Incident Tracking
Mike Frandsen
September 1, 2000

Introduction

The purpose of this research paper is to provide a high-level managerial perspective about what types of information can best assist management in measuring progress in ensuring the confidentiality, integrity, and availability of information resources. The paper does not delve deeply into the technical and operational details of specific vulnerabilities, hacker exploits, or incident response procedures.

The increase in IT security threats due to advancements in technology, the growth of the Internet, and the easy availability of hacking tools have resulted in a need for organizations to vastly improve IT security. Although much attention is given to preventing and handling intrusion attempts, one area that organizations sometimes overlook is measuring and tracking those intrusion attempts, and quantifying the success rate of subsequent corrective actions. Evaluating the frequency and type of hacker attacks that are levied on an organization is essential to identifying trends and staying one step ahead of hackers.

Tracking Vulnerability Scans

In order to obtain meaningful information about intrusion attempts, an inventory must first be conducted of all computer hosts connected to your network. This baseline can be established using a tool such as the Security Auditor's Research Assistant (SARA), which remotely identifies hosts and the network-based services operating on those computers. SARA is a third generation version of the Security Administrator's Tool for Analyzing Networks (SATAN) and is available free at http://www-arc.com/sara. Nmap is another utility that can inventory the hosts connected to a large network through a comprehensive scan. Nmap is free and can be downloaded at http://www.insecure.org/nmap.

A security administrator should scan a network to determine which hosts are active and which services are vulnerable. Before conducting a scan, all system administrators whose systems could be affected should be informed so the scan is not misinterpreted as a malicious attack. Vulnerabilities that are identified must also be prioritized into those that are critical to fix immediately, and those that should be fixed but are not critical. The resultant report should outline how to apply appropriate system configuration changes to remove vulnerabilities. Examples of remediation include applying software patches, upgrading operating systems, or turning off unnecessary services.

Tracking Intrusion Attempts

One of the best ways to identify intrusion attempts is by using intrusion detection software. Whether host-based or network-based, the purpose of intrusion detection software is to detect attempts at unauthorized access or misuse of a computer system. Intrusion detection systems identify intrusion attempts although they do not reveal whether those attempts were successful.

Most intrusion detection systems report intrusion attempts and categorize them into several categories. For example, intrusion attempts may be classified into probes, unauthorized access attempts, denial of service attacks, or malicious software. These classifications can be further broken down into the specific type of attacks used.

However, some intrusion detection systems churn out large amounts of raw data that must be compiled and analyzed to obtain meaningful information. It is important to use this data to create reports from which both technical and management personnel can extract information that demonstrates what trends are occurring and what progress is being made in preventing and responding to attacks.

For example, an increase in a certain type of attack may indicate where your systems are most vulnerable, while a decrease in another type of attack may result from vulnerabilities being successfully fixed or from traffic being filtered out at a firewall. In any case, it is important to document and measure not only the number and type of vulnerabilities, intrusion attempts, and confirmed compromises, but also the relationships between the preventative and corrective actions that affect them. Once intrusion attempts are identified, they can be analyzed to determine whether or not they were successful.

Tracking System Compromises

Keeping a record of intrusion attempts that result in compromises can provide clues as to vulnerabilities present in your networks as well as current and emerging exploits. An incident-tracking database can reveal what remediation has been previously conducted when new incidents occur. This is especially important when similar compromises repeatedly occur. Compromises should be tracked using a database with data elements such as the examples below:

- Incident Number
- Contact/Assigned to
- Category
- Date Identified/Date Closed
- Incident Status
- Description
- Time of Compromise
- System(s) Attacked
- Criticality of System(s) or data attacked
- Service(s) Attacked
- Incident Source
- Corrective Action Taken

The criticality of system(s) or data attacked is important to identify so that incidents can be prioritized and triage can be performed by assigning resources appropriately. Incident status is also significant because management needs to know when incidents have been closed out.

Whatever data elements you use to track compromises, the information should answer the following questions: Who, What, When, Where, How, and Why. If your organization does not have standard incident response procedures, templates such as the SANS Computer Security Incident Handling: Step-by-Step guide are available for purchase over the Internet. Keep in mind that too much information on an incident tracking report can take security personnel away from identifying and responding to incidents quickly. Ideally, the terminology used for the categories and classifications on reports dealing with vulnerability scans, intrusion detection, and incident tracking should be as similar as possible.

Summary

An important part of assuring the confidentiality, integrity, and availability of an organization’s information resources includes providing performance metrics on the effectiveness of a security program. Appropriate corrective actions can then be taken when the number and type of identified vulnerabilities, intrusion attempts, and confirmed compromises affect the ability of the organization to accomplish its mission.

Illustrating a "before and after" picture of corrective actions is important to demonstrate the progress of a security program. Examples of questions that can help show this progress include:

- Of the vulnerabilities identified, how many were repaired?
- Of the intrusion attempts identified, how many resulted in confirmed compromises?
- Of the confirmed compromises, how many were successfully remediated?

Comparing security performance measures against previous results can be accomplished by evaluating lessons learned and implementing specific preventative and corrective actions or processes. A comprehensive security incident tracking process can assist organizations in improving ad-hoc, "firefighting" security programs by employing structured procedures and tracking and analyzing performance measures.