Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Intrusion Detection System

**Neha Pathapati**[*]
Computer Science, M.S. Ramaiah Institute of Technology
Karnataka, India

***Abstract*— An Intrusion Detection System (IDS) aims two detect two types of attacks with equal efficiency. First, the attacks from external, third party hackers. Second, intrusions arising internally due to trusted members misusing and abusing their privileges. An IDS is based upon the principle that the illegitimate actions of an intruder is always noticeably different from the legal actions of an authorized personnel. To derive best benefits of an IDS, it has to be implemented in conjunction with other existing security technologies. This paper underscores in detail the IDS, its need, goals, the detection techniques used by it, its types and its real-time functioning.**

***Keywords*— Intrusion Detection System, Need, Goals, Detection Techniques, Types, Functioning.**

## I. INTRODUCTION

Intrusion Detection Systems (IDS) are being developed in response to the increasing number of attacks on major sites and networks. The safeguarding of security is becoming challenging because – first, the possible technologies of an attack are becoming ever more sophisticated, second, at the same time, decreased technical ability is needed for the novice attacker as proven past methods are easily accessible through the Web. Firewalls, encryption, authentication and Virtual Private Networks (VPN) have been deployed since a long time to secure the network infrastructure and communication over the internet. Intrusion detection is a relatively new addition to set of security technologies.

An intrusion refers to any unauthorized access or malicious utilization of information resources [1].

An intruder or an attacker is an entity that tries to find a means to gain unauthorized access to information, inflict harm or engage in other malicious activities [2].

Intrusion Detection (ID) is concerned with the identification of security breaches in a system. It encompasses the detection of an intrusion, which are the attacks from outside a system and misuse, which are attacks that occur from within an organization [2].

An intrusion detection system (IDS) is a device or software application that closely monitors the network or system activities for malicious activities or policy violations and produces reports to a management station [2].

## II. NEED FOR AN IDS

The primary need for an IDS is to protect information resources and system integrity.

Several security layers are needed to protect data as no one layer can provide all security measures. Hence, IDS is one of the many complementary layers of IT security technology being employed along with firewalls, anti-virus, password, Virtual Private Network (VPN) and other security technologies.

Some of the misconceptions held with respect to computer security are that – a network firewall keeps all intruders at bay, an anti-virus recognizes and wards off all viruses, and password protected access completely prevents all intruders from breaking into the network [3]. However, in reality – firewalls do not recognize and block attacks, an anti-virus software is only well-versed at detecting viruses previously encountered, and passwords can always be hacked and altered by intruders.

Research has shown that large financial losses in organizations have occurred due to internal attack on data, that is, attacks from internal intruders. A firewall is incapable of detecting internal attacks. That is, firewalls function at the periphery of the network. Hence, it cannot detect any malicious activity occurring inside the system; it only monitors traffic which passes between the internal network and the Internet.

An IDS is capable of doing several things that basic firewalls, for instance, cannot do [4]:

- Identify anomalous packet payload or patterns of traffic that are not consistent with the normal for any particular company's network.
- Detect patterns or signatures, of packets with malicious payload entering or exiting a company's network.
- Determine alterations in the "state" of corporate servers.

Hence, there is a pressing need to employ an IDS along with other security technologies.

## III. GOALS OF AN IDS

The major goals of an IDS are [5]:

- To detect a wide panoply of intrusions, which may be previously known or unknown.

- Log information, an IDS should record all suspicious occurrences in the system. This facilitates the accelerated detection of intrusions that have been previously encountered in future.
- Report the administrator of the attack.
- Be accurate. An IDS has to aim to curtail false positives, minimize false negatives. A false positive refers to a situation in which an event signals an IDS to produce an alarm when no attack has taken place. A false negative, on the other hand, refers to a situation in which no alarm is raised when an attack has indeed occurred.

