BAB I
PENDAHULUAN

1.1 Latar Belakang

Banyaknya perusahaan atau lembaga pendidikan yang menggunakan internet sebagai sarana untuk membantu dalam melaksanakan aktifitas rutin perusahaan dan aktifitas rutin lainnya, kemudahan dan kepraktisan merupakan kunci dari mengapa dipilihnya internet ini. Sehinga internet menjadi salah satu daftar penting dalam suatu perusahaan ataupun instansi-instansi pemerintah lainya.

Saat ini perkembangan internet sangat pesat, terbukti dengan keunggulan internet yang berdampak besar bagi kehidupan masyarakat. Internet juga menyediakan banyak fungsi, mulai dari *web server*, *file transfer protocol* (ftp), e-*mail*, dan layanan transaksi publik seperti *e-commerce*, *e-banking*, *dan e-government*. Saat ini, layanan Internet banyak digunakan oleh berbagai kelompok, termasuk bisnis, instansi pemerintah, kantor, rumah, dan universitas. Penggunaan internet disebabkan oleh kemudahan komunikasi dan transfer data. Saat bekerja dengan jaringan komputer berdasarkan jaringan area lokal dan jaringan area lokal nirkabel, topologi yang umum digunakan adalah topologi bintang dengan titik pusat pada perangkat, lebih umum menggunakan perangkat router. (Freeman, 2013).

Disamping kelebihan tersebut, internet juga mempunyai banyak kekurangan yang sangat mengkhawatirkan bagi para penggunanya ataupun instansi instansi perkantoran yang mengunakan internet, sepeti kejahatan komputer, yang meliputi pencurian, penipuan, kompetitif, banyak lagi yang lainya, seperti jatuhnya informasi ke pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik infrormasi (Ashadi Soki Agusaputra, M.Izman, 2013). Banyak kasus yang membuktikan bahwa perusahaan yang tersambung di internet sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Kasus pencurian atau manipulasi data perusahaan saja dapat mencapai kerugian sampai

jutaan rupiah. Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibilang tidak murah.

Dalam faktor keamanan ini salah satu serangan yang sering muncul adalah data flooding (Aprilianto et al., 2017). Data flooding merupakan suatu kejadian di dalam jaringan dimana dalam jaringan tersebut terjadi suatu transfer data dalam jumlah yang besar sehingga mengganggu kinerja komputer yang terhubung di dalam jaringan tersebut, hal ini kemungkinan bisa disebabkan adanya serangan dari luar yang biasa disebut dengan DOS/DDOS (Denial of Service/ Distributed Denial of Services) yaitu serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer, sehingga jaringan komputer menjadi terganggu. Untuk mengatasi hal itu biasanya digunakan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan untuk mengantisipasi agar serangan yang terjadi tidak menimbulkan kerugian yang besar.

Akibat dari kejadian tersebut maka jaringan komputer tidak lagi berfungsi seperti yang diharapkan, karena dampak dari serangan akan menghabiskan resource, menghabiskan RAM, hardisk penuh dengan data-data yang tidak penting, sehingga semua aktifitas terganggu, permintaan yang penting dari seorang user tidak bisa lagi dilayani, karena server sibuk dengan permintaan-permintaan yang tidak jelas. Untuk mengatasi masalah ini umumnya perusahaan menempatkan administrator untuk mengontrol penggunaan jaringan, tetapi administrator tentunya memiliki keterbatasan waktu. Pada saat jam kerja misalnya, kadang kala karena terlalu banyaknya aliran data tentunya administrator akan kesulitan menganalisa data-data yang lewat tersebut. Sedangkan suatu serangan bisa terjadi kapan saja. Baik pada saat administrator sedang bekerja ataupun tengah malam di mana administrator sedang istirahat dalam memantau data-data yang lewat dalam jaringannya. Oleh karena itu dalam mengatasi masalah seperti di atas dibutuhkan sistem ke dalam jaringan. Sistem diusahakan mampu membedakan apakah ini data flood atau tidak, jika data tersebut terbukti

data flood, diusahakan agar sistem bisa mengambil tindakan untuk mengantisifasi hal tersebut agar tidak menimbulkan kerugian yang besar (Nauli & Sekti, 2016).

