BAB I
PENDAHULUAN

1.1. Latar Belakang

Berkembangnya terhadap teknologi dizaman sekarang sangat cepat dalam perkembangannya sehingga banyak dari perusahaan lebih mengutamakan jaringan komputer dapat mempermudah dalam mengatur membagikan data. Dengan adanya jaringan komputer yang dapat menghasilkan kinerja yang optimal daripada tidak memakai jaringan komputer (Ariyadi, 2017).

Dalam penggunaan jaringan komputer banyak yang harus memiliki *IP address* dalam penggunaan suatu perusahaan. Salah satu jaringan yang memerlukan *IP address* agar bisa berkomunikasi antara lain seperti penggunaan komputer satu dengan komputer lainnya. Untuk penggunaan *IP address* dalam jaringan komputer akan memberikan *IP address* secara langsung melalui *DHCP Server*. Untuk *DHCP Server* sendiri memiliki tugas yaitu memberikan *IP* pada komputer-komputer yang sebelumnya sudah diberikan konfigurasi dan setelah itu dihubungkan lagi ke komputer-komputer yang sudah terhubung satu sama lain, agar dari jaringan admin tidak perlu lagi untuk memberikan *IP Address* secara manual dari komputer yang lain (Bayu & Nurhanif, 2018).

Seiring dengan berjalannya waktu pada pengguna jaringan komputer, ada beberapa peretas yang sudah memikirkan berbagai cara agar dapat informasi dari perusahaan. Maka dari itu, diperlukannya dalam meningkatkan keamanan pada jaringan komputer. Sebagai contoh peretas yang sering digunakan yaitu menggunakan *DHCP Rogue,* dimana peretas tersebut dapat membuat *DHCP Server* palsu terhubung dalam satu jaringan komputer utama diperusahaan. Akibatnya, beberapa dari komputer *client* pada saat menggunakan *DHCP Server* yang utama pada perusahaan dapat *IP* dari *DHCP Server* yang palsu dan akan menghasilkan jaringan perusahaan tidak bisa terhubung dengan *DHCP Server* melainkan menghubung ke jaringan si peretas (Toprak, Turker, & Erman, 2018).

Jika *DHCP Server* terkena serang oleh *DHCP Rogue,* maka identitas dari perusahaan akan diketahui *DHCP Server Rogue* sehingga *client* sudah mendapatkan *IP* dari siperetas dan akan diarahkan menuju *IP Rogue* dari peretas. Untuk contohnya seperti pada pengguna komputer *client* dalam mengakses data

perusahaan yang akan diketahui oleh pengguna tidak bertanggung jawab menggunakan *traffic* ke *client*, karena *traffic* digunakan melalui *client* yang sudah dipalsukan dari peretasan. Lalu peretasan hanya mencari informasi yang sudah didapat dari *trafic*, kemudian peretas akan melakukan *phising* yang dibuka dari *client* untuk mendapatkan data *client* seperti mendapatkan *username* dan mendapatkan *password*. Untuk permasalahan ini terjadi dikarenakan adanya penggunaan akses internet dari perusahaan dan masalah tersebut dapat dibahas pada laporan ini. (Naaz & Badroo, 2016).

Dalam menganalisa keamanan komputer seperti penulis deskripsikan, penulis akan menggunakan keamanan jaringan menggunakan *Bridge Filter*. *Bridge Filter* adalah suatu *system* keamanan jaringan yang dimana perangkat komputer hanya dapat menerima *IP DHCP* yang dipercaya server perusahaan.

Dengan penulisan latar belakang yang sudah dijelaskan, maka penulis mulai menganalisa perbandingan jaringan komputer yang menggunakan pada *system* keamanan *Bridge Filter* dengan tidak menggunakan jaringan *system* keamanan *Bridge Filter*. Lalu dalam mempraktekkan tersebut, penulis menggunakan beberapa mikrotik dan laptop sebagai simulasi. Dengan ini, pembaca dapat mengetahuinya secara langsung dampak akan terjadi dan bagaimana cara mengatasi masalah tersebut. Untuk itu, penulis akan membahas dan menjelaskan dengan judul "ANALISA DAN PERANCANGAN DHCP SERVER DARI SERANGAN DHCP ROGUE MENGGUNAKAN ROUTER MIKROTIK".

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang tersebut, bahwa pentingnya sistem dalam mengelola jaringan yang optimal agar menciptakan jaringan yang aman dan terkendali. Lalu penulis akan menjelaskan bagaimana cara kerja dalam membuat suatu system keamanan jaringan *DHCP Server* agar tidak mudah terkena serangan dari *DHCP Rogue* sehingga karya ilmiah ini akan membahas tentang penerapan keamanan dan penjelasan penggunaan dari dampak yang akan terjadi.

1.3. Batasan Masalah

Untuk mempermudah dan dipahami oleh pembaca tentang penelitian yang penulis lakukan, penulis juga akan mecantumkan batasan masalah yang akan dibahas yaitu:

1. Penerapan keamanan jaringan dengan menggunakan teknik keamanan *Bridge Filter.*
2. Pembahasan cara kerja dari system keamanan pada *Bridge Filter.*
3. Menganalisa dampak dari kerugian yang disebabkan oleh penggunaan *DHCP Rogue.*
4. Langkah dalam perancangan dan konfigurasi dalam *DHCP Server*.

1.4. Tujuan Proyek

Tujuan dari penulisan karya ilmiah ini dijelaskan sebagai berikut:

1. Mampu mengetahui *system* kerja dari penggunaan *DHCP Rogue* sehingga dapat menjalankan pencegahan dari serangan peretasan.
2. Mengetahui dampak dari penggunaan serangan dari *DHCP Rogue*.
3. Mampu merancang keamanan jaringan dengan menggunakan *Bridge Filter.*
4. Sebagai syarat kelulusan Strata 1(S-1) Universitas Internasional Batam.

1.5. Manfaat Proyek

Adapun manfaat dari penelitian bagi *User,* peneliti maupun Akademi yaitu:

1. Mengetahui cara kerja dengan menggunakan metode keamanan *Bridge Filter.*
2. Mengetahui dampak sebelum diterapkan keamanan jaringan ini dengan yang sesudah diterapkan keamanan jaringan.
3. Meminimalisir penyerangan ke dalam jaringan perusahaan.

1.6. Sistematika Penulisan

Sistematika pembahasan yang dibuat berfungsi untuk memberikan isi masing-masing bab yang akan dibahas. Berikut sistematika dari bagian tugas akhir yaitu:

BAB I PENDAHULUAN

Penjelasan bab ini mengenai ringkasan dari latar belakang, rumusan, batasan, tujuan proyek, manfaat *project*, dan sistematika dalam laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bagian bab ini menjelaskan tentang teori-teori bahan dari penelitian yang dulu dengan penelitian sekarang. Landasan teori didapat melalui dari berbagai referensi yang ada berkaitan dengan penelitian sekarang, sehingga dapat dijadikan dasar melaksanakan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ini memberikan metode yang digunakan, desain yang baik dalam mencapai suatu tujuan, dan terdiri dari analisa permasalahan penelitian secara terperinci.

BAB IV IMPLEMENTASI

Bagian bab ini berisi suatu implementasi dari penelitian tugas akhir. Menjelaskan tentang implementasi perancagan dan memberi pembahasan tentang hasil penelitian tugas terakhir yang sudah dilaksanakan.

BAB V PENUTUP

Bab ini adalah bagian penutup yang berisi kesimpulan semua laporan tugas akhir, penemuan yang didapat dari hasil analisa dan ada pembahasan.