TASK

1. Crack password windows.

Cracking atau meretas password windows dapat menggunakan tools-tools yang sudah ada pada saat ini, namun pada tugas kali ini salah satu tools yang digunakan adalah "pwdump" dan "cain and abel".

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.

Sedangkan cain and abel adalah alat pemulihan password 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. Langkah-langkah cracking password windows :

 Langkah pertama adalah menggunakan pwdump yang dipanggil lewat command prompt (CMD) untuk mendapatkan hash. CMD dibuka dengan cara "run administrator". Ketikkan perintah seperti gambar berikut : perintah pertama adalah untuk masuk ke direktori atau tempat penyimpanan pwdump. Lalu jalankan pwdump.exe lewat command prom dan buat hash dalam bentuk .txt.



2. Langkah kedua setelah di dapatkan hash, buka aplikasi cain and abel yang sudah diinstall terlebih dahulu. Lalu pilih menu cracker seperti pada gambar dan pilih LM & NTML Hash.

3 珍 😚 🎄 際 際 📮 🕂 珍 🔞 🗜 🐿 🛤 🖼 🗃 🚍 俊 👂 ? 🧵											
ecoders 🔮 Network	c 📦 Sniffer 🥑 Cracke	r 🔕 Traceroute	🔜 CCDU 😵 Wirele	ss 🚯 Query							
icker 🔺	User Name	LM Password	< 8 NT Password	LM Hash	NT Hash	challenge	Туре	Note			
LM & NTLM Hast											
NTLMv2 Hashes (											
MS-Cache Hashe											
PWL files (0)											
Cisco IOS-MD5 H											
Cisco PIX-MD5 Hi											
APOP-MD5 Hash											
CRAM-MD5 Hash											
OSPE-MD5 Hashe											
RIPv2-MD5 Hashe											
VRRP-HMAC Has											
VINC-SDES (0)											
MD2 Hashes (0)											
MD4 Hashes (0)											
CUA 1 Hashes (0)											
SHA-1 Hashes (0)											
RIDEMD-160 Hack											
KarbS BreAuth Ha											
Radius Shared-Ke											
IKE-PSK Hashes (f											
MSSOL Hashes (0											
MySQL Hashes (0											
Oracle Hashes (0)											
(0)											

3. Langkah ketiga adalah klik tanda "plus" di atas, untuk membuka tempat penyimpanan hash yang tadi sudah di dapatkan. Jika berhasil, tampilan akan berubah seperti gambar di bawah :

3 • 鈔 😔 読 職 職 副 🗍 🕂 ⑧   Decoders 🔮 Network 🗐 Sniffer 🥑 Cr Cracker 🔹 User Name	😼 🗟 🚱 🕅	1 📟 🗟 🗃 🖨 😻 🖄	6 2 1					
Decoders Vetwork Sniffer of Ci Cracker	acker 🚺 💶 Tracero	<b>0</b> .0						
-   User Inditie	LAA Dassword	oute MicCDU & Wirele	ss 🗊 Query	NT Hade	challenge	Tune	Note	
A LM & NTLM Hast	LIVI Password	d < o INT Password	LIVI Hash	INT masn	challenge	Туре	Note	
NTLM/2 Hashes (								
MS-Cache Hasher		Add NT Hather from		×				
PWI files (0)		Add HT Hashes Holl						
Cisco IOS-MD5 H		C Import Hashes from	local system					
Cisco PIX-MD5 Hi		Linckide Passwo						
APOP-MD5 Hash		1 1100000 1 00070						
CRAM-MD5 Hash		<ul> <li>Import Hashes from</li> </ul>	a text file					
OSPF-MD5 Hashe		I:\Hacking Tools\Pw	dump\new hash.txt					
RIPv2-MD5 Hashe								
VRRP-HMAC Has		C Import Hashes from	a SAM database					
VNC-3DES (0)		SAM Filename						
2 MD2 Hashes (0)								
📬 MD4 Hashes (0)								
💕 MD5 Hashes (0)		Boot Key (HEX)						
MA SHA-1 Hashes (0)								
뿔 SHA-2 Hashes (0)								
RIPEMD-160 Hash			Cano	el Next->				
🕉 Kerb5 PreAuth Ha								
💑 Radius Shared-Ke								
IKE-PSK Hashes (C								
MSSQL Hashes (0								
D MySQL Hashes (0								
D Oracle Hashes (0)								
D Oracle TNS Hashe								
💰 SIP Hashes (0) 👻			1		1	1		
III III IIII IIIIIIIIIIIIIIIIIIIIIIIII	asnes							

