BAB I

PENDAHULUAN

A. Latar Belakang

Pada saat ini, perkembangan internet terus berkembang pesat dan luas untuk menjangkau semakin banyak orang-orang yang mendapatkan akses internet. Dengan adanya internet, hampir seluruh kegiatan dapat dilakukan secara *online* mulai dari komunikasi dengan orang lain melalui aplikasi *chatting*, kegiatan jual beli di toko *online*, membaca buku atau jurnal pada perpustakaan *online*, dan masih banyak lagi. Akan tetapi karena semakin banyak kegiatan penting dilakukan melalui internet membuat potensi kejahatan *cyber* di internet semakin meningkat. Menurut sumber laporan terbaru dari Check Point, jumlah *cyber attack* di seluruh dunia telah meningkat 7% pada Q1 2023 dibandingkan dengan Q1 2022 [1]. Oleh karena itu diperlukan adanya sebuah sistem keamanan jaringan untuk menjaga jaringan dari *cyber attack*. Keamanan jaringan merupakan salah satu bagian yang penting dalam sebuah sistem jaringan seperti internet yang berfungsi untuk memantau akses jaringan dan untuk mencegah akses yang tidak sah masuk ke dalam jaringan. Salah satu *cyber attack* yang dilakukan melalui jaringan yaitu serangan DoS.

Serangan DoS (*Denial of Service*) merupakan salah satu ancaman *cyber* yang paling umum bagi keamanan jaringan saat ini. Menurut laporan DoS *threat* dari Cloudflare, jumlah serangan DoS meningkat dengan *ratio* 16% pada Q4 2022 dan Q1 2023. Jumlah ini lebih banyak dari Q2 2022 dengan *ratio* 13% dan Q3 2022 dengan *ratio* 14% [2]. Pada Q1 2023 ini, kebanyakan serangan DoS berbasis DNS seperti DNS *flood attack* atau DNS amplification/*reflection attack*. Serangan ini dilakukan dengan membanjiri *traffic* dari banyak sumber ke sebuah situs web atau server yang

mengakibatkan layanan pada situs web atau server tersebut menjadi lambat ataupun menjadi *offline* sehingga tidak dapat diakses oleh pengguna yang sah. Contoh kasus DoS yang pernah terjadi yaitu pada bulan Oktober 2020 yang lalu, terdapat serangan DoS yang menyerang website resmi DPR RI. Akibat serangan tersebut, dpr.go.id tidak dapat diakses dan menampilkan halaman error [3]. Dengan adanya serangan DoS yang terus menargetkan situs web atau server ini, pemilik layanan tentunya memerlukan solusi yang efektif untuk mengatasi masalah tersebut. Salah satu solusi yang dapat digunakan adalah dengan menggunakan honeypot.

Honeypot merupakan sebuah sistem keamanan yang berfungsi sebagai jebakan bagi para *hacker* yang memancing *hacker* untuk menyerang sistem yang memang sengaja dibuat untuk diserang [4]. Honeypot bisa didapatkan dengan gratis dan honeypot juga menggunakan model open source sehingga honeypot dapat dikonfigurasi untuk menyesuaikan dengan kebutuhan *user*. Honeypot juga memiliki komunitas pengguna yang aktif sehingga para pengguna dapat berbagi pengalaman, solusi, atau informasi untuk mengatasi *cyber attack*. Cara kerja honeypot yaitu dengan berpura – berpura terlihat seperti sistem yang rentan untuk diserang oleh para *hacker*. Bagi para *hacker*, sistem yang rentan pada jaringan merupakan target yang ideal untuk diretas. Dengan menggunakan honeypot, serangan dari *hacker* dapat dideteksi dan diamati sehingga membantu pemilik layanan dalam mengidentifikasi dan mengatasi serangan DoS yang menyerang situs web atau server yang dimiliki.

Dengan mempelajari dan menganalisis serangan DoS yang terjadi pada honeypot, pemilik layanan dapat memahami pola dan tipe serangan, serta mengembangkan solusi untuk mengatasi serangan DoS pada jaringan mereka. Oleh karena itu, implementasi honeypot untuk mendeteksi serangan DoS sangat penting untuk memastikan keamanan jaringan dan layanan yang tersedia bagi pengguna layanan.

B. Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana serangan DoS bekerja dan apa dampaknya pada sistem jaringan?
2. Bagaimana mengimplementasikan sistem honeypot sebagai sistem deteksi serangan DoS?
3. Bagaimana teknologi honeypot dapat digunakan untuk mendeteksi dan mengatasi serangan DoS?

C. Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Jenis serangan yang digunakan hanya berfokus pada serangan DoS dan tidak mencakup jenis serangan lainnya.
2. Solusi yang digunakan untuk mendeteksi serangan DoS hanya berfokus pada honeypot dan tidak akan membahas solusi lainnya.
3. Uji coba dilakukan pada jaringan simulasi atau virtual dan bukan pada jaringan produksi yang aktif.

D. Tujuan Penelitian

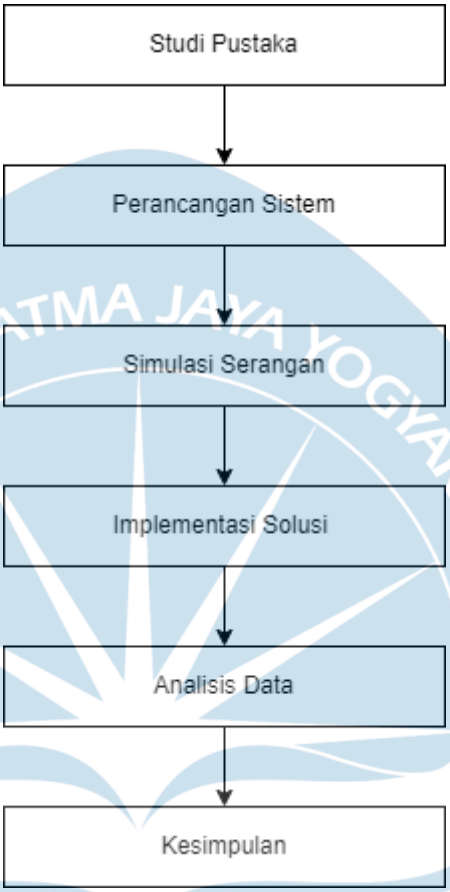
Tujuan dari penelitian ini adalah sebagai berikut:

1. Memahami bagaimana serangan DoS bekerja dan dampaknya pada sistem jaringan.
2. Mengetahui bagaimana honeypot dapat diimplementasikan dalam jaringan sebagai sistem deteksi serangan DoS.
3. Mengetahui bagaimana teknologi honeypot dapat digunakan untuk mendeteksi dan mengatasi serangan DoS.

E. Metode Penelitian

Dalam penelitian ini terdapat 6 tahap kegiatan yang dilakukan yaitu studi Pustaka, konfigurasi jaringan, skenario serangan, implementasi solusi,

analisa data, dan kesimpulan. Tahapan-tahapan tersebut digambarkan pada diagram alur seperti pada Gambar 1.1.



Gambar 1. 1 Metode Penelitian

Tahapan yang pertama yaitu studi pustaka, penulis mengumpulkan teori dan referensi dari penelitian terdahulu yang berkaitan dengan penelitian yang dilakukan penulis. Tahap kedua perancangan sistem, penulis mempersiapkan *tools* dan *device* yang dibutuhkan untuk penelitian mulai dari *setup virtual machine*, instalasi *tools*, membentuk topologi jaringan, dan menyusun skenario simulasi serangan. Tahap ketiga simulasi serangan, penulis melakukan simulasi serangan DoS menuju *device* yang menjadi target serangan. Tahap keempat implementasi solusi, penulis melakukan implementasi honeypot sebagai solusi dari serangan DoS dan melakukan pengujian honeypot. Tahap kelima analisa data, penulis melakukan analisa berdasarkan hasil simulasi serangan DoS dan pengujian honeypot terhadap

serangan DoS. Tahap keenam kesimpulan, penulis menarik kesimpulan dari analisa yang dilakukan sebagai hasil akhir dari penelitian.

