CALCULATING NETWORK SECURITY METRICS

CS EVE Group 206

April 18, 2017

1 Introduction

The calculation of network security metrics is a complex problem which involves understanding the state and configuration of network connections, devices and protocols. This research analyses the problem of calculating network security metrics and proposes a framework which can calculate security metrics for a typical small network comprising of numerous devices, operating systems and hosts. The project will involve the configuration of virtual networks for testing the framework. CVSS or other metric scores may be used to aid the calculation of the metric. This document involves some practical work which may involve setting up a virtual network which has a number of machines on the network and applying a range of scanning, probing and vulnerability testing mechanisms on the network

2 Background to the Problem

The need for metrics is great, because all companies suffer from security-related aches and pains. Sometimes the pain is sharp and incapacitating, such as when an intruder defaces a public-facing website. Perhaps, as with the now-defunct Egghead Software, an intruder successfully obtains sensitive customer data, and the resulting embarrassment causes business losses. Sharp pains are the kind that put companies on the front page of the Wall Street Journal, as the expression goes. Far more common are the dull aches: an unsettling feeling in the CIOs stomach that something just isnt right. Regardless of the source of the pain, security metrics can help with the diagnosis.

3 Problem Statement

The calculation of network security metrics is a complex problem which involves understanding the state and configuration of network connections, device and protocols. Security metrics are essential to comprehensive network security and

CSA management, without good metrics analysts cannot answer many security related questions

4 Objectives

4.1 General Objectives

The main objective of this project is to quantify the vulnerability of a network using CVSS and other metric scores.

4.2 Specific Objectives

1. Understand Security risks
2. Establish emerging problems
3. Understand weaknesses in the security infrastructures
4. Measure performance of counter measure processes
5. Recommend technology improvements

5 Methodology

CVSS(v3) or other metric scores may be used to aid the calculation of the metric. CVSS assigns scores to vulnerabilities, allowing responders to prioritize responses and resources according to the threat. CVSS assessment measures three main areas of concern:

1. Base Metrics for qualities intrinsic to a vulnerability
2. Modified vector. The Modified Base is intended to reflect differences within an organization or company compared to the world as a whole. New metrics to capture the importance of Confidentiality, Integrity and Availability to a specific environment are available
3. Temporal Metrics for characteristics that evolve over the lifetime of vulnerability

A numerical score is generated for each of these metric groups

We shall also quantify the following diagnostic metrics

1. ANTIVIRUS AND ANTISPAM. Under the category of antivirus and antispyware metrics are the usual fun facts: the number of distinct pieces of malware detected by antimalware software scans. Firewall and network perimeter

2. ATTACKS. Quantifying security attacks is a difficult task, but it is getting easier thanks to continuing improvements to the accuracy of intrusion detection software and, in particular, SEIM6 software. Security vendors like ArcSight, IBM (Micromuse), and NetForensics attempt to identify attacks by filtering security information into three levels of criticality.

3. COVERAGE AND CONTROL. Coverage and control metrics characterize how successful an organization is at extending the reach of its security rgime

4. PATCH MANAGEMENT. patching is an essential part of keeping systems up-to-date and in a known state. In other words, it is part of an overall portfolio of security controls. The degree to which an organization keeps its infrastructure up to patch indicates the effectiveness of its overall security program

And many others

6 Anticipated Outcomes

Metrics tell us which security threat outbreaks were bad enough that automated quarantine-and-removal processes could not contain them. Dividing the number of incidents that required human intervention into the total number of incidents gives us a much more honest assessment of the effectiveness of the antivirus system.
This project will come up with CVSS number score for the Basic metrics, Modified metrics and the Temporal metric. Itll also establish metrics for patch management, coverage and control, attacks, antivirus and antispyware and more It will also address vulnerability management and here it will address uptime and downtime metrics, availability and reliability, system recovery, change control and many more

References

[1] Andrew Jaquith *Security Metrics: Replacing Fear, Uncertainity and Doubt ISBN 0-321-34998-9.* First Edition May, 2007.

[2] Lance Hayden *IT Security Metrics, A practical Framework for Measuring Security and Protecting Data ISBN: 978-0-07-171341-2* 2010: The McGraw Hill Companies.

[3] *https://en.wikipedia.org/wiki/CVSS*