BAB I

PENDAHULUAN

1.1 Latar Belakang

Istilah industri 4.0 istilah yang digunakan untuk revolusi industri ke-4. Di berbagai studi dijelaskan bahwa revolusi pertama dimulai dengan penemuan mesin uap pada tahun 1780an yang berkembang hingga pertengahan abad ke-19 yang memunculkan industri mekanik berbasis uap dan air. Kemudian resvolusi kedua terjadi pada akhir abad ke-19 yang ditandai dengan munculnya mesin produksi massal dengan tenaga listrik berbasis pembagian kerja (*assembly line*). Kemudian pada tahun 1970an terjadi revolusi industri yang ketiga dimana mulai era otomasi pekerjaan-pekerjaan kompleks yang didukung dengan teknologi elektronik dan informasi. Dan saat ini dikataka revolusi keempat ditandai dengan kemampuan teknologi sensor, keterhubungan, dan analisis data yang memungkinkan kustomisasi massal, integrasi rantai pasokan dan efisiensi yang lebih tinggi berbasis sistem *cyber-physical* [1].

Tantangan di era industri 4.0 memang bukan main-main, dan tidak dapat dibendung. Bisnis di segala bidang harus bersiap menghadapi perubahan global dunia yang mengkombinasikan manufaktur tradisional dan praktek industri dengan dunia teknologi. Ancaman kejahatan siber di era industri 4.0 akan semakin beragam dan masif [2]. Pasalnya semakin banyaknya perangkat-perangkat yang

terhubung langsung dengan internet atau lebih dikenal Internet of Things (IoT). Bahkan pola serangan yang semakin beragam dan kualitas serangan yang mengakibatkan kerugian yang semakin besar. Para pelaku bisnis di era industri 4.0 juga mengalami ancaman yang sama dengan organisasi lain, dimana bisnis dari semua ukuran menjadi sasaran kejahatan siber yang terus meningkat dari tahun ke tahun. Ponemon Institue dalam studinya di tahun 2018 menyatakan bahwa rata-rata kerugian akibat pelanggaran data secara global pada tahun 2018 saja telah mencapai 3,86 juta dolar atau meningkat 6,4 persen dari tahun 2017 [3]. Dan data tersebut di dukung dengan adanya salah satu mesin pencari yang bisa memberikan informasi terkait *IP Public* dan merek dari perangkat-perangkat *IoT* tersebut. Maka dari itu diperlukannya analisis terkait resiko-resiko yang akan terjadi pada era industri 4.0 ini sehingga tujuan dari penelitian saya ini adalah untuk memberikann edukasi terhadap para pelaku industri 4.0 agar perangkat-perangkat yang mereka gunakan tidak menjadi sasaran dari tindak kejahatan siber.

1.2 Rumusan Masalah

Dari uraian latar belakang diatas dapat dirumuskan sebuah permasalahan sebagai berikut :

1. Bagaimana penyerang mendapatkan informasi terkait korban atau target serangan?
2. Jenis serangan apa saja yang masih sering digunakan untuk menyerang *IP Public* dari perangkat *IoT* di era industri 4.0.
3. Apa yang harus dilakukan pelaku industri 4.0 agar perangkat mereka aman dari para pelaku *cybercrime*?

1.3 Batasan Masalah

Mengingat akan luasnya cakupan permasalahan dan agar tidak terjadi kerancuan atau pelebaran masalah, maka penulis membatasi permasalahan pada beberapa hal, yaitu:

1. Mengumpulkan informasi terkait perangkat apa saja yang mendukung industri 4.0 serta yang memiliki koneksivitas langsung ke internet melaui jaringan *IP Public*.
2. Menggunakan shodan sebagai mesin pencari perangkat *IoT* yang menggunakan *IP Public.*
3. Mencari celah keamanan terkait *device IoT(Internet of Things)* berdasarkan nomor CVE dengan minimal tahun 2016.

4. *Router, IP Cam, NAS Server, ICS, SCADA* sebagai perangkat-perangkat yang nantinya akan di analisis pada penelitian ini.

1.4 Tujuan

Berdasarkan permasalahan yang telah disampaikan oleh penulis, maka tujuan akhir dari penulisan tugas akhir ini adalah :

1. Mengumpulkan hasil analisa dari proses pengumpulan informasi secara pasif
2. Memberikan edukasi terhadap pelaku bisnis industri 4.0 agar mempunyai kewaspadaan terkait isu *cybercrime.*

1.5 Manfaat

Dari penulisan tugas akhir ini penulis mengharapkan dapat memberi beberapa manfaat. Adapun manfaat dari penulisan tugas akhir ini adalah:

1. Manfaat bagi para pelaku industri 4.0

   Memberikan informasi terkait kerentanan jaringan atau perangkat yang digunakan sebagai pendukung industri 4.0.
2. Manfaat bagi para peneliti

   Memberikan pengetahuan baru yang berlandas pada kerentanan sebuah jaringan atau perangkat yang dapat dimanfaatkan oleh para pelaku *cybercrime*.
3. Manfaat bagi para akademisi

   Memberikan referensi bagi akademisi terkait topik kerentanan jaringan atau perangkat pada industri 4.0.

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan merupakan langkah-langkah dalam penyusunan laporan tugas akhir, adapun sistematika yang digunakan penulis dalam penyusunan laporan tugas akhir adalah sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini diuraikan berisikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, metodologi penelitian, sistematika penulisan.

BAB II : LANDASAN TEORI

Berisi teori yang mengacu pada daftar pustaka, terutama menerangkan teori – teori pendukung dan aplikasi apa saja yang digunakan dalam pembuatan tugas akhir.

BAB III : PERENCANAAN DAN ANALISA PERANCANGAN SISTEM

Dalam BAB III diuraikan tentang langkah-langkah penulis dalam menganalisa permasalahan dan merancang sistem berdasarkan teori yang menunjang.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

BAB IV terdiri dari implementasi sistem yang sebelumnya telah direncanakan dan disusun.

BAB V : PENUTUP

BAB V terdiri dari kesimpulan dan saran-saran untuk melengkapi dan menyempurnakan susunan laporan tugas akhir.