BAB I
PENDAHULUAN

1.1 Latar Belakang

DHCP merupakan protokol *client-server* yang digunakan untuk memberikan alamat IP sepada komputer *client* atau perangkat jaringan secara otomatis. DHCP *server* tidak hanya memberikan alamat IP saja, tetapi juga memberikan *netmask*, *host name*, *domain name* DNS dan alamat *gateway* juga.

Diantara 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 distem terpusat. Kelemahan lain yang ada didalam protokol ini adalah adanya celah keamanan jaringan sehingga kemungkinan hadirnya *client* dan *server* yang nakal sangatlah besar. Sebagai contohnya adalah serangan *Man in the Middle* yaitu *client* yang berperan sebagai *Rogue* DHCP *server* atau DHCP *server* palsu yang bertujuan untuk menyediakan informasi palsu, membaca *traffic* pengguna lain dan bahkan melakukan serangan *Denial of Service* (DoS), sehingga DHCP *server* asli tidak dapat berfungsi secara optimal dalam memberikan layanan terhadap *client*.

Dengan adanya permasalahan ini penelitian dilakukan untuk mengetahui bagaimana proses terjadinya serangan terhadap DHCP *server*, sebelum adanya

Rogue DHCP *server*, setelah adanya *Rogue* DHCP *server*, dan setelah adanya pencegahan terhadap *Rogue* DHCP *server* di dalam jaringan DHCP berbasis IPv4.

1.2 Rumusan Masalah

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

1. Bagaimana proses terjadinya serangan terhadap DHCP?
2. Bagaimana proses pertukaran paket DHCP ketika terdapat *Rogue* DHCP *server* di dalam sebuah jaringan?
3. Bagaimana solusi pencegahan terhadap Rougue DHCP *server* di dalam sebuah jaringan?

1.3 Batasan Masalah

Untuk mendapatkan arah dan tujuan yang baik dan tidak terlalu menyimpang, maka masalah akan di batasi sebagai berikut :

1. Penelitian menggunakan *virtual machine* (VMWare Workstation 11.0.0) untuk membangun scenario jaringan meliputi 1 DHCP *server* (OS Mikrotik v 5.20) yang terkoneksi dengan internet, 1 DHCP *client* (OS Windows 7 Ultimate), 1 DHCP *client* sebagai pemantau (OS Windows 7 Ultimate + Wireshark 1.4.0), 1 DHCP *client attacker* yang berperan sebagai *Rogue* DHCP *server* (OS Kali Linux), dengan koneksi antar *host* dalam jaringan menggunakan wmnet.
2. Penelitian difokuskan pada proses terjadinya serangan terhadap DHCP *server* dan menganilis paket DHCP pada jaringan antara DHCP *server*

asli, *Rogue* DHCP *server* dan DHCP *client* dengan menggunakan aplikasi *Wireshark Network Protocol Analyzer*.

3. DHCP *server* dibangun sekaligus di dalam jaringan menggunakan mode *bridge* yang tujuannya dijadikan layaknya sebuah *switch*.
4. Implementasi *Rogue* DHCP *server* dibuat agar DHCP *client* mendapatkan konfigurasi alamat IP yang salah dengan alamat IP *gateway* ditujukan pada alamat IP *Rogue* DHCP *server*.
5. Penerapan keamanan jaringan yang menghubungkan antara DHCP *server* dengan DHCP *client* dilakukan terbatas.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Maksud dari penelitian dengan judul "Analisis serangan *Man in the Middle* sebagai *Rogue* DHCP *server* menggunakan Wireshark" adalah.

1. Untuk memenuhi persyaratan dalam mencapai gelar sarjana pada program studi S1 Informatika di Universitas AMIKOM Yogyakarta.
2. Untuk mengetahui proses terjadinya serangan terhadap sebuah jaringan dan untuk mengembangkan kualitas jaringan di masa mendatang.

1.4.2 Tujuan Penelitian

Tujuan dari penelitian yang dibuat adalah sebagai berikut:

1. Untuk mengetahui proses terjadinya serangan terhadap DHCP *server* dan melakukan pencegahan.
2. Menerapkan pengetahuan yang dimiliki untuk diterapkan di keadaan yang sebenarnya.

1.5 Manfaat Penelitian

Manfaat dari penelitian yang dibuat adalah

1. Mahasiswa mampu membuat sebuah jaringan didalam *virtual machine* dan melakukan analisi terhadap jaringan tersebut.
2. Mahasiswa mengetahui alur terjadinya serangan *Rogue* DHCP *server* dan agar dapat melakukan pencegahan terhadap serangan *Rogue* DHCP *server*.
3. Memperkuat keamanan sebuah jaringan untuk meminimalisir serangan yang kemungkinan akan terjadi.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah

1. Studi Pustaka

   Mengumpulkan literature berupa teori-teori seperti: jurnal, buku, dan artikel-artikel yang berhubungan dengan penilitian yang dilakukan.

2. Eksperimen

   Membuat dan merancang sebuah jaringan kemudian melakukan pengamatan terhadap proses terjadinya serangan *Rogue* DHCP *server* dan melakukan pengamatan paket DHCP sebelum adanya *Rogue* DHCP *server* dan sesudah adanya *Rogue* DHCP *server*.

1.7 Sistematika Penulisan

Dalam penelitian ini penulis membuat sistematika penulisan kedalam beberapa bab dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan membahas dasar-dasar teori yang digunakan dalam penelitian dan mendukung pelaksanaan penulisan penelitian.

BAB III METODE PENELITIAN

Bab ini akan membahas mengenai pemaparan yang digunakan dalam pengumpulan data.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini akan membahas mengenai proses analisis bagaimana terjadinya serangan terhadah DHCP *server*, alur lalu lintas paket DHCP sebelum adanya *Rogue* DHCP *server* dan sesudah adanya *Rogue* DHCP *server* dan juga bagaimana melakukan pencegahan terhadap serangan *Rogue* DHCP *server*.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran dari penulis berdasarkan hasil analisis yang ada untuk meningkatkan keamanan jaringan terutama pada jaringan yang menggunakan DHCP *server*.