Bab 4

Analisis dan Pembahasan

Analisis dan implementasi penelitian *SIEM* ini dilakukan dalam beberapa tahap, masingmasing tahap bertujuan untuk dapat menganalisa serangan dan melakukan proses *network forensic* dengan baik. Hasil analisa *network forensic* juga digunakan sebagai salah satu acuan untuk dapat mengukur apakah indeks Keamanan Informasi (KAMI) di Dinas Komunikasi dan Informatika Kota Tegal dapat dipengaruhi dengan ketersediaan *SIEM*. Adapun tahap yang dilakukan dalam prosesnya adalah mencakup beberapa hal berikut:

- 1. Pre-assesment indeks Keamanan Informasi (KAMI) Diskominfo Kota Tegal
- 2. Pembuatan Network Environment
- 3. Penyerangan Network Environment
- 4. Network Forensik
- 5. Post-assesment indeks Keamanan Informasi (KAMI) Diskominfo Kota Tegal
- 6. Analisa Data

4.1 Pre-assesment Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal

Sebelum melakukan analisis dan simulasi, dalam penelitian ini dilakukan *pre-assesment* terhadap Dinas Komunikasi dan Informatika Kota Tegal dengan kuisioner indeks Keamanan Informasi (KAMI) untuk dapat mengukur nilai yang dimiliki oleh instansi tersebut, dan dari hasil kuisioner tersebut peneliti memasukan data kuisioner yang ada kedalam aplikasi dan didapatkan nilai indeks Keamanan Informasi (KAMI) sebagai berikut.



Gambar 4.1 Nilai Indeks (KAMI) Pre-Assessment Diskominfo Kota Tegal

Gambar 4.1 menunjukan tingkat kematangan keamanan informasi yang masih di level I dimana Dinas Komunikasi dan Informatika Kota Tegal masih di level awal kematangan keamanan informasi. Sedangkan nilai untuk masing masing aspek dapat dilihat di grafik pada gambar 4.2 dibawah ini.



Gambar 4.2 Grafik nilai per-Aspek indeks (KAMI) Diskominfo Kota Tegal

Dari grafik diatas dapat dilihat bahwa Dinas Komunikasi dan Informatika Kota Tegal mempunyai ketergantungan dan peran kepentingan IT yang tinggi yaitu dengan nilai poin 26, akan tetapi tidak ditindak lanjuti dengan nilai Indeks Keamanan Informasi (KAMI) yang tinggi, hasil evaluasi dari indeks Keamanan Informasi (KAMI) menunjukan nilai dari Dinas Komunikasi dan Informatika Kota Tegal adalah 35 yang mencakup 5 aspek (Tata Kelola, Managemen Resiko, SOP, Pengelolaan Aset dan Teknologi). Khusus untuk Aspek Teknologi Nilai 6 didapatkan dari poin yang ada pada tabel dibawah ini. Tabel 4.1 : Aspek Teknologi yang dilakukan Diskominfo Kota Tegal

No	Evaluasi Teknologi dan Keamanan Informasi	Status	Poin
1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
2	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Perencanaan	1
3	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login dan penarikan akses?	Dalam Perencanaan	2

4.2 Pembuatan Network Environment

Sebelum melakukan tahapan selanjutnya maka dibuat topologi *environment* yang sesuai dengan rancangan topologi yang ada pada metode penelitian. Proses pembuatan *network environment* ini dilakukan di Lab Inixindo Jogja yang beralamat di Jl. Kenari No.69, Muja Muju, Umbulharjo, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55165. Dan berikut gambaran besar konfigurasi yang dibuat

a. Router Mikrotik

Router dikonfigurasi sesuai dengan topologi yang sudah didesain dalam perancangan *network environtment* jaringan yaitu dengan konfigurasi dan pembagian jaringan sebagai berikut:

Interface List						
Interface Interface List	themet FolP Tunne	I IP Tunnel GRE Tunnel VI.	AN VERP Bon	ding LTE		
				ong Lit		
+• - 🗸 🗶 🖆]	1000				
Name		/ Type	Actual MTU L	2 MTU Tx	Rx	
F .ether1 - INTERNET	r i i i i i i i i i i i i i i i i i i i	Ethemet	1500	1600	191.2 kbps	420.3 kbps
ether2 - GOES TO	SWITCH A - SIEM	Ethemet	1500	1598	170.2 kbps	7.0 kbps
ether3 - GOES TO	SWITCH B - HACKER	R Ethemet	1500	1598	116.4 kbps	74.0 kbps
ether4 - USER		Ethernet	1500	1598	0 bps	0 bps
ether5 - NOT USEI)	Ethemet	1500	1598	0 bps	0 bps
wlan1 - SIEM ENV	(WIFI)	Wireless (Atheros AR9	. 1500	1600	0 bps	0 bps
Address List					Sangt 2	
	I I					
Address	/ Network	Interface	A		diam'r ar	
D 🕆 10,10.4.208/24	10.10.4.0	ether1 - INTERNET	_			
宁 10.0.0.1/24	10.0.0.0	ether2 - GOES TO SWITCH A -	SIEM			
· 🕆 10.10.13.1/24	10.10.13.0	ether3 - GOES TO SWITCH B -	HACKER			
10.10.14.1/24	10.10.14.0	ether4 - USER	- Contract (
10.10.15.1/24	10.10.15.0	ether5 - NOT USED			- - - - -	
# 10.10.16.1/24	10.10.16.0	wlan1 - SIEM ENV (WIFI)				
					the second se	

Gambar 4.3 Konfigurasi Ip Router Mikrotik

Selain konfigurasi diatas router Mikrotik dikonfigurasi agar sesuai dengan kebutuhan yang dibutuhkan oleh SIEM semua log topik yang ada (account, async, backup, bfd, bgp, calc, caps, certificate, dns, ddns, dude, dhcp, e-mail, event, firewall, gsm, hotspot, igmpproxy, ipsec, iscsi, isdn, interface, kvm, l2tp, lte, ldp, manager, mme, mpls, ntp, ospf, ovpn, pim, ppp, pppoe, pptp, radius, radvd, read, rip, route, rsvp, script, sertcp, simulator, state, store, smb, snmp, system, telephony, tftp, timer, ups, vrrp, watchdog, web-proxy, wireless, write) router Mikrotik agar dikirimkan ke SIEM server.

