BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada industri 4.0 sudah menunjukan peningkatan lalu lintas jaringan internet yang signifikan, disamping fenomena tersebut serangan terhadap kemanan jaringan komputer juga meningkat, salah satu serangan yang sering terjadi atau sering dilakukan oleh peretas adalah *brute force attack*. Jenis serangan *brute force* adalah serangan yang bertujuan untuk membobol otentikasi sistem dengan menggunakan setiap *password* yang memungkinkan dengan kata lain serangan ini mencoba menggunakan password yang acak, metode *brute force attack* cukup banyak, mulai dari yang sederhana sampai melakukan *crack password* yang tersimpan pada database.

Berdasarkan data dari F5 yang merupakan salah satu perusahaan global yang bergerak di bidang aplikasi dan keamanan, disebutkan bahwa serangan yang paling sering digunakan oleh penyerang adalah serangan *brute force* yang jumlah kemunculannya 2,7 kali lebih tinggi dari serangan *HTTP* dan tiga kali lebih tinggi dibandingkan dengan serangan terhadap layanan *telnet*. [1]

Berdasarkan penelitian tersebut, diperlukan adanya sistem keamanan jaringan untuk mendeteksi dari serangan *brute force*, salah satunya yaitu dengan menggunakan *honeypot. Honeypot* sendiri adalah suatu cara membuat sistem palsu atau layanan palsu yang berfungsi untuk menjebak pengguna yang mempunyai tujuan buruk atau menangkal usaha-usaha yang dapat merugikan sistem atau layanan, *honeypot* sendiri terdiri dari beberapa macam yaitu; *low interaction honeypot, medium interaction honeypot dan high interaction honeypot,* disini menggunakan *medium interaction honeypot*, *honeypot* jenis ini memberikan ilusi dari operasi sistem palsu yang dapat berkomunikasi dengan penyerang. Kemudian melakukan pencatatan aktivitas dari si penyerang. *Cowrie* adalah salah satu contoh dari *medium interaction honeypot*. *Cowrie* adalah interaksi *medium SSH* dan *Telnet honeypot* yang dirancang untuk mencatat serangan *brute force* dan *interaksi shell* yang dilakukan oleh penyerang.

Cowrie juga berfungsi sebagai *proxy SSH* dan *telnet* untuk mengamati perilaku penyerang ke sistem lain. *SSH* adalah program paket yang dapat bertindak sebagai pengganti yang aman untuk *rlogin, rsh, dan rcp. SSH* menggunakan kriptografi kunci publik untuk mengenkripsi komunikasi antara dua *host*, dan juga digunakan untuk otentikasi pengguna. [2]

Adapun penelitian terkait yang menjadi referensi dalam pembuatan proyek akhir ini yaitu penelitian berjudul *Honeypot Cowrie Implementation to Protect SSH Protocol in Ubuntu Server with Visualisation Using Kippo-Graph* tahun 2019. Pada penelitian ini pemateri mengimplementasikan *Honeypot Cowrie* pada *Ubuntu server* kemudian melakukan konfigurasi menggunakan *software PuTTy* agar hasil serangan dapat divisualisasikan menggunakan *Kippo-Graph*, peneliti tidak menggunakan sistem operasi Ubuntu secara langsung melainkan menggunakan *Ubuntu server* [2]. Penelitian berikutnya yaitu *Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software Defined Network (SDN)* pada tahun 2019. Penelitian tersebut mengimplementasikan sistem deteksi serangan DDOS menggunakan *Machine Learning SVM Classifier* pada SDN dengan menggunakan 6 switch pada software mininet, penelitian dilakukan hanya simulasi menggunakan software mininet tidak mengimplementasikan SDN itu sendiri [3]. Lalu penelitian *berjudul Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack* tahun 2016. Pada penelitian tersebut proses *bruteforce* menggunakan program Aplikasi *Scaning*, maka dengan cara ini dapat dilihat secara jelas proses yang terjadi ketika sebuah *website* di serang dengan proses *bruteforce*, penelitian tidak menggunkan sistem *honeypot* sehingga serangan *bruteforce* akan masuk ke sistem asli tidak akan terperangkap ke sistem *honeypot* [4].

