Bab 5
Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini dilakukan untuk menjawab penggunaan *SIEM* untuk monitoring keamanan *router Mikrotik* di jaringan suatu instansi yang dapat membantu *security officer* untuk memonitor dan mengamankan jaringannya, serta implikasi *SIEM* dalam menaikan nilai indeks Keamanan Informasi (KAMI) di suatu instansi. Dalam penelitian yang dilakukan ternyata terbukti bahwa:

1. Penggunaan *SIEM* untuk melakukan *monitoring* keamanan terbukti dapat memberikan informasi mengenai serangan yang terjadi pada *router Mikrotik* kepada *security officer*. Akan tetapi tidak semua serangan dapat di kenali oleh *SIEM*. Hanya serangan *DHCP Starvation, DHCP Rogue, SSH Bruteforce* dan *FTP Bruteforce* dikenali oleh *SIEM*. Sedangkan untuk serangan *Mac Flooding, ARP-Poisoning, CDP Flooding* dan *Syn Flooding* tidak dapat dikenali oleh *SIEM* karena *Mikrotik* tidak mengirim *log* ke *SIEM*
2. Dalam hubungannya dengan indeks keamanan informasi (KAMI) pengunaan teknologi *SIEM* terbukti menaikan nilai indeks Keamanan Informasi (KAMI) Dinas Komunikasi dan Informatka Kota Tegal di aspek Teknologi, adapun kenaikan ini karena kemampuan *SIEM* dalam menganalisa kelemahan dan perubahan konfigurasi asset informasi di Dinas Komunikasi dan Informatka Kota Tegal, kemampuan SIEM untuk dapat memonitor dan melakukan proses analisa dan audit terhadap asset yang dimiliki Dinas Komunikasi dan Informatka Kota Tegal secara rutin dan sistematis

5.2 Saran

Dalam penelelitian ini peneliti banyak menyadari bahwa masih banyak kekurangan terkait penelitian SIEM ini,

1. Pada penggunaa SIEM di *router Mikrotik* serangan *Mac Flooding, ARP-Poisoning, CDP Flooding* dan *Syn Flooding* tidak dapat dikenali oleh SIEM. Untuk penelitian berikutnya perlu riset yang lebih dalam bagaimana serangan tersebut dapat dikenali oleh SIEM
2. Infrastruktur jaringan akan sangat berkembang sesuai dengan kebutuhan organisasi oleh karena itu perlu adanya analisa serangan dan SIEM dengan menggunakan objek yang lain *(IDS, IPS, Server, Switch dll)* dan dengan serangan yang berbeda dan lebih banyak.

3. Adapun kaitannya indeks Keamanan Informasi (KAMI) perlu dilakukan penelitian yang lebih dalam untuk dapat menaikan nilai indeks Keamanan Informasi (KAMI) dari berbagai aspek bukan hanya teknologi saja.