Logging		
Rules Actions		
+- * * 7		
Topics	Prefix	Action
account, async, backup, bfd, bgp, calc, caps, certificate, ddns, dhcp, dns, dude, e-mail, event, firewall, hotspot		remote
* critical		remote
debug		remote
enor		remote
* info		remote
ldp, ssh, snmp, wireless, write, system		remote
* waming		remote

Gambar 4.4 Konfigurasi Topik Logging Router Mikrotik

Dalam konfigurasi *log router Mikrotik* semua *log* diarahkan ke alamat *ip* dari *remote SIEM* yaitu 10.0.0.10 sebagai tujuan dari *log* yang di produksi oleh *router Mikrotik*. Berikut merupakan konfigurasi untuk mengarahkan semua *log* ke *SIEM server*.



Gambar 4.5 Konfigurasi Remote Logging router Mikrotik

Untuk lebih detail mengenai konfigurasi *router Mikrotik* dapat diperjelas dengan merujuk pada lampiran 1.

b. Switch A - Cisco Catalyt 2950 Series

Switch A adalah switch berbasis Cisco Catalyt 2950 Series dengan konfigurasi mirroring port dimana semua trafik yang ada dari router Mikrotik ke SIEM ataupun sebaliknya akan di kirimkan pula ke port dimana sniffer berada, dan berikut merupakan pembagian portnya:

- *Port 9* = Menuju *router Mikrotik*
- Port 10 = Menuju SIEM
- Port 11 = Menuju Sniffer (SPAN PORT)



Gambar 4.6 Konfigurasi Mirroring Port Switch A

c. Switch B - Cisco Catalyt 3750 Series

Switch B adalah switch berbasis berbasis Cisco Catalyt 2950 Series dengan konfigurasi mirroring port dimana semua trafik yang ada dari router Mikrotik ke hacker ataupun sebaliknya akan di kirimkan pula ke port dimana sniffer berada, dan berikut merupakan pembagian portnya:

- *Port 1* = Menuju *router Mikrotik*
- Port 3 = Menuju SIEM
- Port 5 = Menuju sniffer (SPAN PORT)



Gambar 4.7 Konfigurasi Mirroring Port Switch B

d. SIEM

SIEM yang digunakan adalah Log Sign SIEM yang di install dan dijalankan di Vmware WorkStation yang di install dikomputer berbasis Windows 7. Alamat yang digunakan sebagai alamat ip SIEM adalah 10.0.0.10.

e. Hacker

Untuk OS yang digunakan *hacker* adalah OS Kalilinux dengan alamat ip 10.10.13.252 yang dijalankan di *Vmware WorkStation* yang di install dikomputer berbasis *Windows* 10.

f. Sniffer

Sebagai *sniffer* digunakan *wireshark* yang di *install* sistem operasi *Windows* 7 akan tetapi mempunyai 2 buah *lan card*. *Lan card* yang pertama terhubung ke *switch* A dimana *sniffer* menangkap trafik *router Mikrotik* ke *SIEM* atau sebaliknya, serta *Lan card* yang kedua menangkap semua trafik *Hacker* ke *router Mikrotik* ataupun sebaliknya.

4.3 Penyerangan Network Environment

Setelah pembuatan *environment* jaringan dilakukan, selanjutnya proses penyerangan aset *router Mikrotik* dengan menggunakan *Kalilinux OS*. Dalam proses penyerangan ini digunakan beberapa *software* yang ada di *Kalilinux* yaitu:

a. MacOF

Macof adalah *software* yang digunakan untuk *flooding* didalam jaringan dengan alamat MAC. *Macof* bisa membanjiri jaringan dengan alamat MAC acak dan membuat jaringan bermasalah terutama switch. (*source: kalilinuxtutorials.com/macof/_*)

b. Etterchap

Etterchap adalah sebuah *software* yang dibuat oleh Alberto Ornaghi (AloR) dan Marco Valleri (NaGa) dan pada dasarnya adalah sebuah *software* untuk penyerangan *MITM* (*man in the middle attack*) di sebuah jaringan. Salah satu serangan yang bisa dilakukan oleh software ini *adalah arp poisoning*.

c. Hping3

Hping adalah program perakit paket dimana *hping* mengirim dan membuat paket sesuai dengan kebutuhan *hacker*. *Hping* protokol TCP, UDP, ICMP dan RAW-IP, memiliki mode *traceroute*. Adapun penggunaan hping digunakan untuk

- Pengetesan Firewall
- Advanced port scanning
- Pengetesan *Network* dengan *protocol, Tos* dan fragmentasi yang bisa di modifikasi sesuai kebutuhan
- *MTU discovery*
- *Remote OS fingerprinting*
- Remote uptime guessing
- Audit TCP/IP
- d. Yersinia

Yersinia adalah *framework* untuk melakukan beberapa serangan dijaringan. *Software* ini dirancang untuk memanfaatkan beberapa kelemahan dalam protokol jaringan yang ada. Dan berikut merupakan protokol jaringan yang dapat diserang oleh *Yersinia*:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)

- *Hot Standby Router Protocol (HSRP)*
- 802.1q, 802.1x
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)
- e. Hydra

Hydra adalah *software craking password* yang mendukung banyak protokol untuk menyerang. *Hydra* juga menyediakan banyak *tools* yang cepat dan fleksibel dengan modul-modul yang mudah ditambahkan. *Software* ini memungkinkan untuk menunjukkan betapa mudahnya mendapatkan akses yang tidak sah ke sistem yang ada di suatu instansi.

