BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan uraian penjelasan dan pembahasan keseluruhan materi pada bab-bab sebelumnya dan dalam rangka mengakhiri pembahasan tentang **"ANALISIS SERANGAN *MAN IN THE MIDDLE* SEBAGAI *ROGUE* DHCP *SERVER* MENGGUNAKAN WIRESHARK"** telah diambil kesimpulan pokok mengenai permasalahan sebagai berikut :

1. *Rogue* DHCP *server* menginterupsi jaringan DHCP dengan paket DHCPOFFER ketika DHCP *client* meminta konfigurasi alamat IP dengan mem-*broadcast* paket DHCPDISCOVER di dalam jaringan.
2. Ketika DHCP *client* melakukan proses *renew* IP di dalam jaringan DHCP yang terdapat *Rogue* DHCP *server* aktif, maka akan terjadi 2 kemungkinan yaitu mendapatkan konfigurasi alamat IP yang benar dari DHCP *server* asli atau bias jadi mendapatkan konfigurasi alamat IP yang salah dari *Rogue* DHCP *server*.
3. Ketika DHCP *client* mendapatkan alamat IP yang salah dari *Rogue* DHCP *server* dengan alamat IP gateway ditujukan pada *Rogue* DHCP *server*, maka dapat menimbulkan serangan jaringan seperti *man in the middle* dimana proses komunikasi yang dilakukan oleh DHCP *client* dengan jaringan luar terlebih dahulu melalui *Rogue* DHCP *server*.

4. Sistem *monitoring* terhadap *Rogue* DHCP *server* dilakukan dengan mengaktifkan fitur *alert* pada konfigurasi DHCP *server* di dalam mikrotik. Ketika terdapat *Rogue* DHCP *server* maka DHCP *alert* akan mencatat mac dan alamat IP sumber *server* tersebut lalu memberikan notifikasi pada *log* di dalam mikrotik.
5. Solusi pencegahan yang dibuat adalah dengan mengembangkan hasil yang didapat dari sistem *monitoring* menggunakan DHCP *alert* kemudian menggunakan *firewall* filter *rules* untuk mencegah DHCP *packets* berupa DHCPOFFER dan DHCPACK yang berasal dari *Rogue* DHCP *server* berdasarkan parameter yang ada di dalamnya.
6. Hasil pencegahan dapat dilihat dari DHCP *client* saat melakukan pencarian alamat IP di dalam jaringan DHCP dengan memperoleh konfigurasi alamat IP yang berasal dari DHCP *server* asli secara konsisten.

5.2 Saran

Dari hasil penelitian yang sudah dilakukan, terdapat beberapa saran yang dianggap perlu dipertimbangkan untuk penelitian maupun penggunaan selanjutnya, antara lain :

1. Pencegahan terhadap *Rogue* DHCP *server* dapat dilakukan dengan mengembangkan pencegahan dari sisi DHCP *client* dengan metode tertentu.
2. Penelitian akan lebih sempurna jika di teliti lebih detail tentang factor-faktor yang mempengaruhi sebuah DHCP *server* dalam merespon dan

mengirimkan DHCPOFFER kepada DHCP *client*. Sehingga dapat menghasilkan pengembangan dan teknik pencegahan yang ada.

3. Penelitian dapat dikembangkan dengan mengimplementasikan pada topologi secara umum seperti menggantikan *bridge* dengan sebuah *switch* yang umumnya lebih banyak digunakan pada infrastruktur jaringan lokal.
4. Penelitian dapat dikembangkan dengan scenario *real machine* (mesin nyata) atau dengan kata lain diimplementasikan pada jaringan yang nyata.
5. Hasil dan penelitian ini dapat dijadikan sebagai referensi pada pengembangan fitur *monitoring* dan pencegahan terhadap adanya *Rogue* DHCP *server* di dalam sebuah jaringan.