International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-2, December 2011

Intrusion Detection Systems Technology

Tripti Sharma, Khomlal Sinha

ABSTRACT : ***Network security is one of the most important nonfunctional requirements in a system [1]. Over the years, many software solutions have been developed to enhance network security and this paper provides an insight into one such solution which has become prominent in the last decade i.e. Intrusion Detection System (IDS) [2]. In this paper, we have proposed an overview of intrusion detection system and their classification with advantages and disadvantages, and also providing the basic requirement of intrusion detection system.***

Keywords : Host based IDS, Intrusion Detection System, misuse IDS, network security, texanomy, etc.

1. INTRODUCTION

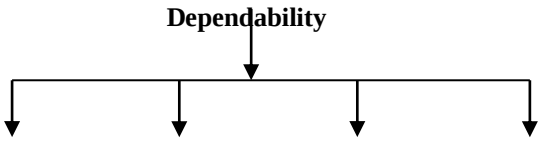
In the last few years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

1.1 *Computer Security and its Role :* One broad definition of a secure computer system is given by Garfinkel and Spafford as one that can be depended upon to behave as it is expected to. It is always a point of benefit to integrate security with dependability and how to obtain a dependable computing system. Intrusion detection analyzes

Manuscript published on 30 December 2011.
* Correspondence Author (s)
Tripti Sharma, Assistant Professor & Head, Department of Computer Science & Engineering, Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, (E-mail ID - triptisharma@csitdurg.in)
Khomlal Sinha, M.Tech. Scholar (Computer Science & Engineering), Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, Mobile – 00919302451423, (E-mail ID - Khomlal_sinha@yahoo.co.in)

Dependability is the trustworthiness of a system and can be seen as the quality of the service a system offers. Integrating security and dependability can be done in unauthorized accesses and malicious behaviors and finds intrusion behaviors and attempts by detecting the state and activity of an operation system to provide an effective means for intrusion defense. various ways. One approach is to treat security as one characteristic of dependability on the same level as availability, reliability and safety as shown in the figure. 1.



Availability Reliability Safety Security

A narrower definition of security is the possibility for a system to protect objects with respect to confidentiality, authentication, integrity and non-repudiation.

Confidentiality: Transforming data such that only authorized parties can decode it.
Authentication: Proving or disproving someone's or something's claimed identity.
Integrity checking: Ensuring that data cannot be modified without such modification being detectable
Non – repudiation: Proving that a source of some data did in fact send data that he might later deny sending

1.2 Need For Intrusion Detection : A computer system should provide confidentiality, integrity and assurance against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. These subversion attempts try to exploit flaws in the operating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988 [3].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

There are two ways to handle subversion attempts. One way is to prevent subversion itself by building a completely secure system. We could, for example, require all users to identify and authenticate themselves; we could protect data by various cryptographic methods and very tight access control mechanisms. However this is not really feasible because:

1. In practice, it is not possible to build a completely secure system. Miller gives a compelling report on bugs in popular programs and operating systems that seems to indicate that (a) bug free software is still a dream and (b) no-one seems to want to make the effort to try to develop such software. Apart from the fact that we do not seem to be getting our money's worth when we buy software, there are also security implications when our E-mail software, for example, can be attacked. Designing and implementing a totally secure system is thus an extremely difficult task.

2. The vast installed base of systems worldwide guarantees that any transition to a secure system, (if it is ever developed) will be long in coming.

3. Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords, and entire crypto-systems can be broken.

4. Even a truly secure system is vulnerable to abuse by insiders who abuse their privileges.

5. It has been seen that that the relationship between the level of access control and user efficiency is an inverse one, which means that the stricter the mechanisms, the lower the efficiency becomes.

The history of security research has taught us a valuable lesson – no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in.

We thus see that we are stuck with systems that have vulnerabilities for a while to come. If there are attacks on a system, we would like to detect them as soon as possible (preferably in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active agent. It plays the role of an informant rather than a police officer. Section 2 discusses about background of IDS and basic requirement of IDS system. in Section 3 discusses about the taxonomy of IDS.. . Section 4 provides a conclusion of this paper.

