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

0 0		0) 🕜	$\langle \rangle$			0
Load Dele	te Save	Tables Sto	ip Help	Exit			Abou
rogress Statist	ics Preferences						
User $ abla$	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2		NT Pwd	
Administrador	41163b31ff9b73b	ea7c23f2efca850e	0000	empty	0000		
nvitado		31d6cfe0d16ae93			empty		
USR_ADMINISTRA.	865e7d12f2e3576	dde0b9e5766c26					
WAM_ADMINISTR	d6701d3c85d40b	bcda55553cecaaa					
sistente de ayuda	7063033e67242c	73f16496b6c2bcd		UFCXUXI			
5UPPORT_388945a0		3897899793443e					
ireNA	46981350e496c7	a5df8f8f4f5563b6		В			
Tabla	Directory	Shotur			Dense source		
Table ⊉…	Directory	Status 100% in RAM			Progress		
Table ∄ ● XP free smal	Directory //mt/hdc/tables/x	Status 100% in RAM			Progress		
Table ∰– ● XP free smal	Directory I //mnt/hdc/tables/x	Status 100% in RAM			Progress		
Table ∄- ● XP free smal	Directory I //mnt/hdc/tables/x	Status 100% in RAM			Progress		
Table ⊕- ● XP free smal	Directory //mnt/hdc/tables/x	Status 100% in RAM			Progress		

• 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.

			ophcrack			- 0
0 0	1	0) 🕜	$\langle \rangle$		OS
Load Dele	te Save	Tables Sto	p Help	Exit		About
rogress Statisti	cs Preferences					
User $ abla$	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd	
Administrador	41163b31ff9b73b	ea7c23f2efca850e	0000	empty	0000	
Invitado		31d6cfe0d16ae93			empty	
USR_ADMINISTRA	865e7d12f2e3576	dde0b9e5766c26				
WAM_ADMINISTR	d6701d3c85d40b	bcda55553cecaaa	01Z3AKD			
Asistente de ayuda	7063033e67242c	73f16496b6c2bcd		UFCXUXI		
SUPPORT_388945a0		3897899793443e				
FireNA	46981350e496c7	a5df8f8f4f5563b6		В		
misticvb		4b113000a2b5bf				
superusuario	d57d2487647f8a6	b4593be71ff5518	FIRENOV	AT01214	FireNovato1214	
vba	e51ce2374841e24f	05361f221bd45a7	FIRENA3	019	FireNA3019	
Table	Directory	Status			Progress	
🗄 🌒 XP free smal	//mnt/hdc/tables/x	100% in RAM				
eload: done	Brute	force: 96%	Pwd fe	ound: 4/10	Time elapsed:)h 2m 26s

