STUDY ON SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION

Tang Thanh Dat

Course: QH-2010-I/CQ, Major: Electronics and Telecommunications Engineering

Abstract:

Nowadays, when Internet expands rapidly, Network Security becomes an important problem. Many devices were deployed like Firewall, IDS/IPS, and Antivirus… but they may not be fully effective. Network Security needs a new approaching.

Security Information and Event Management (SIEM) is a new solution in security for network. It helps administrators to monitor and manage all security events and all devices in network, from this provide a new way to defense organizations from Cyber Attacks. SIEM creates an overview of security status of network, indicates the weak point, the main target of attacks.

This Thesis focuses on demonstrating features of SIEM which superiors than other Network Security solutions. The first part of thesis introduces the main concepts of SIEM solution. The next section is experiments to demonstrate 3 feature capacities SIEM: ability to combine security information from many devices; ability to manage, asset devices in network; ability to customize of an open-source SIEM product.

The initial results show that Security Information and Event Management (SIEM) has advantages which excel other Network Security solution and can be implemented in network monitoring in Vietnam. However, to be taken into operation and use effectively, there is needed evaluation and addition research, require both time and investment to testing infrastructure. The last chapter of thesis, beside of the results of experiment models, there are remain problems when implementing SIEM system that are considered.

Keywords: Security Information and Event Management (SIEM), Network Security, Log Management.