2. Background On Intrusion Detection: In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions [4].

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the "signatures" of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

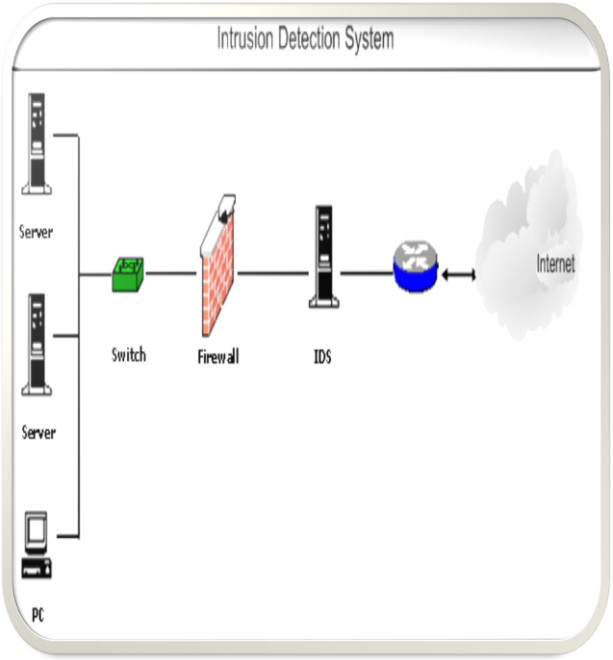


Figure 2.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station Intrusions to your corporate network can be blocked by the implementation of IDS. It can be very powerful if it is implemented the right way.

Intrusion Detection System (IDS) is a system that will constantly monitor the corporate networks from all types of attacks and vulnerabilities. IDS look for the attack signatures which are specific patterns that usually indicate malicious or suspicious event [5].

2.1 IDS Requirements : At least one past effort has identified desirable characteristics for IDS. Regardless on what mechanisms an ID is based, it must do the following [6]:

- Run continuously without human supervision,
- Be fault tolerant and survivable,
- Resist subversion,
- Impose minimal overhead,
- Observe deviations from normal behavior
- Be easily tailored to a specific network
- Adapt to changes over time, and
- Be difficult to fool.

We have developed a similar set of requirements along two themes: functional and performance requirements.

2.1.1 Functional Requirements : As the network-computing environment increases in complexity, so do the functional requirements of IDSs. Common functional requirements of an IDS being deployed in current or near-term operational computing environments include the following:

- The IDS must continuously monitor and report intrusions.
- The IDS must supply enough information to repair the system, determine the extent of damage, and establish responsibility for the intrusion.
- The IDS should be modular and configurable as each host and network segment will require their own tests and these tests will need to be continuously upgraded and eventually replaced with new tests.
- Since the IDS is assigned the critical role of monitoring the security state of the network, the IDS itself is a primary target of attack. The IDS must be able to operate in a hostile computing environment and exhibit a high degree of fault-tolerance and allow for graceful degradation.
- The IDS should be adaptive to network topology and configuration changes as computing elements are dynamically added and removed from the network.
- Anomaly detection systems should have a very low false alarm rate. Given the projected increase in network connectivity and traffic, simply decreasing the percentage of overall false alarms may not be sufficient as their absolute number may continue to rise.
- The IDS should be able to learn from past experiences and improve its detection capabilities over time. A self-tuning ID will be able to learning from false alarms with the guidance of system administrators and eventually on its own.
- The IDS should be able to be easily and frequently updated with attack signatures as new security advisories and security patches become available and new vulnerabilities and attacks are discovered.
- Decision support tools will be necessary to help system administrators respond to various attacks. The IDS will be required not only to detect anomalous events, but also to take automated corrective action.
- The IDS should be able to perform data fusion and be able to process information from multiple and distributed data sources such as firewalls, routers, and switches. As real-time detection demands push networked-based solutions to re-programmable hardware devices that can download new capabilities, the IDS will need to be able to communicate with the hardware-based devices.
- Data reduction tools will be necessary to help the IDS process the information gathered from data fusion techniques. Data mining tools will be helpful in running statistical analysis tools on archived data in support of anomaly detection techniques.
- The IDS should be capable of providing an automated response to suspicious activity.
- Rapid changes in network conditions and limited network administration expertise make it difficult for system administrators to diagnose problems and take corrective action to minimize the damage that intruders can cause.
- The ability to detect and react to distributed and coordinated attacks will become necessary. Coordinated attacks against a network will be able to marshal greater forces and launch many more and varied attacks

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

against a single target. These attacks can be permutations of known attacks, be rapidly evolving, and be launched at little cost to the attackers.

- Distributing the computational load and the diagnostic capabilities to agents scattered throughout the network adds a level of fault-tolerance, but it is often necessary for the system administrator to have control over the IDS from a central location.

- The IDS should be able to work with other Commercial Off-the-Shelf (COTS) security tools, as no vendor toolset is likely to excel in or to provide complete coverage of the detection, diagnosis, and response responsibilities. The IDS framework should be able to integrate various data reduction, forensic, host-based, and network-based security tools. Interoperability and conformance to standards will further increase the value of the IDS.

