Intrusion Detection And Prevention System

PalikaJajooDayamaMeeta
M.Tech (Software Engineering)Lecturer (C.S.E Department)
Engineering College Bikaner, Bikaner Marudhar EngineeringCollege,Bikaner
palikajajoo@gmail.commadhu_dayama2000@yahoo.com

***Abstract*-As the importance of computers areincreasingly integrated into the systems the ability to detect intruders in computer systems also increases as we rely on for the correct functioning of society.Intrusion detection is a mechanism used to detectvarious attacks on a wired or wireless network.The process of monitoring the events occurring in a computer system or network and analyzing them for sign of intrusions is known as Intrusion Detection System (IDS).There are two basic approaches: anomaly detection and misuse detection. Both have naturally scaled to use in distributed systems and networks. This paper reviews the history of research in intrusion detection as performed in software in thecontext of operating systems for a single computer, a distributed system, or a network ofcomputers.**

***Keywords*- Anomaly detection, Distributed System, Intrusion Detection , Network.**

I.INTRODUCTION

Nowadays, using computers and computer networks in all communities all over the world has made computer networksecurity an international precedence. Because, it is not feasibleto build a secure system with no vulnerabilities, intrusiondetection becomes an important area of research.An intrusion detection system (IDS) is an automated systemdesigned to detect malicious attacks on computer systems through the Internet. The main aim of Intrusion DetectionSystems (IDS) is to protect the availability, confidentiality andintegrity of critical networked information systems byidentifying preferably in real time, unauthorized use, misuse,and abuse of computer systems.When a user of an information system takes an action that that user was not legallyallowed to take, it is called intrusion. The intruder may come from outside, or the intruder maybe an insider, who exceeds his limited authority to take action. Whether or not the action is detrimental, it is of concern because it might be detrimental to the health of the system, or to theservice provided by the system.As information systems have come to be more comprehensive and a higher value asset oforganizations, complex, intrusion detection subsystems have been incorporated as elements ofoperating systems, although not typically applications.Intrusion detection involves determining that some entity, an intruder, has attempted to gain, or worse, has gained unauthorized access to the system.Intruders are classified in two groups. External intruders do not have any authorizedaccess to the system they attack. Internal intruders have some authority, but seek to gainadditional ability to take action without legitimate authorization.

II. CURRENT INTRUSION DETECTION SYSTEMS

Intrusion detection is defined as the process ofintelligently monitoring the events occurring in a computersystem or network, analyzing them for signs of violations ofthe security policy. The primary aim of Intrusion DetectionSystems (IDS) is to protect the availability, confidentiality andintegrity of critical networked information systems. IntrusionDetection Systems (IDS) are defined by both the method usedto detect attacks and the placement of the IDS on the network.IDS may perform either misuse detection or anomalydetection and may be deployed as either a network-basedsystem or a host-based system.

A)Anomaly Detection

Anomaly detection is the general category of intrusion detection which works by identifying activities which vary from established patterns for users, or groups of users. Since masquerading as a legitimate user is a very powerful method for an attacker to gain access to system resources, this type of approach looks for the variations in behavior which might indicate a masquerade. Anomaly detection typically involves the creation of knowledge bases which contain the profiles of the monitored activities.

Several types of profiles are generally used in anomaly detection. User profiles contain the parameters of auser's typical session. While these profiles are potentially the most useful in identifying indications of anomalous behavior, they are also the most difficult to create and to maintain. A balance must be struck between establishing short-term profiles, which establish patterns of recent activity and long-term profiles, which establish a historical overview of a user's activities. Unless they are updated frequently, user profiles can lead to a large number of false alarms as the user's activities change over time. To avoid, or at least modify, the adverse effects of the system's legitimate users, some anomaly detection systems include the use of user group profiles. In this method the user is

UACEE
Globalize The Research
Localize The World

placed in a work group which may or may not represent the actual assigned duties of the user. More frequently the group characterizes individuals with similar computer usage patterns. While group profiling assists in the maintenance of the detection mechanism, these profiles are often defined so broadly that unauthorized users can slip through the screen by behaving roughly similar to the typical user in the group.Other profiles which are frequently used in anomaly detection include resource profiling, (monitoring the system-wide use of accounts, applications, communication ports, etc.), and executable profiling, (monitoring the use of printers, files, and other resources which cannot easily be attributed to a single user). This user independent form of profiling is useful in detecting the presence of viruses and Trojan horses.