Adapun protocol yang di dukung oleh Hydra adalah Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 dan v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC dan XMPP

4.3.1 Link Layer Attack





Applications 👻 🛛 Places 👻	⊾ Terminal 👻	Fri 11:31	
		root@kali: ~	
File Edit View Search	Terminal Help		
4:f9:e7:44:85:d 5:26:1 ae:7c:c5:11:f2:34 50:1	lc:59:c3:b3 0.0.0.0.25181 > (la:eb:le:6b:71 0.0.0.0.61774	0.0.0.0.18940: S 631480189:631480 > 0.0.0.0.42158: S 1946670976:19	0189(0) win 512 046670976(0) win 512
37:d7:1c:41:9c:41 19:c 49:76:2d:54:d7:55 dd:1	c1:f4:b:6:61 0.0.0.0.10009 > 18:73:6f:97:c9 0.0.0.0.40369	0.0.0.0.13028: 5 887022348:88702 > 0.0.0.0.27639: 5 1544661279:15	22348(0) win 512 544661279(0) win 512
46:cd:9e:12:a4:93 7e:b d1:9a:6d:6c:1d:3d 4:f6	0:46:c:21:19 0.0.0.0.0.20728 >	0.0.0.0.63070: 5 458426741:45842 0.0.0.0.17724: 5 1135458512:11	26741(0) win 512 35458512(0) win 512
df:3e:28:1:f4:46 1d:bo 87:36:89:5a:f8:8 9e:5	1:63:76:57:c8 0.0.0.0.33675	0.0.0.0.44605: S 1964979188:196 0 0 0 0 62224: S 1116984635:1116	64979188(0) win 512
84:b2:d:5d:d:9f 52:8:8	82:2:ad:ed 0.0.0.0.14152 > 0	.0.0.0.14617: S 968438907:9684389	907(0) win 512
98:e1:42:21:95:4a 68:6	5f:2:4a:3c:1f 0.0.0.0.16556	0.0.0.0.7257: S 342964772:34296	54772(0) win 512
15:9d:ce:19:c0:ba a9:9	91:a1:28:9e:b1 0.0.0.0.48357	> 0.0.0.0.35938: S 1282760327:12	282760327(0) win 512
4d:c:ee:59:d3:3a e:8d:	:70:71:c5:5d 0.0.0.0.51369 >	0.0.0.0.52625: S 2004342265:2004	4342265(0) win 512
e4:ba:bd:le:54:84 bf:e 74:4c:d0:lc:a3:f5 f3:4	47:ab:55:45:aa 0.0.0.0.50378	> 0.0.0.0.15781: S 1509269115:15	5177133(0) Win 512 509269115(0) Win 512
c0:bd:3d:20:ac:de b9:8 75:cc:4e:25:2f:c1 15:t	84:8c:65:7c:5c 0.0.0.0.42704 b0:81:48:2c:19 0.0.0.0.50584	> 0.0.0.0.34075: S 327209997:32 > 0.0.0.0.39399: S 515605161:51	209997(0) win 512 5605161(0) win 512

Gambar 4.8 Mac Flooding dengan Macof

Dengan menggunakan perintah *macof -i eth0, macof* software melakukan *flooding* paket kejaringan dengan *source* dan *destination ip* yang berbeda-beda/*random*, dan membuat tabel *mac address switch* penuh dan harusnya mempengaruhi tabel *arp* dari *router Mikrotik* karena *flooding* paket yang banyak kejaringan. Dalam proses *flooding* ini paket akan dikirimkan ke semua *port* yang aktif yang ada di-*switch* baik ke *router Mikrotik*, dan *end user Windows*. Selain melakukan penyerangan, dalam penelitian ini juga dilakukan proses *sniffing* untuk melihat trafik yang lewat.

Dan berikut merupakan tampilan dari *end user windows* yang berada satu jaringan dengan *hacker*. Bisa terlihat pada gambar dibawah ini tabel *arp* dari *user* menunjukan bahwa muncul *ip address* yang tidak dikenal dengan *mac address* yang berbeda-beda.

CAWINDOWS\system32\cmd.exe		
C:\Users\Apang>arp -a		- 3 6.0
Interface: 10.10.13.251	0x7	
Internet Address	Physical Address	Type
10.10.13.1	00-0c-42-f7-cb-0c	dynamic
10.10.13.253	9c-eb-e8-5f-24-ea	dynamic
10.10 13 255	ff ff ff ff ff ff	static
224.0.0.22	01-00-5e-00-00-16	stati
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-0 0-f c	static
224.74.145.32	01-00-5e-4a-91-20	static
224.86.25.72	01-00-56-56-19-48	static
224.94.103.61	01-00-5e-5e-67-3d	static
224,116,55,90	01-00-50-74-37-5a	static
224,167,8,65	01-00-50-27-08-41	static
224, 173, 184, 35	01-00-5e-2d-b8-23	static
224 188 180 119	01-00-5e-3c-b4-77	static
225 1 17 17	01-00-50-01-11-11	static
225.1.1/.1/	01-00-50-10-07-18	static
225.10.7.24	01-00-50-11-22-79	static
225.17.170.121		static
225.00.01.38	01-00-50-44-51-26	Static

Gambar 4.9 Tabel Arp End User Windows Jaringan Yang di Mac Flooding Dari hasil serangan yang dilakukan terlihat bahwa end user-pun terpengaruh dengan serangan yang dilakukan oleh hacker.

b. Simulasi Serangan Arp Poisioning

Penyerangan selanjutnya yaitu *arp-poisioning* terhadap *router Mikrotik* dan *end user* yang ada didalam jaringan dengan menggunakan *Ettercap*, proses *arp poisioning* dilakukan terhadap *end user* dan *router Mikrotik* dengan harapan *hacker* bisa meracuni tabel *arp* kedua alat tersebut dan *hacker* dapat menyadap komunikasi mereka. *hacker* melakukan pemilihan

target yaitu *ip address* mana yang akan di *MITM*. Dan memilih *ip address* yang akan dijadikan sebagai target pertama dan target kedua. Dan berikut merupakan gambaran proses penentuan target serangan.

10.10.13.1 dipilih sebagai target pertama karena alamat tersebut merupakan alamat *router Mikrotik* dan alamat 10.10.12.251, 10.10.12.252, 10.10.12.253 dimasukan sebagai target kedua yang akan disadap komunikasinya.



Gambar 4.10 Proses Pemilihan Target Aset router Mikrotik dan End User

Setelah melakukan pemilihan target dilakukan *arp poisoning* dan melakukan penyerangan untuk merubah tabel *arp* yang ada pada *router Mikrotik*. Dan dilanjutkan dengan melakukan proses *sniffing* untuk melihat trafik yang lewat didalam jaringan. Proses *arp poisoning* digambarkan seperti gambar 4.11 yang ada dibawah ini.

