BAB 4

Hasil dan Pembahasan

Bab ini berisikan penjelasan yang diperoleh dari proses penelitian yang telah dilakukan berdasarkan rumusan masalah dan tujuan penelitian yang diajukan sebelumnya, yaitu: 1) Melakukan setting jaringan, 2) Simulasi *Remote Access Trojan (RAT)*, 3) Konfigurasi keamanan data, 4) Hasil pengujian *Remote Access Trojan (RAT)*.

4.1 Settingan Jaringan Router

4.1.1 Melakukan Pengaturan IP Network

Sebelum melakukan konfigurasi ke sistem, terlebih dahulu digunakan aplikasi WinBox versi 3.18. Dalam simulasi ini menggunakan 2 (dua) buah laptop yaitu laptop attacker (penyerang) dan laptop korban, juga menggunakan 2 (dua) buah MikroTik router jenis Router RB931-2nD sebagai Router A untuk laptop attacker dan RB951Ui Versi 6 untuk laptop attacker sebagai Router B untuk Settingan laptop korban. dimulai dengan aplikasi Winbox dengan mengkoneksikan admin user untuk membuat IP Address di laptop attacker dengan alamat IP Address adalah 192.168.3.1 dan IP Address laptop korban adalah 192.168.2.1 dalam gambar berikut :



Gambar 4. 1 Setting IP Address Laptop Attacker

Addres	is List		
+	- 🖉 🔛 [~ 7	Find
Ac	ddress 🛆	Network	Interface 🗸 🗸
-8	10.10.10.1/30	10.10.10.0	ether1
-8	192.168.2.1/24	192.168.2.0	ether2
2 items	1		
1			

Gambar 4. 2 Setting IP Address Laptop Korban

Tahap selanjutnya kita akan menyambungkan ke IP router baik laptop korban dengan Destination-Address 192.168.3.0/24, Gateway 10.10.10.2 dan laptop attacker dengan Destination-Address 192.168.2.0/24, Gateway 10.10.10.1, terlihat dalam topologi berikut :



Gambar 4. 3 Topologi Settingan Jaringan

IP Address pada suatu Port Router bisa juga dapat berarti Gateway pada Network. IP Gateway biasa dijadikan sebagai target dari suatu aktivitas serangan pada jaringan lokal sesuai tab informasi IP Address List masing-masing laptop. Setelah pembuatan IP Address tahap selanjutnya membuat IP Routing untuk menghubungkan ke router baik router A dan router B.

4.1.2 Melakukan Settingan Jaringan Router

Tahap berikutnya melakukan settingan jaringan IP Router baik pada Router A dengan IP Route 10.10.10.1/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.2.1/24 sebagai ether2 status DAC dan Router B dengan IP Route 10.10.10.2/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.3.1/24 sebagai ether2 status DAC. DAC artinya menunjukkan ether yang aktif dan mempunyai IP Route, sedangkan AC (*Active Static*) artinya ada sebuah *route static*.



Gambar 4. 4 Hasil Setting IP Route

Untuk mengetahui setting jaringannya berhasil dilakukan koneksi lokal dengan membuka Command Prompt lalu ping IP laptop baik laptop korban dan laptop attacker. Jika statusnya udah reply berarti settingannya sudah bisa diakses IP Address secara static.

C:4.	Administrator: Command Prompt		- ÉTI	×
C:\\ Pin Rep Rep Rep Rep	<pre>vindows\system32>ping 192.168.3. ging 192.168.3.1 with 32 bytes o ly from 192.168.3.1: bytes=32 ti g statistics for 192.168.3.1:</pre>	1 me=1ms TTL=64 me<1ms TTL=64 me<1ms TTL=64 me<1ms TTL=64 me<1ms TTL=64	A I S	
App C:\\ Pin Rep Rep Rep	Packets: Sent = 4, Received = 4 coximate round trip times in mil Minimum = 0ms, Maximum = 1ms, A Vindows\system32>ping 192.168.2. ging 192.168.2.1 with 32 bytes o ly from 192.168.2.1: bytes=32 ti ly from 192.168.2.1: bytes=32 ti ly from 192.168.2.1: bytes=32 ti	<pre>, Lost = 0 (0%] li-seconds: verage = 0ms 1 f data: me<1ms TTL=63 me<1ms TTL=63 me<1ms TTL=63 me<1ms TTL=63</pre>	loss),	
Pin App C:\	g statistics for 192.168.2.1: Packets: Sent = 4, Received = 4 roximate round trip times in mil Minimum = Oms, Maximum = Oms, A Windows\system32>	, Lost = 0 (0%] li-seconds: verage = 0ms	loss),	~

