Table of Contents

Introduction

Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization.

Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion–detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the information systems or by external parties to abuse their privileges or exploit security vulnerabilities.

Terminology

The term target system is used here to denote the information system being monitored by the intrusion-detection system. It can be a work station, a network element, a server, a mainframe, a firewall, a web server, etc .

The term audit denotes information provided by a system concerning its inner workings and behavior .Examples of audits include, but are not limited to, C2 audit trail, accounting, and syslog in the UNIX world, Syslog in the MVS world, event log in Windows NT, and incident tickets in X25 networks.

Description

An intrusion-detection system acquires information about an information system to perform a diagnosis on the security status of the latter. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. A typical intrusion-detection system is shown in Figure.

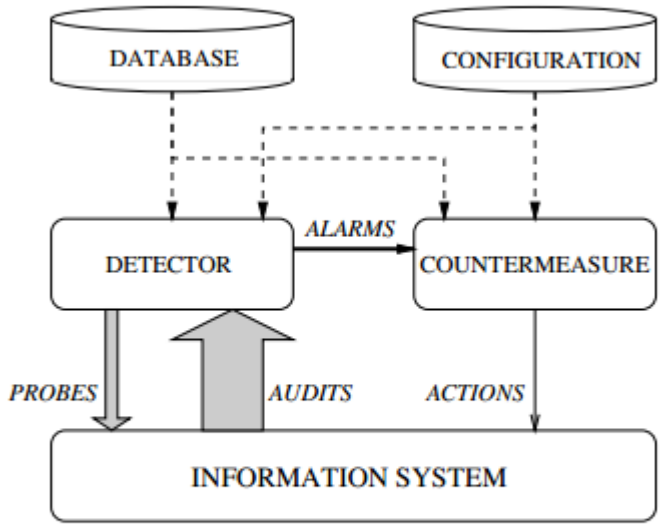

Figure 1: Very simple intrusion-detection system.

An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system to be protected. This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications. It uses three kinds of information: long-term information related to the technique used to detect intrusions (a knowledge base of attacks, for example), configuration information about the current state of the system, and audit information describing the events that are happening on the system. The role of the detector is to eliminate unneeded information from the audit trail. It then presents either a synthetic view of the security-related actions taken during normal usage of the system, or a synthetic view of the current security state of the system. A decision is then taken to evaluate the probability that these actions or this state can be considered as symptoms of an intrusion or vulnerabilities. A countermeasure component can then take corrective action to either prevent the actions

from being executed or change the state of the system back to a secure state.

Characterstics of intrusion-detection systems:

Performance:

The performance of an intrusion-detection system is the rate at which audit events are processed. If the performance of the intrusion-detection system is poor, then real-time detection is not possible.

Completeness:

Completeness is the property of an intrusion-detection system to detect all attacks. Incompleteness occurs when the intrusion-detection system fails to detect an attack. This measure is much more difficult to evaluate than the others because it is impossible to have a global knowledge about attacks or abuses of privileges. Let us introduce two additional properties:

Fault tolerance:

An intrusion-detection system should itself be resistant to attacks, especially denial-of-service-type attacks, and should be designed with this goal in mind. This is particularly important because most intrusion-detection systems run above commercially available operating systems or hard-ware, which are known to be vulnerable to attacks.

Timeliness:

An intrusion-detection system has to perform and propagate its analysis as quickly as possible to enable the security officer to react before much damage has been done, and also

to prevent the attacker from subverting the audit source or the intrusion-detection system itself. This implies more than the measure of performance because it not only encompasses the intrinsic processing speed of the intrusion-detection system, but also the time required to propagate the information and react to it.

Protection of the intrusion-detection system

When an intrusion-detection system is deployed, it becomes the natural primary target of hostile attacks, with the aim of disabling the detection feature and allowing an attacker to operate without being detected.

Disabling the intrusion-detection system can happen in the following ways:

Denial-of-service attacks:

Denial-of-service attacks are a powerful and relatively easy way of temporarily disabling the intrusion-detection system. The attack can take place against the detector, by forcing it to process more information than it can handle (for example by saturating a network link). This usually has the effect of delaying detection of the attack or, in the worst case, of confusing the detector enough so that it misses some critical element of the attack. A second possibility is to saturate the reaction capability of the operator handling the intrusion-detection system. When the operator is presented with too many alarms, he can easily miss the important one indicating penetration, even if it is present on the screen.

Evasion of the detection:

Several techniques have been developed to evade detection of an attack by intrusion-detection systems. Network-based tools, the most popular tools today, particularly suffer

from these attacks involving hand-crafted network packets:

Attack by IP fragmentation:

Intrusion-detection systems have difficulties reassembling IP packets. Therefore, splitting an attack artificially into multiple packets creates a mismatch between the data in the packet and the signature, thus hiding the attack.

Related Posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function

19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer