BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi dan komunikasi pada saat ini mutlak menjadi suatu kebutuhan pokok yang harus dipenuhi. Bahkan untuk sebagian orang, mereka memerlukan informasi kapan pun dan dimanapun mereka berada dan teknologi yang mampu memenuhi kebutuhan tersebut adalah teknologi *wireless.* Oleh karena itu, manusia harus terus mengejar dan meningkatkan kualitas dan kuantitas teknologi komunikasi. Kemajuan teknologi pada saat ini memaksa seluruh jaringan komputer yang ada saat ini untuk mampu menunjukkan bahwa model sistem keamanan terus dianggap masih sangat penting bagi pengguna yang menginginkan suatu keamanan baik dari dalam maupun dari luar jaringan dikarenakan internet merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. Sehingga akibat yang harus ditanggung adalah jaminan keamanan dari pengguna yang terhubung secara langsung kedalam jaringan internet tersebut.[1]

Saat ini perkembangan teknologi *wireless* sangat signifikan sejalan dengan kebutuhan sistem informasi yang *mobile*. Banyak penyedia jasa *wireless* seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan *wireless* pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut. Jaringan *wireless* memiliki lebih banyak kelemahan dibandingkan dengan jaringan kabel.[2]

Dalam beberapa tahun terakhir, perkembangan teknologi *wireless* telah mengalami kemajuan besar dan membawa dampak transformasional dalam komunikasi dan akses data di berbagai bidang, termasuk dalam lingkungan kantor dinas XYZ. Teknologi *wireless* telah menjadi salah satu aspek utama yang memfasilitasi mobilitas dan produktivitas tinggi bagi para pekerja, mengatasi

keterbatasan yang sebelumnya ada pada konektivitas kabel tradisional. Meskipun memberikan manfaat yang besar, penggunaan teknologi *Wireless* juga membawa tantangan baru terkait dengan keamanan jaringan.[3]

Dengan banyaknya akses ke jaringan internet maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut. Perkembangan teknologi jaringan komputer memudahkan orang untuk memenuhi kebutuhan informasi. Salah satu teknologi yang berkembang pesat adalah teknologi media transmisi *nirkabel* atau *wireless*.[4]

Pada umumnya setiap jaringan yang terhubung melalui internet tingkat keamanannya masih rendah dan tidak selalu aman masih dapat diekploitasi oleh para *hacker*. Dalam pembangunan sebuah perancangan sistem keamanan jaringan *wi-fi* yang telah terhubung ke internet haruslah diteliti dan dipelajari sehingga dapat dipahami oleh pengguna agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh seorang *hacker* yang tidak bertanggung jawab.[5]

Kejahatan yang dimaksud berupa serangan yang bisa saja bertujuan untuk mendapatkan sumber daya, merubah konfigurasi sistem jaringan yang ada, memanipulasi data misalnya mengakses server untuk merubah konfigurasi jaringan tertentu. *Wireless* merupakan suatu hubungan telekomunikasi yang menggunakan gelombang elektromagnetik untuk dapat mengganti media kabel sebagai alat transfer data yang menawarkan beragam kemudahan, kebebasan, mobilitas, dan yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan fleksibilitas teknologi kabel yang sudah ada. Kemudahan-kemudahan yang ditawarkan *wireless* LAN menjadi data tarik tersendiri bagi para pengguna komputer dalam menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet. DoS menjadi salah satu jenis serangan siber teratas dan cukup banyak digunakan oleh para *attacker* dengan tujuan untuk melumpuhkan targetnya. Serangan DoS menggunakan volume dan intensitas tertentu yang menyebabkan target menjadi kehabisan *Resource* bahkan *Down*

ketika menangani permintaan layanan dari pengguna, sehingga membuat pengguna layanan yang sah kesulitan atau bahkan tidak dapat mengakses layanan.[6]

DoS memiliki beberapa model basis serangan, diantaranya adalah DoS berbasis *bandwidth*, dimana serangan DoS basis ini bekerja dengan mengirimkan packet data secara massal yang menyebabkan target menjadi *overload* dan kehabisan sumber daya *bandwidth* pada jaringan. Berikutnya adalah DoS berbasis lalu lintas jaringan, yang mana DoS basis ini membanjiri lalu lintas jaringan dengan sejumlah besar packet TCP, UDP, ICMP yang terlihat seolah-olah sah oleh target. Dan yang terakhir adalah DoS berbasis aplikasi, bekerja dengan memanfaatkan serangan DoS pada tingkat layer aplikasi *(layer 7)*, seperti akses ke data base, yang menyebabkan sumber dayapada layer aplikasi tersebut *Overload*.