Gambar 4. 5 Setting IP Berhasil Dilakukan

Selanjutnya dilakukan penyesuaian pada terminal di Winbox untuk mengetahui status daripada IP Host setelah dilakukan pembuatan IP Route di Laptop attacker yang terlihat pada gambar berikut :



Gambar 4. 6 Status Terminal Winbox

Untuk mengetahui trafic port masing-masing jaringan dari Router A dan Router B melalui tab Interface List di Winbox, informasinya menunjukkan port di ether1 dan ether2 telah berjalan (Running) yang ditampilkan dalam kecepatan kbps masing-masing port.



Gambar 4. 7 Hasil Traffic Port Interface List

4.1.3 Simulasi Remote Access Trojan (RAT)

Untuk mengetahui cara kerja dan deteksi serangan RAT dengan melakukan pembuatan *malware* jenis trojan dengan menggunakan tools njRAT v0.6.4,

dimana dalam simulasi ini file njRAT yang digunakan sebagai contoh dalam simulasi ini. Tahap pembuatan *malware* jenis trojan ini dilakukan di laptop attacker dengan menggunakan alamat IP Address Host 192.168.3.254 dengan port 80 dan nama **Victim Hacked** dengan nama file .exe adalah **sss.exe**, seperti gambar berikut :

🏮 nj	jRAT v0.6.4	Port[80]	Online[1]	Selected[0]					- 🗆	\times
	Name		PC	User Install Date Co	ountry Operat	ting system Ca	m Ver. Ping	Ac	tive Window	
							=			
		e Files			Q (1947-044)		1 (Selection(C)			
		Tesis keker	TANGGAL 7	Builder		A	× Contraction			
		20/92/2019		Host	Port	Icon			- - - 22	
	L Z			192.168.3.254	80	Protect Process [B	SOD]	٩.		
	8	Tesis kusto Yeni an Us	jadi 30 Jar Ied last time	VicTim Name HacKed		Randomize Stub				
		an di	7,00			Registy StarUp	- 19 A			
		Progress-	17154-Nani	ExeName RAT eve	Copy		and the second s	2		
		Person or a		Directory			-roff	F		
				%TEMP%	•	Build	The the			
		Decument1				Alkara a				
		21,02,2019	7.52				Vic Tink Control			
				A		Br B		2		
						¥	ExeName	0		Сору
[User	s] [Show	Logs] [Bu	ilder] Sett	tings [About] 🔲 View	Connections[1] Up	load [0 Bytes] Downlo	ad [0 Bytes]			

Gambar 4. 8 Hasil Builder RAT

Tahap selanjutnya file **sss.exe** di copy ke laptop korban dengan double klik di desktop korban, maka akan tampil di tools njRAT dengan nama **?victim_BE4088BD**, IP Address 192.168.2.254, jenis PC Intel, User Asus, Tanggal Install tercantum dan informasi Operating System.

👳 njRAT v0.6.4 🛛 Po	ort[80] Online	e[1] Sele	cted[0]				-	- 0	Х
Name	In Pred	PC U	ser Install Date	Country	Operating system	Cam \	/er. Ping	Active Window	
? victim_BE4088BD	192.168.2.254	INTEL A	SUS 2019-02-21	-	Win 8.1 Single Language SP0 x64	Yes 0	.6.4 00		
					Knogkjuastkjuatkstjins	a luiksa			
Available F	iles								
	ris kelsen (TAHG		1474 5	ы.	(C			an Vec Pag A	ative Wite
- 1 De	e 101	~		-		ь. ^с .		[

Gambar 4. 9 Proses RAT berhasil di remote

Analisis *Remote Access Trojan* (RAT) dalam hal ini jenis *malware* njRAT pada laptop korban setelah berhasil di ambil alih oleh laptop attacker yang bisa meremote laptop korban, bukti digital yang didapatkan berupa data-data File Manager, Run File, Remote Desktop, Remote Cam, Microphone, Remote Shell, Process Manager, Registry, Keylogger, Open Chat, Get Password, Server (Update, Uninstall, Restart, Close, Disconnect, Rename), dan Open Folder.



