TUGAS KEAMANAN JARINGAN KOMPUTER



DISUSUN OLEH: RATIH HANDAYANI 09011181419037 DOSEN PEMBIMBING: Dr. Deris Stiawan, M.T.

JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2018

Cracking Password Sistem Operasi Windows

Pada tugas kali ini, akan dilakukan serangan terhadap password yang lemah dan tidak memakan waktu yang cukup lama untuk melakukan pencurian password dengan menggunakan software pwdump dan cain and abel. Berikut ini adalah langkah yang dilakukan untuk meretas sebuah password:

 Buka command prompt, lalu panggil folder dimana kita menyimpan pwdump. Dalam hal ini saya menyimpannya pada direktori D.



 Kemudian ubah hsh password menjadi file .txt seperti gambar berikut. Pada gambar berikut file .txt diberi nama new_hash.txt.



 Buka aplikasi cain and abel dengan cara run as administrator. Setelah itu masuk ke direktori cracker seperti gambar berikut.

coders 9 Network	ing Snitter of Cracke	r 🔕 Traceroute	CCDU & Wweless	D Query				
-	User Nome	LM Password	< 8 NT Patrovord	LM Hash	NT Hash	challenge	Туре	Not
& NTLM Hast								
WV2 Hashes (Cache Hashe-								
files (0)								
JOS-MD5 H								
K-MD5 H								
MD5 Hashi								
MDS Hashe								
MD5 Hasha								
-HMAC Hax								
-30ES (0)								
Hashes (0)								
A Hashes (0)								
A-1 Hathes (0)								
IA-2 Hashes (0)								
EMD-160 Hash	2/1						-	

4. Setelah itu pilih menu cracker LM & NTLM Hashes dan pilih tools tanda "plus". Kemudian akan muncul kotak dialog seperti gambar berikut.

 Import Hashes fr 	om local system —		
🔲 Include Pass	word History Hashe	es	
Import Hashes fr	om a text file		
			-
Import Hashes fr	om a SAM databas	se	
SAM Filename			
Boot Key (HEX)			

5. Kemudian pilih import hashes from a text file dan masukkan file .txt yang telah disimpan tadi. Lalu pilih next.

 Setelah mendapatkan hash di cain and abel kemudian pilih user yang digunakan. Disini saya menggunakan user Ratih Handayani sebagai administrator.

Decoders 9 Networ	k 🕼 Sniffer 🕜 Crack	er 🔯 Traceroute	CCDU & Wireles	D Query				
Cracker -	User Name	LM Password	< 8 NT Password	LM Hash	NT Hash	challenge	Type	Not
A LM & NTLM Hast	X Administrator	* empty * * empty *	* empty *	NO PASSWOR	471BAE5254F1 NO PASSWOR		NTLM	
PWK file: (0) Cisco 105-M05 H Cisco 105-M05 H Cisco PIX-M05 H Cisco PIX-M05 Hash CRAM-M05 Hash CRAM-M05 Hash CRAM-M05 Hash PK8P-HMAC Has VK8P-HMAC Hash VK8P-HMAC Hash WK02 Hashes (0) M05 Hashes (0)								
Y SHA-1 Hashes (0) SHA-2 Hashes (0) RIPEMD-160 Hash C KerbS PreAuth Ha +	I LM & NTLM Hashe	. [m					_

Kemudian klik kanan kursor pada Ratih Handayani lalu pilih Brute-Force Attack dan pilih NTLM Hashes. Kemudian akan muncul tampilan seperti berikut.

narset		Password length Min 1 🛨	
ibcdefghijklmnopqrstuvwxyz0123456789	Max 16 🕂		
Custom		Start from	
eyspace 8 1860514273734411F+024	Current password		
ey Rate	Time Left		
. hashes of type NTLM loaded Press the Start button to begi	n brute-force attack		

7. Setelah itu klik start dan tunggu hingga password komputer didapatkan seperti gambar berikut.

harset		Password length	
Predefined		Min 5 🛨	
abcdefghijklmnopqrstuvwxyz0123456789	Max 16 🛨		
Custom	Start from		
		ratih	
eyspace	Current password	_F : [
8.1860514273734411E+024			
ey Rate	Time Left		
Plaintext of A01F4DE2344304144 Attack stopped! 1 of 1 hashes cracked	4CA27E9411A5E397 is rat	ih	

Dapat dilihat pada gambar diatas, password yang didapatkan adalah "ratih".