10.10.13.251 08:6 10.10.13.253 9C:E 10.10.13.254 00:1	0:6E:4E:1B:4E B:E8:5F:24:EA			
10.10.13.253 9C:E 10.10.13.254 00.1	B:E8:5F:24:EA			
	193:0057:40	14		
Dele	te Host		Add to Target 1	Add to Target 2

Gambar 4.11 Ettercap Melakukan Arp Poisioning ke router Mikrotik

c. Simulasi Serangan CDP Flooding

CDP flooding merupakan kondisi dimana hacker mencoba untuk menyerang tabel cdp neighbor router Mikrotik dengan tujuan melakukan dos kepada Mikrotik dengan level serangan yang ditentukan oleh kekuatan hardware itu sendiri. Hacker menggunakan versinia untuk melakukan serangan terhadap tabel cdp neighbor. Berikut merupakan gambaran proses penyerangan hacker untuk melakukan dos kepada router Mikrotik.

Î					Yersinia 0.7.3	
File Proto	ocols Actions Op S tack Edit interface	s Load default List att	tačks Člea	द्ध r stats	Capture Edit mode Exit	
Protocols	Packets	CDP DHCP 802.	10 802.1	X DTF	HSRP ISL MPLS STP VTP Yersinia log	
CDP	0	TTL DevID	Interfac	e Cour	nt Last seen	
DHCP	0	FF KKKKKKK	eth0	1	06 Oct 20:09:26	
802.1Q	0	FF 222FFFF	eth0	1	06 Oct 20:09:26	
802.1X	0	FF QQQQQQQ	eth0	1	06 Oct 20:09:26	
DTP	0	FF PPPPPP	eth0	1	06 Oct 20:09:26	
HSRP	0	FF WEEEEEE	eth0	1	06 Oct 20:09:26	
ISL	0	FF WVVVVVV	eth0	1	06 Oct 20:09:26	
MPLS	0	FF TTTAAAA	eth0	1	06 Oct 20:09:26	
		FF SSSSSSS	eth0	1	-06 Oct 20:09:26	
Field Valu	le Description	FF SSSSSSS	eth0	1	06 Oct 20:09:26	
	14	FF WWWWWW Cisco Discovery Pro	N eth0	1	05 Oct 20:09/26	
	ų.	Source MAC 06 Version 01	:45:8B:6	B:41:5	6 Destination MAC 01:00:0C:CC:CC E	xtra

Gambar 4.12 CDP Flooding dengan Yersinia

Dan dapat dilihat pada gambar diatas bahwa Yersinia mencoba melakukan cdp flooding dengan DevID, dan mac address yang berbeda-beda.

4.3.2 Internet Layer Attack

a. Simulasi Serangan DHCP Starvation

ter i i Dhcp starvation merupakan kondisi dimana hacker mencoba untuk menguras semua ip pool yang ada di dhcp server, hacker menyerang dhcp server router Mikrotik dengan Yersinia. Dimana Yersinia mengirim DHCP Discover ke jaringan dalam jumlah yang sangat banyak sehingga router Mikrotik menganggap ada permintaan dari dhcp client dan menjawab dengan mengirimkan DHCP Offer dalam jumlah yang banyak yang membuat ip pool dhcp habis dan membuat *dhcp server* tidak dapat melayani *client* yang ingin mendapatkan *ip* address.

						Yersinia	0.7.3			
File Protocols Actions Op	otions H	lelp			_					
\$	1	1	•	3	v Dậ	v				
Launch attack Edit interface	s Load o	default List attac	ks Clear	stats	Capture	e Ed	it mode	e	Exit	
rotocols Packets	CDP	DHCP 802.1G	802.1X	DTP	HSRP IS	L MPLS	STP	VTP	Yersinia log	
IDP 0	TTL	DevID	Interface	Count	Last seen					
OHCP 0	FF	KKKKKKK	eth0	1	06 Oct 20):09:26				
02.10 0	FF	222FFFF	eth0	1	06 Oct 20	0:09:26				
02.1X 0	FF	۵۵۵۵۵۵۵	eth0	1	06 Oct 20):09:26				
OTP 0	FF	ррррррр	eth0	1	06 Oct 20):09:26				
ISRP 0	FF	WEEEEEE	eth0	1	06 Oct 20):09:26				
SL 0	FF	vvvvvvv	eth0	1	06 Oct 20	0:09:26				
IPLS 0	FF	TTTAAAA	eth0	1	06 Oct 20):09:26				
	FF	SSSSSSS	eth0	1	06 Oct 20	0:09:26	-		100.00	
leid value Description	FF	SSSSSSS	eth0	1	06 Oct 20	0:09:26			- A	
lo -	FF Cisc	o Discovery Proto	eth0 col	1	06 Oct 20	0.04.26				
	Sour	ce MAC 06:4	15:8B:6B	:41:56	Destin	nation MA	C [01:06	:0C:CC:CC:CC	Extra
	Vers	ion 01 TI	L 84	Che	cksum	0000				

Gambar 4.13 DHCP Starvation dengan Yersinia

b. Simulasi Serangan DHCP Rogue

Hacker menggunakan Yersinia untuk membuat serangan dhcp rogue, suatu kondisi dimana hacker mencoba untuk membuat dhcp server disuatu jaringan yang sudah ada dhcp servernya, dengan tujuan agar client mendapatkan ip dari dhcp server yang dibuat oleh hacker. Klien tidak mendapatkan ip dari dhcp server yang asli yaitu router Mikrotik. Dan berikut merupakan gambaran serangan yang hacker gunakan untuk menyerang jaringan router Mikrotik.

