ABSTRACT

Generally, penetration attack to computer in network come trough application from open ports in server. This port vulnerable to exploitation from unwanted access, so a system that can be solution from that problem is needed.

Port Knocking is one of many security system that have a function described above, which is block unwanted access. In principle, port knocking closed all ports in server. If user wants access to server, user doing “knock” to use that service, then if done user do knock again to closed service. A main purpose for this final project is server succeed to protect file server by integrating existing firewall rules with port knocking program, and showing that without sending a right knock or password, user cannot use service from server.

From research, there is conclusion that the different between both port knocking program is knockd not use encryption in his sending knock mechanism, but fwknop did. For fwknop, “sent knock” to server as authentication key is 206 bytes (this sent to just one port 62201 (UDP), and if client quit from file server after 30 seconds limit from software configuration, he must do authentication mechanism like before to access. This is different with knockd that use sending knock mechanism to some port in server, for both opening and closing connection without access time’s limit.

Key Words : ***authentication, exploitation, encryption, firewall, port knocking***