## IV. INTRUSION DETECTION TECHNIQUES

The two types of IDS techniques are [6]:

### *A. Anomaly Based Detection Technique*

Anomaly-based detection is the process of comparing and contrasting the definitions of what activity is considered normal against observed events to identify notable deviations. An IDS employing this technique maintains profiles that represent the normal behaviour of entities such as - users, hosts, network connections, or applications. These profiles are established by observing the characteristics of typical activity over a considerable time period. The IDS then employs statistical methods to compare and contrast the characteristics of current activity to thresholds related to the profile. Profiles can be constructed for almost any measurable attribute (e.g. the number of emails sent from a particular host, login attempts count or the amount of the free memory) [6].

The profiles can be of two types [6]:

- Static: Static profiles remain constant.
- Dynamic: Dynamic profiles are fine-tuned in time in accordance with the development in the network (these changes reflect what is considered to be the accepted legitimate behaviour).

*1) Advantages of Anomaly Based Detection Technique:* Some of the merits of anomaly detection technique are as follows [6].

- Detection of new attacks
  Anomaly detection is able to detect new, unknown attacks if they change observed attributes over current thresholds.
- Insider attacks detection
  Legitimate action (e.g. file copying) can be considered an attack if it is executed in an unauthorized manner (e.g. by an employee who should not have access to the file).

*2) Disadvantages of Anomaly Based Detection Technique*: Some of the demerits of anomaly detection technique are as follows [6].

- Dynamic profiles learning
  An attacker can perform her activity gradually without significant changes in time (e.g. slowly increase the amount of spam she sends into the network). An IDS which uses dynamic profiles than incorporates attacker's activity in its definition of normal behaviour.
- Complexity
  Anomaly detection is hard to understand and requires extensive study.
- Choice of characteristics
  Apposite choice of monitored attributes is vital for the successful detection. Every environment is distinctive and the IDS must be configured accordingly.
- Attack analysis difficulties
  It is the administrator's responsibility to discover the source and the inflictor when an alert is engendered. Anomaly-based IDS proposes the interpretation of the attack only with a certain probability.
- Learning period
  When an anomaly-based IDS is deployed in the network there is a time window for building of profiles. During this period, the IDS is unable to detect attacks.

### *B. Signature Based Detection Technique*

A signature is a pattern that concurs with a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible attacks. If the match occurs, an alert is generated. An event might be a capture of a packet, appearance of certain record in system log etc. The examples of signatures could be - packet with invalid combination of flags in TCP header, connection attempt between two specific IP addresses, or packet being transmitted to port 22 of a specific server, which contains "suroot" string in its payload [6].

*1). Advantages of Signature Detection Technique*: Some of the merits of signature based detection technique are as follows [6].

- Understandability
  Signatures are easy to understand, to create and to modify. Every signature clearly states under what conditions the alert was generated. Even inexperienced security administrators are able to learn the common set of rules to their environment.

- Accuracy
  If rules are suitably defined there is a minimum of false positives. On the other hand irresponsibly designed rules can lead to a high amount of false positives (e.g. too general rules). False negatives rate is difficult to assess. If the monitored packet stream contains an attack described by one or more rules it is always discovered. However we do not have any indication of for how many attacks we lack signatures.
- Rapid deployment
  Signature-based IDS can operate immediately after the installation and the setting of rules, it does not require any learning period.
- Logging abilities
  If an attack is detected, many properties can be logged (e.g. which signature matched, what packet was the source of attack in what exact time) or the packet itself can be stored for the further analysis.

*2). Disadvantages of Signature Detection Technique*: Some of the demerits of signature based detection technique are as follows [6].

- Inability to detect new attacks
  Attacks for which signatures do not exist yet cannot be detected.
- Variability of attacks
  Attacks with multiple variants require a separate signature for each of them.
- Signature database updates
  Signature database must be regularly updated with signatures of new attacks and some signatures must be modified. Also, for performance reasons it is recommended to remove signatures for attacks that are no longer applicable in the environment.
- Heterogeneity of environments
  A signature which detects an attack in a given environment may not be able to detect an attack when it is used in a different environment (e.g. on a different operating system).

## V. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

The Intrusion Detection System can be classified based on the following criteria.

### *A. Based on the System Being Protected*

Based upon the target system that the IDS is protecting from the attack of an intruder, an IDS can be classified into the following two types.

