentificar un usuario (Windows 95/98).

De esta forma, ambos hashes de Contraseñas se almacenan en la SAM permitiendo utilizar uno u otro de acuerdo al cliente desde el cual se conecte el usuario.

Unos de los defectos mas importantes del hash LAN Manager es la división de la contraseña en dos mitades de siete caracteres. Debido a esto en realidad cualquier contraseña de, por ejemplo ocho caracteres, será traducido al momento de su encriptación, como una contraseña de siete caracteres y otra de un caracter.

Como si esto fuera poco el la función hash de LAN Manager, como primera medida convierte absolutamente todos los caracteres del password en cuestión a mayúsculas, degradando aun mas la efectividad final de las Contraseñas seleccionadas y por consecuencia del hash almacenado en la SAM.

Para clarificar lo mencionado en los párrafos anteriores, le propongo analizar un ejemplo publicado en el libro "Hacking Exposed: Network Security Secrets and Solutions" de Stuart McClure, Joel Scambray, George Kurtz el cual a mi modesto entender ilustra claramente la debilidad comentada:

"passfilt" es una DLL incluida con el SP2 de Windows NT la cual será comentada mas adelante en este mismo documento.

[...]
Supongamos, por ejemplo, una contraseña de 12 caracteres que cumpla con passfilt*, <<123456Qwerty>>. Cuando esta contraseña se encripta con el algoritmo LanMan, en primer lugar, todos sus caracteres se convierten a mayúsculas <<123456QWERTY>>. A continuación, se rellena la contraseña con caracteres nulos (blancos) para convertirla en una palabra de 14 caracteres de longitud <<123456QWERTY__>>. Antes de encriptarla, se divide la cadena de 14 caracteres en dos mitades, dejándola en <<123456Q>> y <<WERTY__>>. Cada cadena se encripta individualmente, y el resultado se concatena. El valor encriptado para <<123456Q>> es 6BF11E04AFAB197F y el valor correspondiente a <<WERTY__>> es 1E9FFDCC75575B15. La información concatenada es 6BF11E04AFAB197F1E9FFDCC75575B15.
[...]

De esta forma una contraseña que en principio podría ser considerada medianamente segura, teniendo en cuenta que contiene números, mayúsculas y minúsculas, al ser transformada a mayúsculas y posteriormente fraccionada en dos palabras se convierte en un blanco sencillo para algunas utilidades de cracking, pues las mismas no solo que se enfrentan a 2 passwords de 7 caracteres (En vez de 1 de 14 caracteres) sino que en caso de lograr adivinar con éxito la primer mitad, lo mas probable es que quien este practicando el cracking deduzca el contenido de la mitad restante, como muy probablemente pasaría en el ejemplo <<123456Qwerty>>.

Nota: *Podrá obtener una explicación mas detallada acerca de este punto en la siguiente URL:*

http://www.atstake.com/research/lc3/documentation/doc.html#Technical Details About Network SMB Capture

04. Obteniendo datos de la SAM

Imagino que llegado este punto habrá quedado absolutamente claro la necesidad de obtener o acceder de alguna forma a la base de datos SAM del sistema NT a auditar, a los efectos de poder lanzar sobre ella alguna de las herramientas de cracking convencionales.

Antes de continuar, vale la pena recordar que NT guarda los datos de la SAM en un archivo llamado preciSAMente SAM. Dicho archivo se encuentra en:
%systemroot%\system32\config

Este archivo no es ni mas ni menos que la representación física de los valores presentados en la llave HKEY_LOCAL_MACHINE\SAM

Tanto la mencionada clave como el archivo SAM no se encuentran disponibles para ser revisados o copiados pues el sistema operativo los mantiene bloqueados mientras se encuentra funcionando.

Bien, dicho esto mencionaremos tres o cuatro de las formas en las cuales se podrá acceder a la SAM de un sistema del tipo Windows NT.

a. Arrancar con un sistema operativo distinto (NTFSDOS)

Debido a que, tal como acabo de mencionar, el archivo SAM se encuentra bloqueado mientras el sistema operativo esta en uso, se deberá bootear con un segundo sistema operativo para lograr el acceso a la carpeta deseada.

