## 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 adalah cara pertama dengan menggunakan USB Flash Drive (BIOS) dengan tools Trinity Rescue Kit. Adapun langkah-langkahnya adalah sebagai berikut :

- 1. Download ISO tools Trinity Rescue Kit.
- 2. Kemudian Burn ISO tools Trinity Rescue Kit yang telah didownload ke USB Flash Drive.

	YUMI 2.0.2.0 Setup Drive Selection and Distro Options Page Choose your Flash Drive, and a Distro, ISO/ZIP file. Additional Distributions can be added each time this too	- □ × Pendrivelinux.com YUMI
	Step 1: You Selected E: as your USB Device E:\KINGSTON 14GB \ Show All Drives? Step 2: Select a Distribution to put on E: Trinity Rescue Kit \ Step 3 PENDING: Browse to your trinity-rescue-kit*.iso D:\Received\trinity-rescue-kit.3.4-build-372.iso	View or Remove Installed Distros? Format E: Drive (Erase Content)? Local iso Selected. Visit the TRK Home Page Show All ISOs? Browse
YI	Click HERE to visit the YUMI page for additional Help!	Create Cancel

Gambar 1. Proses Burning ISO tools Trinity Rescue Kit

- 3. Lalu, masukkan USB Flash Drive ke PC/laptop target (PC/laptop dalam keadaan mati).
- Selanjutnya, hidupkan PC/laptop target dan masuk ke menu BIOS dengan cara menekan F2 atau F10 (tergantung jenis PC/laptop target). Dilanjutkan memilih BOOT menu, kemudian aturlah agar system reboot dari USB Flash Drive.



Gambar 2. Menu BIOS PC/Laptop Target

5. Kemudian simpan pengaturan tersebut dilanjutkan dengan reboot system.



Gambar 3. Tampilan Setelah System Reboot

 Lalu, pilih system tools yang dilanjutkan dengan memilih tools Trinity Rescue Kit.



Gambar 4. Tampilan Setelah System Tools

7. Selanjutnya, otomatis tools Trinity Rescue Kit akan running dan mencari file TRK USB Flash Drive.

Trini	ty Rescue Kit 3.4 build 372
Run Triv	ity Rescue Kit 3.4 (default mode, with text more)
1 : TRK	3.4 in failsafe mode (No menu, VGA, noacpi, noapic
Z : TRK	3.4 running from RAM (best >= 512mb, 256mb min)
3 : TRK	3.4 - Run 'mclone' in client mode (!)
4 : TRK	3.4 in simple VGA mode (debugging of kernel output
5 : TRK	3.4 with Belgian keyboard (use menu for other)
6 : TRK	3.4 - Virusscan all drives (Clamav, non interactiv
7 : TRK	3.4 - Try more pencia and usb nics (when not detec
B TRK	3.4 - Try more SCSI drivers (when disks not detect
O . TRK	3.4 with a secure shell server enabled
10. TPK	3.4 - Execute local scripts on harddrive of PD
11. TPK	3 4 as bootserver to boot other TRK clients
12. TDK	3 4 - Fileshare all drives as guest, no security
12. TRN	34 - Single user mode (no menu)
13: IKK	3.4 - Acpi=off, noapic PCI=bios (Hiterhate boot
14: IRK	3.4 - Acni=off, noapic PCI=any CHIternate out
15: IRK	3.4 - PCI=conf2 (Alternate boot 3)
16: TRK	3.4 - Verbose startup for debugging unb mean
16: TRK	3.4 - Verbose startup for debugging und ment

Gambar 5. Menu Tools Trinity Rescue Kit

8. Setelah beberapa saat, akhirnya ditemukanlah Trinity Rescue Kit USB Flash Drive yang dimaksud.



Gambar 7. Trinity Rescue Kit USB Flash Drive

9. Selanjutnya, ketikkan sdb1 pada console.



Gambar 8. Ketikkan sdb1 Pada Console

10. Kemudian, sistem akan otomatis masuk ke Trinity Rescue Kit Easy Menu. Lalu, pilih Windows Password Resetting.



Gambar 9. Trinity Rescue Kit Easy Menu

11. Lalu, pilih Reset Password On Build-in Administrator (Default Action).



Gambar 10. Menu Reset Password

12. Lalu, tools Trinity Rescue Kit akan mencari letak File System Windows PC/laptop target yang akan direset passwordnya. Disini ditemukan dilokasi 1 yaitu berisi data sda2/windows. Selanjutnya, ketikkan 1 pada console.



