BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan uraian penjelasan dan pembahasan keseluruhan materi pada bab-bab sebelumnya dan dalam rangka mengakhiri pembahasan tentang **"ANALISIS ROGUE DHCP PACKETS MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER"** telah diambil kesimpulan pokok mengenai permasalahan sebagai berikut :

1. Pertukaran Rogue DHCP *packets* menggunakan komunikasi paket-paket DHCP pada umumnya yaitu menggunakan paket DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, dan DHCPACK.
2. Rogue DHCP *server* menginterupsi jaringan DHCP dengan paket DHCPOFFER ketika DHCP *client* meminta konfigurasi alamat IP dengan mem-*broadcast* paket DHCPDISCOVER di dalam jaringan.
3. Balasan paket DHCPOFFER yang tercepat dari DHCP *server* asli maupun Rogue DHCP *server* adalah pemenang, yang berarti proses pertukaran paket akan ditindaklanjuti oleh DHCP *client* sampai mendapatkan paket DHCPACK dari server pemenang.
4. Ketika DHCP *client* melakukan booting 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 bisa jadi mendapatkan konfigurasi alamat IP yang salah dari Rogue DHCP *server*

5. Ketika DHCP *client* mendapatkan alamat IP yang salah dari Rogue DHCP *server* dengan alamat IP *gateway* ditujukan pada Rogue DHCP *server*, maka akan menimbulkan serangan jaringan seperti *man-in-the-middle* dimana proses komunikasi yang dilakukan DHCP *client* dengan jaringan luar terlebih dahulu dilewatkan melalui Rogue DHCP *server*.
6. Sistem *monitoring* terhadap Rogue DHCP *server* dilakukan dengan mengaktifkan fitur *alert* pada konfigurasi DHCP *server* di dalam mikrotik. ketika terdapat Rogue DHCP *server* di dalam jaringan, DHCP *alert* akan mencatat alamat mac, alamat IP dan *interface* sumber *server* tersebut, lalu memberikan notifikasi pada sistem.
7. Solusi pencegahan yang dibuat adalah dengan mengembangkan hasil yang diperoleh dari sistem *monitoring* menggunakan DHCP *alert* yang dilakukan pada *intermediate device* berupa bridge mikrotik OS menggunakan *firewall filter rule*, dengan mencegah DHCP *packets* berupa DHCPOFFER dan DHCPACK yang berasal dari Rogue DHCP *server* berdasarkan parameter yang ada di dalamnya.
8. 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. Penelitian akan lebih sempurna jika diteliti lebih detail tentang faktor-faktor yang mempengaruhi kecepatan sebuah DHCP *server* dalam merespon dan mengirimkan paket DHCPOFFER kepada DHCP *client*, sehingga dapat menghasilkan pengembangan dari teknik pencegahan yang ada.
2. Pencegahan terhadap Rogue DHCP *server* dapat dilakukan dengan mengembangkan pencegahan pada sisi DHCP *client* dengan metode tertentu.
3. Penelitian dapat dikembangkan dengan mengimplementasikan skenario pada *real machine* (mesin nyata) atau dengan kata lain diimplementasikan pada jaringan yang nyata.
4. Penelitian dapat dikembangkan dengan mengimplementasikan pada topologi secara umum, seperti menggantikan bridge dengan sebuah switch yang secara umum lebih banyak digunakan pada infrastruktur jaringan lokal, serta membangun DHCP *server* di luar *intermediate device* tersebut.
5. Hasil dari penelitian ini dapat dijadikan sebagai referensi pengembangan fitur *intermediate device* seperti switch atau bridge yang dapat dikembangkan untuk melakukan *monitoring* dan pencegahan terhadap Rogue DHCP *server*.