Dalam serangan DoS, para penyerang memanfaatkan sejumlah besar perangkat yang telah terinfeksi untuk secara bersamaan menyerang satu target, menyebabkan beban lalu lintas yang berlebihan sehingga sistem menjadi tidak dapat diakses oleh pengguna yang sah. Jenis serangan semacam ini berpotensi menyebabkan gangguan serius dalam operasional dan dapat mengakibatkan kerugian finansial yang signifikan bagi kantor dinas XYZ.[7]

Metode untuk melakukan uji coba tersebut disebut dengan metode pentest atau *penetration testing*. Metode pentest merupakan metode dimana dilakukan proses percobaan menyerang pada sistem yang digunakan, dan juga diperlukan sertifikasi keamanan jaringan untuk mencegah *hacker* yang dapat menyebabkan kehilangan data dan asset sistem target. *Pentester* adalah sebutan orang yang melakukan metode tersebut. Dalam setiap pengujian diperlukan persetujuan dari pemilik sistem, jika hal tersebut tidak dilakukan maka pengujian tersebut disebut sebagai tindakan yang ilegal atau di-*hack*, yang dimana diperlukan sertifikasi keamanan jaringan untuk mencegah *hacker* yang dapat menyebabkan kehilangan data dan aset sistem target. Hasildari test pentest sangat penting bagi administrator jaringan untuk meningkatkan keamanan sistem melalui celah keamanan yang berhasil diketahui.[8]

Penetration testing (disingkat pentest) adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi/perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Metode *Penetration testing* yang akan kamigunakan menggunakan sistem operasi *tool kali linux* merupakan sistem operasi distribusi *linux* tingkat lanjut untuk melakukan pengujian keamanan, audit keamanan dengan *penetration testing* menggunakan *tool kali linux Hping3*, *Wireshark,* dan *Aircrack-ng*.[9]

Pentester adalah sebutan orang yang melakukan metode tersebut. Metode *penetration testing* dilakukan dengan cara mensimulasikan bentuk-bentuk serangan terhadap jaringan komputer. Pada pentest (sebagai lawan dari penilaian kerentanan), penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, jika memungkinkan untuk menilai apa yang mungkin diperoleh penyerang setelah eksploitasi yang berhasil.[10]

Dalam konteks ini, proposal penelitian ini bertujuan untuk menyelidiki secara mendalam tentang keamanan jaringan *wireless* dan efisiensi. Penelitian ini akan mencoba mengidentifikasi celah keamanan dan kemungkinan tantangan yang dihadapi dalam menerapkan metode *Penetration testing* di lingkungan *wireless*, khususnya pada kantor dinas XYZ. Dengan demikian diharapkan hasil penelitian ini akan memberikan wawasan yang berharga dalam mengamankan jaringan *nirkabel* dari ancaman serangan DoS, serta membantu kantor dinas XYZ untuk menghadapi tantangan keamanan yang mungkin akan muncul di masa depan.[7]

Hasil dari penelitian ini dapat memberikan kontribusi positif bagi perkembangan teknologi informasi dan keamanan di tingkat institusi, sehingga menciptakan lingkungan kerja yang lebih aman dan produktif dalam menggunakan teknologi *wireless* yang semakin berkembang pesat. Penelitian ini juga berpotensi memberikan manfaat nyata dalam upaya meningkatkan keamanan jaringan *wireless* di kantor dinas XYZ.

1.2 Permasalahan

Berdasarkan latar belakang di atas permasalahan yang timbul pada penelitian ini adalah:

1. Apa saja kelemahan keamanan pada jaringan *wireless* di kantor dinas XYZ yang memungkinkan terjadinya serangan *DoS.*
2. Bagaimana meningkatkan keamanan jaringan *wireless* dari serangan DoS (*Denial Of Service)* dengan menerapkan metode *Penetration testing.*

1.3 Tujuan

Berdasarkan permasalahan di atas, tujuan dari penelitian ini yaitu sebagai berikut:

1. Untuk mengetahui Apa saja kelemahan keamanan pada jaringan *wireless* di kantor dinas XYZ yang memungkinkan terjadinya serangan *DoS.*
2. Untuk mengetahui bagaimana meningkatkan keamanan jaringan *Wireless* dari serangan *DoS* (*Denial Of Service)* dengan menerapkan metode *Penetration testing*

1.4 Manfaat

Dalam penelitian ini, penulis mengharapkan bahwa penulisan skripsi dengan judul "Analisis Keamanan Jaringan *wireless* terhadap Serangan DoS *(Denial of Service)* menggunakan Metode *Penetration testing* pada Kantor Dinas XYZ" memiliki kegunaan dan manfaat sebagai berikut: Secara teoritis, penelitian ini dapat memberikan pemahaman mendalam terhadap keamanan jaringan *wireless* dari serangan DoS *(Denial Of Service.*

1. Secara peraktis, penelitian ini dapat memeberikan wawasan maupun pengetahuan keberbagai pihak agar lebih bisa mengembangkan suatu keamanan jaringan *wireless* yang lebih baik dari sebelumnya.