En aquellos casos en los que la partición del sistema objetivo se encuentre bajo NTFS, aun se podrá recurrir a la popular herramienta de Sysinternals "NTFSDOS" (http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml) para lograr el acceso requerido.

Este producto accede y monta particiones NTFS como unidades lógicas en un entorno MS-DOS.

La distribución de NTFSDOS ofrecida gratuitamente en la web de Sysinternal, esta compuesta por tan solo tres archivos (readme.txt, ntfsdos.exe y ntfshlp.vxd) y pesa alrededor de 39KB y nos permitirá copiar la información deseada (También existe una versión comercial, la cual permite acceso total)

Debido a su sencillez (Solo existen seis parámetros de línea de comando) no haré otra cosa que mencionar el procedimiento de utilización básico el cual consta de tres pasos:

Paso 1 Generar un disco booteable, preferentemente MS-DOS 7.0 (He encontrado que bajo ciertas circunstancias otros sistemas de arranque como MS-DOS 5.0 o MS-DOS 6.22 se vuelven un tanto inestable)

Paso 2 Reiniciar el equipo y bootear con el disco recientemente generado.

Paso 3 Estando en el nuevo command prompt ya estaremos en condiciones de correr "ntfsdos.exe".

Luego de ejecutar la pequeña aplicación se nos devolverá un mensaje similar al que se muestra a continuación:

```
A:\>ntfsdos

NTFS File System Driver for DOS/Windows V3.02R (Read-Only)
Copyright (C) 1996-2001 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com

Initialized 500 KB of XMS cache.

Mounting NTFS partition(0x80:1) as drive: D
Mounting NTFS partition(0x80:1) as drive: E
Mounting NTFS partition(0x80:1) as drive: F

A:\>
```

Una vez accedida la carpeta %systemroot%\system32\config solo tendrá que utilizar el comando copy que seguramente habrá incluido en su disco de arranque junto a los archivos de NTFSDOS, para obtener el archivo SAM.

b. Obtener la copia de seguridad de la SAM del directorio repair

Cada vez que se ejecuta la aplicación RDISK en un sistema NT se crea una copia de el archivo SAM en el directorio %systemroot%repair.

RDISK es una utilidad de los sistemas operativos Windows NT que permite generar un juego de disquetes de recuperación con información vital que suele ser una herramienta importante al momento de recuperar el sistema operativo ante una falla.

En caso de que esta utilidad haya sido ejecutada en algún momento, y que el administrador no haya eliminado esta información luego de generar los disquetes de recuperación, tan solo tendrá que copiar de la ruta especificada, el archivo SAM._ el cual se encuentra comprimido.

c. Extraer los hashes de la SAM (PWDUMP)

La idea en este caso es simple. Se trata de volcar los hashes contenidos en la SAM objetivo, a un archivo plano de forma tal que pueda ser interpretado por las herramientas de cracking de Contraseñas mas populares.

PWDUMP es sin lugar a dudas una de las herramientas mas utilizadas a tal efecto.

Al momento de escribir esta nota la versión mas avanzada de esta herramienta denominada PWDUMP3 v2.0 se encuentra disponible para su descarga en forma gratuita en la siguiente URL:

http://www.polivec.com/pwdump3download.html

PWDUMP3 es sumamente sencillo de utilizar. Una vez descargado, tan solo será necesario descomprimir el download en una carpeta desde la cual se lanzara la herramienta, y ejecutarla pasándole como parámetro el equipo objetivo así como el archivo de destino y el nombre de usuario:

ATENCION: Para que esta herramienta funciona se requiere que el usuario que la ejecute tenga permisos de ADMINISTRATOR en la maquina objetivo.

