Abstract

With increasing dependency on IT infrastructure, the main objective of a system administrator is to maintain a stable and secure network, with ensure that the network is robust enough against malicious network users like attackers and intruders. Security risk management provides way to manage the growing threats to infrastructures or system. This paper proposes a framework for risk level estimation that uses vulnerability database National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS). The proposed framework measuresthe frequency of vulnerability exploitation; converges this measured frequency with standard CVSS score and estimates the security risk level which helps in automated and reasonable security management. In this paper, equation for the Temporal score calculation with respect to availability of remediation plan is derived and further, frequency of exploitation is calculated with determined temporal score. The frequency of exploitation along with CVSS score is used to calculate the security risk level of the system. The proposed framework uses the CVSS vectors for risk level estimation and measures the security level of specific network environment, which assists system administrator for
assessment of security risks and making decision related to mitigation of security risks.

References

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


20. Red Hat Customer Portal, Available:

21. CVE-2016-4051: SECURITY PATCH FOR SQUID (ALAS-2016-713), Available:

22. Red Hat Customer Portal

23. CVE-2016-4051: Security Patch for Squid

Index Terms

Computer Science  Security

Keywords

CVSS metrics, risk level, security measurement, severity score, vulnerability category.