Abstract

With all the news on cyber attacks and computer security in the last few years, it does not take much time to realize that some action must be taken to protect our organization before it hits close to our home. In fact, security has gone from backroom to the boardroom in a lightning speed. Network security depends on most of network configuration and vulnerabilities. Each machines overall susceptibility to attack depends upon the vulnerabilities of another machine. An attacker tries to exploit the least secure system by small attacks iteratively, where each exploit in the network provide the platform for subsequent exploit. Such a series is known as attack path and the set of all possible paths will form an attack graph. By their highly interdependencies, it is much complex to draw traditional vulnerability analysis. Several works have been done to construct an attack graphs. The goal of this paper is to provide a framework, architecture, and an intelligent approach to vulnerability analysis by utilizing the concept of automated scanning tools. By the changing environment, conducting a periodic in-house vulnerability assessment is very much essential.
References


**Index Terms**

Computer Science  
Networks

**Keywords**

network security, cyber attack, attack graph, vulnerability analysis, vulnerability assessment.