BAB 1 PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi sudah berkembang dengan pesat dan membuat teknologi menjadi peranan penting dalam kehidupan kita saat ini. Dengan perkembangannya saat ini menjadikan keamanan teknologi informasi menjadi saat penting untuk melindungi informasi. Seseorang dapat melakukan pencurian informasi jika keamanan teknologi informasi tidak terus berkembang. Dengan keamanan yang terus berkembang kemungkinan seseorang mencuri data akan semakin kecil, keamanan informasi berkembang saat telah terjadinya penyerangan dengan teknik baru yang belum pernah terjadi.

Saat ini *server* banyak dipergunakan oleh perusahaan untuk dipergunakan sebagai penyimpanan data baik data yang bersifat umum maupun bersifat sensitif untuk perusahaan itu sendiri. Perawatan *server* memerlukan pengeluaran yang tidak sedikit begitu pula dengan keamanan pada *server* tersebut harus memiliki keamanan yang ketat. Kebocoran informasi menjadi sangat fatal saat data sensitif menyebar, kebocoran terjadi bisa disebabkan dengan *human error* atau lemahnya kemanan pada *server* tersebut. Menurut *website* berita kompas (Conney Stephanie. 2021, hlm.1) banyak terjadi kebocoran data yang terjadi di Indonesia pada tahun 2020. Perusahaan GoDaddy pengelola *web-hosting* mengalami kebocoran data yang disebabkan seseorang mengakses ilegal ke *login* pelanggan untuk terhubung ke *secure shell* (SSH) pada akun *hosting*-nya menurut Comes chief information security officer GoDaddy (cyberthreat.id dan Andi Nugroho, 2020). Untuk mencegah kebocoran data pribadi kita bisa tidak dengan sembarangan untuk memberikan data kita pada aplikasi dan *website* yang tidak kita percayai. Pada sisi administrator bisa dengan lebih teliti dan mengamankan *server* dengan lebih baik lagi.

Layanan *secure shell* atau SSH memberikan kemudahan Seorang administrator yang diberi hak untuk mengatur *server*. Administrator tidak perlu datang ke lokasi fisik *server*, dengan bantuan SSH, administrator dapat *control*

penuh pada *server*. Dengan bantuan OpenSSH kita dapat menggunakan SSH pada Ubuntu yang digunakan pada VirtualBox sebagai *virtual machine*. Adminnistrator dapat mengakses layanan dengan menggunakan *username* dan *password* yang keamanannya masih kurang, dengan menggunakan teknik *brute force attack, username* dan *password* memiliki kemungkinan untuk dapat di rentas jika *username* dan *password* hanya menggunakan kata yang umum digunakan untuk *username* dan *password.* Hydra merupakan salah satu *tool* yang dapat digunakan untuk melakukan *brute force*, pada kali linux biasanya sudah ada saat melakukan *install* kali linux sebagai *operating system.*

Layanan SSH menggunakan *port, port* merupakan mekanisme untuk mengizinkannya sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya. Pengamanan *port* menggunakan *firewall* yang akan mengatur *port* itu dibuka atau ditutup. Dengan bantuan teknik *port knocking*, *port* yang ditutup oleh *firewall* dapat dibuka dengan mengirim paket-paket yang telah ditetapkan pada *port* yang ditutup. Dengan bantuan Knockd *tool* yang dapat di *install* pada linux yang nantinya kita dapat menggunakan *port knocking* pada *port* linux yang kita gunakan. *Port knocking* memiliki kelemahan, jika menggunakan *wifi public* saat kita mengetuk *port* yang tertutup tertinggal jejak digital yang dapat dilihat menggunakan aplikasi wireshark. Wireshark digunakan untuk mementoring jaringan yang sering dipakai oleh seorang *network* administrator.

Key Authentication merupakan cara lain masuk pada *server* menggunakan SSH. Dengan bantuan algoritma RSA, *public key* akan disimpan pada *server* dan *private key* yang akan di pegang oleh adminnistrator untuk digunakan untuk masuk ke *server* dari komputer atau laptop milik adminnistrator.

Oleh karena itu dirancang "pengamanan *server* dengan metode *port knocking* dan *key Authentication* pada layanan *secure shell* (SSH)" untuk mengamankan *server* dengan lebih ketat dan dapat diatur dari jauh tanpa harus mendatangi lokasi fisik *server*.

1.2. Rumusan Masalah

Adapun rumusan masalah berdasarkan latar belakang di atas sebagai berikut:

1. Bagaimana keamanan *port* SSH tanpa *port knocking* dan *key Authentication*?
2. Bagaimana keamanan *port* SSH dengan menggunakan *port knocking* dan *key Authentication?*

1.3. Batasan masalah

Adapun Batasan permasalahan pada pengamanan *server* pada layanan *secure shell* adalah sebagai berikut:

1. Pengamanan *server* dengan *port knocking* dan *key Authentication.*
2. Pengujian hanya menggunakan sistem operasi linux.
3. Pengujian keamanan dengan menggunakan *brute force attack* pada ssh dan *sniffing* wireshark.
4. Semua perangkat keras terhubung dalam satu LAN (*Local Area Network*).

1.4. Tujuan

Tujuan dari penelitian ini antara lain adalah:

1. Menerapkan metode *port knocking* dan *key Authentication* pada layanan *secure shell* atau *SSH.*
2. Mengamankan *server* dengan metode *port knocking* dan *key Authentication* pada layanan *secure shell* atau *SSH.*

1.5. Manfaat

Manfaat pembuatan penelitian ini adalah sebagai berikut:

1. Pengamanan berikut dapat menjadi salah satu alternatif untuk mengamankan *server*.
2. Untuk para administrator mereka dapat mencoba alternatif keamanan berikut.
3. Dapat menjadi referensi bagi peneliti dengan topik peneliti yang sama.

1.6. Sistematika Penulisan

Penulisan dalam pembuatan penelitian ini menggunakan sistematika penulisan supaya lebih mudah dipahami dan memudahkan dalam penyusunan. Di bawah ini adalah bentuk daripada sistematika penulisan penelitian sebagai berikut:

BAB 1 PENDAHULUAN

Penjelasan isi dari bab ini yaitu menyangkup tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat, serta sistematika penelitian.

BAB 2 LANDASAN TEORI

Penjelasan isi dari bab ini yaitu definisi, konsep yang telah disusun rapi serta sistematis tentang variable-variabel dalam sebuah penelitian.

BAB 3 METODOLOGI PENELITIAN

Penjelasan isi dari bab ini memuat tentang metode yang digunakan dalam penelitian ini beserta apa saja yang digunakan sebagai sarana dalam melakukan penelitian ini.

BAB 4 PEMBAHASAN

Penjelasan dari bab ini memuat tentang pembahasan mengenai rumusan masalah yang telah dibuat dan melakukan.

BAB 5 PENUTUP

Penjelasan dari bab ini memuat tentang kesimpulan dan sara dari semua penelitian yang telah dilakukan.

DAFTAR PUSTAKA