BAB 1
Pendahuluan

1.1 Latar Belakang

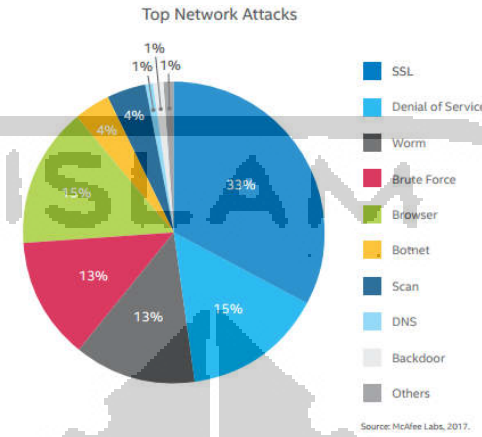
Keamanan informasi menjadi salah satu kebutuhan dan upaya organisasi untuk dapat mengamankan aset informasi yang dimiliki oleh organisasi, dalam prosesnya berbagai macam teknologi keamanan akan digunakan untuk dapat mengamankan aset informasi tersebut, baik keamanan di sisi *physical, network* maupun di *application*. Dalam ranah tata kelola keamanan IT banyak perusahaan yang mengacu kepada *best practice framework* seperti ISO 27001 Family, PCI-DSS, HIPPA dan SOX sebagai acuan dalam membuat *security policy* dan SOP untuk mengamankan aset informasi yang ada di organisasinya. Di pemerintahanpun sudah ada standar SMKI (Sistem Managemen Keamanan Informasi) yang mengatur standar dan audit keamanan informasi didalam lembaga pemerintahan.

Selain pembuatan standar keamananan SMKI, pemerintahpun berusaha untuk mengukur keamanan informasi instansi pemerintahan dengan menggunakan indeks Keamanan Informasi (KAMI) (Keamanan Informasi) sebagai tolak ukur untuk menilai tingkat dan indeks keamanan dan kematangan keamanan informasi instansi pemerintahan. Indeks KAMI merupakan aplikasi untuk mengevaluasi tingkat kematangan dan tingkat kelengkapan penerapan SNI ISO/IEC serta peta area tata kelola keamanan informasi di suatu instansi pemerintah yang mencakup aspek Tata kelola, Managemen resiko, SOP, Pengelolaan Aset dan Teknologi.

Berdasarkan peraturan menteri komunikasi dan informatika No.4 Tahun 2016 tentang Standar Sistem Managemen Keamanan Informasi. Setiap lembaga pemerintah wajib mematuhi SMKI dengan memegang nilai CIA *(Confidentiality, Availability* dan *Integrity)* terhadap aset informasi yang ada di instansinya.

Dinas Komunikasi dan Informatika Kota Tegal adalah salah satu contoh dari instansi pemerintahan dengan kebutuhan untuk mengamankan informasi yang dimiliknya. Dengan infrastruktur jaringan yang mereka sudah buat untuk menghubungkan antar SKPD di jaringan lokal Kota Tegal yang berbasis teknologi *Fiber Optic* dan dengan munculnya aplikasi-aplikasi penting yang menunjang berjalannya proses birokrasi pemerintahan Kota Tegal, Maka muncul pula kebutuhan untuk mengamankan infrastruktur dan aset informasi yang ada di Kota Tegal. Selama ini untuk mengukur tingkat peran TI serta kematangan keamanan informasi Dinas Komunikasi dan Informatika Kota Tegal menggunakan indeks Keamanan Informasi (KAMI) sebagai tolak ukur tingkat keamanan informasi mereka.

