BAB 1
PENDAHULUAN

1.1. Latar Belakang

Teknologi jaringan komputer yang menjadi salah satu teknologi yang berkembang dengan sangat pesat, sehingga berperan besar dalam meningkatkan efisiensi berbagi data pada suatu pekerjaan. Perkembangan teknologi jaringan komputer dapat mengarah pada dua hal, yaitu perkembangan yang mengarah ke sisi positif, dan ke sisi negatif. Contoh positif dari perkembangan tersebut adalah tersedianya metode berbagi data atau mengatur perangkat keras dari jarak jauh dapat dilakukan lebih stabil dan efisien, sedangkan contoh negatifnya adalah dari sisi keamanan, dimana data yang dikirim melalui jaringan lebih rentan dari peretas, karena akan selalu ada celah dalam jaringan. Peretas bisa mengakses tanpa izin, mencuri, dan merusak data penting atau yang bersifat privasi, dengan memanfaatkan kemajuan jaringan komputer hal itu menjadi lebih mudah dilakukan oleh peretas, karena hal itu metode keamanan sangat dibutuhkan. “Faktor keamanan begitu penting, dikarenakan tidak semua informasi data bersifat terbuka untuk umum, dan tak semua orang berhak mengaksesnya” (Husnan, 2013).

Pada komputer server yang melayani banyak pengguna dalam waktu yang bersamaan, pada umumnya menggunakan sistem operasi khusus untuk server. Contoh beberapa sistem operasi yang menyediakan khusus untuk server adalah Windows, Linux, DOS, dan lain – lain. Pada umumnya sistem operasi server yang banyak digunakan oleh perusahaan atau skala enterprise lebih mengacu pada sistem operasi Linux dibandingkan dengan sistem operasi yang lain, karena sistem operasi Linux dinilai lebih stabil dan aman dibanding sistem operasi lain, selain itu Linux bersifat *open source* yang dapat menekan biaya untuk keperluan bisnis karena gratis (Gafar, 2017). Linux memiliki fitur yang melimpah dibanding dengan sistem operasi lain, sehingga memungkinkan untuk membuat server sesuai kebutuhan. Dukungan pada sistem operasi Linux juga sangat banyak karena banyak komunitas Linux.

Ada beberapa distro Linux di seluruh negara salah, satu distro Linux yang sangat direkomendasikan untuk keperluan enterprise server adalah distro CentOS, distro ini sangat mirip dengan Redhat karena memang turunan dari distro tersebut, tetapi CentOS lebih banyak dukungannya dan bersifat *open source* yang lebih memudahkan pengguna untuk mengeksplorasi fitur di dalamnya. Kelebihan CentOS dalam hal keamanan tidak

bisa diragukan lagi, karena memang distribusi ini adalah turunan dari Redhat tetapi berbeda dengan Redhat (Suryoko, 2012). Salah satu fitur CentOS yang membuat transfer file lebih aman adalah adanya layanan SFTP yang berbeda dengan FTP pada umumnya, layanan SFTP ini lebih aman karena layanan ini mengenkripsi data yang melewati *port* tersebut, sedangkan FTP tidak terenkripsi, jadi dapat disadap oleh orang yang tidak memiliki kewenangan (Wibowo, 2013).

Pada penerapan Linux server masalah keamanan adalah fokus utama untuk di selesaikan. Isu utama yang dihadapi penggunaan sistem Linux adalah peretas yang selalu mencoba masuk ke dalam sistem melalui jalur SSH, karena layanan SSH pada Linux sudah aktif sejak awal pemasangan sistem operasi dengan *port* awal yaitu nomor 22, selain itu kelemahan SSH adalah akses pengguna *root* telah mendapatkan izin sejak awal (Boss & Poll, 2012). Kelemahan SSH banyak dimanfaatkan para peretas dengan menggunakan metode *port scanning* untuk melihat *port* yang terbuka dan membuka sistem pada server tanpa izin. Setelah *port* sudah berhasil diakses maka metode yang selanjutnya dilakukan oleh peretas adalah *brute force* untuk membuka *password* dari sistem Linux dengan pengguna *root*. SSH yang belum dikonfigurasi akan lebih mudah terserang oleh peretas dengan metode tersebut (Boss & Poll, 2012).

Port knocking adalah salah satu metode untuk mengamankan jalur komunikasi jarak jauh dengan memanfaatkan *firewall* untuk menjatuhkan paket yang masuk pada layanan dan waktu yang telah di tentukan. Prinsip kerja dari metode *port knocking* ini adalah seperti pintu yang dapat terbuka dan tertutup, pintu ini dapat terbuka setelah pengguna yang ingin masuk mengetuk pintu lain yang sudah ditentukan urutannya. Cara kerja dari metode *port knocking* ini adalah menggunakan *firewall* sebagai alat untuk menjatuhkan paket – paket yang mencoba masuk ke dalam layanan, atau *port* tertentu yang ditentukan oleh pengguna, hal ini bertujuan agar layanan dapat tersembunyi dalam *firewall*, sehingga peretas akan sulit dalam menemukan dan membuka layanan tersebut (Amarudin & Ulum, 2018).

