BAB I
PENDAHULUAN

1.1 Latar Belakang

Sejak awal internet mulai diimplementasikan, manusia sudah tertarik untuk berbagi informasi ke seluruh dunia dan memperluas jaringan koneksinya. Berbagai perusahaan mulai melirik internet sebagai sarana perluasan jaringan dan sistem yang dapat mempermudah berjalannya sistem didalamnya.

Kemudahan-kemudahan yang ditawarkan dari adanya jaringan internet membuat manusia semakin bergantung pada keberadaan internet. Mobilitas manusia yang tinggi mempersulit akses ke internet, hal ini menjadi sebab lahirnya jaringan internet nirkabel yang dapat mengakomodasi kebutuhan ini. Standar yang digunakan dalam jaringan nirkabel kemudian dikelompokkan dan disahkan oleh IEEE melalui IEEE 802.11 yang sampai saat ini sudah terdapat 5 varian, yaitu a, b, g, n, dan y.

Data yang akan dilewatkan pada jaringan nirkabel pada umumnya adalah data yang public atau memang ditujukan untuk dipublikasikan, tetapi ada pula data-data yang bersifat rahasia. Kerahasiaan data ini harus dapat dijamin dalam pengirimannya melalui jaringan nirkabel. Selain kerahasiaan data, hal lain yang harus diperhatikan oleh implementasi jaringan nirkabel adalah adanya bermacam-macam kartu jaringan yang digunakan. Untuk mengakomodir kedua hal ini, dibangun suatu protokol yang dinamai WEP atau Wired Equivalent Privacy.

WEP adalah standard untuk otentikasi dan enkripsi yang digunakan dalam protokol ethernet nirkabel 802.11. Enkripsi yang digunakan pada WEP adalah algoritma RC4. Tetapi sangat disayangkan karena desain dan implementasi WEP yang kurang baik, sehingga membuat WEP memiliki

celah-celah keamanan yang bisa ditembus oleh para hacker untuk mengakses jaringan. Celah keamanan tersebut diantaranya terletak pada initialization vector (IV) yang hanya sebesar 24 bit, besar IV ini terlalu pendek, sehingga kemungkinan terjadi perulangan kunci hanya dalam waktu beberapa jam saja. Selain itu proses enkripsi RC4 memiliki kunci yang lemah, dan digunakan secara berulang-ulang pada proses enkripsi.

Meskipun WEP diketahui memiliki kelemahan, tetapi protokol WEP masih banyak digunakan sebagai sistem pengamanan jaringan nirkabel. Berdasarkan latar belakang ini, maka akan dilakukan studi literatur yang akan membahas proses enkripsi pada WEP serta beberapa celah-celah keamanan dari proses enkripsi tersebut. Diharapkan hasil dari penulisan ini bisa memberikan kesadaran akan adanya kelemahan pada WEP yang bisa membahayakan sistem jaringan, serta bisa digunakan sebagai sumber untuk penelitian-penelitian selanjutnya yang berhubungan dengan WEP.

1.2 Perumusan Masalah

Masalah pokok yang mendasari pemilihan topik penulisan tugas akhir ini adalah:

1. Kelemahan teknologi enkripsi yang digunakan oleh WEP
2. Kelemahan-kelemahan yang terdapat pada WEP
3. WEP masih banyak diterapkan pada jaringan nirkabel

1.3 Batasan Masalah

Batasan masalah dari penulisan tugas akhir ini adalah :

1. Analisis terhadap proses enkripsi, serta proses autentikasi pada WEP.

2. Analisis terhadap ancaman keamanan yang mungkin terjadi pada WEP.
3. Jenis serangan yang mungkin terjadi pada sistem keamanan jaringan WEP.

1.4 Tujuan dan Manfaat Penelitian

Tujuan dari penulisan tugas akhir ini adalah :

1. Untuk mengetahui bagaimana proses enkripsi pada WEP (Wired Equivalent Privacy).
2. Untuk meningkatkan kesadaran akan adanya lubang-lubang keamanan pada WEP.
3. Memberikan solusi atas beberapa celah keamanan yang mungkin terjadi pada WEP.

Manfaat penelitian ini adalah sebagai berikut :

1. Sebagai bahan pertimbangan dalam pemilihan sistem keamanan jaringan nirkabel.
2. Menjadi sumber bacaan untuk menambah pengetahuan mengenai keamanan jaringan nirkabel.

1.5 Metode Penelitian

Dalam proses meneliti, metode-metode penelitian yang digunakan dalam rangka mengumpulkan data adalah sebagai berikut :

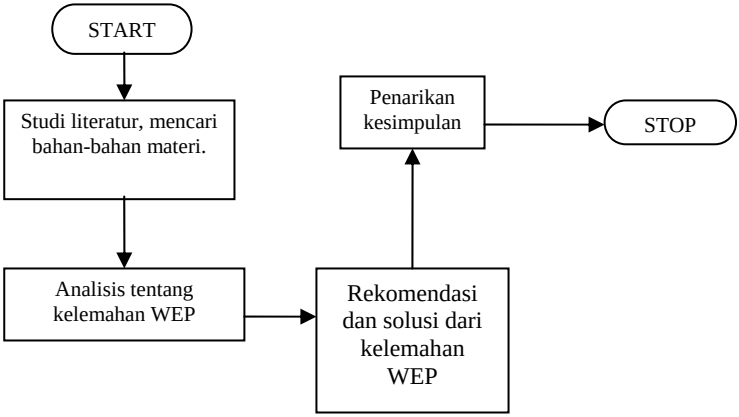
1. Studi literature

   Melakukan studi literatur dengan mencari dan mengumpulkan data-data yang berhubungan dengan *wired equivalent privacy*

(WEP) melalui beberapa sumber buku, jurnal, maupun media elektronik seperti internet.

2. Analisis data

   Melakukan analisis dari teori-teori yang membahas tentang proses enkripsi pada WEP serta kelamahannya yang didapat pada proses studi literature.



Gambar 1.1 Diagram Kegiatan Penelitian

1.6 Sistematika Penulisan

Penulisan Tugas Akhir ini dibagi dalam 5 bab, yang akan dibahas lebih rinci dalam tiap bab. Sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini, akan dibahas mengenai latar belakang, perumusan masalah, serta tujuan dari penulisan tugas akhir yang berjudul *"Analisis Proses Enkripsi pada Sistem Security Wired Equivalent Privacy (WEP)"*.

BAB II LANDASAN TEORI

Berisi tentang penjelasan teoritis dalam berbagai aspek yang akan mendukung ke arah analisis tugas akhir yang dibuat.

BAB III METODE ENKRIPSI PADA WEP

Pada bab ini, dijelaskan secara detail teknik enkripsi yang terdapat pada WEP beserta kelemahan dari proses enkripsi tersebut.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini, dibahas hasil dari pembahasan pada bab sebelumnya tentang kelemahan-kelemahan dari proses enkripsi pada WEP. Serta beberapa rekomendasi untuk menutupi kelemahan-kelemahan tersebut.

BAB V KESIMPULAN DAN SARAN

Pada bab ini, kesimpulan yang diperoleh dari serangkaian kegiatan terutama pada bagian analisa dan pembahasan. Selain itu saran-saran untuk mengamankan infrastruktur jaringan wireless yang menggunakan WEP.