Sintaxis: PWDUMP3 machineName [outputFile] [userName]

Al ejecutar la herramienta con los parámetros requeridos, se nos presentara una pantalla con el siguiente aspecto:

```
D:\pwdump3v2>pwdump3 pcobjetivo c:\destino.txt administrator

pwdump3 (rev 2) by Phil Staubs, e-business technology, 23 Feb 2001Copyright 2001
e-business technology, inc.

This program is free software based on pwpum2 by Todd Sabin under the GNU
General Public License Versión 2 (GNU GPL), you can redistribute it and/or modify
it under the terms of the GNU GPL, as published by the Free Software Foundation.
NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Pleasee see the COPYING file included with this program (also avaible
at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Please enter the password >********** <-------- Solicita Password

Completed.      <-------- Proceso Terminado

D:\pwdump3v2>type c:\destino.txt   <-------- Consulto Resultado

 Administrator:500:51365BA539C0B51C7586247B8D2C9F9E:178FE8F0 (
Informacion
  Guest:501:NO PASSWORD**********************:NO PASSWORD*****
recortada por
  VUSR_NOMUSER:1000:9EA4EE76350A6CBF300EDB7D8C243531:234BF879
el  editor )
```

Como se puede observar el contenido muestra claramente la información que PWDUMP puede conseguir por nosotros. Una vez obtenidos estos datos, solo habrá que importarlos desde la herramienta de cracking / auditoria por nosotros elegida.

Tal como se menciona en la documentación que acompaña a PWDUMP3, esta herramienta inicialmente se conecta al equipo remoto, utilizando el recurso compartido $ADMIN, luego aprovechando la posibilidad de Windows NT/2000 de instalar y desinstalar servicios en forma remota, PWDUMP instala el servicio que acompaña esta distribución llamado "pwservice.exe" el cual extrae la información de los hash almacenados temporalmente en la registry remota.

A partir de allí utiliza una técnica denominada DLL Injection que le permite correr con altos privilegios bajo el espacio de procesos de otros subsistemas, en este caso LSASS (Local Security Authority Subsystem) con el cual termina obteniendo la información necesaria para generar el archivo de output.

Nota: *Podrá obtener una explicación mas detallada acerca de este punto revisando la documentación que acompaña la herramienta. Recomiendo enfáticamente su lectura pues considero sumamente enriquecedor los procedimientos utilizados por PWDUMP.*

d. Obtener hashes por medio de escuchas en la red

Este es quizás uno de los métodos mas avanzado respecto a la obtención de hashes, en este escenario, se requiere la instalación de algún tipo de sniffer encargado de capturar datos en la red (Específicamente paquetes SMB) los cuales contienen los hashes encriptados que puedan servirnos a los efectos de ser procesados por alguna herramienta de cracking de Contraseñas.

05. Infalible: L0phtCrack

Llegado este punto y luego de haber pasado por la tarea de obtener información de la SAM, utilizando a tal efecto alguno de los procedimientos descriptos en los párrafos anteriores, solo nos quedara seleccionar algún programa que nos permita auditar / crackear los hash conteniendo usuario y passwords.

Si bien existen un par de buenas herramientas algunas de ellas freeware (Ver articulo de Nihil en Phrack 50) nos olvidaremos de ellas por un momento para conversar acerca de la que a mi entender es la mejor herramienta de auditoria de passwords disponible hoy día: LC3 (L0phtCrack Versión 3.02)

LC3 es la evolución del primer producto desarrollado por la gente del grupo L0pht (L0pht Heavy Industries). Algunos años después, transformados en lo que hoy es la empresa @Stake, aun siguen distribuyendo, en realidad "comercializando" su producto de auditoria de Contraseñas.

Como la mayoría de los productos de su tipo, LC3 es en esencia, un software que utiliza distintos métodos de comparación entre el hash del usuario y un dato de

entrada previamente convertido según el algoritmo de encriptación utilizado en la generación original de la contraseña a auditar, hasta hallar la combinación correcta.

Los mas común es que el mencionado dato de "entrada" provenga de un diccionario de palabras, o sea producto algún tipo de generación aleatoria.

Si ha esto le sumamos la debilidad anteriormente comentada respecto de los Hash LAN Manager, estaremos en condiciones de afirmar que una vez que se alimenta a LC3 con la información correcta todo pasa a ser una cuestión de tiempo antes de lograr el objetivo deseado.

a. LC3 en Acción

Realmente no hay mucho para explicar acerca de la forma de operar con LC3 puesto que gracias a su impecable interfaz grafica, la mayoría de las funciones son absolutamente intuitivas.

A modo de ejemplo repasaremos los pasos que se deberán seguir al momento de realizar la auditoria de Contraseñas.

