BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

DHCP (*Dynamic Host Configuration Protocol*) adalah protokol jaringan berbasis arsitektur *client-server* yang dipakai untuk memudahkan pengalokasian alamat IP (*Internet Protocol*). Pengalokasian tersebut dilakukan oleh *server* kepada *client* yang terhubung dalam satu jaringan secara dinamis. Informasi yang diberikan DHCP tidak hanya alamat IP, akan tetapi diberikan juga informasi seperti, *default gateway*, *subnet* mask, DNS *server* dan informasi lainnya yang mendukung konektifitas antar *host* dalam satu jaringan.

DHCP adalah protokol yang paling banyak digunakan di dunia, baik digunakan dalam jaringan kabel maupun nirkabel seperti pengelolaan jaringan warung internet, jaringan perkantoran, jaringan lab kampus, *hotspot* pada *cafe* atau sarana umum, jaringan antar ISP dan *tethering* atau *portable hotspot* pada *smartphone*. Protokol ini mempunyai banyak keunggulan dibandingkan menggunakan pengalokasian alamat IP secara manual/ statis. DHCP telah digunakan secara luas, terutama pada jaringan yang berskala besar, penggunaan DHCP tersebut merupakan suatu usaha meminimalisasi konfigurasi alamat IP dan konfigurasi lainnya pada seluruh *client* dalam suatu jaringan, karena seluruh konfigurasi *client* telah diatur dan ditetapkan oleh DHCP *server*, sehingga saat terjadi penambahan *client* baru pada jaringan, dapat secara langsung berkomunikasi dengan *client*/ *host* lainnya dengan menggunakan alamat IP yang

telah ditetapkan oleh DHCP *server*. Hal ini dapat memberikan keutungan bagi *administrator* jaringan yang tidak perlu mengkonfigurasi alamat IP pada setiap *client* yang ada dalam suatu jaringan yang dapat menyita waktu kerja *administrator*, jika *client* berjumlah puluhan bahkan ratusan. DHCP juga dapat mencegah terjadinya IP *conflict* atau kesamaan alamat IP antar *client* dalam satu jaringan, yang biasanya terjadi pada konfigurasi alamat IP secara statis.

Di antara banyak keunggulan serta keuntungan yang ada, DHCP juga mempunyai beberapa kelemahan. Penggunaan DHCP diperlukan sebuah *server* untuk bertanggung jawab atas pemberian alamat IP kepada *client*, jika DHCP *server* mati maka seluruh *client*/ *host* dalam jaringan tersebut tidak terhubung satu sama lain karena DHCP dibangun dengan sistem terpusat. Kelemahan lain dari protokol ini adalah adanya celah keamanan jaringan yang dapat digunakan oleh *network attacker* untuk melakukan jenis serangan *man-in-the-middle* menggunakan Rogue DHCP *server*. Rogue DHCP *server* adalah DHCP *server* pada sebuah jaringan komputer yang tidak memiliki wewenang administratif atau bisa disebut *server* palsu yang digunakan untuk melakukan serangan jaringan dengan menggunakan beberapa *tools* atau aplikasi didalamnya terhadap *server* maupun *client*, sehingga DHCP *server* asli tidak dapat berfungsi secara optimal dalam memberikan layanan terhadap *client*. Rogue DHCP *server* di dalam sebuah jaringan akan merusak sistem keamanan dan menimbulkan masalah privasi bagi *client* yang dapat menciptakan serangan jahat seperti *sniffing* lalu-lintas jaringan, serangan *masquerading*, dan serangan DoS. Hal ini dapat digunakan oleh para penyerang untuk mengarahkan dan mengintersepsi lalu lintas jaringan dari

perangkat apapun yang tergabung dalam jaringan DHCP sehingga penyerang menjadi *man-in-the-middle* yang dapat melihat dan memodifikasi isi asli dari komunikasi (Razaque dan Elleithy, 2012).

Rogue DHCP *server* adalah ancaman jaringan yang nantinya akan dibahas dalam penelitian ini, dengan lebih memfokuskan pada analisis paket-paket DHCP yang berasal dari Rogue DHCP *server* yang disebut Rogue DHCP *packets* maupun paket DHCP yang berasal dari DHCP *server* asli yang berjalan dalam jaringan DHCP ketika DHCP *server* asli dan Rogue DHCP *server* saling mengirim dan membalas pesan terhadap DHCP *client* dengan menggunakan Wireshark *Network Protocol Analyzer*, sehingga dalam penelitian ini akan mendapatkan informasi akurat yang nantinya dapat menjadi acuan untuk memecahkan masalah keamanan jaringan DHCP terhadap Rogue DHCP *server*.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah :

1. Bagaimana proses pertukaran paket DHCP dalam sebuah jaringan DHCP?
2. Bagaimana proses pertukaran paket DHCP ketika terdapat Rogue DHCP *server* dalam sebuah jaringan DHCP?
3. Apa dampak yang terjadi dengan adanya Rogue DHCP *server* dalam jaringan DHCP?
4. Bagaimana solusi pencegahan terhadap Rogue DHCP *server* di dalam sebuah jaringan DHCP?

