Hacking with ProRat

Muhammad Fikri Hidayatullah

muhammadfikri.uad@gmail.com http://cari-info.blogspot.com

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Bagi kamu yang suka iseng ngejahilin komputer teman, nih aku kasih tools yang cocok buat kamu. Namanya ProRat. ProRat adalah salah satu tool hacking yang sangat luar biasa sekali. Tools ini buatan orang Turkey. Tools ini berfungsi untuk menyusup ke komputer orang lain. Caranya sangat gampang dan mudah sekali, tinggal kita mengetahui IP dan Port komputer korban saja, maka kita dapat langsung menginfeksinya.

A. Cara penggunaan ProRat :

 Pertama kali kita harus mengetahui terlebih dahulu IP dan Port korban yang terbuka. Kita dapat melakukannya dengan cara manual atau juga dengan bantuan tool Ports Scanner.

Ikatlah limu dengan menuliskannya



Dari gambar diatas kita mengetahui semua IP komputer yang aktif dan Port mana saja yang terbuka. Yang akan dijadikan korban pada percobaan kita kali ini adalah komputer dengan IP 192.162.10.233.

2. Langkah selanjutnya yaitu kita jalankan ProRat, tools ini dapat kamu download di <u>http://www.prorat.net</u>. Sebelumnya matiin dulu Anti Virus kamu (*disable*), karena ProRat akan terdeteksi sebagai virus. Padahal dia tidak berbahaya bagi komputer kita. Setelah itu isikan IP korban pada form IP dan Portnya (default 5110).

Ikatlah limu dengan menuliskannya



Apabila kita klik tombol *Connect* maka koneksi ke komputer korban belum bisa, karena komputer korban belum kita infeksi. Untuk menginfeksi komputer korban kita terlebih dahulu membuat server yang akan dijalankan pada komputer korban. Caranya klik tombol *Create – Create Prorat Server*. Lalu muncul tampilan *Notifications* :

Ikatlah limu dengan menuliskannya

Notifications ProConne General Settings IP (DNS) Bind with File Mail Notif Server Extensions ICQ Page Doesn't Use II Server Icon ICQ UIN: CGI Notif Doesn't	ective Notification (Network and Router) s Reverse Connection ProConnective Notification Address: 192.168.10.232 fication support Reverse Connection Mail Notification Test muhammadfikri@mail.org
General Settings IP (DNS) Mail Notif Doesn't Use N E-MAIL : ICQ Page Doesn't Use II ICQ UIN: CGI Notif Doesn't	Address: 192.168.10.232
Bind with File Bind w	fication support Reverse Connection Mail Notification Test muhammadfikri@mail.org
Server Extensions	muhammadhkri@mail.org
Server Icon ICQ UIN: CGI Notif Doesn't	er Notification
CGI Notif Doesn't	support Reverse Connection CQ Pager Notification 157116797
Help GI URL:	fication support Reverse Connection CGI Notification Test
Server Size: 342 Kbayt	rauzi.web.id

Centang pilihan *Use Proconnective Notifications* dan isi *IP(DNS)Address* dengan IP kita.

Pada tab *General Setting* kita isikan Server Port (default 5110), Server Password dan *Victim Name*.

Ikatlah limu dengan menuliskannya

Create Server			_ ×
Notifications	Server Port:	5110	
	Server Password:	123456	
General Settings	Victim Name:	korban	
	🔽 Give a fake en	ror message.	Configure
Pind with File	Melt server on	install.	
	Kill AV-FW on	start.	
	🛛 🔽 Disable Windo	ws XP SP2 Security Cente	er
Server Extensions	🛛 I 🔽 Disable V	Windows XP Firewall.	
	🛛 🔽 Clear Windows	s XP Restore Points.	
Server Icon	📕 Don't send LAI	N notifications from (192.1	68.*.*) or (10.*.*.*)
	Protection for r	emoving Local Server	
	Invisibility		
	🛛 🔽 Hide Processe	s from All Task Managers	(9x/2k/XP)
🕜 Help	Hide Values Fi	rom All kind of Registry Edi	tors (9x/2k/XP)
	Hide Names F	rom Msconfig (9x/2k/XP)	
UnTerminate Process (2k/XP)]
			Cropto Sorrier
Server Size: 342 Kbay	t.		Create Server

Pada tab *Bind with File* kita dapat menyusupkan file yang akan dijalankan bersama Server. Extensi file bebas.

