BAB I
PENDAHULUAN

1.1. Tujuan

Skripsi ini bertujuan untuk membuat sistem keamanan jaringan nirkabel LAN menggunakan *FreeRadius*, dengan protokol *Protected Extensible Authentication Protocol* (PEAP) yang akan digunakan dalam pembelajaran matakuliah keamanan jaringan.

1.2. Latar Belakang

Perkembangan teknologi informasi saat ini telah sampai pada era *Broadband*. Berbeda dengan era sebelumnya, dimana akses internet, bukan saja lambat, kapasitasnya juga relatif kecil, sehingga berbagai konten yang berkembang juga masih terbatas. Namun, di era *broadband*, yang justru akan banyak berkembang adalah aplikasi-aplikasi baru yang membutuhkan *bandwidth* yang besar.

Kebanyakan orang lebih memilih teknologi *mobile* (bergerak) agar dapat mempermudah aktifitas mereka. Maka teknologi nirkabel diciptakan untuk *area network* yang langsung bersentuhan dengan orang per orang, yaitu jaringan nirkabel. Teknologi ini sangat menunjang dan menjaga tingkat produktivitas di tengah mobilitas yang tinggi. Teknologi yang juga diterapkan pada jaringan komputer atau yang lebih dikenal dengan *Wireless Local Area Network* (WLAN) atau yang trend disebut *Wi-Fi*.

Adanya peningkatan tersebut telah membawa kepada tuntutan kebutuhan suatu sistem keamanan yang tinggi. Salah satu metode keamanan yang dapat menanggulangi masalah ini adalah dengan menggunakan sistem autentikasi. Sistem ini akan melakukan proses pengesahan identitas pengguna yang biasanya diawali dengan pengiriman kode unik yang dapat berupa *username* dan *password*, bertujuan untuk memastikan benar-benar pengguna yang sah.

Wired Equivalent Privacy (WEP) adalah standar keamanan dan enkripsi pertama yang digunakan pada jaringan nirkabel, WEP adalah suatu metode keamanan jaringan nirkabel yang disebut juga dengan *Shared Key Authentication*. Enkripsi WEP menggunakan kunci yang dimasukan oleh administrator ke klien maupun *Access Point* (AP). Masalah kunci statik yang lemah dan algoritma yang mudah dipecahkan membuat WEP tidak digunakan.

Wi-fi Protected Access (WPA) adalah teknologi yang digunakan untuk menggantikan WEP. WPA dirancang menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik, dengan menggunakan *Temporal Key Integrity Protocol* (TKIP). Proses autentifikasi WPA menggunakan standar 802.1X dan *Extensible Authentication Protocol* (EAP). Secara bersamaan implementasi tersebut akan menyediakan kerangka kerja yang kokoh pada proses autentikasi *user*.

Protected EAP (PEAP) merupakan salah satu metode EAP. PEAP adalah tipe protokol autentikasi yang berbasis *username* dan *password* untuk mengamankan proses autentikasi. PEAP kebanyakan digunakan pada jaringan LAN nirkabel, tetapi dapat juga digunakan pada autentikasi kabel, *Network Access Protection* (NAP), bahkan *virtual Private Network* (VPN). PEAP hampir hanya memerlukan sertifikat digital pada sisi server saja untuk membuat TLS *tunnel* yang aman untuk melindungi autentikasi *user*. PEAP menggunakan *server-side public key certificates* untuk mengautentikasi server. Kemudian membuat TLS *tunnel* antara klien dan server autentikasi. PEAP adalah pilihan ideal untuk protokol autentikasi karena kompatibel dengan hampir semua perangkat keras dari semua vendor. Tidak hanya dari Microsoft, CISCO, Funk, dan vendor lainya juga mendukung PEAP.

PEAP merupakan pendekatan berbasis *username* dan *password* terbaik di bandingkan dengan metode EAP lainya. Selain dengan adanya TLS *tunnel* yang aman untuk memproteksi autentikasi user, PEAP juga di dukung oleh metode EAP lainya seperti EAP-MS-CHAP v2.

Remote Authentication Dial In User Service (RADIUS) adalah sebuah protokol keamanan klien/server yang berjalan di *application layer*, dan menyediakan manajemen *Authentication, Authorization, Accounting* (AAA) terpusat bagi komputer *user* yang ingin menggunakan layanan jaringan.