Dalam melakukan analisis dan mengimplementasikan Honeypot untuk mendeteksi serangan DoS, peneliti menggunakan beberapa infrastruktur *hardware* dan *software* dalam proses pengerjaannya yaitu:

1. Perangkat Keras (*Hardware*)
   a. PC dengan spesifikasi:
      Processor : AMD Ryzen 5 5600G 3,9 GHz
      RAM : 16 GB
      Storage : Harddisk 500 GB
      OS : Windows 11

2. Perangkat Lunak (*Software*)
   a. Oracle VM VirtualBox yang menjalankan sistem operasi:
      - Linux Ubuntu 22.04 LTS sebagai honeypot yang menjalankan Apache2 Web Server, Wireshark, dan PenTBox 1.8
      - Kali Linux 2023 sebagai *attacker* yang menjalankan Nmap, Slowloris, dan LOIC (Low Orbit Ion Cannon)

F. Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bagian ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan dari penelitian yang dilakukan.

A. Latar Belakang

Berisi penjelasan singkat mengenai masalah yang diteliti serta alasan dibuatnya penelitian ini.

B. Rumusan Masalah

Berisi pertanyaan – pertanyaan mengenai masalah yang diteliti.

C. Batasan Masalah

Berisi batasan atau ruang lingkup untuk memfokuskan masalah yang diteliti.

D. Tujuan Penelitian

Berisi hasil yang ingin didapat dari pemecahan masalah yang diteliti.

E. Metode Penelitian

Berisi rancangan dari penelitian yang ingin dilakukan untuk memecahkan masalah yang diteliti.

F. Sistematika Penulisan

Berisi urutan dari penelitian yang dilakukan dari awal hingga akhir.

BAB II TINJAUAN PUSTAKA

Pada bagian ini berisi ringkasan dari penelitian – penelitian terdahulu seperti hasil penelitian, pendapat dari peneliti, maupun teori yang digunakan peneliti, yang dijadikan sebagai acuan dalam pembuatan penelitian yang dilakukan.

BAB III LANDASAN TEORI

Pada bagian ini berisi penjelasan teori – teori yang digunakan untuk mendukung penelitian yang dilakukan.

A. DoS

Berisi informasi mengenai pengertian DoS, cara penyerangan DoS, contoh serangan DoS, dan dampak dari serangan DoS.

B. Honeypot

Berisi informasi mengenai pengertian honeypot, jenis-jenis honeypot, dan contoh dari honeypot *tools*.

C. Ethical Hacking

Berisi informasi mengenai pengertian *ethical hacking*, jenis-jenis *hacker*, dan 5 fase untuk melakukan *ethical hacking* beserta *tools*nya.

BAB IV PERANCANGAN SISTEM

Pada bagian ini berisi gambaran dari sistem yang akan menjadi simulasi serangan DoS dan proteksi honeypot.

A. Topologi Jaringan

   Berisi penjelasan dari topologi jaringan yang digunakan dalam penelitian yang dilakukan.

B. Skenario Serangan DoS (*Denial of Service*)

   Berisi penjelasan dari skenario serangan DoS.

C. Kerangka Pemodelan

   Berisi penjelasan mengenai alur dari skenario serangan DoS.

BAB V HASIL ANALISIS DAN PEMBAHASAN

Pada bagian ini berisi simulasi dari proses implementasi honeypot dalam mendeteksi serangan DoS dan hasil analisisnya.

A. Persiapan Tools dan Device

   Berisi *tools* dan *device* yang digunakan dalam penelitan yang dilakukan.

B. Simulasi Serangan DoS (*Denial of Service*)

   Berisi kegiatan dari serangan DoS yang dilakukan beserta dampaknya.

C. Implementasi Honeypot

   Berisi proses dari implentasi honeypot yang kemudian dilanjutkan dengan pengujian honeypot dengan melakukan simulasi serangan DoS.

BAB VI PENUTUP

Pada bagian ini berisi kesimpulan dan saran mengenai penelitian yang dilakukan.

A. Kesimpulan

   Berisi ringkasan dari hasil penelitian yang dilakukan dan menjadi jawaban dari pertanyaan pada rumusan masalah.

B. Saran

   Berisi pendapat dari peneliti terhadap penelitian yang dilakukan.

DAFTAR PUSTAKA

Pada bagian ini berisi referensi yang digunakan penulis sebagai dasar informasi dalam mengerjakan penelitian ini.