|  |
| --- |
|  |
| SYSTEM SECURITY AND INTRUSION DETECTION |
| Submitted by:VANDANA KATYAYAN |

|  |
| --- |
|  |

ACKNOWLEDGMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this report.  A special gratitude we give to our final year project head, Mr Laxman Sayana, whose contribution in stimulating suggestions and encouragement, helped us to coordinate our project especially in writing this report.

Furthermore we would also like to acknowledge with much appreciation the crucial role of the staff FST, who gave the permission to use all required equipment and the necessary materials to complete the  task SYSTEM SECURITY AND INTRUSION DETECTION. We have to appreciate the guidance given by other supervisor as well as the panels especially in our project presentation that has improved our presentation skills thanks to their comment and advices

CONTENTS

* System security
* Intruders
* Examples of Intrusions
* Intrusion detection
* Approaches to Intrusion detection
* Audit Records
* Statistical Anomaly Detection
* Rule based detection
* References

SYSTEM SECURITY

Security is a concern of organizations with assets that are controlled by

Computer systems. By accessing or altering data, an attacker can steal tangible assets or lead an organization to take actions it would not

otherwise take. By merely examining data, an attacker can gain a competitive advantage, without the owner of the data being any the wiser. It refers to the techniques for ensuring that data stored in the computer cannot be read or compromised by any individual without authorization.

**Why we need to protect our system?**

A hacked system can be used to:

* + - Steal passwords
    - send spam and phishing emails
    - Access restricted and personal data on a system
    - Infect other systems

**System security is concerns with:**

* **Confidentiality:** Only authorized users can access the data or information stored in the computer.
* **Integrity:** Only authorized users are allowed to change or modify the data or information in the system.
* **Availability:** Data or information must be available to the users when needed.
* **Authenticity:** The user must be a genuine or legitimate user.

**Common measures to be taken :**

* Password programs which require the user to change passwords periodically.
* Make sure your system is protected with up to date antivirus software.
* Some users choose their password as their name, city or address since it can be easily guessed by any attacker or intruder so they must choose some complex password

**INTRUDER**

One of the two most publicized threats to security is the intruder (the other is viruses), generally referred to as a hacker or cracker. An individual who breaks into the system without authorization and might exploit users data.

The three classes of the intruders are:

* **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
* **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
* **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

Examples of the intrusions are:

* Guessing and cracking passwords
* Copying a database containing credit card numbers
* Viewing sensitive data, including payroll records and medical information, without authorization
* Running a packet sniffer on a workstation to capture usernames and passwords
* Dialing into an unsecured modem and gaining internal network access
* Posing as an executive, calling the help desk, resetting the executive’s e-mail password, and learning the new password

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider. Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system. The high level were sophisticated users with a thorough knowledge of the technology; the low level were the "foot soldiers"who merely used the supplied cracking programs with little understanding of how they worked. This teamwork combined the two most serious weapons in the intruder armory: sophisticated knowledge of how to intrude and a willingness to spend countless hours "turning doorknobs" to probe for weaknesses. In addition to running password-cracking programs, the intruders attempted to modify login software to enable them to capture passwords of users logging on to systems. This made it possible for them to build up an impressive collection of compromised passwords, which was made available on the bulletin board set up on one of the victim's own machines.

**INTRUSION DETECTION**

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions

**Approaches to IDS:**

**Statistical anomaly detection:** Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

* **Threshold detection:** This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
* **Profile based:** A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

**Rule-based detection:** Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

* **Anomaly detection:** Rules are developed to detect deviation from previous usage patterns.
* **Penetration identification:** An expert system approach that searches for suspicious behavior.

In a nutshell, statistical approaches attempt to define normal, or expected, behavior, whereas rulebased approaches attempt to define proper behavior.

