TUGAS V

MATA KULIAH KEAMANAN JARINGAN KOMPUTER



Oleh :

Rofby Hidayadi 09011281020132

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA 2018

I. Judul Tugas

Hacking Computer Password

II. Prosedur

Untuk melakukan hack pada password komputer terdapat 2 cara, yaitu cara pertama dengan menggunakan USB Flash Drive (BIOS) dan menggunakan tool tambahan untuk mendapatkan file database SAM. Berikut ini merupakan cara kedua dengan mendapatkan file database SAM dengan menggunakan *tool* Cain & Able yang bisa didapatkan di <u>http://www.oxid.it/cain.html</u>. Adapun langkah-langkahnya adalah sebagai berikut :

- 1. Instal Cain & Able.
- 2. Setelah berhasil menginstal, bukalah aplikasi Cain & Able tersebut.
- 3. Klik menu Cracker > LM & NTLM Hashes > Klik kanan pada mouse lalu pilih add to list. Kemudian akan muncul berbagai macam user pada komputer.

File View Conf	figure Tools Help								
🗅 🏟 👶 📩 翻訳 開	¥ 🖳 🕂 🐨 🐼	P64 🕥 🔝 📟	1	🖬 🔲 % 💋	0 ? <u>i</u>				
, Decoders 🔮 Network	🙀 Sniffer 🥑 Cracker	🔕 Traceroute	L. C	CDU 😗 Wireless	D Query				
Cracker 🔨	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Туре	Note
👪 LM & NTLM Hast	X Administrator	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
- 😹 NTLMv2 Hashes (X DefaultAccount	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
MS-Cache Hashe:	🗙 Guest	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
😤 PWL files (0)	🗙 rofby	* empty *	*		AAD3B435B51	49DCA3F75622		LM & NTLM	
Cisco IOS-MD5 H	🗙 WDAGUtilityAccount	* empty *	*		AAD3B435B51	92A7AD123378		LM & NTLM	
Cisco PIX-MD5 Hi									
APOP-MD5 Hash									
🗢 CRAM-MD5 Hash									
+ OSPF-MD5 Hashe									
+ RIPv2-MD5 Hashe									
+ VRRP-HMAC Has									
🚾 VNC-3DES (0)									
md MD2 Hashes (0)									
- MD5 Hashes (0)									
SHA SHA-1 Hashes (0)									
SHA-2 Hashes (0)									
- RIPEMD-160 Hash									
(1) Kerb5 PreAuth Ha	<								

Gambar 1. Add to list user computer

4. Kemudian pilih *username* komputer, dalam hal ini adalah *username* dengan nama "rofby".

File View Con	figure Tools Help								
🖻 🏟 🕹 👬 🏙 🕅	¥ 🖳 🕇 🖗 🐱	B ₆₄ 🕙 🛲 📟	M	🖬 🔁 % 💋	0 ? İ				
Cecoders 🔮 Network	🛯 🎒 Sniffer 🥑 Cracker	🔇 Traceroute	C R	CDU 😵 Wireless	🔂 Query				
Cracker ^	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Туре	Note
🛃 LM & NTLM Hast	X Administrator	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
- 😹 NTLMv2 Hashes (X DefaultAccount	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
MS-Cache Hashe	🗙 Guest	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
PWL files (0)	X rofby	* empty *	*	1.2	AAD3B435B51	49DCA3F75622		LM & NTLM	
Cisco IOS-MD5 H	X WDAGUtilityAccount	* empty *	*		AAD3B435B51	92A7AD123378		LM & NTLM	
Cisco PIX-MD5 Hi									
APOP-MD5 Hash									
CRAM-MD5 Hash									
OSPE-MD5 Hashe									
RIPv2-MD5 Hashe									
VRRP-HMAC Has									
VNC-3DES (0)									
md MD2 Hashes (0)									
md MD4 Hashes (0)									
md MD5 Hashes (0)									
SHA SHA-1 Hashes (0)									
SHA SHA-2 Haches (0)									
R RIDEMD-160 Hack									
A Kerb5 BreAuth Ha	<								

Gambar 2. Username komputer

5. Lalu klik kanan pada *username* yang dipilih > Brute-Force Attack > NTLM Hashes > Start.

Brute-Force Attack		×
Charset Predefined abcdefghijkImnopqrstuvwxyz0123456789 Custom	▼ Passwo Min Max	ard length
Keyspace Current password 8.1860514273734411E+024		
1 hashes of type NTLM loaded Press the Start button to begin brute-force attack		
	Start	Exit

Gambar 3. Menu Brute-Force Attack

Brute-Force Attack	×
Charset	Password length Min 1
Abcdefghijklmnopqrstuvwxyz0123456789	Max 16
Keyspace	Current password
8.1860514273734411E+024	58he7
Key Rate	Time Left
6184632 Pass/Sec	4.19811e+010 years
	Stop Exit

Gambar 4. Finding password

Seperti yang diketahui perlu waktu yang lama untuk menemukan password yang cocok. Cara lain agar dapat lebih cepat menemukan passwordnya adalah dengan menggunakan Dictionary Attack yang artinya kita menyisipkan dictionary password berupa kumpulan kemungkinan password yang diharapkan merupakan password yang sebenarnya.

 Lalu klik kanan pada *username* yang dipilih > Dictionary Attack > NTLM Hashes > Add to List Dictionary Password > Start.

rie	Position				
✓ C:\Program Files (x86)\Cain\Wordlists\password.txt	92				
ey Rate	Options As Is (Password)	 			
lictionary Position	Reverse (PASS) Double (Pass - F Lowercase (PAS Uppercase (Pas	WORD - DROWSSAP 'assPass) 'SWORD - password) sword - PASSWORD)	1		
Current password	 ✓ Num. sub. perms (Pass,P4ss,Pa5s,P455P455 ☐ Case perms (Pass,pAss,pass,pass,PaSsPASS) ✓ Two numbers Hybrid Brute (Pass0Pass99) 				
Plaintext of 49DCA3F75622CE22D5600C Attack stopped! 1 of 1 hashes cracked	1B58E7C065 i	s 79	1		

Gambar 5. Password ditemukan

III. Referensi

http://www.oxid.it/cain.html