ABSTRACT

Storage Area Network (SAN) has become standard infrastructure in various IT-aware companies. Mutual use of SAN and virtualization software becomes unique attraction for many companies since it offers lower cost in IT expenses, compared to traditional use of server infrastructure. Reviewed from security aspect, the use of SAN is relatively secure since connection between host and storage layers uses different protocol (fiber channel) separated from TCP/IP. For common user, this will make it harder to conduct attack or data-stealing. Nevertheless, SAN infrastructure has a weakness that holds potentials to become entrance for data-stealing or attack, impacting in total paralysis of SAN infrastructure. The weakness point resides in services provided by each component layers of SAN, i.e. storage and fabric layers. For the convenience of SAN infrastructure management, services are provided both web-based and shell-based (command-prompt). These two services are the entrance gate to SAN infrastructure. In this research, a penetration testing for Denial of Service was conducted on services provided on storage and fabric layers commonly used in SAN infrastructure management, in order to test the resilience of operating system implemented in those layers. Result shown that management storage and fabric layer susceptible to denial of service attack.

To solve this problem, ssh tunneling became one of the answer. In this research SSH tunneling system proposed as intermediary system to forward access from client to storage and fabric services. In this scheme, client and attacker does not have direct access to storage and fabric services, but accessing the services through tunnel was created by ssh server.

The proposed ssh tunneling scheme give better performance compared to system without it. Without ssh tunneling, when dos attack was conduct to storage and fabric, all services (http/https, telnet and ssh) were down and client cannot access at all due to higher flow rate and goodput accepted by the interface of host target, filling up network resources. Applying ssh tunnel as intermediary system could reduce flow rate and goodput caused by dos attack.