Parameters list 🖨 🎯 🕲		Yersinia 0.7.3
Server ID 192.168.100.2	File Protocols Actions Op	tions Help
Start IP 192.168.100.2	k Launch attack Edit interfaces	E Load default List attacks Clear stats Capture Edit mode Exit
End IP 192.168.100.200	k Protocols Packets	CDP DHCP 802.1C 802.1X DTP HSRP ISL MPLS STP VTP Yersinia tor
Lease Time (secs) 60000000	the CREdnet 0	SIP DIP MessageType Interface Count Last seen
Renew Time (secs) 60000000	DHCP 0	0.0.0.9 255.255.255.255 01 DISCOVER eth0 1 06 Oct 21:02:04
ubnet Mask 255.255.255.0	802.10.0	0.0.0.0 255 255 255 255 01 DISCOVER eth0 1 06 Oct 21:02:51
Router 192.168.100.1	802.1X 0	0.0.0.0 255.255.255.255-01 DISCOVER eth0 1 06 Oct 21:03:21
NS Server 8.8.8.8	k enu att o	10.10.13.253 10.10.13.1 03 REQUEST eth0 1 06 Oct 21:03:54
Domain arfan.com	tk Milliget 0	0 10.10.13.1 10.10.13.253 05 ACK eth0 1 06 Oct 21:03:54
Cancel OK	ISL 0	0.0.0.0 255.255.255.255.01 DISCOVER eth0 1 06 Oct 21:04:12
	MPLS 0	10.10.13.252 10.10.13.1 03 REQUEST eth0 1 06 Oct 21:05:13
	Field Value Description	10.10.13.1 10.10.13.252 05 ACK etho 1 06 Get 21:05:13
THE CARLES AND A C		Dynamic Host Configuration Protocol Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:
- TINGT target 10-20-11.1 (dg		SIP 0.0.0.0 DIP 255.255.255 SPort 68 DPort 67
A 210071 target 14.14.13.1.1 - 104 - 210711 target 18.23.13.3 - 104		Op 01 Htype 01 HLEN 06 Hops 00 Xid 00009869 Secs 0000 Flags 8000
11001) target 14.20.20.1		CI 0.0.0.0 YI 0.0.0.0 SI 0.0.0.0 GI 0.0.0.0
		CH 02:48:33:66:02:51

Gambar 4.14 DHCP Rogue dengan Yersinia

Hacker melakukan konfigurasi parameter *dhcp Rogue* dan melakukan penyerangan terhadap jaringan 10.10.13.0/24 dan terlihat bahwa *Yersinia* dapat melihat aktifitas *dhcp* yang ada dalam jaringan tersebut.

4.3.3 Transport Layer Attack

a. Simulasi Serangan SYN flooding

Hacker menggunakan Hping3 untuk membuat serangan Syn Flooding, suatu kondisi dimana hacker mencoba untuk mengirimkan tcp state syn untuk memulai koneksi ke target akan tetapi tidak mengirimkan tcp state ack. tujuan syn flooding adalah untuk membebani komputasi router dan membuat router bermasalah. Dan berikut merupakan gambaran serangan yang hacker gunakan untuk menyerang jaringan router Mikrotik.



Gambar 4.15 Syn Flooding dengan Hping3

Hacker melakukan syn flooding dengan menggunakan alamat ip address yang random ke ftp yang ada pada router Mikrotik. Bisa terlihat pada gambar diatas menunjukan sudah terkirim 6333663 paket yang dikirimkan ke router Mikrotik.

4.3.4 Application Layer Attack

a. Simulasi Serangan Brute Force Ssh

Brute Force Attack adalah metode untuk meretas *password (password cracking)* dengan cara mencoba semua kemungkinan kombinasi yang ada pada "*wordlist*". Metode ini dijamin akan berhasil menemukan *password* yang ingin diretas akan tetapi waktu yang dibutuhkan akan sangat tergantung dari seberapa komplek *password* dan kualitas dari *wordlist* itu sendiri. *Brute Force Attack* merupakan metode yang digunakan untuk masuk ke suatu sistem agar mendapatkan akses kedalam sistem. *Hacker* menggunakan *hydra* dengan menggunakan *user* admin dengan *password* yang tersimpan kedalam *wordlist* dengan nama *AllPasswords.txt*. Detail serangan dapat dilihat pada gambar 4.16 dibawah ini.

root@kali: ~
File Edit View Search Terminal Help
r <mark>oot@kali:</mark> -# hydra -t 1 -l admin -P Desktop/LAB/AllPasswords.txt -vV 10.10.13.1 ssh Nydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Avdra (http://www.thc.prg/thc-hydra) starting at 2017-10-06 20:52:40
WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort
DATA] max 1 task per 1 server, overall 64 tasks, 4319607 login tries (l:1/p:4319607), -67493 tries per task
DATA] attacking service ssh on port 22 Lab Hydra
VERBOSE] Resolving addresses done
INFO] Testing if password authentication is supported by ssh://10.10.13.1:22
INFO] Successful, password authentication is supported by ssh://10.10.13.1:22
ATTEMPT] target 10.10.13.1 - Login "admin" - pass "[] - 1 of 4319607 [child 0]
ATTEMPI] target 10.10.13.1 - login "admin" - pass "!" - 2 of 4319607 [child 0]
ATTEMPT] target 10.10.13.1 - Login "admin" - pass "!" - 3 of 4319607 [child 0] Labor transformer and 10 15.1 To
AllEMP1; target 10.10.13.1 - Login "admin" - pass "!" - 4 of 431960/ [child 0]
AllEMPI target 10.10.13.1 - Login "admin" - pass "!2004" - 5 of 4319507 [child 0]
AlleMPI] target 10.10.13.1 - Login "admin" - pass "(@#\$%" - 6 of 431906/ [child 0]
AlleMPIj target 10.10.13.1 - Login "admin" - pass "(@#\$%" - / of 431960/ [child 0]
Allehrij target 10.10.13.1 - Login "admin" - pass "[@LUPF" - 8 of 431960/ [child 0]
Allempij target 10.10.13.1 - Login Batmin - pass "InAuke" - 9 of 431950/ [child 0]
Allempij target 10.10.13.1 - Login admin - pass "Hollast" - 10 of 431900/ [child 0]
Altempij target 10.10.13.1 - Login admin - pass julnisu - 11 of 431900/ [child 0]
ATTEMPT Cardel 10, 10, 13, 1 - Cogin adulti - pass "MAADM - 12 of 41960/ [Child 0]
ATTEMPTI target 10.10.13.1 - Login admin pass TVALENC 13 of 431960/ [Child 8]

Gambar 4.16 Bruteforce SSH dengan Hydra

Terlihat bahwa hydra mencoba untuk menyerang port ssh dengan username admin dan password yang ada pada AllPassword.txt.

b. Simulasi Serangan Brute Force Ftp

Hal yang sama hacker lakukan dengan protocol ftp. hacker menggunakan hydra dengan menggunakan user admin dengan password yang tersimpan kedalam wordlist Allpasswords.txt. Detail serangan dapat dilihat pada gambar dibawah ini.

