Automated Software Vulnerability Management

Table of Contents

Abstract. Text of the summary of your article

1 Introduction

One of the main concerning area for most of organizations is information and software assets security which can can be achieved by bt utilizing the software and network security techniques like firewall, but this is not sufficient to ensure the safety of the information assets due the continuous discovery of software vulnerabilities and put the organization's IT assets in risk of cyber attacks by adversary. Most of organization should be ware and updated about the open software vulnerabilities and perform the need actions like installing the corresponding patch if available, an such information about open vulnerabilities can be retrieved from repositories like National Vulnerability Database NVD. The manual processing of vulnerabilities data requires a quite amount of human resource and could be not affordable for all organizations that motivates for building an automated software vulnerabilities management systems which in general try to alert in organizations about the open vulnerabilities related to the organization's IT assets utilizing the data of on-line repositories such NVD, also another sources of data can be also used like the software vulnerability information provided on social media or blogs.

1.1 Software Vulnerability Management

The software Vulnerability Management concept can be defined as the process of identifying the related vulnerabilities for the software components inside the organization, the process requires firstly managing the inventory of organization's IT assets and periodic search for the related vulnerabilities, and in case of vulnerability discovery a certain action should be performed such alerting the administrators or trying to install the corresponding patch es to avoid possible threats based on those known vulnerabilities.

2 Automated Vulnerability Management

2.1 System Components

2.2 System Work flow

3 Standards

This section introduces on of the most related standards for the software vulnerability management which is the Security Content Automation Protocol(SCAP) [1].

3.1 SCAP

SCAP is collection of open standards and enumerations related to software flaws and security configurations allow the communication of that informations, to support the automated vulnerability and security information management. It provided and maintained by The U.S. National Institute of Standards and Technology (NIST)[2], and the large and public of the SCAP content is the National Vulnerability Database (NVD)[3] that provides data feed for each SCAP standard which can be used free by the public security community, which also is managed by NSIT. The SCAP standards consist of different open standards and enumerations, and the following subset of them:

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)

4 Alternatives to NVD Repository

5 Discussion

6 Conclusion

The results in this section are a refined version

References

[1] https://scap.nist.gov/
[2] https://www.nist.gov/
[3] https://nvd.nist.gov/