ABSTRAK

HANDRIYAN SAPUTRO, RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN *FIREWALL* DENGAN METODE *RANDOM PORT KNOCKING* PADA KONEKSI *SSH* Skripsi, Jakarta: Program Studi Teknik Informatika, FSTI, ISTN, Agustus 2019.

Remote Login seperti *SSH* telah menjadi yang paling sering dilakukan oleh administrator jaringan untuk pemecahan masalah atau hanya memantau keadaan *Server* jaringan. Ketika seorang *administrator* jaringan ingin melakukan *SSH*, hal yang dilakukan adalah mengakses port *SSH* dan masuk sehingga koneksi untuk *SSH* akan terjadi, dapat dikatakan bahwa port *SSH* ini sangat penting, karena dengan mengakses port ini, *SSH login* jarak jauh akan dilakukan. Pada dasarnya port *SSH* ini akan selalu terbuka untuk menerima koneksi dari luar untuk dapat melakukan *SSH*, dengan ini seorang penyerang memiliki lebih banyak celah ke dalam *server*, dan dapat dinyatakan bahwa *server* berada dalam kondisi yang tidak aman. Metode *port knocking* sangat berguna untuk administrator jaringan atau *server* yang harus menjaga jaringan atau *server* yang harus dipantau terus menerus dari mana saja, karena *port knocking* aman digunakan untuk melakukan komunikasi antara komputer di jaringan komputer dan dengan *firewall* dapat juga mencantumkan IP yang diizinkan untuk mengakses *login SSH* dari jarak jauh ke *server*.

Kata kunci: *port knocking*, *firewall*, *SSH*

ABSTRACT

HANDRIYAN SAPUTRO, RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN *FIREWALL* DENGAN METODE *RANDOM PORT KNOCKING* PADA KONEKSI *SSH* Skripsi, *Informatics Engineering* Program, Jakarta, *August* 2019.

Remote logins such as SSH have become the most frequently done by a network administrator for troubleshooting or just monitoring the state of a network Server. When a network administrator wants to do SSH, the thing that is done is accessing the SSH port and logging in so that a connection for SSH will occur, it can be said that this SSH port is very important, because by accessing this port, SSH remote login will be done. Basically this SSH port will always be open to accept connections from outside to be able to do SSH, with this an attacker has more gaps into the Server, and it can be stated that the Server is in an unsafe condition. The port knocking method is very useful for network administrators or Servers who have to take care of networks or Servers that must be monitored continuously from anywhere, because port knocking is safe to use to make communication between komputer*s on a* komputer *network and with a firewall can also list any IP which is allowed to access SSH logins remotely to the Server.*

Key words: *port knocking, firewall, SSH*