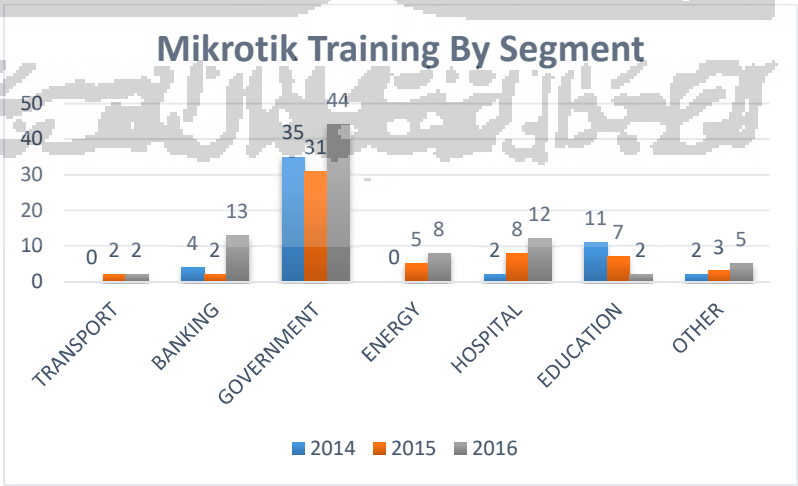
Berdasarkan penelitian yang dilakukan oleh *McAfee* dan dituangkan dalam *McAfee Labs Threats Report April 2017.* Jenis serangan di network yang biasanya ada pada aset infrastruktur suatu instansi adalah *SSL, DOS, Worm, Brute Force* dan serangan-serangan yang lainnya *(McAfee,2017)*



Gambar 1.1 *Top Network Security Attack*

Dari data statistik di gambar 1.1 terlihat masih banyak serangan yang terjadi di lapisan *network* yang perlu kita waspadai. *Router* yang merupakan salah satu *hardware* penting menjadi salah satu korban yang bisa diserang.

Dari segmen pemerintahan banyak instansi pemerintahan yang menggunakan *router Mikrotik* sebagai pilihan *hardware* mereka karena *router Mikrotik* merupakan salah satu produk jaringan yang banyak dipakai untuk skala jaringan *medium to low* dan dengan harga yang relatif murah dibandingkan dengan solusi dari produk sejenis. Berikut merupakan data training *router Mikrotik* di salah satu vendor training di Indonesia yang menunjukan penggunaan *router Mikrotik* yang banyak di segmen pemerintahan dari tahun 2014-2016 seperti digambarkan pada gambar 1.2 dibawah ini.



Gambar 1.2 *Mikrotik Training* 2014-2016 (*Source:Inixindo Jogja Internal Data*)

Karena banyaknya pengguna *router Mikrotik* di instansi pemerintahan, dan dengan adanya kebutuhan keamanan infrastruktur jaringan ada sisi dimana s*ecurity officer* mempunyai kebutuhan untuk dapat melihat serangan-serangan apa saja yang terjadi pada Infrastruktur IT-nya secara *real time*, solusi yang bisa digunakan untuk memonitor serangan yang ada adalah penggunaan *Security Information and Event Management (SIEM)* , *Security Information and Event Management (SIEM)* adalah Sistem *monitoring* yang dapat mendeteksi serangan dan respon suatu sistem keamanan melalui analisis *log* dari berbagai *event* yang berasal dari berbagai sumber data seperti *(IPS, IDS, UTM, Router, Server dll*) secara *real-time* (Gartner,2016).

Security Information and Event Management (SIEM) juga mendukung pelaporan dan investigasi insiden keamanan melalui analisis data *historis* dari berbagai sumber data secara *realtime*. Kemampuan inti dari teknologi *Security Information and Event Management (SIEM)* adalah cakupan pengumpulan data yang banyak dan kemampuan untuk mengkorelasikan dan menganalisis *event* kejadian dari berbagai sumber yang berbeda dan melihat apakah *event* tersebut merupakan sebuah serangan atau tidak (Gartner,2016)

Dengan adanya kebutuhan instansi pemerintahan untuk dapat menerapkan Standar Managemen Keamanan Informasi sesuai dengan SMKI dan Kebutuhan *monitoring* terhadap *network* menjadi pilihan yang mutlak agar *security officer* dapat dengan jelas melihat apa yang terjadi dengan jaringannya dan juga berimbas pada nilai indeks keamanan informasi di instansi tersebut. Akan tetapi yang menjadi pertanyaan adalah apakah penggunaan *Security Information and Event Management (SIEM)* benar-benar mendeteksi semua serangan yang ada pada jaringan berbasis *router Mikrotik* dan efektif mengamankan jaringan dari serangan yang ada.