Gambar 4. 10 Hasil Bukti Digital Laptop Korban

Diantaranya contoh sebahagian dari hasil *Remote Access Trojan* (RAT) digambarkan dalam gambar-gambar dibawah ini :



Gambar 4. 12 Hasil Remote Cam







Gambar 4. 15 Hasil Open Chat

njRAT v0.6.4 Port[80] Online[1] Selecte Name IP PC Use	d[1] Install Date Country	Operating sys	stem Cam Ver. Ping	Active Window	
? victim_BE4088BD 192.168.2.254 INTEL ASU	S 2019-02-21	Win 8.1 Single Langu	ageSP0 x64 Yes 0.6.4 00		
		24 Conference 24 Excellence 23 Second das Propie 24 Action Francis			
Tesis keken (TANGGAL 7 FE	🚯 Passwords			– 🗆 X	
20/02/2012 20.01	User	Pass	URL	App USER	
and the second second second second	13917154	13917154	https://tagihan.uii.ac.id/index.php/login	Chrome [victim_BE4088BD/A	รเ
Virsion created last time t	9 2vs23m	uganxq r5f7zj	http://superhotspot.co.id/login	Chrome Victim_BE4088BD/A	SL
01/01/15010/200	Snanystimednp@gmail.		https://accounts.google.com/ServiceLo	gin .Chrome [victim_BE4088BD/A	SI
I Findrets 13 17154-Nanny					
Verrior created from the I 21/02/2019 17.52		200		ar 23 i	
and the Mark Market Proven					
	Passwords(4)			100 C	<u>></u>
	Tablicitas()			-01	
	and the second s				
			The address of the	8	
				M. C. C.	
			La La L		
Users] [Show Logs] [Builder] [Settings] [About] View Conn	ections[1] Upload [8	Bytes] Download [8 Bytes]		

Gambar 4. 16 Hasil History Get Password

4.1.4 Konfigurasi Keamanan Data

Melakukan keamanan data daripada laptop korban maka perlu memasang firewall di IP Address laptop korban dengan cara menentukan IP Address di aplikasi Winbox \rightarrow IP \rightarrow Firewall dengan IP Address Src Address : 192.168.2.254 adalah IP Address laptop korban, Destination Address 192.168.3.254 adalah IP Address laptop attacker dengan Destination Port 80 berdasarkan lokasi port yang bisa diakses oleh njRAT dan status di tab Action **drop**, terlihat pada gambar berikut :



Gambar 4. 17 Pembuatan Firewall Traffic

4.1.5 Hasil Pengujian Remote Access Trojan (RAT)

Pengujian dilakukan untuk membuktikan bahwa apakah pemblokiran *firewall traffic* berhasil atau tidaknya, maka dilakukan kembali pengujian penyerangan ke laptop korban dengan melakukan penyerangan dari laptop attacker ke laptop korban. Kemudian dilakukan pengecekan ternyata laptop korban sudah tidak bisa deteksi lagi melalui file *malware* jenis njRAT, karena otomatis tidak bisa lagi menarik data-data atau meremote laptop korban dan dibuktikan dalam gambar berikut :



Gambar 4. 18 Hasil Pemblokiran Firewall Traffic

Pengujian dilakukan dengan menggunakan beberapa tool forensik diantaranya tools Disk Investigator yang membuktikan bahwa didalam disk terdapat file-file yang merupakan program *malware* jenis berbahaya yang berekstensi .exe. Disk Investigator menunjukkan file mana yang terdapat *malware* dengan memberikan tanda 2 (dua) warna yaitu hijau menunjukkan direktori atau folder dan warna hitam menunjukkan sebuah file. Jenis *malware* yang terjangkit di laptop korban dengan nama file sss.exe dengan size **29,696** sector, tanggal dan waktu (*timestamp*) penyerangan terjadi (*Modifed/Create*).