Intranet adalah konsep LAN yang mengadopsi teknologi Internet dan mulai diperkenalkan pada akhir tahun 1995. Atau bisa dikatakan Intranet adalah LAN yang menggunakan standar komunikasi dan segala fasilitas Internet, diibaratkan berInternet dalam lingkungan lokal. umumnya juga terkoneksi ke Internet sehingga memungkinkan pertukaran informasi dan data dengan jaringan Intranet lainnya *(Internetworking)* melalui *backbone Internet*. Intranet juga disibut sebuah jaringan komputer berbasis protokol TCP/IP seperti internet hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet *(WARNET)* pun dapat di kategorikan Intranet (Haeruddin, 2021). Antar Intranet dapat saling berkomunikasi satu dengan yang lainnya melalui sambungan Internet yang memberikan tulang punggung komunikasi jarak jauh. Akan tetapi sebetulnya sebuah Intranet tidak perlu sambungan luar ke Internet untuk berfungsi secara benar. Intranet menggunakan semua *protocol TCP/IP Protokol TCP/IP*, alamat IP, dan *protokol* lainnya), klien dan juga *server*. *Protokol HTTP* dan beberapa protokol Internet lainnya *(FTP, POP3, atau SMTP)* umumnya merupakan komponen protokol yang sering digunakan. sebuah intranet dapat dipahami sebagai sebuah "versi pribadi dari jaringan Internet", atau sebagai sebuah versi dari Internet yang dimiliki oleh sebuah organisasi (Freeman, 2013)

Oleh karena itu dalam mengatasi masalah seperti di atas dibutuhkan sistem pertahanan (keamanan jaringan) di dalam server yang bisa menganalisa langsung setiap paket yang masuk ke dalam jaringan. Sistem diusahakan mampu membedakan apakah ini data *flood* atau tidak, jika data tersebut terbukti data *flood*, diusahakan agar sistem bisa mengambil tindakan untuk mengantisifasi hal tersebut agar tidak menimbulkan kerugian yang besar. Akan lebih baik jika server bisa mengantisipasi langsung, sehingga kerugian bisa mendekati nol atau tidak sama sekali.

Sekolah Menengah Kejuruan Nahdlatul Ulama 1 Kedungpring merupakan salah satu Lembaga SMK di bawah naungan Yayasan Pendidikan Ma'arif Empat Lima Kalen, yang dimana SMK NU 1 Kedungpring mempunyai 4 Kompetensi Keahlian salah satunya TKJ (Teknik Komputer dan Jaringan). Selama ini sistem

keamanan yang diterapkan di SMK NU 1 Kedungpring hanya melakukan keamanan pada segi *gateway* saja karena menganggap tidak akan ada penyerangan yang demikian. Hal tersebut tidaklah benar, serangan bisa terjadi kapanpun, dimanapun, dan kepada siapapun. Oleh karena itu Penelitian ini bertujuan untuk memberikan pemahaman saat terjadi serangan terhadap perangkat *router mikrotik* terutama terhadap serangan *DoS/DDoS* yaitu *Syn Flood Attack* dengan melakukan penigkatan keamanan jaringan menggunakan fitur pada *mikrotik router* yaitu *firewall*.

Sistem Keamanan jaringan yang baik merupakan hal yang sangat penting untuk menjaga akses data-data penting pengguna serta menjamin kenyamanan dalam penyimpanan data bagi penggunaannya. Sistem Kemanan jaringan yang ada di SMK NU 1 Kedungpring biasanya masih membutuhkan pengembangan agar terbaharui dengan perkembangan teknologi dan mampu meminimalisir segala bentuk serangan yang mungkin bisa masuk ke dalam sistem jaringan. Menyikapi keamanan tersebut dipandang perlu untuk menerapkan kebijakan teknis yang digunakan untuk mengelola user, yakni mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan (Triandi, 2015).