Banyak penelitian yang membahas *SIEM* tentang bagaimana implementasinya penggunaan untuk *Server, IPS/IDS, UTM* atau korelasi *SIEM* dengan *system audit* dan disiplin ilmu lain seperti *forensic* terutama *network forensic* dengan menggunakan metode penelitian *OSCAR* (*Obtain Information -> Strategize -> Collect Evidence -> Analyze -> Report)* agar didapat hasil yang valid dalam pengujian serangan dan hasil serangan, tapi masih belum banyak yang secara detail mengimplementasikan di jaringan *router Mikrotik*. Penelitian tentang *SIEM* pada *router Mikrotik* belum ada dan hal yang harus diungkap adalah bagaimana *SIEM* dapat membantu mengamankan jaringan berbasis *router Mikrotik*. Apakah *SIEM* dapat memberikan *monitoring* keamanan terhadap semua serangan terhadap atau tidak secara *real time* sehingga hasil penelitian dapat memberikan gambaran implementasi *SIEM* di jaringan.

1.2 Identifikasi Masalah

Dari uraian diatas di identifikasi beberapa masalah yang ada, yaitu:

a. Instansi pemerintahan wajib mengikuti Peraturan Menteri Komunikasi dan Informatika No.4 Tahun 2016 tentang Standar Sistem Managemen Keamanan Informasi yang relefan dengan ISO 27001 dan indeks Keamanan Informasi (KAMI) (Keamanan Informasi)
b. Keamanan aset informasi merupakan kebutuhan organisasi dan *network security* menjadi salah satu komponen keamanan aset informasi di instansi Dinas Komunikasi dan Informatika Kota Tegal.
c. Banyak Organisasi yang berencana menggunaan *Security Information and Event Management (SIEM)* untuk memonitor serangan yang ada pada infrastruktur mereka tanpa tahu apakah *SIEM* ini bermanfaat untuk keamanan infrastruktur mereka atau tidak
d. Banyak instansi pemerintahan yang menggunakan *router Mikrotik* sebagai pilihan *hardware* jaringan mereka.

1.3 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah :

a. Apakah *Security Information and Event Management (SIEM)* dapat memberikan informasi kepada s*ecurity officer* agar dapat melihat serangan pada aset *router Mikrotik* secara *real time*.
b. Apakah ada pengaruh penggunaan *SIEM* terhadap nilai indeks Keamanan Informasi (KAMI) terutama dari aspek Teknologi di instansi pemerintahan.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah :

a. *SIEM* yang digunakan dalam penelitian adalah *LogSign SIEM*
b. Tipe serangan yang akan disimulasikan adalah *Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, Syn flooding, SSH Bruteforce* dan *FTP Bruteforce.*
c. Menggunakan *router Mikrotik* sebagai aset yang akan diserang
d. Menggunakan *KaliLinux OS* untuk simulasi serangan
e. Penelitian ini menggunakan studi kasus instansi Dinas Komunikasi dan Informastika Kota Tegal

1.5 Tujuan Penelitian

Dalam penelitian dilakukan dengan tujuan untuk:

a. Membangun simulasi serangan dengan beberapa tipe serangan ke *router Mikrotik* dan melihat aktifitas *SIEM.*
b. Membuktikan dan menganalisa secara *real time* apakah penggunaan *Security Information and Event Management (SIEM)* untuk *monitoring* keamanan jaringan berbasis *router Mikrotik* dapat mendeteksi seranga yang ada secara *real time*.
c. Membuktikan dampak penggunaan *SIEM* terhadap nilai indeks Keamanan Informasi (KAMI) terutama aspek Teknologi di instansi Pemerintahan.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat memberi kontribusi dalam topik keamanan jaringan dan dapat diterapkan dalam dunia nyata. Adapun manfaat penelitian ini antara lain :

