BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Saat ini perkembangan teknologi yang semakin pesat membawa pengaruh yang cukup besar bagi pengguna yang memafaatkan internet untuk melakukan berbagai hal misalnya transmisi data, transaksi *online*, dan lain-lain. Dalam mengikuti perkembangan teknologi banyak bidang yang membutuhkan jaringan komputer. Jaringan komputer memberikan kemudahan antar pengguna komputer, dengan adanya jaringan komputer pertukaran data antar komputer dapat dilakukan dengan mudah dan cepat. Juga bisa melakukan kontrol jarak jauh, salah satunya yaitu *remote* akses dengan menggunakan *Telnet*.

Server sekarang yang dipakai *ubuntu server*, dan mengontrol jarak jauh antara dua komputer dengan sistem *telnet*. Namun sekarang ini *telnet* tidak aman lagi dipakai karena proses *remote* akses, dan transmisi data tidak ada enkripsi sehingga rentan terhadap serangan peretas maka perlu diterapkan *secure shell*. *Secure shell* merupakan sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur *client* dan *server,* serta seorang *user* untuk *login* ke *server* secara *remote*. *Secure shell* mengenkripsi data selama proses komunikasi sehingga menyulitkan peretas yang mencoba membobol *login* dan *password* pengguna.

(Garimella, Kumar: 2015) *Secure Shell* merupakan salah satu solusi untuk masalah keamanan yang ada melalui jaringan. Kedua, tidak hanya mengamankan

transfer *file*, juga membantu dalam *remote login*, *port forwarding* dan mekanisme kontrol akses lainnya. Ini tidak hanya menghilangkan resiko keamanan tetapi juga memberi kita ruang untuk mengembangkan jaringan besar dengan fitur-fitur canggih.

Pada saat ini serangan pada suatu *server* semakin hari semakin meningkat. Terbukanya *port* akan memudahkan peretas untuk menerobos masuk ke dalam *server* melalui *port* tersebut. Para peretas akan mencoba untuk mengeksploitasi berbagai aplikasi yang sedang dijalankan melalui port yang terbuka pada sisi *server*, terutama pada *port* untuk aplikasi *remote server* tentunya akan menjadi titik utama perhatian peretas untuk di eksploitasi. Metode *port knocking* merupakan salah satu metode autentikasi yang dapat digunakan untuk mengatasi masalah tersebut.

(Ricard, Susanto: 2007) *Port knocking* dapat dijadikan altenatif untuk koneksi pada *server*, yang ingin mempertahankan kondisi semua *port* tertutup sepanjang tidak dibutuhkan. Proses *port knocking* lebih tepat digunakan oleh *standalone server*. Yang membutuhkan proses *login* setiap kali hendak mengakses sistem, pembukaan *port* secara spesifik pada pihak tertentu membantu mengontrol akses *port* serta layanannya dari pihak yang tidak sah.

Berdasarkan latar belakang yang dijabarkan diatas tentang rentannya *telnet* terhadap serangan peretas, maka perlu menerapkan *secure shell* dengan metode *port knocking*. Oleh karena itu peneliti akan melakukan **"ANALISIS DAN IMPLEMENTASI *SECURE SHELL* PADA *UBUNTU SERVER* DENGAN METODE *PORT KNOCKING*".**

1.2 Identifikasi Masalah

Berdasarkan pembahasan latar belakang permasalahan dapat di identifikasi beberapa masalah sebagai berikut:

1. *Server* masih menggunakan *TELNET*.
2. *Telnet* rentan terhadap serangan peretas.
3. *Server* belum menerapkan SSH.
4. Masih belum menggunakan metode *PORT KNOCKING*.

1.3 Pembatasan Masalah

Agar pembahasan tidak terlalu meluas pada penelitian ini, maka penelitian ini membatasi permasalahan sebagai berikut:

1. *Secure shell* dan metode *port knocking* diimplementasikan pada jaringan LAN.
2. *Server* menggunakan OS *Ubuntu* 16.04 1 LTS.
3. Tidak membahas sistem operasi secara detail.
4. Hanya menguji keamanan *remote* akses ke *server* dengan aplikasi *Hydra* dan *Nmap*.
5. Menguji keamanan *remote* akses ke *server* dengan melakukan peretasan menggunakan cara *dictionary attack*.

1.4 Perumusan Masalah

Berdasarkan indentifikasi masalah yang telah diuraikan, maka penelitian ini merumuskan masalah sebagai berikut:

1. Bagaimana mengimplementasi *secure shell* pada *ubuntu server* dengan metode *port knocking*?
2. Bagaimana keamanan *server* setelah menerapkan *secure shell* dengan metode *port knocking*?

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penenlitian ini sebagai berikut:

1. Untuk mengimplementasi *secure shell* pada *ubuntu server* dengan *metode port knocking*.
2. Keamanan *remote* akses ke *server* tidak mudah dibobol oleh para pihak yang tidak berhak.

1.6 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak antara lain:

1.6.1 Aspek Teoritis

1. Agar menambah pengetahuan dalam penelitian tentang *secure shell* pada *unbuntu server* dengan metode *port knocking*.

2. Sebagai tambahan ilmu pengetahuan dan untuk mengembangkan kemampuan dalam melakukan penelitian.

1.6.2 Aspek Praktis

1. Bagi penulis untuk dapat memahami keamanan remote akses ke *server* dengan menggunakan *secure shell* dan metode *port knocking*.
2. Bagi mahasiswa dan masyarakat hasil penelitian ini dapat digunakan sebagai media informasi atau panduan penelitian selanjutnya dan menambah wawasan tentang *secure shell* dengan metode *port knocking*.