**Audit Records:**

A fundamental tool for intrusion detection is the audit record. Some record of ongoing activity by users must be maintained as input to an intrusion detection system. Basically, two plans are used:

**● Native audit records:** Virtually all multiuser operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.

● **Detection-specific audit records:** A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system. One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

A good example of detection-specific audit records is one developed by Dorothy Denning .

Each audit record contains the following fields:

* **Subject:** Initiators of actions. A subject is typically a terminal user but might also be a process acting on behalf of users or groups of users. All activity arises through commands issued by subjects. Subjects may be grouped into different access classes, and these classes may overlap.
* **Action:** Operation performed by the subject on or with an object; for example, login, read, perform I/O, execute.
* **Object:** Receptors of actions. Examples include files, programs, messages, records, terminals, printers, and user- or program-created structures. When a subject is the recipient of an action, such as electronic mail, then that subject is considered an object. Objects may be grouped by
* type. Object granularity may vary by object type and by environment. For example, database actions may be audited for the database as a whole or at the record level.
* **Exception-Condition:** Denotes which, if any, exception condition is raised on return.
* **Resource-Usage:** A list of quantitative elements in which each element gives the amount used of some resource (e.g., number of lines printed or displayed, number of records read or written, processor time, I/O units used, session elapsed time).
* **Time-Stamp:** Unique time-and-date stamp identifying when the action took place.

**Statistical Anomaly Detection**

As was mentioned, statistical anomaly detection techniques fall into two broad categories: threshold detection and profile-based systems. Threshold detection involves counting the number of occurrences of a specific event type over an interval of time. If the count surpasses what is considered a reasonable number that one might expect to occur, then intrusion is assumed. Threshold analysis, by itself, is a crude and ineffective detector of even moderately sophisticated attacks. Both the threshold and the time interval must be determined. Because of the variability across users, such thresholds are likely to generate either a lot of false positives or a lot of false negatives.

However, simple threshold detectors may be useful in conjunction with more sophisticated techniques. Profile-based anomaly detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations. A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert. The foundation of this approach is an analysis of audit records. The audit records provide input to the intrusion detection function in two ways. First, the designer must decide on a number of quantitative metrics that can be used to measure user behavior. An analysis of audit records over a period of time can be used to determine the activity profile of the average user. Thus, the audit records serve to define typical behavior. Second, current audit records are the input used to detect intrusion. That is, the intrusion detection model analyzes incoming audit records to determine deviation from average behavior.

Examples of metrics that are useful for profile-based intrusion detection are the following:

* **Counter:** A nonnegative integer that may be incremented but not decremented until it is reset by management action. Typically, a count of certain event types is kept over a particular period of time. Examples include the number of logins by a single user during an hour, the number of times a given command is executed during a single user session, and the number of password failures during a minute.
* **Gauge:** A nonnegative integer that may be incremented or decremented. Typically, a gauge is used to measure the current value of some entity. Examples include the number of logical connections assigned to a user application and the number of outgoing messages queued for a user process.
* **Interval timer:** The length of time between two related events. An example is the length of time between successive logins to an account.
* **Resource utilization:**Quantity of resources consumed during a specified period. Examples include the number of pages printed during a user session and total time consumed by a program execution.

**Rule-Based Intrusion Detection**

Rule-based techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. In very general terms, we can characterize all approaches as focusing on either anomaly detection or penetration identification, although there is some overlap in these approaches.

**Rule-based anomaly detection**: is similar in terms of its approach and strengths to statistical anomaly detection. With the rule-based approach, historical audit records are analyzed to identify usage patterns. And to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.

**Rule-based penetration identification** :Takes a very different approach to intrusion detection, one based on expert system technology. The key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records. The normal procedure is to interview system administrators and security analysts to collect a suite of known penetration scenarios and key events that threaten the security of the target system.

Thus, the strength of the approach depends on the skill of those involved in setting up the rules.

**REFERENCES**

* Wikipedia
* Tutorials point
* Cryptography and Network Security by William Stallings