Paso 1 Inmediatamente después de haber instalado el software, estaremos en condiciones de iniciar una nueva "session", lo cual podremos lograr fácilmente haciendo click sobre el icono correspondiente o accediendo al menú "File / New Session".

Paso 2 Iniciada una "session" el próximo paso será tal como nos indica el mismo LC3, utilizar el menú "Import" desde el cual se podrá seleccionar el tipo de importación deseado, entre las siguientes opciones:

Import From Local Machine (Requiere derechos de Admin)
Import From Remote Registry... (Requiere derechos Admin)
Import From SAM File...
Import From Sniffer...
Import From .LC File
Import From PWDUMP File...

Paso 3 De acuerdo a la opción que se haya seleccionado en el paso anterior LC3 comenzara a displayar, en forma inmediata los nombres de usuario encontrados, como así también la información correspondiente a los valores LM Hash y NTLM Hash.

Paso 4 Finalmente, llegado este punto, nos encontraremos listos para seleccionar las opciones a utilizar en el cracking de Contraseñas. Estas podrán utilizarse en forma particular o por una combinación de las mismas.

- Dictionary Crack
Tal como se expresa en la documentación de LC3, esta suele ser la vía mas rápida para dar con los passwords mas sencillos. Su efectividad se encuentra directamente relacionada con el tamaño y tipo del diccionario a utilizar.

Por defecto la versión 3.02 de LC3 utiliza un diccionario ingles de 25000 palabras, aunque siempre existe la posibilidad de seleccionar un diccionario diferente.

Nota: *Podrá encontrar una gran variedad de diccionarios en formato estándar dirigiendo su explorador a la siguiente URL:*

http://ftp.cerias.purdue.edu/pub/dict/wordlists/

- Dictionary/Brute Hybrid Crack
Este particular método utiliza el diccionario de datos seleccionado sumado a "n" variaciones que pueden ser dispuestas utilizando el cuadro "Characters to vary (moreis slower)"

De esta forma se podrán encontrar con algo mas de esfuerzo aquellas passwords que complementen las palabras del diccionario con algún juego de "n" caracteres, tal como lo demuestran los ejemplos mencionados por LC3:

"Dana99" o "monkeys!".

- Brute Force Crack
Este es el método de cracking mas abarcativo, durante este proceso se intentan todas las posibilidades respecto del set de caracteres escogido (Letras, letras y números, letras números y caracteres especiales, etc)

Debido a sus características, este método puede implicar un tiempo considerable de proceso, hasta descubrir passwords como las mostradas por LC3 en sus ejemplos "WeR3pl6s" o "vC5%69+12b"

Paso 5 Habiendo completado los pasos anteriores, habremos finalizado la configuración de las "session" de auditoria, por lo tanto bastara con clickear sobre el icono de play ("Begin audit.") para que LC3 comience a realizar su trabajo.

Inmediatamente después de haber lanzado el proceso de auditoria, LC3 comenzara a mostrar la información correspondiente a los passwords mas sencillos.

Es fascinante ver la velocidad con la que aparecen por ejemplo aquellos passwords que coinciden con el nombre mismo del usuario, o con palabras sencillas incluidas dentro del diccionario.

Lo mas probable es que al cabo de algunas horas LC3 haya acabado por mostrar la información completa de un centenar de usuarios / passwords con combinaciones sencillas o de mediana complejidad.

En aquellos casos en los que LC3 se tope con Contraseñas realmente complejas, el cracking podría demorar varios días. Lo cierto es que... a partir de este momento solo será una cuestión de tiempo...

Nota: *La versión 3.02 de LC3 que al momento de escribir este articulo se encuentra disponible en la web de @STAKE, es una versión de Evaluación y como tal, no solo limita su utilización a 15 días, sino que por otro lado no incluye la funcionalidad de ataques de brute force que si posee la versión comercial.*

b. Mejoras en la versión 3.02

Si bien la versión 3.02 de esta potente herramienta no deslumbra por sus novedades hay algunas de ellas que vale la pena señalar.

