BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Pada zaman yang sudah maju ini, internet merupakan suatu hal yang dibutuhkan oleh semua aspek pada kehidupan manusia, melalui jaringan nirkabel kita dapat menghubungkan dua perangkat atau lebih untuk berkomunikasi tanpa harus menggunakan kabel sebagai media transmisi data. Dengan internet kita dapat berkomunikasi dengan orang yang berada jauh di luar sana melalui media sosial yang sudah beredar banyak di internet sekarang.

Pada saat ini, keamanan jaringan komputer menjadi sangat penting untuk diperhatikan, karena pada dasarnya jaringan yang terhubung ke internet tidak selalu aman dan besar kemungkinan diekspoitasi oleh hacker. Dalam perencanaannya, sistem keamanan jaringan *wireless* yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi data yang berada dalam jaringan terhadap serangan oleh para hacker.

Jenis-jenis serangan yang dilakukan oleh para hacker antara lain, *Packet sniffer, ARP Spoofing, Probe scan, Root compromise* dan *Denial of service* (Dos). Salah satu ancaman yang akan diterima oleh pengguna jaringan *wireless* adalah serangan *Packet sniffing. Packet sniffing* merupakan teknik pemantauan setiap paket yang melintasi jaringan, dan bagian dari perangkat lunak atau keras yang memoonitor semua lalu lintas jaringan. Potensi bahaya *Packet sniffing* adalah hilangnya privasi, dan tercurinya informasi penting yang dimiliki user.[1]

Dalam melakukan serangan *Packet sniffing* banyak *tools* yang digunakan, Salah satu *tools* untuk melakukan serangan *Packet sniffing* adalah *Ettercap. Ettercap* adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. *Ettercap* memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri *password*, dan melakukan penyadapan aktif terhadap protokol-protokol umum.[2]

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, rumusan masalah yang akan dikaji adalah sebagai berikut :

1. Bagaimana menganalisis keamanan jaringan internet (Wifi) untuk mengetahui sejauh mana kualitas keamanan jaringan internet (Wifi).
2. Bagaimana menganalisis keamanan jaringan internet (Wifi) terhadap serangan *Packet Sniffing*.

1.3 Batasan Masalah

Adapun yang menjadi batasan dalam penelitian ini adalah sebagai berikut :

1. Penggunaan *software Ettercap* untuk menganalisa keamanan jaringan internet (Wifi).
2. Sistem operasi yang digunakan adalah Kali Linux.
3. Pengujian hanya dilakukan pada *Protocol HTTP* dan *HTTPS*.
4. Tidak melakukan implementasi peningkatan keamanan jaringan yang ada dan hanya memberi solusi yang dilakukan ketika terjadi serangan.

1.4 Tujuan Penelitian

Adapun tujuan yang akan dicapai oleh peneliti adalah :

1. Meningkatkan keamanan terhadap topologi jaringan setelah implementasi dilakukan.
2. Berhasil mendapatkan paket data koneksi dari user yang menggunakan jaringan internet (Wifi).
3. Memberikan cara yang tepat untuk mencegah terjadinya penyerangan *Packet Sniffing*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Memberikan pemahamam bagi pengguna jaringan internet (Wifi) terhadap bahaya *Packet Sniffing* yang menyebabkan kebocoran data pengguna.
2. Memberikan solusi terbaik untuk keamanan jaringan internet (Wifi)
3. Menjadi acuan penelitian selanjutnya tentang keamanan jaringan atau keterkaitan dengan tema penelitian bagi mahasiswa maupun pembaca

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan sebagai berikut :

BAB I PENDAHULUAN

Pada BAB 1 berisi dari pokok permasalahan yang terdapat pada skripsi ini yang berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada BAB II berisi penjelasan tinjauan pustaka dan dasar teori yang mendasari permasalahan menjadi referensi dalam pembuatan penelitian.

BAB III METODE PENELITIAN

Pada BAB III berisi tentang metode yang digunakan dalam penelitian yang berisi alur dan langkah yang ditempuh dalam proses penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada BAB IV berisi tentang implementasi, hasil dan pembahasan dari pengujian serangan *packet sniffing* terhadap *protocol* HTTP dan HTTPS menggunakan *software Ettercap*.

BAB V KESIMPULAN DAN SARAN

Pada BAB V berisi tentang kesimpulan dari hasil penelitian yang

sudah dilakukan serta saran yang diharapkan dapat bermanfaat bagi penulis maupun pembaca.