- IDS data often requires additional analysis to assess any damage to the network after an intrusion has been detected. Although the anomalous event was the first detected, it may not be the first attempt to gain
unauthorized access to the network. Post event analysis will be needed to identify compromised machines before the network can be restored to a safe condition.

- The IDS itself must also be designed with security in mind. For example, the IDS must be able to authenticate the administrator, audit administrator actions, mutually authenticate IDS devices, protect the IDS data, and not create additional vulnerabilities.

2.1.2 Performance Requirements : An IDS that is functionally correct, but that detects attacks too slowly is of little use. Thus we must enumerate several performance requirements for IDSs. The IDS performance requirements include:

- To the extent possible, anomalous events or breaches in security should be detected in real-time and reported immediately to minimize the damage to the network and the loss or corruption of confidential information.

- The IDS must not place undue burden or interfere with the normal operations for which the systems were bought and deployed to begin with. This requirement makes it necessary for the agents to be cognizant of the consumption of network resources for which they are competing.

- The IDS must be scalable. As new computing devices are added to the network, the IDS must be able to handle the additional computational and communication load.

3. Taxonomy : Intrusion detection system can be broadly classified based on two parameters as shown in figure 3.

(a) Analysis method used to identify intrusion, which is classified into Misuse IDS and Anomaly IDS.

(b) Source of data that is used in the analysis method, which is classified into Host, based IDS and Network based IDS [7].

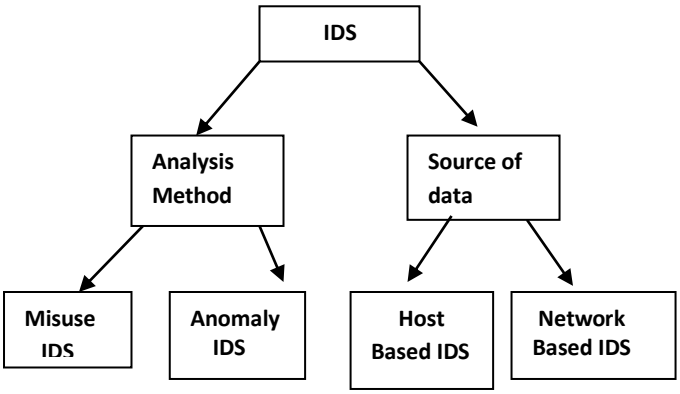


Figure 3. Taxonomy of IDS

We can divide the techniques of intrusion detection into two main types [8][9][10].

3.1 Anomaly Detection : Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities: (1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are). This is a dangerous problem, and is far more serious than the problem of false positives. The main issues in anomaly detection systems thus become the selection of threshold levels so that neither of the above 2 problems is unreasonably magnified, and the selection of features to monitor. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics. Some systems based on this technique are discussed in Section 4 while a block diagram of a typical anomaly detection system is shown in Figure below:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

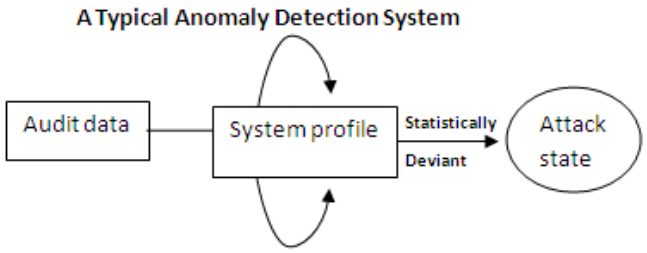


Figure 4

3.2 Misuse Detection : The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems -- they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity. A block diagram of a typical misuse detection system is shown in Figure 5.

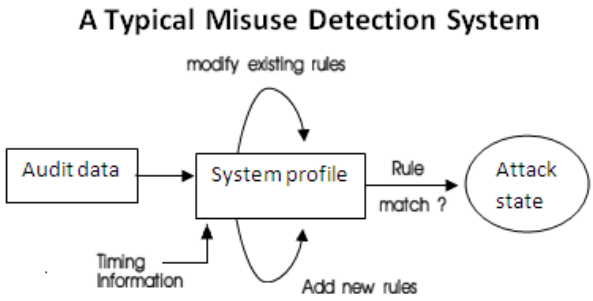


Figure 5

Advantages:

- Simplicity and no intrusiveness (which translate into ease of deployment).

Disadvantages:

- Inspecting each packet on the wire is becoming increasingly more difficult with the recent advances in network and wireless technology in terms of complexity and speed.
- Most intrusion detection systems employ a combination of both techniques, and are often deployed on the network, on a specific host, or even on an application within a host.

