BAB I

PENDAHULUAN

1.1. Latar belakang

Perkembangan di dunia internet saat ini mengalami kemajuan yang sangat pesat salah satunya di dunia jaringan komputer dan internet sehingga memicu pengguna internet yang semakin banyak. Hal ini menyebabkan Masalah – masalah baru yang bermunculan seperti serangan dan ancaman bagi pengguna internet saat ini. [1] Ada berbagai macam serangan yang dimaksudkan untuk mencuri data dan informasi penting dan berharga untuk di salah gunakan demi kepentingan pribadi. [2]

Perkembangan dan exploitasi kelemahan pada system jaringan komputer dan internet dengan menggunakan *malware, virus, Trojan* dan *botnet* menyebabkan setiap *user* harus waspada terhadap serangan yang dimaksud.[3]. Botnet sendiri adalah salah satu malware yang memiliki ancaman serius bagi keamanan internet. Dikarenakan botnet mampu melakukan serangan ilegal yakni *spam, phishing, klik faund,* pencurian password dan *distributed denial of serfice (DDoS) attack.*[4]

Botnet jenis baru yang telah menerapkan arsitektur *peer to peer* (P2P) Command and Control (C&C) adalah *Conficker.* Botnet ini bisa dibilang tidak memiliki kegagalan terpusat pada system, port dinamis yang digunakan

juga *payload* yang terenkripsi sehingga sulit terdeteksi. Alasan lain adalah fitur botnet dalam jaringan yang sangat mirip dengan fitur sah pada jaringan sehingga sulit untuk membedakan man jaringan yang sah dan mana yang botnet.

Metode *K-Nearest Neighbor* merupakan salah satu metode yang digunakan dalam pengklasifikasian data. Prinsip kerja K-Nearest Neighbor (K-NN) adalah mencari jarak terdekat antara data yang akan di evaluasi dengan K tetangga (neighbor) terdekatnya dalam data pelatihan (Rismawan, dkk. 2008).

Berdasarkan latar belakang tersebut, tujuan dari penelitian ini adalah mengembangkan sebuah model untuk mendeteksi anomali yang disebabkan *Peer To Peer* (P2P) botnet dengan menggunakan teknik K-Nearest Neighbor (K-NN).

1.2. Rumusan Masalah

Adapun yang menjadi rumusan masalah yaitu sebagai berikut :

a) Apakah K-NN bisa mendeteksi Anomaly Botnet?

b) Apakah K-NN dapat membedakan jaringan yang sah dan tidak sah.

1.3. Batasan Masalah

Batasan masalah penulis pada penelitian ini adalah :

a) System operasi yang digunakan adalah windows 10
b) Software yang digunakan adalah Visual Studio Code.
c) Bahasa pemograman yang digunakan adalah bahasa pemograman Python 3.

1.4. Maksud Dan Tujuan Penulisan

Tujuan dari penelitian ini adalah ;

a. Mendeteksi botnet pada jaringan peer to peer dengan menggunakan metode K-NN.
b. Membedakan jaringan yang sah dan tidak sah dengan Metode K-NN.

1.5. Manfaat Penelitian

Dengan adanya penelitian ini maka di harapkan dapat menemukan solusi atau kemungkinan terbaik memecahkan masalah serangan jaringan tidak sah yang sering terjadi dalam sebuah perusahaan/organisai tertentu sehingga dapat mencegah terjadinya pencurian data dan informasi penting dalam suatu perusahaan atau organisasi tertentu yang memiliki jaringan komputer interkoneksi yang menyebabkan kerugian bagi pemilik data dan informasi tersebut.

1.6. Metode penelitian

Metode yang digunakan didalam penelitian ini yaitu metode *K-Nearest Neighbor* adalah algoritma untuk mengklasifikasi objek baru berdasarkan atribut dan training samples (data latih). Adapun model peneliatian yang digunakan dalam penulisan ini ialah ujicoba apakah KNN dapat mendeteksi botnet secara akurat.

Setelah perangkat keras dan lunak telah siap, maka selanjutnya dilakukan instalasasi perangkat lunak kedalam PC/Laptop. Selanjutnya ialah mempersiapkan dataset yang digunakan sebagai bahan penelitian untuk mendeteksi apakah adanya botnet atau tidak pada data tersebut.

1.7. Sistematika Penulisan

Sistematika penulisan yang digunakan pada penelitian ini adalah :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, metode penelitian, rumusan masalah, tujuan penelitian, batasan masalah, dan manfaat penelitian.

BAB II LANDASAN TEORI

Bab ini membahas tentang tinjauan pustaka dan dasar teori penelitian yang menjadi dasar dalam penelitian.

BAB III METODE PENELITIAN

Bab ini membahas implementasi dari penelitian secara lengkap yang berisi alur, dan langkah-langkah yang digunakan dalam penelitian yang di jalankan

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang bagaimana cara k-NN dapat mendeteksi anomaly jaringan atau Anomaly botnet dari dataset dan menampilkan hasil akurasi keberhasilan.

BAB V KESIMPULAN DAN SARAN

Bagian ini berisi mengenai kesimpulan yang dapat diambil dari penyusunan tugas akhir, serta saran –saran penulis yang diharapkan dapat bermanfaat bagi pihak –pihak yang berkepentingan.