Anomaly detection mechanisms are usually dependent on input from an operating system's audit record. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must is utilized by the anomaly detector. Dependingon the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

B) Misuse Detection

The second general approach to intrusion detection is misuse detection. This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information. The misuse knowledge bases include specific metrics on the various techniques employed by attackers when the knowledge base was created. While anomaly detection typically utilizes threshold monitoring to indicate when a certain established metric has been reached, misuse detection techniques frequently utilize a rule-based approach. When applied to misuse detection, the rules become scenarios for network attacks. The intrusion detection mechanism identifies a potential attack if a user's activities are found to be consistent with the established rules. The use of comprehensive rules is critical in the application of expert systems for intrusion detection.Like anomaly detection techniques, misuse detection systems suffer from the potential performancedegradation which results from a dependency on audit trails for input. This disadvantage can be mitigatedby improved system performance and reduced audit record sets.

C) Combined Anomaly/Misuse detection

Research has also been conducted into intrusion detection methodologies which combine the anomaly detection approach and the misuse detection approach.These techniques seek to incorporate the benefits of both of the standard approaches to intrusion detection. The combined approach permits a single intrusion detection system to monitor for indications of external and internal attacks. While a significant advantage over the singular use of either method separately, the use of a combined anomaly/misuse detection mechanism does possess some disadvantages. The use of two knowledge bases for the intrusion detection system will increase the amount of system resources which must be dedicated to the system. Additional disk space will be required for the storage of the profiles, and increased memory requirements will be encountered as the mechanism compares user activities with information in the dual knowledge bases. In addition, the technique will share the disadvantage of either method individually in it's inability to detect collaborative or extended attack scenarios.

D) Pattern Recognition

One of the few intrusion detection methodologies which has departed from the established use of anomaly and misuse detection profiles is pattern recognition. In this approach, a series of penetration scenarios are coded into the system. Pattern recognition possesses a distinct advantage over anomaly and misuse detection methods in that it is capable of identifying attacks which may occur over an extended period of time, a series of user sessions, or by multiple attackers working in concert. This approach is effective in reducing the need to review a potentially large amount of audit data. The key disadvantage of pattern-recognition techniques is the reliance of the system on predefined intrusion scenarios. If an attack characteristic do not match one which has been coded into the system, the intrusion may not be detected. As a result, pattern-recognition mechanisms are still dependent on a statistical-type of intrusion detection approach to be a truly effective security mechanism.

E) Network Monitoring

A final method of detecting system intrusions which is currently in use is the use of various network monitoring techniques. These methodologies passively monitor network activity for indications of attacks. Network monitoring offers several advantages over traditional audit-based intrusion detection systems. Because many intrusions occur over network at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by audit-based intrusion detection mechanisms. The greatest advantage of network monitoring mechanisms is their independence from reliance on audit data. Because these methods do not require input from any operating system's audit trail they can use standard network protocols to monitor heterogeneous sets of operating systems and hosts.

Independence from audit trails also frees network monitoring systems from possessing an inherent weakness caused by the vulnerability of the audit trail to attack. Intruder actions which interfere with audit functions or which modify audit data can lead to the prevention of intrusion detection or the inability to identify the nature of an attack. Network monitors are able to avoid attracting the attention of intruders by passively observing network activity and reporting unusual occurrences. Another significant advantage of detecting intrusions without relying on audit data is the improvement of system performance which results from the removal of the overhead imposed by audit trails. The process of analyzing audit trails increases the performance degradation of the system. In addition, techniques which move the audit data across network connections reduce the bandwidth available to other functions. Network monitoring techniques can increase performance of networks by 5 to 20 percent compared to audit based systems.

