Tugas Keamanan Jaringan Komputer



Nama	:	WahyuniOktarina
NIM	:	09011181419027
Kelas	:	SK8 PIL
DosenPembimbing	:	DerisStiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2017

HACK SISTEM OPERASI WINDOWS 7

Pwdump

Pwdump adalah nama dari berbagai program Windows yang output LM dan password NTLM hash dari akun pengguna lokal dari Account Manager Security (SAM). Dalam rangka untuk bekerja, itu harus dijalankan di bawah account Administrator, atau dapat mengakses account Administrator pada komputer di mana hash harus dibuang. Pwdump bisa dikatakan membahayakan keamanan karena bisa memungkinkan administrator berbahaya untuk mengakses password pengguna. Sebagian besar program-program ini open-source.

Cain & Abel

Cain & Abel adalah pemulihan password alat untuk Microsoft Sistem Operasi. Hal ini memungkinkan pemulihan mudah berbagai jenis password dengan mengendus jaringan, cracking password terenkripsi menggunakan Dictionary, Brute-Force dan serangan pembacaan sandi, rekaman percakapan VoIP, decoding password orak-arik, memulihkan kunci jaringan nirkabel, mengungkapkan kotak password, mengungkap password cache dan menganalisis routing yang protokol. Program ini tidak mengeksploitasi kerentanan software atau bug yang tidak dapat diperbaiki dengan sedikit usaha. Ini mencakup beberapa aspek keamanan / kelemahan hadir dalam standar protokol, metode otentikasi dan mekanisme caching; tujuan utamanya adalah pemulihan disederhanakan password dan kredensial dari berbagai sumber, namun juga kapal beberapa "non standard" utilitas untuk pengguna Microsoft Windows.

Hacking password dari dalam :

Langkah pertama dengan membuka command prompt via run as administrator, setelah itu memanggil pwdump yang kali ini menggunakan versi 7.1. Perintahkan pwdump menjalankan aplikasi .exe nya agar hash password pada komputer bisa didapatkan. Kemudian hash password tersebut ubah menjadi pass_coba.txt seperti gambar dibawah ini.



Langkah kedua jalankan Cain & Abel via run as administrator. Kemudian dibagian menu pilih "cracker" dan pada menu cracker pilih "LM & NTLM Hashes (0)" seperti gambar dibawah ini.

Computer	▶ yuhuuuu (D:) ▶ Hacking Tools ▶ Cain and Abel ▶				👻 🐓 Search Cain	and Abel
Organize 👻 📑 Open	Burn New folder	dified Two Circ				
Favorites	File View Configure Tools Help					
Recent Places	⊇ • ↔ ↔ 職 職 早 + ♡ ⊌	P. 🕥 🚥 📟 📧 📾 🚍 🧐 🖉	1 ? 1			
🥽 Libraries	🔔 Decoders 🔮 Network 🏟 Sniffer 🥑 Cracke	er 🔕 Traceroute 🔜 CCDU 😵 Wirele	ss D Query			
Documents J Music Pictures Videos	Image: Second	LM Password < 8 NT Password	LM Hash NT Hash	challenge	Type Note	
🐏 Computer 🏜 Local Disk (C:) 👝 yuhuuuu (D:)	Cisco IOS-MDS H Cisco PIX-MDS H Gisco PIX-MDS Hash GRAM-MDS Hash GPC RAM-MDS Hash OSPF-MDS Hash GSPF-MDS Hash					
🗣 Network						
	Kerb5 PreAuth Ha +				•	
	http://www.oxid.it	2			ĥ.	
CA Date Application	modified: 8/3/2016 11:30 AM Date created: 3/20/20 Size: 7.86 MB	18 11:46 AM				
📀 🧷 🔚	0 0 0				- 🕅	12:33 PM ∰ .all ♠) 12:33 PM 3/20/2018

Langkah ketiga pilih "add to list" dan masukkan pass_coba.txt tadi ke bagian "import hashes from a text file".



Langkah keempat pada user "emzikrillah" klik kanan mouse lalu pilih "Bruce-Force Attack dan pilih "NTLM Hashes"

cycle Bin SMADA	Can Can Can	
Acrobat ader DC Broadban	File View Configure Tools Help File View Configure Tools Help File Sime Bile Bile Sime Sime Bile	
ctivators CodeBloc	Cracker User Name LM Password K NT Password LM Hash NT Hash challenge Type Note Status Country Countr	
adguard Google Chrome	Image: Circo IOS-MOS H Brute-Force Attack Image: Circo IOS-MOS H Image: Circo IOS-MOS H Cryptanalysis Attack Image: Circo IOS-MOS H Image: Circo IOS-MOS Hash Cryptanalysis Attack Image: Circo IOS-MOS Hash Image: CRAM-MOS Hash Rainbowcrack-Online NTLM Hashes Image: CRAM-MOS Hash ActiveSync NTLM Hashes + challenge Image: CRAM-MOS Hash ActiveSync NTLM Session Security Hashes	
on Quick LINE Menu		
India Sec.	Part SHA-2 Hashes (0) Remove Delete Remove Delete Remove Machine Accounts C KebS PreAuth Ha Remove All Image: A transmission of the transmissin of the transmission of the transmission of the transmis	
andeley esktop	+ 378, 409px 11 819 × 460px 100% © - 0 •	
e	🔚 🔍 🗘 🛷 🖪 🛷	12:34 (1) 3/20

Selanjutnya akan muncul menu seperti gambar dibawah ini.

Bin SMADAV	Cain ain Untitled - Paint	X
at Try AOL fo DC Broadban	File View Configure Taske Make Pail Pail Pail Bute-Force Attack Pail Decoders Network Pail Cracker UserN Pail Pail NLMx/L Pail Pail NLMx/L Pail Pail NLMx/L Pail Pail Pail Pail Pail NLMx/L Pail Pail Pail Pail	Assword length Max 9 + NTLM NTLM
Lard Coople Coople Chrome Line U	■ Ciscs IOS-MDS H F ■ Ciscs IOS-MDS H 104461663716084 ● CRAM-MDS Hashe 104461663716084 ● CRAM-MDS Hashe Tme Left ● CRAM-MDS Hashe F ● CRAM-MDS Hashe F ● CRAM-MDS Hashe F ● VRP-HMSC Hashe F ● VRP-HMSC Hashe F ● VRP-HMSC Hashe F ● VRD-HAshe	
Phototes	Star2 Hashes (0) K RIPEMD-100 Hash KerbS Preduth Ha ~ M Http://www.oxid.it	t Exit
lay Winamp	+ 1⊡ 1⊡ 819 × 460px	· • • • • • • • • • • • • • • • • • • •

Langkah kelima pada bagian "charset" pilih "predefined" dan masukkan pola karakter yang digunakan hash password. Penulis memilih karakter abjad kecil supaya memudahkan serangan brute-force, password length juga kita minimalkan menjadi seperti gambar diatas agar estimasi waktu yang terpakai tidak terlalu lama. Setelah itu klik start kemudian tunggu hingga password komputer didapatkan seperti gambar diatas.

Hacking password dari luar :

1. Dengan mencoba masuk kedalam sistem boot dengan USB



2. Dan masuk ke dalam Sysyem Recovery Options, dan menekan Load Driver

a sy	stem Recovery Option	s		×	
•	Use recovery tools that of Select an operating system If your operating system install drivers for your ha	can help fix problems s em to repair. Isn't listed, click Load [Ird disks.	tarting Windows. Drivers and then		
	Operating System Windows 7	Partition Size 99898 MB	(D:) Local Disk		
ŕ	Restore your computer u earlier.	Load Driver	s Next >		

3. Dan mengcopy file cmd dan mengganti namanya dengan utilnet

Use recovery to Select an onera			
and the second se	iols that can help fix problems starting Window	s.	
Open	the sector to repar		
Look in:	System 32	- 010	HFF -
Ca	Name -	- Date modified -	Туре
3	UtoResources.dll	1/10/2017 5:04 PM	Application es
Recent Places	🖲 utidi.di	7/13/2009 5:41 PM	Application e.
	In utiman	11/20/2010 7:23	Application
	Utima city	3/1-2/2000 5:39 PM	Application
Lbraries	Company: Microsoft Corporation	9 5:41 PM	Application es
	CX1nit File version: 6.1.7601.17514	9 5:41 PM	Application e
	Size: 337 KB	10 7:24	Application e
Computer	S uvers di	P 5:33 PM	Application e
	S withere di	7/13/2009 5:41 PM	Application et
	NAN.dl	7/13/2009 5:41 PM	Application e
	No Vault di	11/20/2010 7:24	Application e
	No vaulto di	11/20/2010 7:24	Application es
	VaultCmd	7/13/2009 5:41 PM	Application es
	VaultCredProvider dl	7/13/2009 5:39 PM	Application
-	4]	711-37/2009 5:41 PM	Annication ex
	File name: Utiman		and the second second
		1	Oper
	and the second s		

4. Kemudian masuk lagi kedalam windows, dan memilih switch user dan mencoba masuk kedalam cmd



5. Ketika didalam cmd, maka ketikan (net user L^*) untuk mengganti password baru. Dan terlihat gambar di bawah



6. ketika sudah, maka masuk kedalam windows lagi dengan password baru

Wendowskystem	utilman.exe			
cound expires cound changeable cound required on any change password				
relations allowed gan script me grafile me directory me logen				
ound hours allowed	A11			
ecal Group Memberships Inhal Group memberships be command completed succe	#Users #Hone ssfully.			
r Windows ageten 32 >net use spe a paraword for the use stype the pastword to conf he constant completed succe	r marini * r: irn: ssfully.			
:\Vindous\system32>		Curteb Uror	and the second second	
		Switch User		

7. Maka tampilannya sebagai berikut dalam user L.