4. Langkah keempat adalah klik next dan tampilan akan tampak seperti gambar di bawah. Lalu pilih user mana yang tadi kita ingin crack passwordnya. Setelah itu pilih brute force attack dan NTLM Hashes.

ork 🛍 Sniffer 🦪 (	racker	🛄 CCDU 🕅 Wirel						
User Name	LM Password	< 8 NT Password	LM Hash	NT Hash	challenge	Type	Note	
Administrator	* empty *	* empty *	NO PASSWOR	31D6CFE0D16		NTLM		
Guest	* empty *	* empty *	NO PASSWOR	NO PASSWOR				
🗙 ХВее	* amnh/ *		NO PASSWOR	33EDCEB87A79		NTLM		
K HomeGroupUs	Dictionary Attack	· 上	NO PASSWOR	D0A58F3FA0E7	_	NTLM		
	Brute-Force Attack	+	LM Hashes					
	Cryptanalysis Attack	+	LM Hashes + challe	nge				
			NTLM Hashes					
	Rainbowcrack-Online	•	NTI M Hashes + ch	allenge				
	ActiveSync	•	NTLM Session Secu	rity Hashes				
	Select All							
	Select Mil							
	ivote							
	Test password							
	Add to list	Insert						
	Remove	Delete						
	Remove Machine Acces	unte						
	Remove Machine Acco	ints						
	Kemove All							
	Export							

5. Langkah kelima setelah muncul tampilan seperti gambar di bawah adalah mengisi beberapa kemungkinan yang di dapat dari instuisi seperti password length atau start from lalu klik start.

oderr 🥝 Network 🕅	Sniffer		Es Ouer		
er A Userl	Name Brute-Fo	rce Attack		×	Note
M & NTLM Hast	ministratorChara	al		- Recovered length	1
TLMv2 Hashes ( 🛛 🕅 Gu	est	et		Password length	
IS-Cache Hashe: 🕺 🕅 XB	ee (* P	redefined		Min 1 🗄	и
WL files (0) 🛛 🗙 Ho	meGroupUserS	lalakik kapagastu unun	-	Max 16 -	и
isco IOS-MD5 H	Internet in the second s	angripan napatsawakyz	<u>•</u>		
isco PIX-MD5 Hi	C C	ustom		Start from	
POP-MD5 Hash					
RAM-MD5 Hash					
SPF-MD5 Hashe	Keysp	ace	Current password		
Pv2-MD5 Hashe		45353092615406036000000			
RRP-HMAC Has	Kauf	hate.	Time Lab		
NC-3DES (0)	Noy r	late	Tille Leit		
ID2 Hashes (0)					
ID4 Hashes (0)					
ID5 Hashes (0)	1 h	ashes of type NTLM loaded			
HA-1 Hashes (0)	Pre	ss the Start button to begi	h brute-force attack		
HA-2 Hashes (0)					
PEMD-160 Hash					
erb5 PreAuth Ha					
adius Shared-Ke					
E-PSK Hashes (C					
ISSOL Hashes (0				Start Exit	
VSOL Hashes (0					
racle Hashes (0)					
(0)					

6. Langkah terakhir adalah menunggu sampai di dapatkan password seperti gambar di bawah.

ecoders 🔮 Netwo	k 🛍 Sniffer 🥑 Crack	er 🔕 Traceroute 🕅 CCDU 🕅 Wireless	To Query			
acker 🔺	User Name	Brute-Force Attack	and at the	×	Note	
LM & NTLM Hast NTLMv2 Hashes (	Administrator	Charset		Password length	и	
MS-Cache Hashe	XBee	Predefined		Min 1 🛨	и	
PWL files (0)	X HomeGroupUser\$	abcdefghiikImnopgrstuvwsvz	•	Max 16 🕂	и	
Cisco IOS-MD5 H		C. Duston		- Start from		
APOP-MD5 Harba		Custom				
CRAM-MD5 Hash		Į				
OSPF-MD5 Hashe		Keyspace	Current password			
RIPv2-MD5 Hashe		45353092615406036000000				
VRRP-HMAC Has		Key Rate	Time Left			
VNC-3DES (0)						
MD4 Hashes (0)						
MD5 Hashes (0)		Plaintext of 33EDCEB87A79F89DAD	880D936654C6A4 is xbee	eproo		
SHA-1 Hashes (0)		Attack stopped! 1 of 1 hashes cracked				
SHA-2 Hashes (0)						
RIPEMD-160 Hash						
Radius Shared-Ke						
IKE-PSK Hashes (C						
MSSQL Hashes (0				Start Exit		
MySQL Hashes (0)						