IIICURRENT INTRUSION DETECTION TECHNIQUES

The following is a review of the significant developments inintrusion detection research which have been made in the past several years.

A) NIDES

The Intrusion Detection Expert System (IDES) has become a standard in intrusion detection systems. Several current systems are based in part on IDES prototype technology, The Next -Generation Intrusion Detection Expert System (NIDES) is the comprehensive enhancement to IDES. NIDES is a real-time intrusion detection application which integrates a statistical analysis –based anomaly detector and a rule-based misuse detection system. This combination gives NIDES the ability to detect penetrations from internal and external attacks. A number of significant improvements incorporated into NIDES. In addition to modularizing the application, NIDES includes an enhanced statistical analysis component and additional support for a strict client-server model. NIDE also includes a comprehensive user interface that permits access to all of the applications capabilities, as well as a context -sensitive help system. While NIDES is regarded as the current state-of-the-art in a combined anomaly and misuse detection system, the application retains the difficulty possessed by all similar models in detecting collaborative attacks, long-term penetration scenarios and virus propagation. Another potential disadvantage is that NIDES retains a reliance on the system's audit record for input. Future expansions of the rulebase and the development of profiles of entities other than users should reduce the potential vulnerabilities which are not adequately addressed by the current system.

B) DIDS

The Distributed Intrusion Detection System (DIDS) is an intrusion detection mechanism combines attributes of a network monitoring system with the system-level capabilities of an audit record-based combined anomaly/misuse detector. DIDS incorporates a monitor on each host, a monitor on the local area network (LAN), and a DIDS director. Each host monitor consists of a host event generator and a host agent. The host event generator reviews the audit data from the host for indications of events which may be part of an attack. The DIDS host event generators also utilize user and group profiles to identify anomalous behaviors in the audit record. The information identified by the host event generator is reported to the DIDS director by the host agent. The LAN monitor is the network equivalent of the host monitor. It includes the LAN event generator and the LAN agent. However, unlike the host event generator, the LAN event generator does not review audit data. The LAN event generator utilizes the network monitoring approach to review all network traffic, including host-to-host connections and resources used. The information obtained by the LAN event generator is reported to the DIDS director by the LAN agent. The DIDS director forms the heart of the intrusion detection mechanism.

C) STAT/USTAT

The State Transition Analysis Tool (STAT) and USTAT, the variation of STAT which was designed specifically for the UNIX operating system environment, are rule-based penetration detection approaches which characterize the process of an attack on a computer system as a series of transitions from an initial state to a compromised state. The technique defines specific events, called signature actions, which occur between each of the intermediate transitions. The omission of any of the signature actions results in a failed attack on the system. Once the relevant system states have been defined and the required signature actions have been identified, the approach utilizes state transition diagrams to describe the attack's progress through a penetration scenario. State transition diagrams are useful because they provide a graphical representation of the requirements and compromise of the penetration while describing the events which must occur for the attack to be successful.

D)TRIPWIRE

Tripwire is anintegrity checking program which permits a system administrator to monitor system files for addition, deletion, or modification. The program is estimated to have been installed on several thousand systemsworldwide.

While it is not an intrusion detection mechanism, Tripwire does provide valuable information for theprocess of detecting attacks on a system. Tripwire is designed for the UNIX operating system environment the program has proven to be scaleable, portable, and manageable.Tripwire utilizes input from a configuration file and a database to identify areas of interest. Theconfiguration file consists of a description of the file systems which are to be monitored. The databasecontains the signatures of files which match the configuration. The signatures of the files are calculatedbased on the contents of the system files. The signature computation is easy to derive but impossible toreverse.Tripwire operates in one of four modes. In the database initialization mode, the program generate adatabase which contains all of the relevant information on the system files, including signatures. Becausethe baseline database is being generated based on the files which currently exist in the system, it is criticalthat the existing database is free of logic bombs, viruses, Trojan horses, or other attack programs.