Gambar 11. File System Windows PC/Laptop Target

13. Kemudian secara otomatis akan masuk ke User Edit Menu. Lalu, ketikkan 1 untuk memilih Clear (Blank) User Password pada console.



Gambar 12. Clear (Blank) User Password

14. Selanjutnya, keluar dari tools Trinity Rescue Kit dan lakukan reboot pada PC/laptop target (jangan lupa untuk mengubah kembali pengaturan BOOT pada Menu BIOS ke default). Maka, PC/laptop target yang awalnya memiliki password, setelah dilakukan langkah-langkah diatas password tersebut akan hilang atau clear. 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.

	≝ ∰  ] <b>+</b> ⊗   ₩	le₄ №] IIII III	· •						
Decoders 💆 Network	📓 Sniffer 🥑 Cracke	r 🔯 Traceroute	C III	CDU 😗 Wirele	is 🚯 Query	1			
Cracker ^	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Not
LM & NTLM Hast	🗙 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	X 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)									
MD2 Hashes (0)									
MD4 Hashes (0)									
MD5 Hashes (0)									
SHA-1 Hashes (0)									
SHA-2 Hashes (0)									
R RIDEMD-160 Hart									
60 RIPEIVID-TOU Hast									

Gambar 1. Add to list user computer

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

File View Con	ifigure Tools Help								
🛛 🛥 🔹 🐼 🏙 🖁	# 🖼   🕂 🔊   🖻	P. 1	•	🖬 🔲 % 💋	<b>1</b> % <b>0</b>				
💰 Decoders 🔮 Network	k 🔹 Sniffer 🥑 Cracke	r 🔯 Traceroute	IN C	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	
	🗙 Guest	* empty *	*	* empty *	AAD3B435B51	31D6CFE0D16		LM & NTLM	
PWL files (0)	X rofby	* empty *	*		AAD3B435B51	49DCA3F75622		LM & NTLM	
Cisco IOS-MD5 H	X WDAGUtilityAccount	* empty *	*		AAD3B435B51	92A7AD123378		LM & NTLM	
Cisco PIX-MD5 Ha									
APOP-MD5 Hash									
CRAM-MD5 Hash									
OSPF-MD5 Hashe									
RIPv2-MD5 Hashe									
VRRP-HMAC Has									
VNC-3DES (0)									
MD2 Hashes (0)									
MD4 Hashes (0)									
MD5 Hashes (0)									
SHA SHA-1 Hashes (0)									
SHA-2 Hashes (0)									
RIPEMD-160 Hash									
() Kerb5 PreAuth Ha	<								>
< · · · · · · · · · · · · · · · · · · ·	LM & NTLM Hashes								
http://www.oxid.it									

Gambar 2. Username komputer

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

Charset Predefined abcdefghijklmnopqrstuvwxyz0123456789 Custom	<u>.</u>	Passwo Min Max	rd length
Keyspace 8.1860514273734411E+024 Key Rate	Current password		
1 hashes of type NTLM loaded Press the Start button to begin bu	rute-force attack		
	[	Start	Exit

Gambar 3. Menu Brute-Force Attack

Brute-Force Attack					
Charset © Predefined abcdefghijklmnopqrstuvwxyz0123456789	×	Password length Min 1			
Keyspace 8.1860514273734411E+024	Current password 58h	e7			
Key Rate 6184632 Pass/Sec	Time Left 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.

 $\times$ 

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

File		Position		
C:\Program Files (x86)\Cain\Wordlists\password.txt		92		
Key Rate	Optic	ons		
Dictionary Position		Reverse (PASS) )ouble (Pass - F .owercase (PAS Jppercase (Pas	VORD - DROWSSA 'assPass) SWORD - password sword - PASSWORD	P) ))
Current password		Num. sub. perms Case perms (Pas Two numbers Hy	: (Pass,P4ss,Pa5s,) s,pAss,paSs,PaSs /brid Brute (Pass0)	P45sP455 PASS) Pass99)
Plaintext of 49DCA3F75622CE22D560 Attack stopped! 1 of 1 hashes cracked	0C1B9	58E7C065 i	s 79	1

Gambar 5. Password ditemukan

III. Referensi

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