	rootgikau:
File Edit	View Search Terminal Help
root@kali	:-# hydra -t 1 -l admin -P Desktop/LAB/AllPasswords.txt -vV 10.10.13.1 ftp
Hydra v8.	2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
nyura (nu	tp://www.thc.org/thc-nydra) starting at 201/10-00 20:50:25
[WARNING]	Restorerite (,/nydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort
[DATA] ma	IX I task per I server, overall of tasks, 4319007 login tries (L:1/p:4319007), ~67493 tries per lask
[UATA] dt	Lacking service rup on port 21
[VERBUSE]	Resoluting addresses done
[ATTEMPT]	target 10.10 13.1 login "admin" - pass " - 1 of 4319607 [child 0]
ATTEMPT	
TATTEMPT	target 10 10 13.1 login admin pass 3 3 0 431907 [thitd 0]
TATTEMPT	
TATTEMPT	target 10 10 13 1 - Login domin" - pass "12004 - 5 of 4310607 [child 4]
ATTEMPT	target 10 10 13.1 - login "admin" - pass "loges" of d310607 [child Al
TATTEMPTI	target 10 10 13 1 - Login damin" - pass "JAFLUFF" - 8 of 431067 [child A]
TATTEMPTI	tarnet 10 10 13 1 - Login "admin" - pass "H4X00E" - 9 of 4310607 [child 01
[ATTEMPT]	tarnet 10 10 13 1 - Login "admin" - pass "IMANSEL" - 10 of 4310607 [child 0]
ATTEMPT	target 10 10 13 1 - Login "admin" pass "IniNUM" - 11 of 431067 [child 0]
TATTEMPT	target 10.10.13.1 - Login "admin" - pass "IPWADM" - 12 of 4319607 [child 8]
TATTEMPT	target 10.10.13.1 - login "admin" - pass "!VALENC" - 13 of 4319507 [child 0]

Gambar 4.17 Bruteforce FTP dengan Hydra

Terlihat bahwa hydra mencoba untuk menyerang port Ftp dengan username admin dan password yang ada pada AllPassword.txt

4.4 Network Forensic

Setiap serangan yang disimulasikan oleh *hacker* di *capture* oleh *sniffer* untuk tujuan analisa. Dengan adanya analisa terhadap semua simulai serangan yang *hacker* lakukan berguna untuk mengvalidasi apakah serangan memang benar-benar terjadi dan menjawab bagaimana komunikasi dan trafik apa saja yang lewat dalam jaringan tersebut.

4.4.1 Link Layer Attack

a. Network Forensic Mac Flooding

Pada serangan *mac flooding* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.2 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 2.

Serangan	Trafik Mikrotik- Hacker	Respon Mikrotik	Trafik <i>Mikrotik -</i> SIEM	Respon SIEM	Hasil Serangan <i>SIEM</i>
Mac	Ditemukan	Tidak ada	Saat serangan	Tidak ada	SIEM tidak
Flooding	trafik data	aktifitas	mac flooding	notifikasi/log	berhasil
	dengan	yang	terjadi tidak ada	apapun yang	mendeteksi
	<i>source</i> dan	menunjukan	komunikasi yang	muncul di	serangan
	destination	adanya	dilakukan oleh	SIEM karena	_
	<i>ip</i> yang	serangan	10.0.0.1/10.0.0.10	tidak ada <i>log</i>	
	berbeda-beda	yang	kecuali	yang	
	(Random)	terjadi,	komunikasi	terkirim.	
	bukti bahwa	tidak ada	dengan NTP		
	mac flooding	pengiriman	server		
	telah terjadi	log ke			
		SIEM			
	194		-	100	

 Tabel 4.1: Pelaporan Network Forensic serangan Mac flooding

b. Network Forensic Arp Poisioning

Pada serangan *Arp Poisioning* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.3 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 3.

Serangan	Trafik <i>Mikrotik-</i> Hacker	Respon <i>Mikrotik</i>	Trafik <i>Mikrotik -</i> SIEM	Respon SIEM	Hasil Serangan <i>SIEM</i>
Arp	Ditemukan	Adanya	Saat arp	Tidak ada	SIEM
poisioning	trafik <i>arp</i>	perubahan	poisioning	notifikasi/lo	tidak
	<i>reply</i> berisi	tabel arp	terjadi tidak ada	g apapun	berhasil
	alamat ip	yaitu ip yang	komunikasi	yang	mendete
	berbeda	berbeda akan	yang dilakukan	muncul di	ksi
	tetapi mac	tetapi	oleh	SIEM	serangan
	address sama	memiliki mac	10.0.0.1/10.0.0.	karena tidak	
	yaitu 00-0c-	address yang	10 kecuali	ada <i>log</i>	
	29-ab-a5-e8	sama yaitu	komunikasi	yang	
	bukti adanya	00-0c-29-ab-	dengan NTP	terkirim.	
	aktifitas arp	а5-е8	server		
	poisioning				

Tabel 4.2: Pelaporan Network Forensic serangan Arp Poisioning

c. Network Forensic CDP Flooding

Pada serangan *CDP flooding* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.4 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 4.

Serangan	Trafik Mikrotik- Hacker	Respon Mikrotik	Trafik <i>Mikrotik - SIEM</i>	Respon SIEM	Hasil Serangan <i>SIEM</i>
CDP	Ditemukan	Munculnya	Saat serangan <i>cdp</i>	Tidak ada	SIEM tidak
Flooding	trafik <i>cdp</i>	banyak <i>ip</i>	flooding terjadi	notifikasi/log	berhasil
	yang banyak	neigbors	tidak ada	apapun yang	mendeteksi
	menggunakan	table	komunikasi yang	muncul di	serangan
	<i>ip</i> dan <i>mac</i>	dengan <i>ip</i>	dilakukan oleh	SIEM karena	
	address yang	address dan	10.0.0.1/10.0.0.10	tidak ada <i>log</i>	
	berbeda-beda	тас		yang	
	dan bukti <i>cdp</i>	address		terkirim.	
	flooding telah	yang			
	dilakukan	berbeda-			
		beda			

Tabel 4.3: Pelaporan Network Forensic serangan CDP flooding

4.4.2 Network Layer Attack

a. Network Forensic DHCP Starvation

Pada serangan *DHCP Rogue* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.5 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 5.