IV.LATEST TRENDS IN INTRUSION DETECTION RESEARCH

Artificial Intelligence, Neural Networks and Machine Learning

The practical application of artificial intelligence techniques to the area of intrusion detection has been anticipated for several years. However, while expert systems have been widely incorporated into many intrusion detection systems, the effective application of AI has been elusive. There are tangible areas where AI techniques could be applied to intrusion detection methodologies. In general, AI could provide significant benefits to intrusion detection through data reduction, the ability to analyze a collection of data to identify the most important components, and classification, the process of identifying intruders. In particular, there are four areas where AI and machine learning could be applied to intrusion detection systems:

1. By using concept learning, the ability to train a system to classify elements into categories, the intrusion detection system would have enhanced capabilities to differentiate normal activities from intrusive.
2. Clustering, the partitioning of elements into groups based on a specified criteria, could be applied to the effective classification of users, groups, sessions, etc.
3. Predictive learning techniques applied to intrusion detection would allow the system to develop a temporal model of data and permit the system to learn of intrusive behavior from temporal data and sequences of individual events.
4. The ability to extract relevant features from irrelevant data and the possibility of combining relevant features into functions that identify intrusive events. In addition to AI and machine learning, neural networks could provide a valuable addition to intrusion detection systems because of the flexible pattern recognition capabilities of the technology. The ability to adaptively model users and system behaviors, and the capability to effectively handle intrusive events aresome of the potential advantages of neural networks. Most importantly, neural networks are particularlyuseful in identifying gradual changes to a system or in the behavior of a user. While expert systems arecurrently capable of recognizing rapid changes in a system, the identification of slower changes in behaviorrequires the employment of improved techniques.AI, machine learning techniques, and neural networks, properly refined and implemented, result inthe development of a comprehensive intrusion detection system.

V.INTRUSION PREVENTION SYSTEM

Intrusion Prevention Systems (IPS), also knownas Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of ‘’’intrusion prevention systems’’’ are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

A) CLASSIFICATIONS

Intrusion prevention systems can be classified into four different types:

Network-based Intrusion Prevention (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

Wireless Intrusion Prevention Systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Network Behavior Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

Host-based Intrusion Prevention (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

B)DETECTION METHOD:

The majority of intrusion prevention systems utilize one of three detection methods: signature-based,statistical anomaly-based, and stateful protocol analysis.

Signature-based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

Statistical Anomaly-based Detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Stateful Protocol Analysis Detection: This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity.

VI. CONCLUSION

We have presented an overview of the technologies which are being utilized for the detection of attacks against computer systems, and a survey of the experiences of those most effected by intrusion detection technology. We have also reviewed of some of the significant techniques which hold the promise of effectively protecting computer systems. The security of information in computer-based systems and networks continues to be a major concern to researchers. The work in intrusion detection techniques and methodologies which has been a major focus of information security-related research in the past two decades is certain to continue. The area of intrusion detection is continuing to evolve. While a number of methodologies and tools have been designed to assist in the identification of intruders, no definable standard has been developed which could serve as the basis for a deployable intrusion detection tool. However, as the processing capabilities of computer systems improve and the innovative approaches to intrusion detection continue to be developed, the creation of an effective intrusion detection standard is inevitable.

REFERENCES

[1] Anderson, D., Frivold, T. & Valdes, A. (May, 1995). Next -generation Intrusion Detection Expert System(NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07.

[2] Anderson, J.P. (April, 1980). Computer Security Threat Monitoring and Surveillance. Technical Report,J.P. Anderson Company, Fort Washington, Pennsylvania.

[3] Castano, S., Fugini, M., Martella, G. &Samarati, P. (1995). Database Security. Addison-WesleyPublishing Company, New York.

[4] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model.IEEE Transactions on SoftwareEngineering, Vol. SE-13, No. 2.

[5] Frank, Jeremy. (1994). Artificial Intelligence and Intrusion Detection: Current and Future Directions.Proceedings of the 17th National Computer Security Conference.

[6]"NIST - Guide to Intrusion Detection and Prevention Systems (IDPS)". 2007-02. Retrieved 2010-06-25.