A continuación le propongo revisar la traducción de la documentación de LC3 v3.02 que he realizado respecto de la sección "Wath's New in LC3":

Lo Nuevo en LC3

LC3 agrega numerosas mejoras a las capacidades aclamadas en sus predecesor L0phtCrack:

Soporte para Windows 2000
LC3 corre en forma transparente sobre Windows 2000. Puede extraer Hashes no encriptados de Contraseñas que utilicen la protección SYSKEY. También se provee un sniffer (Tal es el caso de WinPcap) con soporte total para Windows 2000.

Soporte para Set de Caracteres Internacionales
LC3 soporta la entrada de caracteres internacionales, esto le permite trabajar con sistemas operativos y passwords con Set de Caracteres como: Europo, Cirilico, Griego, Hebreo, Arabigo y otros lenguajes.

Crackig Distribuido
LC3 brinda al administrador la posibilidad de acelerar los tiempos de auditoria distribuyendo la carga en varias partes que pueden ser ejecutadas en forma simultanea por multiples equipos.

Ocultar Contraseñas Crackeadas
LC3 brinda a los administradores la opción de conocer cuando un password haya sido crackeado, sin que necesariamente esto signifique conocer dicho password.

Tiempo de Auditoria
Los Auditores podrán obtener una comparación cuantitativa de la fortaleza o debilidad de las Contraseñas, revisando los informes de LC3 sobre el tiempo requerido para crackear cada contraseña.

Asistente
LC3 ofrece un asistente que ayuda a los nuevos auditores de Contraseñas a configurar y ejecutar sus primeras auditorias con facilidad y rapidez.

Exportación
Con mayor facilidad que en versiones anteriores se pueden manipular los resultados de una revisión de contraseña, exportándolos a un archivo delimitado por tabs.
Soporte de Producto Mejorado
Los usuarios registrados de LC3 cuentan con soporte vía e-mail con un tiempo de respuesta menor a 24 horas.

Nuevo Diccionario
LC3 incluye un diccionario de 250.000 palabras en ingles.

Manipulación de Contraseñas Importadas
Fácilmente borre Contraseñas encriptadas directamente desde la ventana de LC3, para de esta forma concentrarse únicamente en las passwords que usted desea auditar.

Seguramente quienes hayan trabajado con versiones anteriores de L0phtCrack, no notaran grandes cambios en LC3, aunque aquellos que como yo utilicen esta herramienta en forma habitual muy probablemente hayan visto con agrado la inclusión o mejora en puntos como el de proceSAMiento distribuido o la eliminación de Contraseñas desde la misma ventana de auditoria.

06. Windows 2000

Si bien este documento esta específicamente dedicado a Windows NT me gustaría mencionar que a pesar de los esfuerzos de Microsoft y algunas nuevas características incorporadas en Windows 2000, en la practica algunas cosas no han cambiado mucho.

Alguna de las mayores diferencias sean quizás la inclusión de AD (Activate Directory) en "reemplazo" de la SAM, y la inclusión de la autenticación Kerberos.
Ahora bien... volviendo a las fuentes... aquellos administradores que decidan mantener instalaciones Híbridas (Windows NT / Windows 2000) seguramente verán estas mejoras como una utopía.

En aquellos casos, en los que no se haya implementado AD, la SAM seguirá cumpliendo prácticamente la misma función de días pasados, y respecto de la autenticación Kerberos, así como sucede entre Windows NT y Windows 95/98, los hashes NT Lan Manager heredados, siguen siendo distribuidos por la red pues Windows 2000, siguiendo la línea de su antecesor, degrada el nivel de autentificación en caso de que uno de los extremos de la conexión no soporte kerberos.

De esta forma, la mayoría de los ataques de Contraseñas sobre Windows 2000, siguen siendo en la practica, tan efectivos como en Windows NT.

Ahora bien, como contraposición a lo expuesto en el párrafo anterior podremos hallar al menos un par de características distintivas de Windows 2000 respecto al almacenamiento y gestión de Contraseñas:

En principio, Windows 2000 utiliza la encriptación SYSKEY como la opción por defecto, dificultando bastante la tarea de cracking en determinadas circunstancias, pero lo que es aun mejor, a partir de Windows 2000 el largo de las passwords rompe

la barrera de los 14 caracteres para brindar la posibilidad al usuario de registrar passwords de hasta 128 caracteres, haciéndolas "prácticamente" indescifrables (En parte, producto de que el viejo LanMAn hash entenderá y almacenara una clave de tamaño superior a 15 caracteres como un valor null, para mas información sobre este hecho sírvase visitar la siguiente URL:

http://www.securityfriday.com/Topics/win2k_passwd.html)

07. Contramedidas

Si bien el panorama no parece ser el mejor, respecto de la posibilidad de asegurar las Contraseñas de sus sistemas, existen una serie de herramientas que en conjunto podrán colaborar al fin en cuestión.