Berikutnya penelitian berjudul *Implementasi Honeypot Sebagai Sistem Keamanan Jaringan pada Virtual Private Server* tahun 2020. Dalam penelitian tersebut pemateri mengimplementasikan *Honeypot Cowrie* pada *Virtual Private Server*, hasil penelitian tidak divisualisasikan sehingga data serangan hanya berupa *logging* pada *honeypot cowrie* [5]. Kemudian penelitian dengan judul Perancangan dan implementasi *honeypot* pada perangkat *Internet Of Things* (IOT). Penelitian tersebut tidak di implementasikan pada SDN melainkan pada sistem IOT dan hasil atau data serangan tidak divisualisasikan menggunakan grafana [6].

Perbedaan proyek akhir ini dengan penelitian diatas adalah dengan pengimplementasian SDN dan penggabungan antara sistem *honeypot* dengan SDN.

1.2 Tujuan dan Manfaat

Adapun tujuan dari Proyek tingkat ini, sebagai berikut:

1. Dapat mengintegrasikan *Honeypot Cowrie* pada SDN menggunakan RYU *controller*
2. Mampu mengimplementasikan penyerangan *bruteforce* dengan *kali linux* pada topologi SDN
3. Dapat menampilkan data penyerangan pada *mysql database* dan *grafana*
4. Dapat menganalisa serangan ke *server Honeypot Cowrie*

Adapun manfaat dari proyek akhir ini, sebagai berikut:

1. Sebagai penunjang keamanan pada jaringan SDN
2. Sebagai penelitian terhadap sistem *honeypot*

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek akhir ini, sebagai berikut:

1. Bagaimana mengintegrasikan *Honeypot Cowrie* pada SDN menggunakan RYU *controller*
2. Bagaimana mengimplementasikan penyerangan *bruteforce* pada topologi SDN
3. Bagaimana menampilkan data penyerangan pada *mysql database* dan *grafana*
4. Bagaimana menganalisa serangan ke *server Honeypot Cowrie*

1.4 Batasan Masalah

Dalam Proyek akhir ini, dilakukan pembatasan masalah sebagai berikut:

1. Perancangan topologi SDN dengan menggunakan *RYU Controller*
2. Sistem penyerangan menggunakan teknik *bruteforce*
3. Penampilan data penyerangan menggunakan *mysql database* dan *grafana*

1.5 Metodologi

Metodologi pada penelitian ini, sebagai berikut:

1. Studi Literatur

   Hal yang dilakukan adalah mencari informasi dan pendalaman materi-materi yang terkait seperti sdn, *honeypot cowrie* dan serangan *bruteforce* melalui referensi yang tersedia di berbagai sumber.

2. Analisis Kebutuhan Sistem

   Metode yang dilakukan adalah mengumpulkan berbagai kebutuhan untuk mengerjakan proyek akhir seperti perangkat switch untuk SDN, sistem operasi *Ubuntu* dan *resource* yang dibutuhkan untuk instalasi *honeypot cowrie* dan untuk konfigurasi SDN.

3. Perencanaan Sistem

   Hal ini dilakukan dengan merencanakan sistem yang akan dibangun, seperti topologi SDN yang akan dikonfigurasi dengan sistem *honeypot cowrie*.

4. Simulasi

   Metode simulasi dilakukan dengan membangun topologi SDN pada *software mininet*, hal ini dilakukan untuk memastikan apakah *honeypot cowrie* dapat berjalan pada topologi SDN dan juga sebagai perbandingan pada saat implementasi

5. Implementasi

   Implementasi dilakukan dengan membangun topologi SDN menggunakan perangkat *switch* yang nyata dan mengkonfigurasikannya dengan sistem *honeypot cowrie*.

1.6 Sistematika Penulisan

Dalam penulisan Proyek Akhir terdiri atas lima bab, dengan keterangan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan Proyek Akhir, seperti konsep SDN, sistem *Honeypot cowrie* , serangan *bruteforce* dan lain sebagainya.

BAB III PERANCANGAN SISTEM

Pada bab ini membahas tentang deskripsi Proyek Akhir, alur pengerjaan Proyek Akhir dan perancangan sistem yang akan dibuat.

BAB IV PENGUJIAN DAN HASIL

Pada bab ini membahas tentang implementasi sistem dan pengujian.

BAB V PENUTUP

Pada bab ini membahas tentang kesimpulan dari pengerjaan Proyek Akhir dan saran untuk pembaca yang akan mengambil penelitian dengan topik yang sama.