

## ABSTRAK

### IMPLEMENTASI KEAMANAN REMOTE SERVER MENGGUNAKAN METODE PORT KNOCKING DENGAN MENGIRIMKAN KE TELEGRAM SEBAGAI NOTIFIKASI

**Kurniawan Akbar Wael<sup>1</sup>, Salkin Lutfi<sup>2</sup>, Hairil Kurniadi Sirajuddin<sup>3</sup>**

Program Studi Teknik Informatika, Fakultas Teknik, Universitas Khairun  
Jl. Jati Metro Kota Ternate Selatan

E-mail: <sup>1</sup>pti07351411074@gmail.com, <sup>2</sup>salkin.lutfi@unkhair.ac.id,

<sup>3</sup>hairil.kurniadi@unkhair.ac.id

Perkembangan teknologi jaringan khususnya *system* keamanan jaringan komputer yang terus berkembang menuntut adanya pengembangan *system* keamanan jaringan, khususnya dalam *remote server* melalui *port* ssh. Pentingnya untuk menjaga kerahasiaan data dan informasi yang terdapat pada *server*. Data dan informasi ini hanya ditujukan untuk *administrator* dan *user* yang berhak mengakses melalui *port* layanan, membiarkan *port* penting terbuka adalah suatu kesalahan yang fatal dapat mengakibatkan serangan pada *server*. Penelitian ini dilakukan dengan mengimplementasikan keamanan *server* dengan metode *port knocking* mengirimkan pesan serangan ke *telegram* sebagai notifikasi untuk *sysadmin* dalam hal mengetahui adanya serangan yang dilakukan *attacker* saat mencoba *login* kedalam *server* melalui *port* ssh sehingga *system* dapat menangani permasalahan keamanan jaringan serta pencurian data dan informasi. Dari pengujian serangan yang dilakukan menggunakan tehnik *brute force*, *sniffing* dan salah *password* lebih dari tiga kali dapat mengirimkan pesan notifikasi pada *telegram* berupa data dari hasil serangan pada *sysadmin*.

Kata Kunci: Keamanan Remote Server, Port Knocking, Telegram

*The development of network technology, especially computer network security systems, which continues to develop requires the development of a network security system, especially in remote servers via the SSH port. It is important to maintain the confidentiality of data and information contained on the server. This data and information is only intended for administrators and authorized users to access through the service port, leaving important ports open is a fatal error that can result in attacks on the server. This research was carried out by implementing server security with the port knocking method sending attack messages to the telegram as notification to the sysadmin in the event that an attacker was aware of an attack when trying to log into the server via the SSH port so that the system could handle network security problems as well as data and information theft. From testing attacks carried out using brute force, sniffing and wrong password techniques more than three times, it can send notification messages on telegram in the form of data from the results of attacks on sysadmins.*

Keywords: Remote Server Security, Port Knocking, Telegram