ABSTRACT

Port knocking is a method to access a remote computer by sending packets to certain ports in the server. When the order of the port are match with the specified port on the server, the server will overwrite the firewall rules with new rules that created by the configuration of iptables, so client can connect. By the end, this assignment is expected if network administrators can control who has access to a computer. Applications that use the TA is a program based on phyton language.

In this final assignment will be discussed about how the functionality of port knocking that simulated on a simple network, and how well the influence of the configuration that are made for filtering IP Address and MAC Address in order to improve the quality of port knocking works. Then, it will be tested by attack the server, see if it can interrupt the server performance and the client attempt to access the server. The parameters used are the parameters of success.

From the experimental results, it was concluded that the port knocking system that made, successfully protecting information and services on the server, and the iptables configuration that made to add quality of security server, successfully managed to filter the client based on its IP and MAC Address, beside of the knocking. SYN flood attacks that suffered by the server has effected the client attempt to access the server, but its not completely broke the access, depending on the density of the intensity of the attacks. Then,from the performance test we know that used application are stable in the server resource usage (not fluctuate), and from the access speed, known that the use of Linux OS on the client side are more efficient.

Keyword: Port Knocking, Firewall, IPtables, Phyton