5. Bagaimana proses pertukaran paket DHCP setelah dilakukan pencegahan terhadap Rogue DHCP *server*?

1.3. Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Penelitian difokuskan pada pengamatan lalu-lintas dan analisis paket DHCP pada jaringan IP versi 4 antara DHCP *server* asli, Rogue DHCP *server* dan DHCP *client* dengan menggunakan aplikasi Wireshark *Network Protocol Analyzer*.
2. Penelitian menggunakan *virtual machine* (VMWare Workstation 9.0.2) untuk membangun skenario jaringan meliputi 1 DHCP *server* (OS Mikrotik v 5.20) yang terkoneksi dengan internet, 1 DHCP *client* (OS Windows XP SP2), 1 client sebagai pemantau (OS Windows XP SP2 + Wireshark 1.12.0), 1 DHCP client *attacker* yang berperan sebagai Rogue DHCP *Server* (OS Linux Backtrack 5. R1), dengan koneksi antar *host* dalam jaringan menggunakan vmnet.
3. DHCP *server* dibangun sekaligus di dalam *intermediate device* menggunakan mode *bridge* yang tujuannya dijadikan layaknya sebuah *managable switch*.
4. Implementasi Rogue DHCP *server* dibuat agar DHCP *client* mendapat konfigurasi alamat IP yang salah dengan alamat IP *gateway* ditujukan pada alamat IP Rogue DHCP *Server*.
5. Penerapan keamanan jaringan pada *intermediate device* (bridge) yang menghubungkan antara DHCP *server* dengan DHCP *client*, dilakukan terbatas

pada pencegahan dan *monitoring* paket DHCP menggunakan fitur yang ada di dalam mikrotik OS.

1.4. Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini dimaksudkan untuk menganalisis Rogue DHCP *packets* yang disebarkan oleh Rogue DHCP *server* di dalam jaringan DHCP, serta memberikan solusi pencegahan dan *monitoring* pada *intermediate device* yang menghubungkan antara DHCP *server* dengan DHCP *client* terhadap Rogue DHCP *server* di dalam jaringan DHCP.

1.5. Manfaat Penelitian

Adapun manfaat yang dapat diambil dari hasil penelitian ini adalah :

1. Sebagai referensi atau acuan dalam penerapan sistem keamanan jaringan DHCP terhadap Rogue DHCP *server*.
2. Sebagai acuan untuk pengembangan fitur pada perangkat jaringan dalam pencegahan Rogue DHCP *server*.
3. Memberikan alternatif pengembangan keamanan jaringan DHCP terhadap Rogue DHCP *server* dengan biaya rendah dan hasil maksimal.
4. Untuk meningkatkan keamanan DHCP *server* yang menggunakan Mikrotik Router OS pada mode *bridge*.
5. Kerahasian, integritas, dan ketersediaan data bagi *client* yang tergabung dalam jaringan DHCP dapat terjamin.
6. Menjaga stabilitas DHCP *server* dalam memberikan pelayanan terhadap *client*.

1.6. Metode Penelitian

1.6.1. Metode Pengumpulan Data

Demi mendapatkan data yang benar, relevan dan terarah sesuai topik yang dihadapi, maka diperlukan metode yang tepat untuk mencapai maksud dan tujuan penelitian. Adapun sumber data untuk kelengkapan kegiatan penelitian ini menggunakan metode-metode sebagai berikut:

1.6.1.1. Metode Studi Pustaka

Mengumpulkan dan mempelajari referensi yang berhubungan erat dengan analisis jaringan DHCP, ancaman jaringan seperti Rogue DHCP Server dan teknik keamanan jaringan DHCP dalam bentuk jurnal ilmiah internasional, jurnal ilmiah nasional, buku, artikel atau video yang didapat dari koleksi pribadi, perpustakaan, atau dari internet.

1.6.1.2. Metode Uji Coba

Uji coba dilakukan pada jaringan DHCP dengan satu DHCP *server* asli yang ditambahkan Rogue DHCP *server* pada salah satu DHCP *client* di dalamnya. Uji Coba dilakukan dengan menggunakan salah satu DHCP *client* untuk melakukan permintaan alamat IP di dalam jaringan. Uji coba dilakukan untuk melihat proses pertukaran paket DHCP antara DHCP *server* asli, Rogue DHCP *server* dan DHCP *client*.

1.6.1.3. Dokumentasi

Pada tahap ini dilakukan pembuatan laporan mulai dari studi pustaka sampai dengan implementasi, serta penarikan kesimpulan dan saran.

1.6.2. Metode Analisis

Analisis dilakukan dengan pengamatan terhadap pertukaran paket DHCP serta menguraikan paket tersebut untuk mengetahui parameter apa saja yang terkandung di dalamnya guna sebagai acuan pencegahan, dan dilakukan perbandingan pertukaran paket DHCP pada kondisi sebelum terdapat ancaman, setelah terdapat ancaman dan setelah adanya solusi pencegahan terhadap ancaman Rogue DHCP *server* di dalam jaringan DHCP.

1.6.3. Metode Perancangan

Sebelum melakukan penelitian, dibuat skenario berupa desain topologi jaringan yang akan dibangun serta kerangka kerja yang akan dilakukan untuk memudahkan dalam penelitian.