MikroTik Routerboard merupakan salah satu jenis router yang memiliki berbagai fitur yang lengkap dalam mendukung keamanan jaringan seperti *firewall*. *Firewall* akan memfilter data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak. Meskipun *firewall* tidak dapat mencegah serangan secara keseluruhan, setidaknya *firewall* lebih dapat membantu membuat data menjadi lebih aman daripada tanpa *firewall* sama sekali. *Firewall* yang digunakan pada penelitian ini adalah *firewall raw*. Merupakan fitur baru pada *MikroTik RouterOS* yang memungkinkan kita untuk melewatkan atau mendrop suatu koneksi sebelum masuk ke proses *connection-tracking*, oleh karena itu maka penggunaan firewall raw bisa mengurangi beban CPU secara signifikan. (Jaya et al., 2020).

Bedasarkan Penelitian sebelumnya yang di lakukan Oleh (Muhammad Fakhmi, 2021) dengan judul "Peningkatan Keamanan *Router Mikrotik* Terhadap Serangan *Ping Flood* Data dengan Menggunakan *Firewall Filter*" bahwa pemanfaatan *Router MikroTik* sebagai media keamanan jaringan dari *Ping Flood*

dengan menggunakan *Firewall Filter* dapat disimpulkan bahwa penggunaan *Firewall Filter* pada *RouterBoard MikroTik* belum terlalu efektif dalam melakukan pengamanan sistem jaringan, karena serangan-serangan diberikan salah satunya seperti *Ping Flood* yang melakukan serangan dengan melakukan pengiriman paket *PING request* kepada mesin sasaran ternyata terjadi serangan penolakan layanan sederhana di mana penyerang telah memanipulasi dan membanjiri korban dengan paket *"echo request" (ping) ICMP*.

Didalam Instansi Pendidikan khusunya sekolah-sekolah yang melakukan aktifitas pertukaran informasi, media-media pembelajaran *Online* pastinya menggunakan jaringan komputer, maka ancaman terhadap jaringan komputer akan selalu membayangi keamanan jaringan tersebut, terutama ancaman data *flooding* yang bisa terjadi kapan saja.

Berdasarkan latar belakang di atas, maka penulis akan melakukan penelitian dengan judul "*Penerapan Rancang Bangun Jaringan Intranet Berbasis Pengamanan Serangan Flooding Data Menggunakan Mikrotik di SMK NU 1 Kedungpring*". Fokus yang akan dibahas yaitu bagaimana merancang, menganalisa dan mengatasi keamanan jaringan terhadap ancaman terjadinya data *flooding* dengan model serangan *SYN Flood* pada jaringan komputer menggunakan *MikroTik* dengan Fitur *Firewall Raw*, dengan tujuan dapat mengurangi resiko ancaman keamanan jaringan yang akan mengganggu aktifitas yang yang sedang berlangsung yang disesuaikan dengan kondisi.

1.2 Rumusan Masalah

Dari uraian Latar Belakang diatas, penulis dapat menyimpulkan beberapa rumusan masalah yaitu :

1. Bagaimana membangun kamanan jaringan di SMK NU 1 Kedungpring ?
2. Bagaimana melakukan pengujian pada router *Mikrotik* menggunakan serangan *SYN Flood* di SMK NU 1 Kedungpring ?
3. Bagaimana mengatasi serangan *Syn Flood* dengan menggunakan *firewall Raw* di SMK NU 1 Kedungpring ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan dari penelitian ini adalah :

1. Mengetahui membangun kamanan jaringan di SMK NU 1 Kedungpring
2. Mengetahui melakukan pengujian pada router *Mikrotik* menggunakan serangan *SYN Flood* di SMK NU 1 Kedungpring.
3. Mengetahui mengatasi serangan *Syn Flood* dengan menggunakan *firewall Raw* di SMK NU 1 Kedungpring.

1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka di buat batasan masalah yaitu :

1. Metode pengamanan menggunakan *Firewall Raw* pada *Mikrotik.*
2. Skenario penyerangan menggunakan metode serangan *Syn Flood* pada saat proses jaringan *Router* sedang beroperasi.
3. Penyerangan dilakukan menggunakan Fitur Terminal yang ada di *Mikrotik.*
4. Penggunaan *routerboard mikrotik* sebagai keamanan jaringan hanya mencangkupi distribusi IP.
5. Topologi Jaringan yang digunakan hanya sesuai dengan yang ada di SMK NU 1 Kedungpring.

