

Secure University Network Architecture, Vulnerabilities, Risk Priority Level Classification and Countermeasures

Idris Ismaila, Muhammad Umar Majigi, Shafi'I Muhammad Abdulhamid, *Morufu Olalere*, & Muhammad Bashir Abdullahi, Vivian O. Nwaocha

Abstract

In order to safeguard a University's networked assets, a network administrator must decide how to harden the network. To aid the decision-making process, network administrators may use network hardening suggestions. A critical drawback of currently available analyses is the lack of consideration for the network administrator on identified vulnerabilities, risk figure, risk priority level classification, and network security mechanism. Nessus and Nmap are network vulnerability scanners used for this research. Internal and external scan results were tabulated. The result shows that firewall constitute 81 on scale of 1-100 risk priority level classification of university Information and Technology Service (ITS) network with high risk security level and open email relay constitute two with low risk level. Thus, the research established a university secure network architecture model that contributed towards understanding risk priority level and also overcame shortcomings in choosing appropriate security measures

<https://www.proquest.com/openview/1f4cc5b716973e28627b8251917f1809/1?pq-origsite=gscholar&cbl=2030610>