BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi terus mengalami peningkatan dan kemajuan yang pesat. Hal tersebut juga mendorong adanya ancaman dalam teknologi tersebut yang terus berkembang yang harus diwaspadai oleh setiap penggiat atau orang-orang yang mengerti tentang teknologi informasi, terutama pada ancaman yang dapat memberikan dampak buruk pada suatu instansi.

Pada tahun 2010, terdapat berita besar ketika worm *Stuxnet* menyerang *Programmable Logic Controller* (PLC) pada fasilitas pengayaan nuklir di negara Iran. Secara halus memanipulasi data umpan balik pada unit sentrifugal yang dipercaya sebagai serangan pertama yang dilancarkan oleh sebuah negara sehingga fasilitas nuklir tersebut mengalami mati total.

Berdasarkan laporan dari *Cybersecurity Ventures*, ancaman terhadap jaringan pada tahun 2017 mengakibatkan kerugian sebesar 65 Triliun Rupiah, meningkan 15 kali lipat dari tahun 2015 yang memiliki kerugian sebesar 4.3 Triliun Rupiah. Sebagian besar serangan di tahun 2017 menggunakan *Malware* atau *Ransomware* yang dapat berakibat sangat buruk pada kelangsungan industri tersebut.

Honeypot merupakan sebuah sistem palsu yang sengaja dipasang oleh administrator jaringan dalam sistem yang ada untuk mengelabuhi *hacker* dimana *Honeypot* ini akan bekerja layaknya sistem asli yang lemah dan mudah untuk di serang. Konsep *Honeypot* adalah membiarkan *hacker* untuk mempenetrasi server sehingga administrator jaringan dapat mempelajari dan menganalisa perilaku penyerang, jenis serangan dan asal serangan.

Modern Honey Network merupakan *Project Honeypot* secara *Open Source* yang dikembangkan oleh *ThreatStream* yang mempunyai banyak fitur yang dapat dihubungkan dengan IDS, beberapa jenis *Honeypot*, serta database dan juga dapat menampilkan grafik serangan secara virtual dalam sebuah peta digital. *Modern Honey Network* termasuk *Honeypot* yang terbatas pada *port* dan *service* yang di berikan, namun MHN ini dapat mengumpulkan berbagai data serangan dalam satu peta serangan grafik digital.

Industrial Control System (ICS) merupakan kontrol sistem dalam industri, pengawasan atau pengandalian dalam kelompok atau organisasi dalam sebuah perusahaan atau industri secara sistematis. ICS merupakan bagian yang terpenting dalam berjalannya proses dalam sistem industri yang menggunakan teknologi. Jaringan yang bekerja dengan ICS merupakan jaringan yang sangat rawan oleh ancaman *cyber* yang dapat merugikan seluruh perusahaan atau industri tersebut.

Splunk yang merupakan aplikasi untuk pencarian, monitoring dan menganalisa *log* dari sebuah sistem atau *server* dapat mempermudah proses monitoring, *indexing* dan juga pencarian permasalahan dalam sistem.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, dapat dibuat beberapa rumusan masalah, antara lain:

1. Bagaimana cara mengetahui serangan dan merancang alat untuk mendeteksi serangan yang terjadi dan tertuju pada sistem?
2. Bagaimana cara menampilkan data dari serangan yang terjadi terhadap sistem?

1.3 Batasan Masalah

Agar pembahasan lebih terarah, maka penulis memberikan batasan-batasan pembahasan masalah, yaitu:

1. Pembahasan hanya dalam batasan *Modern Honey Network*.
2. Hanya membahas *Industrial Control System* (ICS), tidak menjelaskan *Supervisory Control and Data Acquisition* (SCADA) secara lengkap.
3. Hanya mengambil beberapa aplikasi yang ada pada MHN, yaitu : *Snort* untuk IDS/IPS, Cowrie untuk koneksi dan keamanan SSH, Dionaea untuk keamanan protokol dan juga port untuk *sharing file*, serta ConPot untuk keamanan pada ICS/SCADA atau protokol yang digunakan pada jaringan industri. Lingkup jaringan menggunakan *Virtual Private Server*.
4. Menggunakan sistem operasi Ubuntu 14.04 dan 16.04.
5. Tidak membahas *Honeypot* secara menyeluruh.