Ikatlah limu dengan menuliskannya

Create Server		_ ×
Notifications	Bind server with a file.	
General Settings	Select File	
Bind with File	THIS THE WILL DE DIFICED.	
Server Extensions		
Server Icon		
🕑 Help		
Server Size: 342 Kbayt		Create Server

Selanjutnya adalah tab *Server Extension*, ada beberapa pilihan extensi server. Kita pilih yang berekstensi .Exe.

IlmuKomputer.Com Ikatlah limu dengan menuliskannya

Create Server		_ ×
Notifications	Select Server Extension	SCR (Has icon support)
General Settings	PIF (Has no icon support) BAT (Has no icon support)	COM (Has no icon support)
Bind with File		
Server Extensions		
Server Icon		
🕐 Help		
Server Size: 342 Kbay	,t	Create Server

Untuk membuat icon server kita klik tab Server Icon, pilih icon apa saja yang kamu inginkan.

IlmuKomputer.Com Ikatlah Iimu dengan menuliskannya

Create Server				_ ×
Notifications			N	
General Settings	🥖 🙆 渗	👬	.	
Bind with File	😫 🎺 🌯	ا 🚵 🚯	🔊 🎉	cn_ 🕑
Server Extensions	E * *	່ 🏅 🚳 [₹!≥	in 1997 (1997)
Server Icon		РНР	k 📂	Y»
🥐 Help	Server Icon:	OMB Choos	e new Icon	
Server Size: 342 Kbay	ut			Lieate Server

Langkah terakhir dari pembuatan server ini adalah klik Create Server.

Ikatlah limu dengan menuliskannya

Create Server			_ × _
Notifications			🐹 🎇
General Settings	🥖 🙆 🐐	ف 📾 🌶	<u>i, i, i</u>
Bind with File	2 🎺 🐌 🦉) 🔊 💰	🎇 🔤 🕑
Server Extensions			
Server Icon] 🚍 🤻	/// Y >//
🥑 Help			•
	Server Icon: 80MB	Choose new	lcon
Server Size: 342 Kbay	t		Create Server

Setelah berhasil, akan tampil :



server yang sudah jadi

- Kita tinggal menjalankan Server tersebut dikomputer korban. Caranya terserah kamu... mau disusupkan diam-diam atau memakai teknik *Social Engineering* (ajaran Mas Fauzi) dan juga dapat kamu infeksikan langsung pada komputer tersebut (kalo bias sihh).
- 4. Setelah Server tersebut berhasil berjalan pada komputer korban, maka kita langsung mencoba mengkoneksikannya dengan komputer kita.

5. Untuk koneksi kita dapat menggunakan ProConnective atau langsung mengetikkan IP address dan Port komputer korban. ProConnective adalah tools bawaan dari ProRat yang berfungsi sebagai *Bridge* (jembatan koneksi) antara komputer server dan komputer client (korban). Akan nampak IP korban apabila dia sedang on.



