Abstract

The goal of this work is to advance a new methodology to measure a severity cost for each host using the Common Vulnerability Scoring System (CVSS) based on base, temporal and environmental metrics by combining related sub-scores to produce a unique severity cost by modeling the problem's parameters into a mathematical framework. We build our own CVSS Calculator using our equations to simplify the calculations of the vulnerabilities scores and to benchmark with other models. We design and develop a new approach to represent the cost assigned to each host by dividing the scores of the vulnerabilities to two main levels of privileges, user and root, and we classify these levels into operational levels to identify and calculate the severity cost of multi steps vulnerabilities. Finally we implement our framework on a simple network, using Nessus scanner as tool to discover known vulnerabilities and to implement the results to build and represent our cost centric attack graph.
Methodologies to Develop Quantitative Risk Evaluation Metrics


Index Terms
Computer Science Applied Mathematics

Keywords
Quantifying Security CVSSv2 Overall CVSS Score Attack Graph