	Trafik	Respon	Trafik		Hasil
Serangan	Mikrotik-	Mikrotik	Mikrotik -	Respon SIEM	Serangan
100	Hacker	MILLIOUL	SIEM	1.	SIEM
DHCP	Ditemukan	router	Pada saat	Respon SIEM	SIEM
Starvation-	adanya	Mikrotik	serangan	menunjukan	berhasil
-	serangan <i>dhcp</i>	merespon	dhcp	bahwa tingkat	mendeteksi
	starvasion	dengan	starvation	event	serangan
	dimana	menjawab	terjadi ada	meningkat	
	hacker	dengan dhcp	komunikasi	dan	
	mengirimkan	offered	yang	menampilkan	
	dhcp discover	sampai <i>ip</i>	dilakukan	<i>log</i> yang	
	secara terus-	pool router	oleh 10.0.0.1	diberikan	
	menerus	Mikrotik	ke 10.0.0.10	router	
		habis	dalam bentuk	Mikrotik	
			syslog.	kepada SIEM	

Tabel 4.4: Pelaporan Network Forensic serangan DHCP Starvation

b. Network Forensic DHCP Rogue

Pada serangan *DHCP Rogue* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.6 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 6.

Serangan	Trafik Mikrotik- Hacker	Respon Mikrotik	Trafik <i>Mikrotik -</i> <i>SIEM</i>	Respon SIEM	Hasil Serangan <i>SIEM</i>
DHCP	router Mikrotik	router	Pada saat	Respon	SIEM
Rogue	mengirimkan	Mikrotik	serangan	SIEM	berhasil
	log ke SIEM	merespon	dhcp rogue	menunjukan	mendeteksi
	berupa log dhep	dengan	terjadi ada	menampilkan	serangan
	alert dimana	menjawab	komunikasi	<i>log</i> yang	
	router Mikrotik	dengan	yang	diberikan	
	mengenali	mengirimkan	dilakukan	router	
	keberadaan	dhcp alert ke	oleh 10.0.0.1	Mikrotik	
	<i>dhcp rogue</i> lain.	SIEM	ke 10.0.0.10		
	UI 6		dalam		
			bentuk		
			syslog.		

Tabel 4.5: Pelaporan Network Forensic serangan Dhcp Rogue

4.4.3 Transport Layer Attack

a. Network Forensic SYN Flooding

Pada serangan *SYN flooding* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.4 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 7.

Serangan	Trafik Mikrotik- Hacker	Respon <i>Mikrotik</i>	Trafik <i>Mikrotik -</i> <i>SIEM</i>	Respon <i>SIEM</i>	Hasil Serangan <i>SIEM</i>
SYN	Ditemukan	Mikrotik	Saat serangan syn	Tidak ada	<i>SIEM</i> tidak
Flooding	trafik SYN	tidak bisa	<i>flooding</i> terjadi	notifikasi/log	berhasil
	yang banyak	di akses	tidak ada	apapun yang	mendeteksi
	menggunakan	karena	komunikasi yang	muncul di	serangan
	<i>ip</i> yang	diserang	dilakukan oleh	SIEM karena	
	berbeda beda		10.0.0.1/10.0.0.10	tidak ada <i>log</i>	
	ke <i>ftp</i> bukti			yang	
	syn flooding			terkirim.	
	telah				
	dilakukan				

Tabel 4.6: Pelaporan Network Forensic serangan SYN flooding

4.4.4 Application Layer Attack

a. Network Forensic SSH Brute Force

Pada serangan *SSH Brute Force* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.7 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 8.

Serangan	Trafik Mikrotik- Hacker	Respon Mikrotik	Trafik Mikrotik - SIEM	Respon SIEM	Hasil Serangan <i>SIEM</i>
SSH	Ditemukan	router	saat ssh	Respon	SIEM
Brute	trafik <i>hacker</i>	Mikrotik	Bruteforce	SIEM	berhasil
Force	mencoba	merespon	terjadi ada	menunjukan	mendeteksi
	login melalui	dengan	komunikasi	menampilkan	serangan
	protocol ssh	menjawab	10.0.0.1 ke	<i>log</i> yang	
	ke router	dengan	10.0.0.10	diberikan	
	Mikrotik	mengirim	dalam bentuk	router	
	secara	login failure	syslog.	Mikrotik	
	berulang	kepada			
	ulang	hacker	and the second se		

Tabel 4.7: Pelaporan Network Forensic serangan Ssh Bruteforce

b. Network Forensic FTP Brute Force

Pada serangan *SSH Brute Force* dilakukan analisa *network forensic* dan dilakukan pelaporan terhadap aktifitas yang ditemukan. Hasil dari analisa tersebut di laporkan pada table 4.8 dibawah ini, dan lebih detail mengenai data *network forensic* dapat diperjelas dengan merujuk pada lampiran 9.

Serangan	Trafik	Respon	Trafik	Respon SIEM	Hasil
	Mikrotik-	Mikrotik	Mikrotik -		Serangan
	Hacker	124 H Z	SIEM		SIEM
FTP	Ditemukan	router	Pada saat	Respon	SIEM
Brute	trafik hacker	Mikrotik	serangan <i>ftp</i>	SIEM	berhasil
Force	mencoba	merespon	Bruteforce	menunjukan	mendeteksi
	login melalui	dengan	terjadi ada	menampilkan	serangan
	protocol ftp	menjawab	komunikasi	<i>log</i> yang	
	ke <i>router</i>	dengan	yang	diberikan	
	Mikrotik	mengirim	dilakukan	router	
	secara	login failure	oleh 10.0.0.1	Mikrotik	
	berulang	kepada	ke 10.0.0.10		
	ulang	hacker	dalam bentuk		
			syslog.		