ite View Tools Help	Disi	c investigator -	· · · ·				
View	A A A A						
C Disk (+ Directories	Name	DOS name	Ext	Attr	ia Size	Modified	Create
Daultan	Downloads	Downloads		.d	0	12/01/2019 14:02:50	12/01/2019 1
E Desktop	desktop.ini	desktop	ini	ash	282	15/02/2018 17:23:14	15/02/2018 1
😟 🏬 Music	Edraw Max.Ink	Edraw Max	Ink	a	1.056	10/03/2018 1:40:00	10/03/2018
E Download	hosts.zip	hosts	zip	a	8.269	12/01/2019 14:18:14	12/01/2019 1
E Videos	Kamus2.Ink	Kamus2	Ink	a	1.009	16/02/2018 12:57:16	16/02/2018 1
🕀 👔 Document	LanShutDown.Ink	LanShutDown	Ink	a	1.107	05/01/2019 15:24:50	05/01/2019 1
E Local Disk (C:)	Microsoft Excel 2010.Ink	Microsoft Excel	lnk	a	2.967	16/02/2018 12:44:26	16/02/2018 1
🖻 👝 DATA (D:)	Microsoft PowerPoint 2010.Ink	Microsoft Powe	lnk	a	2.953	16/02/2018 12:44:30	16/02/2018 1
E DATA-2 (E)	Microsoft Word 2010.Ink	Microsoft Word	Ink	a	3.037	16/02/2018 12:44:34	16/02/2018 1
DVD RW prive (G	Opera Browser.Ink	Opera Browser	Ink	a	1.331	21/02/2018 16:29:22	21/02/2018 1
🖻 🥦 ASUS	Photoshop CS5.Ink	Photoshop CS5	lnk.	a	1.031	16/02/2018 12:48:40	16/02/2018 1
Downloads Dosts	PRESENTACI PROPOSAL CI.	- PRECENTACI			1.402	00/00/0010 10:40:40	00.00.0010.1
	sss.exe	\$\$\$	exe	a	29.696	22/02/2019 8:41:42	22/02/2019
	I humbs.db	Thumbs	db	ash	17.920	06/02/2019 10:40:46	06702720191
	WhatsApp.Ink	WhatsApp	Ink	a	2.226	18/10/2018 7:11:36	19/03/2018
< >	<						>
					File		

Gambar 4. 19 Analisis Tools Disk Investigator



Hasil propertis menunjukkan dalam bentuk Heksadecimal di Raw file data yang diinformasikan dalam bentuk Cluster disk file *malware* tersebut.

1 4 A		sss.exe	1	×
Raw file data	actview	Cli # #	uster In this file: This cluster: Sector#s 1124508	1 of 8 14056356 48 - 112450855
C Dec			*Next cluster:	14056357
FOfs COfs	Data	Selection POIS: 000000	Selection Se	ctor: 112450848
00000000000000000000000000000000000000	Image SA 90 00 03 00 00 B8 00 0	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	000 MZ	
000000000F0 00F0 00000000100 0100 00000000110 0110 00000000	00 00 00 00 00 10 00 00 9C 8A 00 00 4F 00 00 00 00 00 00 00 00 00 00 00 C0 00 00 00 00 00 00 00 C0 00 00 00 00 00 00	00 00<	0 00	
Start of file		Memory file (saved cl	lusters) n memory file (0 bytes)	End of file
< > <<		Add this cluster	New Save to disk	<u>0</u> k

Gambar 4. 21 Analisis Hasil Hexadecimal

Selanjutnya analisis pada tools Virus Total yang membuktikan bahwa terdapat 55 file jenis *malware* yang terdapat dalam file **sss.exe** yang berhasil dideteksi yang diinformasikan dalam gambar berikut :

55	engines detected this file		
EXE 55/68 State	-256 2654ad3460c1f71ccc37990bfdaf0429 name sss.exe size 29 KB tanalysis 2019-02-22 05:43:19 UTC	153b933f8bab435690ba4d90;	201264ef
		Arl-Awaro	Generic MSIL Bladabindi 4DC 6E902
AhnLab-V3	Trojan/Win32.Bladabindi.C202658	ALYac	Generic.MSIL.Bladabindi.4DC6F902
Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as	Arcabit	Generic.MSIL.Bladabindi.4DC6F902
Avast	MSIL:Agent-BXF [Trj]	AVG	MSIL:Agent-BXF [Trj]
Avira	TR/ATRAPS.Gen	Baidu	MSIL.Backdoor.Bladabindi.a
BitDefender	Generic.MSIL.Bladabindi.4DC6F902	CAT-QuickHeal	Backdoor.Bladabindi.AL3
ClamAV	Win,Trojan,B-468	Comodo	TrojWare.MSIL.Bladabindi.KX@52g0y5
CrowdStrike Falcon	malicious_confidence_100% (D)	Cylance	Unsafe

Gambar 4. 22 Hasil Analisis Virus Total

Hasil analisis selanjutnya dengan menggunakan aplikasi Wireshark yang memberikan informasi bagaimana akses penyerangan terjadi. Dalam Wireshark terlihat alamat IP Address yang menyerang laptop korban dengan Mikrotik Router yang tanpa akses internet.

