ABSTRAK

Sistem keamanan jaringan awalnya mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung maupun tidak langsung. Perangkat yang terhubung dengan jaringan komputer mempunyai tingkat kerawanan yang tinggi karena bisa di akses atau disusupi oleh orang yang tidak bertanggung jawab. Biasanya penyusupan yang terjadi di keamanan jaringan seperti *hacking* dan *cracking*. Oleh sebab itu keamanan jaringan dipasang dengan sistem disebut IDS (*Intrusion Detection System*).Tujuan penelitian ini Untuk melakukan perancangan dan implementasi firewall sebagai tools IDS (*Intrusion Detection System*) pada simulasi jaringan komputer.dalam tugas akhir ini menggunakan metode VNC dan Putty sebagai konfigurasi simulasi jaringan yang dipakai. Penulis bisa membandingkan antara Firewall, ACL, dan IDS dan mana yang cocok digunakan untuk jaringan komputer agar terhindar dari ancaman berbahaya.

Kata Kunci : *hacking, cracking, IDS, VNC, Putty, ACL*

ABSTRACT

Network security systems initially anticipate the risk of computer networks in the form of physical and logical threats, both directly and indirectly. Devices that are connected to a computer network have a high level of vulnerability because they can be accessed or infiltrated by irresponsible people. Usually intrusions that occur in network security such as hacking and cracking. Therefore, network security is installed with a system called IDS (Intrusion Detection System). The purpose of this study is to design and implement a firewall as IDS (Intrusion Detection System) tools on computer network simulations. network used. The author can compare between Firewalls, ACLs, and IDS and which ones are suitable for computer networks to avoid dangerous threats.

Keywords: hacking, cracking, IDS, VNC, Putty, ACL