1.5 Manfaat Penelitian

Berdasarkan hasil penelitian ini diharapkan dapat memberikan kontribusi yang bermanfaat bagi perkembangan ilmu pengetahuan diantaranya sebagai berikut.

1. Memberikan kenyamanan kepada pengguna dilingkungan sekolah khususnya dalam memaksimalkan fasilitas internet yang ada.
2. Mengetahui karakteristik implementasi aplikasi monitoring di *server*.
3. Mengetahui cara melakukan pengamanan pada *Routerboard MikroTik*.
4. Mengetahui dampak serangan *Syn Flood* pada *Routerboard MikroTik.*

5. Mengetahui bukti digital pada perangkat router yang telah dilakukan penyerangan.
6. Meningkatkan sistem keamanan yang dapat di implementasikan, mencegah data *flooding* pada Instansi Sekolah khususnya di SMK NU 1 Kedungpring.

1.6 Metode Penyelesaian Masalah

Dalam penelitian ini penulis menggunakan metode *Action Research* atau penelitian tindakan merupakan salah satu bentuk rancangan penelitian yang mengutamakan tindakan secara langsung ke lapangan guna untuk mengetahui masalah apa yang sedang dihadapi dan upaya apa yang akan dilakukan dalam pemecahan masalah tersebut. Tahapan yang dilakukan dalam *Action research* yaitu :

1. Melakukan diagnosa (*diagnosing*), dalam tahapan ini yang dilakukan adalah mengidentifikasi masalah keamanan jaringan terhadap ancaman data flooding pada instansi tersebut.
2. Membuat rancangan tindakan (*action planning*), dalam tahapan ini penulis mencoba memahami pokok permasalahan dan kemudian menyusun rencana untuk melakukan penelitian.
3. Melakukan tindakan (*action taking*), dalam tahapan ini penulis melakukan penelitian langsung pada pokok permasalahan yang sudah di diagnosa.
4. Pembelajaran (*learning*), pembelajaran atau learning ini adalah tahapan terakhir yang dilakukan penulis. Dalam tahapan ini penulis menganalisa data yang telah diperoleh dari penelitian tersebut.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Merupakan Pengantar tentang latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, kegunaan penelitian, metode penyelesaian Masalah, dan sistematika pembahasan.

BAB II TINJAUAN PUSTAKA

Berisi teori yang relevan dengan penelitian yang akan dilakukan, serta hasil penelitian sejenis yang mendorong atau mendasari dilakukannya penelitian tersebut.

BAB III METODOLOGI PENELITIAN

Berisikan konsep dasar yang mendukung penelitian.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang hasil dan pengolahan data yang telah di peroleh pada saat penelitian.

BAB V PENUTUP

Berisi kesimpulan dan saran dari bab-bab sebelumnya.

LAMPIRAN-LAMPIRAN

1.8 Definisi Istilah

Beberapa definisi istilah yang digunakan dalam penelitian ini sebagai berikut.

1. *Internet*

   Internet merupakan singkatan dari *interconnected network* karena fungsinya yang menghubungkan jaringan dari jaringan-jaringan komputer yang ada di dunia.

2. Sistem

   Sistem adalah seperangkat atau pengaturan unsur yang saling berhubungan sehingga membentuk suatu kesatuan.

3. *Flooding Data*

   Flooding data adalah suatu keadaan di mana terjadi banjir (kebanjiran) data, (data terkirim dalam jumlah yang banyak).

4. *Firewall*

   sistem keamanan jaringan komputer yang mampu melindungi dari serangan *virus, malware, spam,* dan serangan jenis yang lainnya.

5. Topologi

   Cara menghubungkan sebuah komputer dengan komputer lainnya hingga membentuk suatu jaringan.

6. IP *(Internet Protocol)*

   Serangkaian angka yang menjadi identitas perangkat yang terhubung ke internet atau infrastruktur jaringan lainnya.