BAB I

PENDAHULUAN

1.1 Latar Belakang

Belakangan ini perkembangan teknologi semakin melesat kencang, kebutuhan akan setiap pekerjaan baik individu maupun organisasi itu sangat diperlukan untuk dapat mewujudkan pekerjaan yang lebih efisien dan juga mudah. Sehingga banyak jenis industri baru yang semakin banyak bermunculan, salah satunya yang akhir-akhir naik adalah industri perusahaan Fintech. Fintech atau *Financial Technology* ini adalah sebuah arti bagi perusahaan yang bekerja dalam bidang jasa keuangan, berbeda dengan *e-commerce* yang bekerja pada bidang pemasaran barang - barang. Fintech ini lebih berfokus kepada inovasi jasa keuangan dalam bidang digital [1], inovasi dan jasa keuangan digital ini bisa di bagi menjadi dua yaitu mata uang umum atau forex (misal Rupiah, Dollar) dan mata uang kripto. Inovasi - inovasi jasa yang diberikan pada masing - masing perusahaan Fintech itu berbeda - beda, ada yang mengarah kepada investasi, *trading*, tabungan/wallet dll.

Fintech muncul sebagai cara inovatif untuk mencapai inklusi keuangan dan tujuan yang lebih luas dari pertumbuhan inklusif [1]. Selain meningkatkan kecepatan, kenyamanan, dan efisiensi layanan keuangan untuk organisasi atau usaha kecil dan menengah (UMKM) [1]. Untuk detail Fintech sendiri dijelaskan pada (BAB II), kemudian bagi perusahaan Fintech yang berfokus pada keuangan kripto, sebenarnya keuangan kripto sendiri memiliki basis keuangan sendiri yang disebut dengan Blockchain. Blockchain sendiri merupakan sebuah teknologi yang *decentralize* dan dibangun sebagai sistem penyimpanan *bank* data secara digital yang terhubung dengan kriptografi [2]. Disamping itu Blockchain memiliki aset keuangan yang disebut *cryptocurrency* [2], dan itu adalah jenis mata uang digital yang seperti Bitcoin, Ethereum, Firo dll.. Cryptocurrency tersebut dibangun dengan jaringan kriptografi dan terhubung dengan tempat penyimpanannya yang disebut Blockchain tersebut.

Disamping besar fungsionalitas Fintech dalam industri, sebenarnya ada banyak sekali bahaya kejahatan siber yang mengancamnya. Berdasarkan hasil penelitian di Kenya pada tahun 2020 - 2021 ada beberapa serangan yang paling populer di dunia *Information Technology* (IT) yaitu *Malware*, DDoS, *Web Application Attack*, *System Vulnerability* [3]. Dari beberapa daftar serangan tersebut merupakan serangan yang paling banyak diperoleh saat ini, dan dampak dari serangan tersebut sangatlah begitu besar sehingga jika perusahaan terkena dampak serangan tersebut akan dapat mendapatkan kerugian yang sangat besar. Dilansir dari Trustwave's 2015 Global Security Report, ada sekitar 98% *vulnerability* dari pengujian *web application*, serta rata - rata ada di basis *Department of Business*. Kemudian dari Innovatinn and Skills'2015 Security Survey ada skitart 90% di organisasi atau perusahaan besar, 74% dari organisasi atau perusahaan kecil [4].

Maka dari itu peran keamanan siber sangat diperlukan untuk melindungi aset perusahaan yang di miliki dari serangan siber yang ada, dan sebagai salah satu bentuk implementasi, pada dari Tugas Akhir ini saya mendapatkan riset peneilitian untuk Tugas Akhir pada perusahaan Fintech dengan basisnya di Blockchain. Faktor riset yang saya lakukan disini adalah untuk mengimplementasikan sistem keamanan baru pada perusahaan yaitu Crowdsec sebagai *Intrusion Detection/Prevention System* (IDS/IPS).

