World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:06, 2018

Multi-Dimension Threat Situation Assessment Based on Network Security Attributes

Authors : Yang Yu, Jian Wang, Jiqiang Liu, Lei Han, Xudong He, Shaohua Lv

Abstract : As the increasing network attacks become more and more complex, network situation assessment based on log analysis cannot meet the requirements to ensure network security because of the low quality of logs and alerts. This paper addresses the lack of consideration of security attributes of hosts and attacks in the network. Identity and effectiveness of Distributed Denial of Service (DDoS) are hard to be proved in risk assessment based on alerts and flow matching. This paper proposes a multi-dimension threat situation assessment method based on network security attributes. First, the paper offers an improved Common Vulnerability Scoring System (CVSS) calculation, which includes confident risk, integrity risk, availability risk and a weighted risk. Second, the paper introduces deterioration rate of properties collected by sensors in hosts and network, which aimed at assessing the time and level of DDoS attacks. Third, the paper introduces distribution of asset value in security attributes considering features of attacks and network, which aimed at assessing and show the whole situation. Experiments demonstrate that the approach reflects effectiveness and level of DDoS attacks, and the result can show the primary threat in network and security requirement of network. Through comparison and analysis, the method reflects more in security requirement and security risk situation than traditional methods based on alert and flow analyzing.

Keywords : DDoS evaluation, improved CVSS, network security attribute, threat situation assessment
Conference Title : ICICS 2018 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 06-07, 2018