_					-				_		
📕 *Eth	ernet	1 A A A A A A A A A A A A A A A A A A A			10					- 0	×
File Ec	lit View Go	Capture Analyze	Statistics Telephony	Wireless To	ools Help						
4 🔳	đ 💿 📘 🗄	े 🔀 🖾 🤇 👄 🔿	😫 🖲 🖢 📃 📃	⊕, ⊝, ⊜,	12						
Apply	a display filter	<ctrl-></ctrl->		_	1.1	-				Expressi	on +
No.	Time	Source	Destination	Protocol	Length Inf	,					^
664	8 284.542306	0.0.0.0	255.255.255.255	MAC-Telnet	244 64	:d1:54:94:6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
664	49 284.542820	192.168.3.254	255.255.255.255	MAC-Telnet	64 d8	:50:e6:37:3c:5c	> 64:d1:54:94:	6d:9c Direction:	Client->Server	Type: Acknowl.	
665	0 284.681545	192.168.3.254	255.255.255.255	MAC-Telnet	164 d8	:50:e6:37:3c:5c	> 64:d1:54:94:	6d:9c Direction:	Client->Server	Type: Data	
665	1 284.681881	0.0.0.0	255.255.255.255	MAC-Telnet	64 64	:d1:54:94:6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Acknowl.	
665	2 284.692888	0.0.0.0	255.255.255.255	MAC-Telnet	1514 64	:d1:5 <mark>4:94</mark> :6d:9c	> d8:50:e6:37:	3c:5c Direction	Server->Client	Type: Data	
665	3 284.693130	0.0.0	255.255.255.255	MAC-Telnet	1514 64	:d1:5 4:94 :6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
665	4 284.693132	0.0.0.0	255.255.255.255	MAC-Telnet	1514 64	:d1:5 4:94 :6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
665	5 284.693133	0.0.0.0	255.255.255.255	MAC-Telnet	1514 64	:d1:5 4:94 :6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
665	6 284.693249	0.0.0.0	255.255.255.255	MAC-Telnet	1514 64	:d1:54:94:6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
665	57 284.693377	0.0.0.0	255.255.255.255	MAC-Telnet	316 64	:d1:5 4:94 :6d:9c	> d8:50:e6:37:	3c:5c Direction:	Server->Client	Type: Data	
L 665	8 284.693551	192.168.3.254	255.255.255.255	MAC-Telnet	64 d8	:50:e6:37:3c:5c	> 64:d1:54:94:	6d:9c Direction:	Client->Server	Type: Acknowl.	
	_	-		_	_	_					
> Fram	e 1: 164 byt	es on wire (1312 b	its), 164 bytes ca	ptured (131	2 bits) or	interface 0					^
> Ethe	rnet II. Src	: AsustekC 37:3c:5	ic (d8:50:e6:37:3c:	Sc), Dst: B	coadcast (ff:ff:ff:ff:ff:	ff)		and the second s		
> Inte	rnet Protoco	l Version 4, Src:	192.168.3.254, Dst	: 255.255.2	55.255						
> User	Datagram Pr	otocol, Src Port:	65164, Dst Port: 2	:0561							
Y Mikr	olik MAC-lel	net Protocol		-							
P	rotocol vers	10n: 1									
	Vpe: Data (1)	10.50.00.00.00.00.00	-							
5	ource MAC: A	SUSTERC_37:3C:SC (as:50:e6:37:3c:5c)	4.0.0							
	estination M	AC: ROUTEPDO_94:60	:9C (64:d1:54:94:6	d:9c)	_						*
0000 1	ff ff ff ff	ff ff d8 50 e6 37	3c 5c 08 00 45 00	P	·7<\··E						
0010	00 96 19 61 0	30 00 80 11 50 50	co ao 03 fe ff ff	···a···	\p						
0020	TT TT TE 8C :	50 51 00 82 C5 39	01 01 08 50 66 3/	() d T =	·9···/						
0010	52 86 88 58 5	0f dh he 8f 1e 1d	01 30 00 00 01 03 0d a2 29 6e 03 4b	b P/							
0050	cd ec 91 ca	d9 24 d5 85 de 7a	32 82 84 ec 23 47	· · · · · § · ·	·z2···#G						
0060	e8 90 f9 ed (df 63 69 6b e8 fc	04 fa 5c d4 f5 97			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		18 - Alberton Barrier, 1990 (1990)	 A second sec second second sec	63 - C	
0070	ed d9 a0 4a	cc f7 71 8e 0e ad	89 1b 02 06 43 c1	····3···q·	· · · · · · C ·		2 6 1 6 4		100 A 100		
0080	c1 3e 60 a4 a	d6 1a e7 44 90 a5	8f 11 0c b4 f9 6b	• > * • • • D	· · · · · · · k	1. A 1. A 1.		All			
0090	91 db 4b 88 1	54 b/ae c0 d1 5e	24 cb 0b c6 37 c6	···K·4····	·^\$7-						
0080	00 0e 33 4d			- om	-						
	·										