1.2 Informasi Data Serangan

Berdasarkan perolehan data internal perusahaan mengenai serangan yang pernah terjadi pada perusahaan, disini saya memperoleh informasi jenis serangan yang paling dominan sebanyak dua kali dalam 3 (tiga) tahun terakhir. Dari perolehan dominan yang dimaksud ini adalah meruapakn serangan yang paling sering terjadi dan memiliki dampak serangan yang cukup merugikan bagi perusahaan yang saya tempati saat ini. Dan unuk daftar serta jenis serangannya adalah sebagai berikut:

No.	Serangan	Target
1.	Distributed Denial of Service (DDoS)	Network
2.	Login Enumeration	API Backend

Table 1. Daftar perolehan serangan

Kemudian dari daftar serangan diatas dapat di deskipsikan untuk pemetaan resikonya sebagai berikut:

No.	Resiko	Deskripsi
1.	Distributed Denial of Service (DDoS)	*Denial of Service* (DoS) merupakan jenis serangan yang sangat merugikan bagi layanan *server*, karena serangan tersebut membuat sistem dapat mengalami *overload* sistem akibat membanjiri jaringan *server* target dengan *request* yang bertubi-tubi. Kemudian bila di sandingkan dengan *distributed* DoS ini bisa menjadi lebih berbahaya karena menggunakan *bot* atau beberapa komputer *host* agar dapat melakukan serangan yang sama ke target tujuan, hasilnya serangan tersebut bisa mejadi dua kali lipat bahkan lebih banyak dari serangan DoS bisa dengan menggunakan *satu host* saja,
2.	Login Enumeration	*Enumeration* merupakan sebuah serangan *brute-force* yang memanfaatkan kumpulan data atau biasa yang disebut *wordlist* untuk mencocokan data maupun *credential* baik itu *username*, *password* atau data sensitif lainnya. Bisanya serangan ini paling banyak di lakukan untuk mencari *login* akses pada suatu layanan.

Table 2. Daftar pemetaan resiko

1.3 Rumusan Masalah

a. Bagaimana monitoring *multiple endpoint* atau *server* menggunakan Crowdsec?
b. Bagaimana cara menyaring atau *filtering* endpoint dengan Crowdsec?

1.4 Tujuan

a. Mengatur *data sharing* antar tiap *endpoint*/*server* dan membuat halaman dashboard.
b. Menambahkan *middleware module* pada aplikasi *framework* yang dipakai.

1.5 Batasan Masalah

a. Penelitian ini di uji dan implementasi hanya dalam *instance* "latihan" saja atau secara lokal, bergantung pada izin perusahaan.
b. Untuk *operating system* dan layanan yang digunakan adalah *Amazon Web Service* (AWS) atau Virtualbox, bergantung pada izin perusahaan.
c. Penelitian ini bersifat privasi untuk riset internal perusahaan yang saya tempati kerja saat ini.
d. Jaringan internet yang digunakan bisa bersifat publik dengan VPN atau lokal, bergantung pada izin perusahaan.
e. Sebagian data yang digunakan seperti "IP" mungkin tidak semua dapat ditampilkan, bergantung pada izin perusahaan.

1.6 Sistematika Pengerjaan

Berikut ini adalah rencana kegiatan dalam pengerjaan Tugas Akhir:

a. Perancangan metode

   Bagian ini penulis mencari data informasi terkait IP perangkat yang digunakan karyawan dan juga artikel teori untuk aplikasi yang dipakai.

b. Perancangan sistem

   Setelah mencari dan mengolah data informasi tersebut, penulis merancang sistem arsitektur aplikasi kepada sistem yang akan di implementasikannya.

c. Instalasi dan konfigurasi sistem

   Kemudian penulis melakukan implementasi ke dalam sistem sesuai gambaran rancangan yang telah dibuat sebelumnya.

d. Pengujian sistem

   Setelah proses implementasi selesai, penulis mengujikan rancangan arsitektur yang dibuat sesuai dengan tujuan penelitian yang telah dibuat.

e. Analisis penelitian

   Akhir dari penelitian penulis merangkum dan menganalisa hasilnya, kemudian menyimpulkan hasil penelitiannya tersebut.

1.7 Jadwal Pengerjaan

Kegiatan	1	2	3	4	5	6
Pencatian Metode						
Perancangan Sistem						
Instalasi dan Konfigurasi						
Pengujian Sistem						
Analisis						

Table 3. Tabel jadwal pengerjaan TA