- ✓ Elimine la información del directorio %systemroot%repair inmediatamente después de haber generado los discos con RDISK.EXE (ERD)
- ✓ En lo posible NO utilice sistemas de arranque DUAL (FAT / NTFS)
- ✓ Asegure el acceso Físico a sus servidores.
- ✓ Almacene las copias de seguridad y los discos de "Reparación de Emergencia" en lugares seguros.
- ✓ Asegure los directorios de su partición de sistemas con permisos NTFS personalizados.
- ✓ Dedique tiempo a la correcta parametrización de las políticas de cuentas accediendo desde el "User Manager for Domains / Policies / Accounts".Los valores usualmente sugeridos son:

Maximum Password Age	45 Days
Minimum Password Age	Allow Changes in 7 Days
Minimum Password Length	At least 7 Characters
Password Uniqueness	Remember 3 Passwords
Lockout after	3 bad logon attempts
Reset Counter after	240 minutes
Lockout Duration	Forever (until admin unlocks)
Forcibily disconnect remote Users from server when logon hours expire	Check ON
User must log on in order to change password	Check ON

- ✓ No permita Contraseñas menores de 7 dígitos.
- ✓ Implemente SYSKEY

SYSKEY es una funcionalidad de mejora de encriptación del SAM, incluida al mercado a partir de la liberacion del SP2 de Windows NT. Su Implementación permite cifrar los datos del SAM con Contraseñas criptográficas de 128 bits contra los 40 bits de las de las instalaciones por defecto. La puesta en marcha de SYSKEY es sumamente sencilla pues requiere tan solo de la ejecución del

ejecutable (SYSKEY.EXE) y la selección de la casilla de verificación correspondiente (Encryption Enabled).

Concluido este paso se podrá decidir si la llave encriptada como consecuencia de la Implementación SYSKEY se almacenara en disquetes o en el disco local.

Un punto importante a tener en cuenta es que Windows 2000 implementa encriptación SYSKEY por defecto.

Mas sobre SYSKEY en:
http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q143475&

✓ Implemente PASSFILT.DLL

Así como SYSKEY, PASSFILT.DLL se incluye a partir de la liberacion del SP2 de Windows NT. La utilización de PASSFILT.DLL en una instalación estándar permitirá al administrador asegurarse el ingreso por parte de los usuarios, de Contraseñas que cumplan ciertos requisitos mínimos de seguridad.

A partir de la Implementación de PASSFILT.DLL, se establecen los siguientes requisitos:

- Claves de al menos seis caracteres de longitud.
- La clave seleccionada no puede coincidir con el nombre de usuario o cualquiera de las partes del mismo.
- Toda clave debe contener, al menos, tres caracteres de los siguientes:

Letras mayúsculas
Letras minúsculas
Números
Metacaracteres

Nota: *No implemente PASSFILT hasta no haber leido y comprendido por completo, el articulo publicado en la siguiente URL:*

http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q161990&

✓ Implemente PASSPROP

PASSPROP es una utilidad incluida en el NT Resource Kit. Mediante esta herramienta el administrador podrá definir un par de requisitos extras respecto a la seguridad de cuentas de dominio (Inicialmente surge como un complemento ideal de PASSFILT.DLL) En primer lugar PASSPROP nos permitirá forzar el uso de Contraseñas que utilicen una combinación de mayúsculas, minúsculas, números y símbolos.

Por su parte PASSPROP también brinda al administrador, la posibilidad de bloquear la cuenta de ADMINISTRATOR (Tal como cualquier usuario

normal) permitiendo que esta solo pueda ser desbloqueada a posterior, desde la consola.