Gambar 4. 23 Hasil Analisis Penyerangan

Hasil pada tahap pengujian mengenai keamanan pemblokiran *firewall traffic* dapat dilihat pada Gambar 4.24.

😰 Task Manager — 🗆 X									
File Options View									
Processes Performance App history Startup Users Detail	Processes Performance App history Startup Users Details Services								
^	28%	66%	2%	0%					
Name Status	CPU	Memory	Disk	Network					
📧 Runtime Broker	0%	3,4 MB	0 MB/s	0 Mbps 🔨					
🔎 Search	0%	0,8 MB	0 MB/s	0 Mbps					
> sedsvc	0%	2,6 MB	0 MB/s	0 Mbps					
Sink to receive asynchronous ca	0%	0,2 MB	0 MB/s	0 Mbps					
> 🖶 Spooler SubSystem App	0%	0,9 MB	0 MB/s	0 Mbps					
sss (32 bit)	0%	0,9 MB	0,1 MB/s	0 Mbps					
Contraction of the second seco	0%	0,5 MB	0 MB/s	0 Mbps					
WebDiscover Browser (32 bit)	0%	0,6 MB	0 MB/s	0 Mbps					
WebDiscover Browser (32 bit)	0%	1,6 MB	0 MB/s	0 Mbps					
WebDiscover Browser (32 bit)	0%	0,3 MB	0 MB/s	0 Mbps					
WebDiscover Browser (32 bit)	. 0%	4,4 MB	0 MB/s	0 Mbps					
📧 Windows Audio Device Graph Is	0%	12,1 MB	0 MB/s	0 Mbps					
Windows Defender User Interface	0%	2,7 MB	0 MB/s	0 Mbps					
Windows Shell Experience Host	0%	0,1 MB	0 MB/s	0 Mbps					
> 💽 WMI Performance Reverse Ada	0%	0,1 MB	0 MB/s	0 Mbps 🗸					
Fewer details End task									

Gambar 4. 24 Proses Task Manager

Hasil Pengujian pada saat *task manager* berjalan di CPU, *memory*, kecepatan, paket dan status *route*. Dimana kondisi pada saat sebelum diserang, sesudah diserang tanpa dilakukan pengamanan, dan sesudah diserang dengan upaya melakukan peningkatan keamanan yang ditujukan pada Tabel 4.1.

Tabel 4. 1 Hasil Pengujian

Task	Sebelum	Socudah disarang	Sesudah diserang
Manager	Diserang	Sesuali diserang	dengan keamanan
CPU	20 %	28%	20 %
Memory	1,9 GB	0,9 MB	1,9 GB
Kecepatan	1,46 GHz	539.7 kbps	1,46 GHz
Paket	9 Packet	55 Packet	9 Packet
Status Router	Normal	down	Normal

Berdasarkan taha-tahap yang dilakukan diatas, maka cara meningkatkan keamanan data yaitu :

1. Setiap user harus tahu serangan berasal dari mana, jika yang diserang lewat port 80 langkah yang harus dilakukan adalah mengganti port yang digunakan, atau mendisable port atau dimatikan.

- 2. Memasang firewall traffic pada laptop korban dengan penentuan IP Address, maka akan mencegah terjadinya serangan *malware* jenis njRAT ini.
- 3. Menggunakan anti virus berbayar yang bisa memblokir setiap program *malware* akan menyerang.

