1 PENDAHULUAN

1.1 Latar Belakang

PT. Parsaoran Global Datatrans (HSP Net) merupakan salah satu perusahaan Penyedia Jasa Layanan Internet *Dedicated* (*Dedicated Internet Service Provider*) yang menawarkan jasa untuk pemasangan Internet atau disebut juga dengan *Internet Service Provider* (ISP). Untuk menjaga keamanan server atau lintas jaringan lainnya HSP Net terus memantau dan mengantisipasi serangan yang masuk ke dalam jaringannya.

Kantor *Network Operation Center* (NOC) HSP Net Jakarta Timur merupakan kantor untuk melakukan kontrol terhadap suatu jaringan atau *network*. Kontrol ini meliputi kegiatan untuk mengawasi, mengendalikan, serta mencatat aktivitas jaringan yang sedang berlangsung untuk memastikan semuanya berjalan dengan lancar. Saat ini HSP Net belum menggunakan sistem untuk melakukan proses kontrol untuk monitoring keamanan jaringan, akibatnya banyak serangan yang masuk ke dalam server HSPNet, sehingga perlu ditambah keamanan yang menerapkan sistem *Security Information and Event Management* (SIEM).

SIEM adalah teknologi keamanan yang dapat digunakan untuk manajemen log, dan peristiwa mengatur dari komputasi sebuah perangkat, sistem dan layanan terdistribusi dengan *baseline* keamanan. Penerapan SIEM telah banyak dimanfaatkan oleh berbagai perusahaan yang berhubungan dengan server dan jaringan internet (Hardiansyah 2014). Sistem SIEM digunakan untuk menganalsis keamanan jaringan dan mempunyai fitur untuk memantau, mengindentifikasi, mendokumentasikan, dan menanggapi pelanggaran keamanan seperti serangan DoS yang disengaja dan berbahaya seperti virus. Sistem SIEM juga dapat mengidentifikasi peristiwa/event keamanan yang sulit dipahami dari ribuan event tiap detiknya. Tanpa bantuan SIEM event-event ini akan terlewat. Event ini mencakup pelanggaran terhadap kebijakan, upaya akses yang tidak sah, dan serangan yang tidak diketahui yang masuk kedalam lingkungan IT.

IBM QRadar *Security Information and Event Management* (SIEM) merupakan aplikasi yang membantu mendeteksi keamanan dan memprioritaskan ancaman secara akurat dalam suatu perusahaan dan memberikan wawasan yang memungkinkan administrator untuk merespon dengan cepat untuk mengurangi dampak dari sebuah serangan yang terjadi dengan menggunakan gabungan sebuah *log* dan aliran data jaringan dari berbagai perangkat yang berada di suatu jaringan. QRadar mengkorelasikan semua informasi yang didapat dan mengagregasikan informasi tersebut ke dalam satu peringatan guna mempercepat analisis insiden dan perbaikan (Scarfone 2015).

Tujuan dari praktik kerja lapang yang dilakukan adalah untuk mengimplementasikan IBM QRadar SIEM pada perusahaan HSP Net. Hal ini dilakukan karena HSP Net belum menerapkan SIEM pada server yang digunakan. Mengingat bahwa peran SIEM sangat penting dalam keamanan jaringan, implementasi ini adalah hal yang krusial dan tidak boleh diabaikan.

1.2 Rumusan Masalah

Rumusan masalah dari pembuatan sistem Implementasi Manajemen Keamanan Jaringan Menggunakan IBM QRadar SIEM di HSPNET ini, adalah :

1. Bagaimana cara Implementasi SIEM pada IBM QRadar?
2. Bagaimana cara IBM QRadar SIEM memantau keamanan Jaringan?
3. Bagaimana cara IBM QRadar SIEM menemukan pelanggaran?

1.3 Tujuan

Tujuan dari pembuatan sistem Implementasi Manajemen Keamanan Jaringan Menggunakan IBM QRadar SIEM di HSPNET ini, yaitu :

1. Mengimplementasikan Aplikasi IBM QRadar *Security Intelligence* sebagai manajemen keamanan jaringan.
2. Memantau aktivitas jaringan secara *real time* dengan tampilan *Graphical User Interface* (GUI).

1.4 Manfaat

Manfaat dari pembuatan sistem Implementasi Manajemen Keamanan Jaringan Menggunakan IBM QRadar SIEM di HSPNET adalah untuk administrator jaringan di HSPNET. Dengan sistem tersebut, administrator jaringan dengan mudah dapat mengetahui serangan yang terjadi pada server melalui notifikasi yang terdapat pada *website interface* IBM QRadar.

1.5 Ruang Lingkup

Ruang Lingkup dari pembuatan sistem Implementasi Manajemen Keamanan Jaringan Menggunakan IBM QRadar SIEM di HSPNET ini, yaitu :

1. Keamanan jaringan dilakukan dengan memantau aktifitas log pada *Log Activity* pada IBM QRadar SIEM.
2. Aktifitas Log yang tidak wajar atau tidak normal pada *Log Activity* akan dikirimkan ke dalam *Offenses* di IBM QRadar SIEM.
3. Mikrotik hanya mengirimkan log ke IBM QRadar SIEM berdasarkan Konfigurasi *Logging* yang berada di Mikrotik.
4. IBM QRadar SIEM hanya membaca Log yang terdaftar di dalam *Assets*, dan server lainnya yang mengkonfigurasi Lognya