Topologi jaringan dibangun dengan mempertimbangkan kondisi hardware dan software yang ada. Mesin *virtual* menggunakan VMWare menjadi solusi untuk pengimplementasian desain topologi jaringan dalam penelitian ini. Selain lebih ekonomis juga bersifat *realistic, controllable, repeatability*, dan *real-time* sehingga VMWare valid dan layak digunakan dalam penelitian (Zhang dan Sun, 2012).

Kerangka kerja penelitian dibuat secara *step-by-step* sebagai pedoman jalannya penelitian sehingga proses penelitian lebih efektif dan efisien.

1.6.4. Metode Pengembangan

Penelitian dilakukan dengan implementasi topologi jaringan DHCP pada kondisi normal, selanjutnya dianalisis pertukaran paket DHCP yang terjadi. Setelah itu dilakukan implementasi ancaman Rogue DHCP *server* di dalam jaringan, yang selanjutnya dianalisis pertukaran paket DHCP yang terjadi. Setelah itu dilakukan perbandingan pertukaran paket DHCP yang terjadi antara kondisi normal dan kondisi setelah adanya ancaman, serta dilakukan penguraian untuk mendapatkan parameter paket-paket DHCP yang digunakan untuk implementasi keamanan jaringan berupa *monitoring* dan pencegahan terhadap Rogue DHCP *server*. Setelah implementasi *monitoring* dan pencegahan, akan dilakukan kembali analisis pertukaran paket DHCP serta perbandingan dengan kondisi sebelumnya untuk memastikan bahwa *monitoring* dan pencegahan terhadap Rogue DHCP *server* di dalam jaringan berjalan dengan baik.

1.6.5. Metode Testing

Pengujian dilakukan menggunakan Wireshark *Network Protocol Analyzer* untuk mengetahui lalu-lintas paket DHCP yang berjalan sebelum terdapat ancaman, setelah terdapat ancaman dan setelah adanya solusi pencegahan terhadap ancaman Rogue DHCP *server* di dalam jaringan DHCP, serta untuk mengetahui pula kekuatan Rogue DHCP

packets dalam mengiterupsi jaringan DHCP, dan kekuatan keamanan jaringan yang diterapkan.

1.7. Sistematika Penulisan

Secara garis besar laporan penelitian ini terdiri dari 5 (lima) bab dengan beberapa sub bab. Agar mendapat arah dan gambaran yang jelas mengenai hal yang tertulis, berikut ini sistematika penulisannya secara lengkap.

BAB I. PENDAHULUAN

Bab ini menguraikan latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II. LANDASAN TEORI

Bab ini memperkuat gagasan-gagasan yang muncul dengan memberikan landasan teori akurat dari berbagai sumber dan konsep-konsep dasar dalam memecahkan masalah keamanan jaringan DHCP yang meliputi penelitian tentang Rogue DHCP server, teknik analisis yang dipakai dan upaya pencegahannya.

BAB III. ANALISIS DAN PERANCANGAN

Bab ini berisi tentang persiapan hardware dan software yang dibutuhkan dengan membuat skenario berupa desain topologi jaringan yang akan dibangun, serta kerangka kerja yang akan dilakukan untuk memudahkan dalam

penelitian, dan akan dijabarkan pula analisis-analisis tentang variable-variabel yang akan diteliti.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini akan dibahas mengenai implementasi DHCP *server* asli dan Rogue DHCP *server*, penangkapan dan pemfilteran lalu-lintas DHCP *packets* menggunakan Wireshark, implementasi pencegahan ancaman pada *intermediate device* yang digunakan, serta pembahasan hasil pencegahan.

BAB V. PENUTUP

A. Kesimpulan

Berisi pemaparan singkat mengenai hasil dari penelitian.

B. Saran

Berisi saran dari yang direkomendasikan untuk pengembangan penelitian selanjutnya agar hasil yang diperoleh lebih optimal.

DAFTAR PUSTAKA

Berisi seluruh sumber yang digunakan dalam pembuatan laporan penelitian yang berasal dari buku, jurnal, dan informasi dari situs internet.

1.8. Rencana Kegiatan

Penelitian ini diperkirakan akan membutuhkan waktu selama tiga bulan. Uraian dari rencana kegiatan dapat dilihat pada Tabel 1.1.

Tabel 1.1 Rencana Kegiatan

No	Jenis Kegiatan	Sept 2014				Okt 2014				Nov 2014			
		7	14	21	28	7	14	21	28	7	14	21	28
A	**PERSIAPAN**												
1	Pengajuan Proposal												
B	**PELAKSANAAN**												
1	Studi literatur												
2	Membuat skenario dan topologi jaringan.												
3	Implementasi dari skenario dan topologi jaringan												
4	Analisis paket												
5	Perancangan sistem pencegahan												
6	Implementasi dari perancangan sistem pencegahan												
7	Analisis Hasil												
C	**Evaluasi Penulisan Laporan dan penggandaan**												
1	Evaluasi												
2	Perbaikan												
3	Penulisan Laporan dan penggandaan												