Para implementar PASSPROP, solo bastara con que el administrador ejecute la herramienta con alguno de los parámetros propios de dicha utilidad:

/simple	Restaura a la instalación por default.
/complex	Fuerza passwords combinados.
/adminlockout	Permite que la cuenta ADMINISTRATOR sea lockeada.
/noadminlockout	Restaura a la instalación por default (ADMINISTRATOR, no puede ser bloqueada)

- ✓ En ambientes de alta seguridad, y cuando sea posible, implemente sistemas homogéneos, evitando la interacción entre Windows 95/98 - Windows NT – Windows 2000.
- ✓ Mantenga una política activa respecto de auditorias de cuentas.
- ✓ Eduque a los usuarios, gerentes y directores acerca de la potencialidad de los ataques a Contraseñas débiles.
- ✓ No practique la aplicación de Contraseñas para los usuarios ordinarios, que por su extrema complejidad lo lleve a "tomar nota" de su contraseña para recordarla!
- ✓ Utilice caracteres especiales y claves largas para los password de administrador.
- ✓ Renombre la cuenta de administrador por un nombre de usuario convencional y aplique a esta una clave sumamente extensa y aleatoria.
- ✓ Habilite la auditoria sobre los eventos de LOGON / LOGOFF y examine diariamente los logs generados.
- ✓ Deshabilite los enlaces NetBIOS de su placa externa.
- ✓ Revise frecuentemente la definición acerca de sus políticas de contraseñas.

08. Conclusiones

Hemos llegado al final de este articulo, como habrán notado el panorama no resulta del todo alentador.
Mientras el modelo a aplicar siga siendo el de Contraseñas reutilizables, los administradores seguiremos encontrándonos con los inconvenientes comunes a toda Implementación.

Nota: *Revise los siguientes links para evaluar algunas de las alternativas a las Contraseñas reutilizables:*

http://www.rsasecurity.com/products/securid/
ftp://ftp.cert.dfn.de/pub/tools/password/SKey/

Nunca olvidemos uno de los conceptos básicos en seguridad informática, "Un sistema es tan seguro como su eslabón mas débil", usted podría establecer las claves mas poderosas en sus sistemas y de toda forma ser victima de un ataque de ingeniería social.

Otro punto relevante a tener en cuenta, es que los ataques a Contraseñas presuponen, generalmente haber ganado con anterioridad acceso de algún tipo, a los sistemas a atacar. Este es el motivo por el cual las verdaderas contramedidas respecto de este tema, debería ser el conjunto de contramedidas implementadas en nuestros sistemas como una estrategia global.

Por ultimo, recuerde que en la practica, en el 90 por ciento de los casos una vez obtenido acceso a la información del SAM, la obtención de Contraseñas es cuestión de tiempo...

09. Tools

http://www.atstake.com/research/lc3/download.html (LC3 - L0phtCrack 3.02)
http://astalavista.box.sk/cgi-bin/robot?srch=lc3&submit=+search+ (LC3-Crack)
http://www.atstake.com/research/lc3/download.html (L0pht 1.5 source code)
http://www.polivec.com/pwdump3download.html (Free-pwdump3 v2.0)
http://ftp.cerias.purdue.edu/pub/dict/wordlists/ (Diccionarios)

10. Links/Referencias

A continuación encontrara material consultado al momento de confeccionar el presente articulo:

http://www.microsoft.com/security
http://www.microsoft.com/technet
http://www.w2000mag.com/atrasados/2001/52_abr01/articulos/suplemento/proteccion.htm
http://www.w2000mag.com/atrasados/2001/52_abr01/articulos/suplemento/proteccion_columna.htm
http://www.hackingexposed.com
http://www.rsasecurity.com
http://online.securityfocus.com/infocus/1554
http://www.atstake.com/research/lc3/index.html
http://www.atstake.com/research/lc3/documentation/help.htm
http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml
http://online.securityfocus.com/infocus/1554
http://www.microsoft.com/Latam/technet/seguridad/robichaux/ro1299.asp
http://www.microsoft.com/Latam/technet/seguridad/au/junio2000.asp

Hernán Marcelo Racciatti
Alias "Angel Protector"

mailto:paper@hernanracciatti.com.ar
http://www.hernanracciatti.com.ar