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

Misticvb spicrask Operation Spicrask Spicrask Operation Spicrask Spicrask Spicrask Operation Spicrask Spicrask Spicrask Spicrask Operation Spicrask Spicrask <th>Nombre</th> <th>Passwo</th> <th>ord</th> <th></th>	Nombre	Passwo	ord	
Operation Operation Load Delete Save Load Delete Save Tables Crack Weight Exit Administration Teleteric Manipulation Transit Load Statistics Notice Teleteric Manipulation Transit Listics Teleteric Manipulation Transit	Misticvb	taviut0	21Kegr7ypf	
Loss Delete Sue Tele Cack Help Exit Advance Progress Statistics Preferences User LM Hesh NT Hesh LM Ped 1 LM Ped 2 NT Ped Administrator 41/05/D3/167/24. 7/2/37/04/86/04/26/99 0000 empty 0000 IUSR, ADMINISTA EGGer/12/22/37/04 64/05/60/14/99.2. end/2/36/60/14/99.2. end/2/36/60/14/99.2. empty empty UUSR, ADMINISTA EGGer/12/22/37/04 64/06/60/14/99.2. end/2/36/04/14/94.2.		0	ophcrack	- ¤ ×
Losse NT Heals LM Peed NT Peed Losse NT Peed Losse Comparison Losse NT Peed Losse NT Peed Losse NT Peed Losse Losse NT Peed Losse Losse NT Peed Losse <		۵ 🕹 🖉	7 🔅 🕜 곚	05
Uber Litheb NT Heab MT Heab LM Red NT Ped Administration 4163b3218731b. an1/23504.080.0000 empty 0000 Initiation MT Red MT Red empty empty IUSR, ADMINSTA. E05er12172317. 44e01845702.ex. not found empty IUSR, ADMINSTA. E05er12172317. 44e01845702.ex. not found empty VIMAL Administration 107031881940b. biology 3099073445e. empty empty SUPROFT 23106906.ex. not found not found not found mot found SUPROFT 3894320 40931300806.ex. not found not found mot found SUPROFT 40931300806.ex. 40931320896.ex. mot found mot found mot found supersuration 05301761318.ex. 4053120176138.ex. mot found mot found mot found supersuration 05301761318.ex. 40931200806.ex. mot found mot found mot found supersuration 05301761318.ex. 053017761318.e		Programs Statistics Professores	es crack neip Exit	About
Administrader 41.03/b31(Pro/1a ar/2.23/04/b30 00.00 empty IVINAde/		User LM Hash	NT Hash LM Pwd 1 LM Pwd 2	NT Pwd
Table Directory Status Progress ⊡ - ● XP free small //mnth/dc/tables/x 100% in RAM		Administrador 41163b3169b73b. ah7.2 Initiado 3126 3126 IUSRA, ADNINISTRA. 0567412762376. delos MUMAL ASMINISTRA. 0567412762376. delos MUMAL ASMINISTRA. 0507412762376. delos Martina de ayuda 700033667242	21064c8290 0000 empty 6x012ax93 not found send found 9x9750c28 not found uFCXUXI 9x997418 mot found UFCXUXI 9x9750506 MISTEV B 9x9719518 FRENOV B 9x9719518 FRENOV AT01224 1x211x9518 FRENOV O19	0000 empty not found not found not found mit found mit trub firekoato 214 firekoato 214
		Table Directory ① - ● X0 free small //mnthdc/tables/x 10	Status P	

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**.

Ejecuta	r 🛛 🕄
-	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea que Windows abra.
Abrir:	regedit 🗸
	Aceptar Cancelar Examinar

- 2. Busque la siguiente clave del Registro y haga clic en ella:
- 3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS et\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.

💣 Editor del Registro				
Archivo Edición Ver Favoritos Ayuda				
🛛 🚇 Mi PC 📃 🔼	Nombre	Tipo	Datos	
HKEY_CLASSES_ROOT	(Predeterminado)	REG_SZ	(valor no establecido)	
		REG_SZ	USERNAME	
😟 🚞 HARDWARE	ab SystemBootDevice	REG_52	multi(U)disk(U)rdisk(U)partition(1)	
🖶 🚞 SAM	WaitToKillService	REG_32 DEG_57	20000	
SECURITY		Ked_be	20000	
E ControlSet001				
🕀 🦲 ControlSet003				
AGP				
BackupRestore				
- 📄 Biosinfo				
BootVerification				
E Citrix				
E Cass				
COM Name Arb				
🕀 🧰 ComputerName				
🕀 🦲 ContentIndex				
ContentIndexC				