a. Manfaat Untuk Peneliti

   Dengan penelitian ini, diharapkan peneliti dapat menambah ilmu pengetahuan dan pemahaman mengenai Penggunaan *Security Information and Event Management (SIEM)* dalam jaringan *router Mikrotik* sehingga nantinya dengan ilmu tersebut dapat dipergunakan dan bermanfaat bagi orang banyak.

b. Manfaat Untuk Organisasi

   Dengan adanya penelitian ini, diharapkan organisasi mendapatkan informasi mengenai efektifitas dan kualitas implementasi *Security Information and Event Management (SIEM)* di jaringan *router Mikrotik* di instansinya, serta sebagai acuan dalam metode pengamanan jaringan kedepannya dan sebagai pertimbangan penggunaan *SIEM* untuk penerapan SMKI di instansi mereka.

c. Manfaat Untuk Pihak Lain

   Dengan adanya penelitian ini diharapkan akan dapat membantu meberikan gambaran implementasi *Security Information and Event Management (SIEM)* dan Analisa dalam mengamankaan jaringan berbasis *router Mikrotik* di lingkungannya.

1.7 Metode Penelitian

Penelitian ini akan dilakukan menjadi beberapa tahapan, yaitu :

a. Studi Literatur

   Studi literatur digunakan untuk mendalami teknologi *SIEM* dan perkembangan penggunaan *Security Information and Event Management (SIEM)* untuk keamanan

jaringan, selain itu juga studi mengenai Indeks KAMI dan bagaimana implementasinya di pemerintahan.

b. *Pre-assesment* indeks Keamanan Informasi (KAMI)

   Sebelum melakukan analisis dan simulasi serangan dalam penelitian ini dilakukan *pre-assesment* indeks Keamanan Informasi (KAMI) di instansi Dinas Komunikasi dan Informastika Kota Tegal untuk dapat mengukur nilai indeks Keamanan Informasi (KAMI) yang dimiliki oleh instansi tersebut.

c. Pembuatan *Network Environment*

   Dalam tahap ini dilakukan perancangan kebutuhan sistem dan topologi jaringan yang akan diserang dan pembuatan *Network Environment.*

d. Penyerangan *Network Environment*

   Setelah melakukan perancangan dan pembuatan *Network Environment* selanjutnya dilakukan simulasi penyerangan sesuai dengan scenario yang peneliti buat dengan *Kalilinux OS* dengan tipe serangan *Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, Syn Flooding, SSH Bruteforce* dan *FTP Bruteforce*.

e. Network Forensic

   Melakukan analisa serangan terhadap *router Mikrotik* dengan serangan-serangan yang sudah dilakukan dan melihat respon *SIEM* dan *router Mikrotik* secara langsung. Dalam penelitian ini dilakukan proses *network forensic* metodelogi *OSCAR* yang dalam proses forensiknya dilakukan secara *realtime* dengan menggunakan *Wireshark.*

f. *Post-assesment* indeks Keamanan Informasi (KAMI)

   Setelah proses *network forensic*, selanjutnya ditindak lanjuti dengan memaparkan hasil temuan ke Dinas Komunikasi dan Informastika Kota Tegal, dari hasil paparan tersebut ditindak lanjuti dengan melakukan *post-assesment* indeks Keamanan Informasi (KAMI) di Dinas Komunikasi dan Informastika Kota Tegal untuk dapat mengukur nilai indeks Keamanan Informasi (KAMI) yang dimiliki setelah penggunaan *SIEM*

g. Analisa Data

   Dari data yang dikumpulkan dalam *digital forensic* serta *pre-assessment* dan *post-assessment* dari indeks Keamanan Informasi (KAMI) data tersebut dianalisa agar didapatkan hasil penelitian