BAB I

PENDAHULUAN

1.1 Latar Belakang

Dijaman modern saat ini jaringan komputer telah mengalami perkembangan yang begitu cepat dengan berjalannya waktu kebutuhan internet sangat dibutuhkan untuk menunjang kehidupan. Semakin tingginya kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien (Riadi 2011).

Adapun permasalahan yang ada pada keamanan jaringan berada di urutan kedua, atau bahkan di urutan terakhir dalam hal-hal yang di anggap penting. Dalam jaringan komputer seperti WLAN memungkinkan menyediakan informasi yang begitu cepat dan menjadi salah satu kebutuhan bagi pemerintah, perusahaan, maupun pendidikan baik dalam bentuk aplikasi maupun website untuk membantu dalam memberikan informasi maupun dalam hal komunikasi dan meningkatkan performa konektifitas dengan memastikan bahwa lalu lintas data di jaringan

berjalan lancar. Salah satunya dengan cara mendebug jaringan dan mengamati lalu lintas data tersebut.

Pengadilan Negeri Palembang merupakan suatu lembaga pemerintahan yang bertanggung jawab sebagai salah satu pelaksana kekuasaan kehakiman bagi rakyat oleh karena itu dengan memanfaatkan jaringan komputer dapat mendukung kegiatan perkantoran serta kegiatan yang berhubungan dengan adminitrasi dalam pengelolahan data dan informasi yang dikirim melalui jaringan internet. kantor Pengadilan Negeri Palembang merupakan salah satu instansi pemerintahan yang menggunakan jaringan komputer dalam pelaksanaan kegiatan untuk saling terkoneksi dengan instansi lain dalam satu jaringan terdistribusi, memiliki sistem keamanan yang belum begitu kuat sehingga hal ini dapat menyebabkan gangguan dari luar yang ingin menyalah gunakan sistem informasi yang ada pada Pengadilan Negeri Palembang.

Dalam hal ini ada beberapa aspek dalam keamanan jaringan komputer yaitu : (Garfinkel, Spafford et al. 2003)

1. *Privacy* dan *Confidentiality* : Merupakan suatu mekanisme yang melakukan untuk melindungi suatu informasi dari pengguna jaringan yang tidak memiliki hak, sedangkan confidentiality lebih mengarah kepada tujuan dari informasi yang diberikan dan hanya boleh untuk tujuan tersebut.
2. *Integrity* : Merupakan aspek yang mengutamakan akses informasi yang ditunjukkan untuk pengguna tertentu, dimana integritas dari informasi tersebut masih terjaga.

3. *Authentication* : Aspek ini mengutamakan validitas dari user yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.
4. *Availability* : Merupakan aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan ketika data informasi tersebut diperlukan.
5. *Access Control* : Dimana aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.
6. *Repudiation* : Merupakan aspek yang berkaitan dengan pencatatan pengguna, agar pengguna data, informasi atau layanan tidak dapat menyangkal bahwa telah melakukan akses terhadap data, informasi, ataupun layanan yang tersedia.

Permasalahan yang ditemukan disini dengan mengikuti teori Garfinkel maka dalam penyelesaian permasalahan tersebut penulis akan mencoba mengevaluasi keamanan jaringan pada Pengadilan Negeri Palembang dengan menggunakan aspek keamanan yang meliputi *Privacy, Integrity, Authentication*, dan *Access Control* karena ke empat aspek ini yang sesuai dengan permasalahan diatas. Dalam kegiatan evaluasi keamanan jaringan komputer pada pengadilan Negeri Palembang penulis akan menggunakan metode PENTEST (*Penetration Testing*) untuk pengujian sistem keamanan jaringan yang sudah sesuai dengan empat aspek yang telah di sebutkan diatas makan akan menjadi acuan untuk bahan evaluasi.

Mengevaluasi keamanan jaringan dengan metode *Penetration Testing* dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali

Linux. Berbeda dengan distro-distro linux yang lain, semisal Ubuntu yang lebih mengutamakan aspek *user friendly* dan *balancing*, Kali Linux dirancang khusus untuk pengujian keamanan jaringan, dengan dilengkapi aplikasi pendukung yang digunakan dalam aktivitas *hacking* dan memanfaatkannya sebagai alat pengujian keamanan jaringan (Bayu, Yamin et al. 2018).