Mi PC\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Figura 1

🖗 Editor del Registro					
Archivo Edición Ver Fa	avoritos Ayuda				
🕀 🧰 Cl	ass 🔥	Nombre	Tipo	Datos	
<u>-</u> Ca	DeviceInstal	(Predeterminado)	REG_SZ	(valor no establecido)	
	OM Name Arb	auditbaseobjects	REG_DWORD	0×00000000 (0)	
	omputerName	Authentication P	REG_MULTI_SZ	msv1_0	
		Bounds	REG_BINARY	00 30 00 00 00 20 00 00	
	asbCoptrol	📆 crashonauditfail	REG_DWORD	0×00000000 (0)	
	riticalDeviceD	disabledomaincreds	REG_DWORD	0×00000000 (0)	
🕀 🧰 De	eviceClasses	👸 everyoneincludes	REG_DWORD	0×00000000 (0)	
- 🛅 Fil	leSystem	Contraction of the second seco	REG_DWORD	0×00000000 (0)	
🕀 🧰 Gr	aphicsDrivers	orceguest 🔣	REG_DWORD	0×00000001 (1)	
- 🧰 Gr	oupOrderList	fullprivilegeauditing	REG_BINARY	00	
🕀 🧰 H4	AL I	👪 ImpersonatePrivil	REG_DWORD	0×00000001 (1)	
🧰 hiv	velist	👪 limitblankpasswor	REG_DWORD	0×00000001 (1)	
🕀 🧰 ID	ConfigDB	Imcompatibilitylevel	REG_DWORD	0×00000000 (0)	
🕀 🧰 Ke	eyboard Layo	👪 LsaPid	REG_DWORD	0×000002ec (748)	
🕀 📃 Ke	eyboard Layo	式 nodefaultadmino	REG_DWORD	0×00000001 (1)	
• <u> </u>	a	💐 nolmhash	REG_DWORD	0×00000000 (0)	
	ediaCategorie	Notification Pack	REG_MULTI_SZ	scecli	
	ediaInterface ediaBroportio	- Contraction and the second s	REG_DWORD	0×00000000 (0)	
E B Me	ediaResource	Restrictanonymou	REG_DWORD	0×00000001 (1)	

Figura 1.1

Archivo	Edición Ver Favoritos Ayud	а				
	Nuevo	•	Clave		1	Datos
	Permisos Eliminar Supr Cambiar nombre Coniar nombre de clave		Valor alfanumérico Valor binario Valor DWORD Valor de cadena m Valor de cadena e) últiple ×pandible	52	(valor no establecido) 0×00000000 (0) msv1_0 00 30 00 00 00 20 00 00 0×00000000 (0)
			usabicuomainercus		1	0×00000000 (0)
	Buscar Ctri-	FВ	everyoneincludes	REG_DWORD		0×00000000 (0)
	GraphicsDriver: GroupOrderList HAL HAL Inivelist ConfigDB Keyboard Layo Keyboard Layo Keyboard Layo MediaCategorie	(\$) (20 (20 (20 (20 (20 (20 (20 (20	Forceguest Jullprivilegeauditing ImpersonatePrivil Imitblankpasswor Imcompatibilitylevel LsaPid nodefaultadmino Nodefaultadmino Notification Pack	REG_DWORD REG_BINARY REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_MULTI_S	52	0x00000001 (1) 00 0x00000001 (1) 0x00000000 (1) 0x00000000 (0) 0x0000002ec (748) 0x00000001 (1) 0x00000000 (0) seceli
	MediaInterface MediaPropertie MediaPropertie	01	restrictanonymous restrictanonymou	REG_DWORD REG_DWORD		0x00000000 (0) 0x00000001 (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.

	- 		
	Nombre Tipa)	Datos
	(Predeterminado) REG	_SZ	(valor no establecido)
Editar valor DWORD	2 🔀	DWORD	0×00000000 (0)
		MULTI_SZ	msv1_0
Nombre de valor:		BINARY	00 30 00 00 00 20 00 00
nolmhash		DWORD	0×00000000 (0)
		DWORD	0×00000000 (0)
Información del valor:	Base	DWORD	0×00000000 (0)
1	 Hexadecimal 	DWORD	0×00000000 (0)
	O Decimal	DWORD	0×00000001 (1)
	<u> </u>	BINARY	00
	Accelus Consulta	DWORD	0×00000001 (1)
	Aceptar Lancelar	DWORD	0×00000001 (1)
		DWORD	0×00000000 (0)
🕀 🦲 Keyboard Layo	🔣 LsaPid REG	_DWORD	0x000002ec (748)
🕀 📃 Keyboard Layo	🛛 💐 nodefaultadmino REG	_DWORD	0×00000001 (1)
🕀 🔁 Lsa	🔣 nolmhash 🛛 🛛 REG.	_DWORD	0×00000000 (0)
🖽 🛄 MediaCategoria	Notification Pack REG	_MULTI_SZ	scecli
HediaInterface	📗 🕮 restrictanonymous 🛛 REG	_DWORD	0×00000000 (0)
MediaPropertie	REG.	_DWORD	0×00000001 (1)

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.