Pada penelitian sebelumnya yang menjadi literatur penulis, penelitian tersebut membahas tentang implementasi *port knocking* pada router Mikrotik. Penelitian ini diuji dengan simulasi yang berjalan pada aplikasi GNS3. Autentikasi yang digunakan pada penelitian ini adalah *filtering ping request* pada *firewall* Mikrotik, jika pengguna melakukan *ping request* dengan *port* 80 ke salah satu PC yang ditentukan dalam *firewall*

maka pengguna tersebut baru dapat memasuki konfigurasi router. Menurut penulis dengan melakukan *ping* pada IP PC di *port* 80 masih kurang aman, karena peretas bisa saja melakukan ping ke semua IP di dalam atau luar jaringan yang terhubung dengan router.

Pada skripsi ini, penulis mengusulkan implementasi metode *port knocking* dengan sistem Knockd pada *port* SSH. sistem tersebut akan mengatur keterbukaan *port* yang akan dilindungi untuk mencegah serangan *port scanning*, *port* pada SSH juga akan diubah ke *port* yang lain untuk mempersulit peretas menemukan celah keamanan, selain itu akses untuk *username root* melalui *port* SSH akan diblokir untuk mempersulit peretas melakukan *brute force* pada autentikasi *login* server. Sistem tersebut akan diimplementasikan pada sistem operasi Linux CenOS 8, pada sistem operasi tersebut sistem ini dapat berjalan dengan dua pilihan, yaitu *drop packet* yang masuk melalui *port* SSH dengan *firewall*, atau memblokir semua paket dari semua IP dengan aturan IP *Tables*. Dengan adanya sistem ini pengguna bisa melakukan penutupan dan pembukaan akses SSH dari jarak jauh dengan cara melakukan *knock* pada *port* yang sudah ditentukan sesuai urutannya. Selama simulasi sedang berjalan penulis juga menggunakan metode *sniffing* untuk melihat paket – paket yang berjalan pada jarinngan server CentOS, dimana dalam metode tersebut penulis dapat menangkap paket yang dikirim oleh pengguna dan melihat IP pengirim sekaligus membuktikan enkripsi paket tersebut berjalan dengan lancar.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka yang menjadi rumusan masalah dalam penelitian ini adalah:

a. Bagaimana cara membangun topologi untuk mensimulasikan jalannya sistem keamanan menggunakan *port knocking* pada Linux CentOS 8?
b. Bagaimana cara untuk mengimplementasikan *port knocking*, merubah *port* pada layanan SSH, dan menghapus akses *root* untuk layanan SSH pada sistem operasi Linux CentOS 8?
c. Bagaimana cara menangkap paket yang berjalan menuju server atau berasal dari server di dalam jaringan untuk menguji kinerja enkripsi SSH?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

a. Membuat topologi rancangan simulasi *remote* server Linux dari jaringan yang berbeda untuk menguji keamanan *port* SSH dari dalam jaringan dan luar jaringan.

b. Melakukan implementasi metode *port knocking* pada *port* SSH dengan sistem Knockd, dan mengkonfigurasi layanan SSH di server Linux CentOS 8 agar layanan SSH dapat tertutup dan terbuka dari jarak jauh, dan *port* pada SSH lebih aman.

c. Menguji enkripsi yang ada pada port SSH dengan melakukan *packet sniffing* ke dalam jaringan tersebut.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah:

a. Memperbaiki celah keamanan yang ada pada *port* SSH agar admin dapat lebih mudah untuk melakukan pengaturan server dari jarak jauh.

b. Mengetahui hasil analisis tingkat keamanan dari *port* SSH yang sudah dilakukan *sniffing* dengan Wireshark.

c. Menambah perlindungan sistem server dari akses yang tidak sah dengan tidak membiarkan *port* SSH terbuka.

1.5 Batasan Masalah

Adapun batasan masalah yang dilakukan pada penelitian ini adalah:

a. Penelitian ini menggunakan Virtualbox untuk menjalankan semua simulasi sistem operasi dan jaringan.

b. Metode yang digunakan untuk mengamankan *port* SSH adalah *port knocking*.

c. Topologi yang digunakan adalah jaringan LAN dengan router sebagai pemisah jaringan pengguna, dengan tiga jaringan yang berbeda.

d. Untuk melakukan *sniffing* ke jaringan server dan analisis paket data menggunakan aplikasi Wireshark