 Tabel 4.8: Pelaporan Network Forensic serangan Ftp bruteforce

4.5 *Post-assesment* Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal

Setelah melakukan analisis dan simulasi, dilakukan paparan terhadap hasil analisis forensik kepada Dinas Komunikasi dan Informatika Kota Tegal dan melakukan kuisioner ulang sebagai bentuk perbandingan, apa yang terjadi jika *SIEM* di Implementasikan didalam Infrastruktur Pemerintahan Kota Tegal. Peneliti melakukan *post-assesment* terhadap Dinas Komunikasi dan Informatika Kota Tegal dengan kuisioner indeks Keamanan Informasi (KAMI) untuk dapat mengukur nilai indeks Keamanan Informasi (KAMI) yang dimiliki oleh instansi tersebut.

Dengan ketergantungan dan peran kepentingan IT yang tinggi, dan dari hasil analisis serangan dan korelasinya dengan *SIEM* yang dilakukan. Terlihat pada gambar 4.18 menunjukan bahwa nilai dari Dinas Komunikasi dan Informatika Kota Tegal adalah 54, yang menunjukan tingkat kematangan keamanan informasi masih tetap di level I, dan masih di level yang sama pada saat *pre-assesment* dilakukan, akan tetapi dari aspek teknologi menunjukan adanya kenaikan poin nilai dari 35 menuju ke 54.



Gambar 4.18 Nilai Post-assessment indeks KAMI Diskominfo Kota Tegal

Dan untuk detail setiap aspek yang ada diukur dalam indeks dapat dilihat di grafik pada gambar 4.19 dibawah ini, terlihat tidak ada perbedaan untuk aspek tata kelola, management resiko, SOP, pengelolaan asset, hanya aspek teknologi yang menunjukan adanya kenaikan sebanyak 19 poin.



Gambar 4.19 Nilai Indeks (KAMI) Pre-Assessment Diskominfo Kota Tegal

Kenaikan nilai indeks Keamanan Informasi (KAMI) dari aspek teknologi dipengaruhi oleh beberapa poin yang ditunjukan pada tabel 4.9 dibawah ini. Tabel 4.0: Aspek Taknologi yang dipengaruhi Diskominfo Kata Tagal

Tabel 4.9: Aspek	Teknologi yang	dipengaruhi Diskominfo	Kota Tegal
			-

No	Evaluasi Teknologi dan Keamanan Informasi	Status	Poin
1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
2	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
3	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
4	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam <i>log</i> ?	Diterapkan Secara Menyeluruh	3
5	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam <i>log</i> ?	Diterapkan Secara Menyeluruh	3

6	Apakah semua <i>log</i> dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
7	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?	Dalam Perencanaan	2
8	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi secara rutin dan sistematis?	Diterapkan Secara Menyeluruh	6

4.6 Analisa Data

4.6.1 Serangan dan SIEM

Dengan data yang dikumpulkan dari hasil simulasi serangan dan proses *network forensic* yang dilakukan didalam penelitian. Dilakukan perangkuman terhadap data tersebut seperti ditunjukan pada tabel 4.10 dibawah ini agar dapat dianalisa sesuai dengan kebutuhan penelitian

No	Layer	Tipe	Tool	Hasil di	Hasil di	OUTPUT
	Serangan	Serangan		Mikrotik	SIEM	SIEM
1	Link Layer	Mac	MacOF	router Mikrotik	Tidak ada	SIEM tidak
		Flooding		tidak	aktifitas di	berhasil
				memproduksi	SIEM	mendeteksi
				log		serangan
2		Arp	Ettercap	router Mikrotik	Tidak ada	SIEM tidak
	10	Poisioning		tidak	aktifitas di	berhasil
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			memproduksi	SIEM	mendeteksi
				log		serangan
3	1000	CDP	Yersinia	router Mikrotik	Tidak ada	SIEM tidak
		Flooding	11. L	tidak	aktifitas di	berhasil
	- °		1	memproduksi	SIEM	mendeteksi
				log		serangan
4	Network	DHCP	Yersinia	router Mikrotik	Ada aktifitas	SIEM
	Layer	Starvation		memproduksi	di SIEM	berhasil
				log		mendeteksi
						serangan
5		DHCP	Yersinia	router Mikrotik	Ada aktifitas	SIEM
		Rogue		memproduksi	di SIEM	berhasil
				log		mendeteksi
						serangan

Tabel 4.10: Rangkuman Network Forensic Simulasi Serangan

6	Transport	Syn	Hping3	router Mikrotik	Tidak ada	SIEM tidak
	Layer	Flooding		tidak	aktifitas di	berhasil
				memproduksi	SIEM	mendeteksi
				log		serangan
7	Application	SSH	Hydra	router Mikrotik	Ada aktifitas	SIEM
	Layer	Bruteforce		memproduksi	di SIEM	berhasil
				log		mendeteksi
						serangan
8		FTP	Hydra	router Mikrotik	Ada aktifitas	SIEM
	1.1.1	Bruteforce		memproduksi	di SIEM	berhasil
				log		mendeteksi
						serangan

Dari data yang ada pada table 4.10 dapat kita lihat bahwa penggunaan *SIEM* dapat mendeteksi 4 dari 8 serangan yang dilakukan dalam penelitian ini, penggunaan *SIEM* dirasa mampu mendeteksi serangan yang ada walaupun ada beberapa serangan yang tidak dikenali oleh *SIEM* karena *router Mikrotik* tidak memproduksi Log yang harusnya dikirimkan ke *SIEM*.

4.6.2 Indeks Kami

Setelah dilakukan *pre* dan *post-assessment* indeks Keamanan Informasi (KAMI) terhadap Dinas Komunikasi dan Informatika Kota Tegal bisa terlihat perbandingan nilai indeks Keamanan Informasi (KAMI) pada gambar 4.20 dibawah ini.



Gambar 4.20 Nilai indeks (KAMI) Pre dan Post-assessment Diskominfo Kota Tegal

Hasil perbandingan diatas menujukan bahwa penggunaan *SIEM* dapat membantu menaikan nilai poin untuk aspek Teknologi yang ada pada indeks Keamanan Informasi (KAMI) akan tetapi tidak berpengaruh pada aspek-aspek yang lain. Terlihat bahwa nilai dari Dinas komunikasi dan informatika Kota tegal adalah 54, dari sebelummnya adalah 35 poin, yang menunjukan tingkat kematangan keamanan informasi masih di level I, masih di level yang sama pada saat *pre-assesment* dilakukan, akan tetapi dari aspek Teknologi menunjukan adanya perubahan nilai dari 6 menuju ke 25.

