

BAB V

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas tentang kesimpulan dari skripsi yang dibuat mulai dari tahap perancangan, penerapan, dan proses pengujian. Pada bab ini juga berisi saran pengembangan yang nantinya dapat digunakan untuk studi selanjutnya.

5.1. Kesimpulan

Berdasarkan pada hasil pengujian dapat diambil kesimpulan sebagai berikut :

1. Berdasarkan pengujian pedoman praktikum kepada mahasiswa, setiap pedoman praktikum dapat diselesaikan dalam satu sesi praktikum dengan waktu maksimal 180 menit. Berdasarkan evaluasi pedoman praktikum dari mahasiswa dapat disimpulkan bahwa mahasiswa dapat mengikuti langkah-langkah setiap pedoman praktikum yang telah dikerjakan.
2. Berdasarkan pengujian proses autentikasi dengan metode *Protected Extensible Authentication Protocol* (PEAP), proses autentikasi dengan metode PEAP dapat dilakukan dengan sistem operasi *Windows 7*, *Windows 10*, *Ubuntu 14.04*, dan *Android*.
3. Proses autentikasi dan urutan pengiriman paket-paket PEAP dapat dilihat dengan menggunakan perangkat lunak *Wireshark* dan *Microsoft Network Monitor*. Perangkat lunak *Wireshark* digunakan pada sistem operasi *Ubuntu* dengan menggunakan *monitor mode* agar bisa menangkap paket-paket dengan protokol 802.11 dan EAP. Pada sistem operasi *Windows* digunakan perangkat lunak *Microsoft Network Monitor* dengan menggunakan *monitor mode*. Perangkat lunak *Wireshark* pada sistem operasi *Windows* tidak mendukung *monitor mode* oleh karena itu pada sistem operasi *Windows* digunakan perangkat lunak *Microsoft Network Monitor* untuk menangkap paket-paket dengan protokol 802.11 dan EAP.

4. Berdasarkan pengujian serangan terhadap metode PEAP dapat disimpulkan bahwa PEAP tidak dapat ditembus dengan serangan *Dictionary Attack*, karena identitas dari klien dilindungi oleh *tunnel* TLS. Serangan *Dictionary Attack* dapat berhasil jika kata yang dicari ada didalam kamus. Metode PEAP melindungi identitas klien sehingga walaupun identitas asli klien ada pada kamus, serangan ini tidak akan berhasil karena identitas klien sudah terenkripsi oleh *tunnel* TLS yang menyebabkan tidak bisa dicocokkan dengan kata didalam kamus.

5.2. Saran Pengembangan

Beberapa saran untuk pengembangan skripsi ini adalah sebagai berikut :

1. Dapat dilakukan penelitian tentang perbandingan metode-metode EAP lainnya seperti EAP-TLS, EAP-TTLS, EAP-MD5, dan EAP-FAST.
2. Dapat dilakukan pengujian atau penelitian tentang serangan pada jaringan nirkabel menggunakan metode serangan lain seperti *Denial of Service (DOS)*, *Man in the Middle (MITM)* dan *Rogue Access Point*.