6. Setelah berhasil melakukan koneksi ke komputer korban maka status dari ProRat akan berubah dari *Disconnected* ke *Connected*

Ikatlah limu dengan menuliskannya



- Nah...saatnya kita bermain. Ada banyak hal yang dapat kita lakukan pada komputer korban seperti mengetahui informasi dari PC, mengirimkan pesan error, mematikan komputer, mengunci mouse, membuka CD-ROM atau bahkan memotret wajah korban.
- 8. Sekarang kita akan melihat *PC info* korban :

Ikatlah limu dengan menuliskannya

ProRat V1.9 Connected[192.168.10.233]				
PROHACH.NET PROFESSIONAL INTERNET !!!				
lp: <mark>192.168.</mark> 1	10.233 Po	rt: 5110 R: Discon	neo	at 🛛 😻 🍏 🤧 🕄 🥹 🛸
English		////// PC Infor	'Mi	ation /////// 🛛 💆
PC Info	Applications	Computor Namo		DTC_6790E9086D6
Message	Windows	llser Name	-	UR
Chat	Admin-FTP	Windows Ver		Microsoft Windows
Funny Stuff	File Manager	Windows Language	:	English (United St
IExplorer	Search Files	Windows Path	=	C:\WINDOWS
Control Panel	Registry	System Path	E	C:\WINDOWS\system3
Shut Down PC	Screen Shot	ProductId		55274-648-8637434-
Clipboard	KeyLogger	Workgroup		N0
Give Damage	Passwords	Data	-	6/4/2009
R. Downloder	Run		_	
Printer	Services			
Online Editor	ProConnective	System Information		Mail Address in Registry
Cre	ate	Last visited 25 web sites		🕐 Help
Pc information F	Received.			

Dari gambar diatas kita dapat melihat informasi yang dimiliki dari komputer korban.

9. Kita juga dapat mengirimkan pesan error palsu ke komputer korban :



Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com



10. Memasang Keylogger.

KeyLogger			_ = ×
[Windows title: "My Documents"]			
[Windows title: "Run"] Uripconfig rrcmd [Windows title: "Program Manager"]			
ipconfig			
[Windows title: "Run"] msconfig			0
Read Log Delete Log	Save as	Clear Screen	🕐 Help
CharSet: DEFAULT_CHARSET			
KeyLog Received.			

11. Dan yang paling seru adalah melihat wajah dari korban yang kita *hack*.

Screen Shot	X
	SENSOR
Picture quality: 📶 🔽 Open Images	Directory Show in fullscreen 🌒 Help
Screen Shot [Method1]	Screen Shot [Method2]
WebCam Shot [Method1]	WebCam Shot [Method2]
#Method1:	
e 🕍 ProRat V1.9 🖉 ProRat	V1.9 ProRat V1.9 ProRat V



Bagaimana seru kan? Itu masih sebagian kecil dari kegunaan ProRat masih banyak lagi fungsi lainnya, seperti memformat hardisk milik korban, mengacaukan registry, mencuri data-data penting dan lain sebagainya. Akan tetapi, dalam pembahasan kita kali ini kita cukupkan sekian saja ya. Ok !

Gunakan dengan baik ya...

B. Cara Pencegahan

- Update selalu Anti Virus anda agar mampu mendeteksi adanya infeksi dari ProRat. Biasanya server ProRat terdeteksi sebagai Trojan.Dropper.Prorat.DZ.29, Dropped:Backdoor.Prorat.DZ.
- Pasanglah Anti Prorat, anda bisa mendownloadnya di www.softpedia.com/get/Antivirus/Anti-prorat.shtml.

Selamat mencoba.

<u>Biografi Pe</u>nulis



Muhammad Fikri Hidayatullah. Lahir di Pekalongan, 23 oktober 1988. Menamatkan SMU di SMU N1 Kajen, pada tahun 2006. Sekarang kuliah S1 pada jurusan Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Bekerja sebagai koordinator IT pada CV.Surya Cendekia Utama Yogyakarta. Dan menyukai *web programming, desktop programming* dan *hacking*.

Aktif sebagai penulis *Blogger* pada beberapa blog. Senang bermain dengan beberapa program afiliasi dari internet. Penulis juga aktif sebagai salah satu santri Ma'had Ki Bagus Hadikusumo Sekolah Kader Muhammadiyah. Ayo berjuang...!