3.3 Network Based Intrusion Detection : The most obvious location for an intrusion detection system is right on the segment being monitored. Network-based intrusion detectors insert themselves in the network just like any other device, except they promiscuously examine every packet they see on the wire.

Advantage:

- Network-based intrusion detection is straightforward to implement and deploy.

Disadvantage:

- Truly shared segments are rare nowadays, which means a single sniffer cannot be relied to monitor an entire subnet. Instead, detection systems must be integrated in the port of Ethernet switches (the ones that have visibility into all packets on the wire), which is not always feasible, even if such a port is available.
- The fact that a single intrusion detection system is servicing the entire segment makes it an easy target for a DoS attack. Such a system should not contain any user accounts other than the privileged (root/Administrator) user; host any unnecessary network services; offer any sort of interactive network access (console access only); or be hosted on an obscure, proprietary operating system.

3.4 Host Based Intrusion Detection : While network-based intrusion detectors are straightforward to deploy and maintain, there is a whole class of attacks closely coupled to the target system and extremely hard to fingerprint. These are the ones that exploit vulnerabilities particular to specific operating systems and application suites. Only host-based intrusion detection systems (the ones running as an application on a network-connected host) can correlate the complex array of system-specific parameters that make up the signature of a well-orchestrated attack.

Advantage:

The host-based approach is ideal for those high-availability servers that enterprises rely on for everyday business. The most prevalent advantage of the host-based approach is its ability to detect an inside job-that is, an incident where a lawful user is using local host resources in a manner that violates the company's security policy.

This type of offense would be virtually impossible to unveil with a network-based intrusion detection system; because the user could have console access to the system, his or her actions would not even traverse the wire.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Disadvantages:

Not all is well in the world of host-based intrusion detection, however: Since these systems are closely tied to the operating system, they become yet one more application to maintain and migrate. This is a critical point in an environment where operating system levels are upgraded often, as the intrusion detection system must be kept up to date for it to work efficiently. Also, deploying host-based detectors alone will not protect your enterprise against basic, Network-layer DoS attacks (SYN flooding, ping of death, land attack, and so on). These limitations withstanding, host-based detection should be an integral part of your overall intrusion defense.

4. CONCLUSION:

Intrusion detection mechanisms play a crucial role in the security landscape of a organization. In this paper we have focused the basic concepts and requirements for intrusion detection system. We also focused on the classification of IDS.

REFERENCES

1. S. Stanford Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, "Grids - a graph based intrusion detection system for large networks", 19th National Information Systems Security Conference, 1996.
2. R. Heady, G. Luger, A. Maccabe, and M. Servilla. The Architecture of a Network Level Intrusion Detection System. Technical report, Department of Computer Science, University of New Mexico, August 1990
3. Khaled Labib, Computer security and intrusion detection, Crossroads, Volume 11, Issue 1, p.p. 212-219, August 2004
4. S. Axelsson. Research in intrusion detection systems: A survey. In Technical Report 98-17 (revised in 1999) Chalmers University of Technology, 1999.
5. Teresa F. Lunt. A survey of intrusion detection techniques. Computers & Security, 12(4): p.p. 405-418, 1993.
6. Aurobindo Sundaram , An Introduction to Intrusion Detection, Crossroads, Volume 2, Issue 4, Pages: 3 – 7, 1996
7. Sandeep Kumar. Classification and Detection ofComputer Intrusions. Ph.D. Dissertation, August 1995.
8. E. Biermann, E. Cloete and L. M. Venter, A comparison of Intrusion Detection systems, Computers & Security, Volume 20, Issue 8, Pages 676-683, December 2001,
9. Lubomir Nistor, Rules definition for anomaly based intrusion detection, 4th National Information Systems Security Conference, 1999.
10. Elisa Bertino, Ashish Kamra, Evimaria Terzi, and Athena Vakali. Intrusion detection in rbac-administered databases. In ACSAC, pages 170-182, 2005.

AUTHOR PROFILE

Prof. Tripti Sharma, received B.E. (Computer Sc.) and M.Tech. (Computer Sc.) in the years 2002 and 2010 respectively. Currently working as Assistant Professor and Head in the Department of Computer Science & Engineering at Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, Her interests are Digital Image Processing and Data Mining. Also she is having Life Membership of Indian Society of Technical Education, India (ISTE), Membership No- LM 74671 and Institutional Member of Computer Society of India (CSI). Membership No- N1009279.

Khomlal Sinha, received B.E. (Information Technology) in year 2005 and in pursuit for M.Tech. (Computer Sc.) from Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, His interests are Digital Image Processing, Operating Systems and Data Mining. Also he is having Life Membership of Indian Society of Technical Education, India (ISTE) and Institutional Member of Computer Society of India (CSI).

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)