Quantifying Security Risk by Critical Network Vulnerabilities Assessment

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 156
Number 13

Year of Publication: 2016

Authors:
Umesh Kumar Singh, Chanchala Joshi

Abstract

Network vulnerability is the weaknesses in the network configuration that inadvertently allows dangerous operations and poses serious security threats. An attacker can exploit these vulnerabilities to gain unauthorized access to the system. Hence, detection and remediation of network vulnerabilities is critical for network security. This paper proposed method for effective risk level estimation by using a new introduced metric, the Hazard Metric (HM) which identifies the probability of attacks in user environments. As in network environment the number of attacks scenario increases, there is higher probability of compromising a target and thus the overall security of the network reduces. Thus, there is a need for quantification of security level of a specific network. The HM measures the probability of successful exploits by estimation of impact and likelihood of the attacks, which is to quantify the degree of security strength against vulnerability exploit in a network system. The proposed method prioritizes the mitigation of discovered vulnerabilities according to their risk levels. The methodology is tested in Vikram University Ujjain, India’s network environment. The results represent the system trustworthiness.
References

15. CVE - Common Vulnerabilities and Exposures (CVE), Available: https://cve.mitre.org/


Index Terms

Computer Science Security

Keywords

CVSS score; risk level; security measurement; security metrics; vulnerability