Tabel 1.1. Tabel Perbandingan metode EAP-TLS, EAP-TTLS, dan EAP-PEAP.

	TLS	**TTLS**	**PEAP**
Spesifikasi	RFC 2716	RFC5281	RFC4017
Implementasi klien	*Cisco, Funk,* *Meetinghouse, Microsoft,* Open1X (open source)	*Funk, Meetinghouse*	*Cisco, Microsoft, Funk,* *Meetinghouse*
Implementasi server autentikasi	*Cisco ACS, Funk* *Odyssey, Interlink* *Secure.XS, Meetinghouse* *AEGIS, Microsoft IAS,*	*Funk, Meetinghouse,* *Interlink*	*Cisco ACS, Microsoft IAS,* *Interlink Secure.XS,* *Meetinghouse, Funk*
Metode Autentikasi	X.509 *Certificates*	CHAP, PAP, MS-CHAP, MS-CHAPv2, dan EAP *methods*	EAP *methods*; pada umumnya MS-CHAPv2, *token card*, dan EAP-TLS
Struktur protokol dasar	Membuat *TLS session* dan memvalidasi sertifikat dari klien dan server	2 fase: (1) Membuat TLS antara klien dan server TTLS (2) pertukaran nilai atribut antara server dan klien	2 fase: (1) Membuat TLS antara klien dan server PEAP (2) menjalankan metode EAP dalam *TLS tunnel*
Sertifikat server	Dibutuhkan	Dibutuhkan	Dibutuhkan

Sertifikat klien	Dibutuhkan	Opsional	Opsional
Arah Autentikasi	Mutual: sertifikat digital dari klien dan *user authentication*	Mutual: Sertifikat untuk klien, *tunneled method* untuk klien	Mutual: Sertifikat untuk klien, *tunneled method* untuk klien
Proteksi terhadap identitas *user*	Tidak	Ya	Ya

1.3. Spesifikasi

Berdasarkan surat tugas nomor 70/1.3/FTEK/XI/2015, tertanggal 17 November 2015, maka skripsi ini dibuat dengan spesifikasi sebagai berikut ini.

1. Pada skripsi ini akan membuat pedoman pembelajaran dan praktikum sebuah sistem keamanan dengan menggunakan server, *Access Point* (AP), dan klien.
2. Metode yang digunakan adalah metode EAP-PEAP dengan menggunakan RADIUS dengan perangkat lunak *freeradius server*.
3. Materi-materi yang diberikan terbagi menjadi 4 pedoman untuk topik pembelajaran dan praktikum.
4. Format untuk modul pembelajaran dan praktikum adalah:
   a. Judul
   b. Tujuan
   c. Dasar teori
   d. Langkah-langkah percobaan
   e. Tugas dan analisis
5. Skripsi ini dapat direalisasikan pada laboratorium komputer. Peralatan yang dibutuhkan adalah komputer untuk server yang diinstal *Ubuntu* server, *Access Point*, dan 2 klien dengan sistem operasi *windows* dan *Ubuntu*.
6. Pengujian dan analisis sistem dilakukan menggunakan bantuan perangat lunak seperti *wireshark* untuk pembacaan paket-paket yang dikirimkan.
7. Sistem keamanan ini diuji menggunakan salah satu serangan yaitu *Dictionary Attack (Brute Force Attack).*

1.4. Sistematika Penulisan

Penulisan skripsi terdiri dari lima bab, yaitu sebagai berikut.

A. BAB I: Pendahuluan.

   Berisikan mengenai pembahasan latar belakang permasalahan, tujuan, spesifikasi, dan sistematika penulisan.

B. BAB II: Dasar Teori.

   Menjelaskan mengenai dasar teori jaringan nirkabel, RADIUS, EAP dan metode-metodenya, dan PEAP.

C. BAB III: Pedoman-pedoman.

   Membahas mengenai pedoman-pedoman yang telah dibuat sesuai spesifikasi yang telah dijelaskan pada poin 1.3.

D. BAB IV: Pengujian dan Analisis.

   Membahas mengenai hasil pengujian dari proses autentikasi metode PEAP

E. BAB V: Kesimpulan dan Saran.

   Berisikan kesimpulan dari pengujian dan analisis dan saran pengembangan.