6. Sistem mengambil beberapa contoh jenis serangan antara lain *DoS Attack*, *Port Scanning, ICS & SCADA Attack* dan *Dictionary Attack.*
7. Membatasi *port* yang digunakan untuk analisa dan identifikasi serangan.

1.4 Tujuan Penelitian

1. Untuk dapat mengetahui serangan pada sistem atau *server* dan merancang *Modern Honey Network* dengan beberapa sensor *honeypot* sebagai deteksi serangan pada *server* atau sistem.
2. Untuk dapat menampilkan data dari hasil serangan yang tertuju pada sistem atau server dengan menggunakan aplikasi *Splunk* yang terintegrasi dengan *Modern Honey Network.*

1.5 Manfaat Penelitian

1. Mempermudah administrator dalam melakukan *monitoring* jaringan dan juga mengawasi serangan yang terjadi.
2. Mengembangkan *Honeypot* yang dapat digunakan untuk mengamankan ICS yang sangat penting untuk keamanan jaringan pada tingkat industri.
3. Mengerti dan memahami jenis-jenis serangan dan bagaimana membangun sistem keamanan jaringan yang baik.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

1.6.1.1 Studi Kepustakaan

Studi pustaka dilakukan untuk mempelajari dan mendapatkan pengetahuan dari buku, internet, jurnal, atau literatur yang di perlukan untuk dasar teori dalam perancangan sistem.

1.6.1.2 Metode Observasi

Metode observasi dilakukan untuk mengamati secara langsung terhadap *honeypot* yang terpasang pada jaringan publik/internet agar dapat diserang oleh penyerang dari berbagai negara. Tujuan dari observasi ini adalah untuk mendapatkan data penyerang serta mendapat informasi *port* mana saja yang jadi sasaran penyerang. Data yang didapatkan dapat digunakan untuk keperluan analisis selanjutnya.

1.6.2 Metode Pengembangan Sistem

1.6.2.1 Planning

Melakukan persiapan dan perencanaan awal pengembangan sistem seperti analisis masalah dan penjadwalan.

1.6.2.2 Analisis

Menganalisa hal yang berkaitan dengan perancangan sistem seperti identifikasi masalah, analisis kebutuhan dan analisis kelayakan.

1.6.2.3 Perancangan

Proses merancang dan konfigurasi perangkat lunak yang dibutuhkan.

1.6.2.4 Implementasi

Mengimplementasikan aplikasi untuk dapat diuji.

1.6.2.5 Testing

Metode testing atau pengujian dilakukan pada setiap sensor server.

1.7 Sistematika Penelitian

Dalam penyusunan laporan penelitian ini, akan disajikan dalam bentuk bab, antara lain sebagai berikut:

BAB I. PENDAHULUAN

Dalam bab ini, akan dibahas latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penelitian.

BAB II. LANDASAN TEORI

Dalam bab ini, akan dibahas dan dijelaskan mengenai dasar teoritis yang menjadi landasan dan pendukung dalam penulisan penelitian.

BAB III. METODE PENELITIAN

Dalam bab ini, akan dibahas mengenai dasar metode yang digunakan untuk penelitian.

BAB IV. HASIL DAN PEMBAHASAN

Dalam bab ini, akan dibahas dan dianalisa hasil penelitian dari sistem yang telah dilakukan, yaitu uji coba, *monitoring* dan deteksi serta pencegahan terhadap serangan.

BAB V. PENUTUP

Dalam bab ini, akan dibahas kesimpulan yang ada dari penelitian yang dilakukan serta saran yang dapat diberikan dari masalah yang ada dalam penelitian.

DAFTAR PUSTAKA

Dalam bab ini, berisi tentang pustaka yang dijadikan penulis sebagai bahan dan pedoman dalam penelitian.

LAMPIRAN

Berisi tentang keseluruhan *listing* program dan lampiran gambar, grafik serta tabel yang digunakan dalam pembuatan sistem.