Selain itu karyawan juga perlu dilihat mengingat bahwa pelaku *hacking* ini adalah manusia. Terkadang karyawan yang kurang baik dapat membawa dampak buruk baik secara langsung ataupun tidak langsung. Oleh karena itu adanya permasalahan tersebut maka kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan monitor pada *server* yang berada di ruang IT lantai 1 kantor Pengadilan Negeri Palembang dan melakukan *penetration testing*. Maka penuli tertarik untuk mengangkat sebuah permasalahan tersebut sebagai bahan untuk skripsi yang berjudul "**Evaluasi Keamanan Jaringan Pada Pengadilan Negeri Palembang"**.

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah dijelaskan sebelumnya maka penulis dapat menyimpulkan rumusan masalah yang ada dalam penelitian ini, yaitu "Bagaimana keamanan jaringan WLAN Di Pengadilan Negeri Palembang sudah aman atau belum ?".

1.3 Batasan Masalah

Dalam melakukan penelitian ini penulis membatasi permasalahan agar cakupan masalah tidak terlalu luas dan tidak menyimpang dari yang sudah direncanakan sebelumnya. Adapun batasan masalah pada penelitian ini, yaitu:

1. Evaluasi dilakukan dijaringan WLAN (*wireless local area network*) pada Pengadilan Negeri Palembang.
2. Penelitian hanya akan mengevaluasi jaringan WLAN dengan menggunakan metode PENTES (*penetration testing*) pada Pengadilan Negeri Palembang.
3. Metode analisis sampai pada tahap *reporting* dan pengujian dilakukan hanya pada AP (*Accesst Point*) lantai 1.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan yang akan di capai sebagai hasil dari penelitian adalah :

1. Menguji keamanan jaringan WLAN dengan melakukan *penetration* testing agar bisa mengetahui kemampuan WPA2- *Personal* di Pengadilan Negeri Palembang terhadap berbagai macam serangan.
2. Mengetahui kelemahan jaringan WLAN di lantai 1 Pengadilan Negeri Palembang.

1.4.2 Manfaat

Adapun manfaat yang akan diperoleh penulis dan objek sebagai nilai positif yang dapat diambil dari penelitian, yaitu:

1. Bagi objek, dapat meningkatkan kualitas layanan jaringan komputer agar tidak mengalami gangguan dan menyebabkan ketidak puasaan pengguna jaringan itu sendiri.
2. Bagi dunia akademis, penelitian ini dapat menjadi bahan referensi dan dapat dikembangkan kembali apabila diperlukan untuk keperluan penelitian lebih lanjut.

1.5 Metodologi Penelitian

Disini penulis menggunakan metode penelitian kualitatif yang merupakan suatu pendekatan atau penelusuran untuk mengetahui dan memahami suatu gejala sentral. Untuk mengetahui gejala tersebut penulis mewawancarai partisipan dengan mengajukan pertanyaan umum dan sedikit luas. Informasi yang disampaikan oleh partisipan kemudian dikumpulkan, informasi tersebut biasanya berupa kata atau teks. Data yang berupa kata-kata atau teks tersebut kemudian dianalisis.

Hasil analisis tersebut dapat berupa pengambaran atau deskripsi atau dapat pula dengan bentuk tema-tema. Dari data-data itu penulis membuat interprestasi untuk mengkap arti yang terdalam. Setelah itu penulis membuat permenungan pribadi (*self-reflection*) dan menjabarkan dengan penelitian-penelitian ilmuwan lain yang dibuat sebelumnya. Hasil akhir dari penelitian kualitatif dituangkan dalam bentuk laporan tertulis (Semiawan 2010).

Tahapan penelitian kualitatif itu meliputi langkah-langkah sebagai berikut:

1. Menentukan permasalahan
2. Melakukan studi literatur

3. Penetapan lokasi
4. Studi pendahuluan
5. Penetapan metode pengumpulan data (observasi, wawancara, dokumen, diskusi terarah)
6. Analisa data selama penelitian
7. Analisa data setelah validasi dan reliabilitas
8. Hasil (cerita, personal, deskrifsi tebal, naratif, dapat dibantu table frekuensi)

1.5.1 Waktu Penelitian

Penelitian ini direncanakan selama 2 (dua) bulan yang dimulai pada bulan Desember 2018 sampai Februari 2019.

1.5.2 Tempat Penelitian

Penelitian ini beralamat di Jalan Kapten A.Rivai No.16 Palembang, Sumatera Selatan.

1.5.3 Metode Pengumpulan Data

Dalam pengumpulan data penulis menggunakan dua sumber yaitu sumber primer dan sekunder. Sumber primer adalah sumber data yang langsung memberikan data kepada pengumpul data, dan sumber sekunder merupakan sumber yang tidak langsung memberikan data kepada pengumpulan data (Noeraini and Sugiyono 2016).

Adapun tahapan yang akan dilakukan sebelum tahap analisis sistem. Berikut ini tahap – tahapannya :

1. Observasi

Penulis melakukan observasi secara langsung ke objek / lokasi / tempat penelitian yaitu Kantor Pengadilan Negeri Palembang yang kemudian mengamati dan mencatat kondisi jaringan yang tersedia.

2. Studi Pustaka

   Penulis mengumpulkan data ataupun informasi dari berbagai buku dan sumber bacaan di internet baik berupa artikel ataupun jurnal ilmiah informatika.

3. Interview

   Untuk mendapatkan informasi yang tepat, akurat dan bisa dipercaya. Penulis melakukan interview secara langsung kepada pihak terkait, dalam hal ini staff IT Kantor Pengadilan Negeri Palembang.

1.5.4 Metode Pengujian

Metode *Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari security audit. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan *Penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada (Pangalila, Noertjahyana et al. 2015).

Menurut (Wahyudi 2018) tahapan metode *penetration testing* adalah sebagai berikut:

1. Pengumpulan Intelijen *(Intelligence Gathering)* merupakan tahap pengumpulan informasi pada jaringan, layanan aplikasi, informasi tentang objek serangan pada ruang lingkup yang telah ditetapkan. Selama tahap ini, penguji mencoba mengidentifikasi mekanisme perlindungan yang ada pada system.
2. Analisis Kerentanan *(Vulnerability Analysis)* pada tahap ini penguji mencari dan menetapkan tingkat keamanan. Analisa terhadap kemungkinan kerentanan yang ditentukan akan memunculkan laporan teknik seperti *port* yang terbuka, dan lain sebagainya.
3. Model Ancaman *(Threat Modelling)* dari tahap-tahap sebelumnya, pada tahap ini penguji akan menentukan metode serangan yang efektif.
4. Membobol *Password (Password Cracking)* pada tahap ini penguji akan langsung melakukan *cracking password* berdasarkan informasi yang sudah didapatkan dengan menggunakan metode yang ditentukan pada tahap *threat modelling*.
5. Laporan *(Reporting)* adalah hasil akhir dari pengujian sistem. Penguji menyampaikan apa saja yang telah dilakukan dan apa saja temuan selama menguji sistem. Kemudian penguji menyampaikan bagaimana pemilik sistem memperbaiki dan menutup kerentanan.

1.6 Sistematika Penulisan

Dalam penulisan sistematika ini akan dijelaskan secara singkat isi dari setiap bab, yaitu sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini penulis membahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan, manfaat penelitian, metode penelitian yang dignakan, metode pengumpulan data, metode pengujian serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini penulis menjelaskan tentang landasan teori beserta materi-materi pendukung lainnya. Hal tersebut mencakup pembahasan tentang jaringan komputer, kali linux, WLAN, macam-macam keamanan jaringan komputer, macam-macam serangan, metode pengujian *penetration testing* yang dipakai untuk menguji sistem keamanan jaringan *wireless* dan beberapa lampiran penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Pada bab ini penulis menguraikan tahapan-tahapan metode *Penetration Testing* yang dilakukan terhadap beberapa aspek yang menjadi batasan masalah dalam penulisan penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini penulis memaparkan hasil dan pembahasan dari uji keamanan jaringan komputer dengan menggunakan *Penetration Testing.*

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan, serta saran dari masalah yang dihadapi untuk penelitian lebih lanjut.