*1). Host Intrusion Detection System (HIDS*: A host-based IDS is a software application that is installed on the individual hosts of a network which have to be protected. Its primary purpose is to trace the behaviour of a host that could be categorized as unauthorized, illegal and aberrant. The dynamic behaviour and the state of a computer system is thoroughly monitored by a HIDS. For instance, a HIDS may inspect the network packets arriving at the specific host upon which it is installed. It may also keep a close check on which program or application of the system is accessing which system resource and the HIDS may draw a conclusion that some form of anomalous activity is taking place on the system if a word-processor begins to alter the contents of the system password database. On the other hand, a HIDS may check if the stored information in the system appears as expected as a means of monitoring the state of the system – it may inspect the RAM or the log files to ascertain that the contents have not been modified by an attacker or intruder. Some of the commercially available HIDS are OSSEC (Open Source Host-based Intrusion Detection System) and AIDE (Advanced Intrusion Detection Environment) [7].

In most cases, a HIDS is implemented by the setting up of audit trails. An audit trail or an audit log is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event [11]. Consequently, the administrator peruses the HIDS-maintained audit logs to detect suspicious activity and take appropriate action.

The merits of a Host Intrusion Detection System are as follows [8].

- Accurate verification of the occurrence of an intrusion
  As stated earlier, a HIDS depends on the system logs to keep a track of the events actually taking place on the system. Thus, if an attack occurs, the evidence for the attack can be seen in the system logs. Consequently, the administrator can ascertain the occurrence of an attack with greater precision and fewer false positives.
- Monitoring of all system activities
  A HIDS monitors activities like - file accesses, changes made to file permissions, installation of new executables, user log on and log off actions, all user activities while he is connected to the network, activities that are executed by the administrator, changes made to the file system, addition, deletion and modification of user accounts and so on. Hence, a HIDS can certainly detect an illegal action as it is closely monitoring a wide range of activities taking place on the system.
- Installation of a HIDS is economical
  Since a HIDS is a software application installed on the host to be protected, the cost involved in the deployment, maintenance and upgrading of the hardware is overcome.
- Detects attacks than an NIDS cannot identify

A HIDS is equally efficient in protecting the host from attacks of the internal users as well as the external users. For instance, if an authorized user attempts to make changes to the system password database or the system files, this kind of attack would go unnoticed by a NIDS.

- Even distribution of monitoring load
  A HIDS protects the host upon which it resides. Hence, the load associated with monitoring the entire network is fairly distributed across all its individual hosts. This is especially advantageous in case of large network traffic.
- HIDS can function in switched and encrypted environments
  A switch is inclined to isolate communications on the network. Since HIDS runs on individual systems, it is uninfluenced by the traffic isolation properties of the switch. HIDS can scrutinize the decrypted traffic to find an attack signature. Hence, it is adequately equipped to monitor encrypted traffic.

The demerits of a Host Intrusion Detection System are as follows [8].

- Dependent upon the administrator
  The audit trails, system logs and other sources have to be manually and continuously monitored by the administrator to identify an intrusion.
- Provides only local view of the attack
  A HIDS cannot monitor network traffic and can only detect attacks local to the host upon which it is running.
- Operating System dependent
  A HIDS is operating system dependent and the software does not enjoy portability
- Difficult maintenance on large networks
  In large networks with varying operating systems and system configurations, it is difficult to install and maintain HIDS on each individual host.
- Large consumption of space
  Storing of the audit trails upon which HIDS is heavily dependent consumes massive memory space.
- Destroying of the evidence of an attack
  If HIDS system is compromised, the attacker can modify audit logs to leave no trace of his attack.

*2). Network Intrusion Detection System (NIDS):* A Network Intrusion Detection System can occur in two forms – it can be a hardware device such as a network tap, span port or a hub, or an application running on a system connected to the network it is required to protect. It relies on network traffic alone to detect unauthorized, illegal and aberrant activity. A NIDS is usually deployed at the entry and exit points of data from the network to the outside world. In cases where a higher level of security is needed, additional NIDS can be placed at strategic locations of the network where maximum traffic is expected to flow [1]. Some commercially available NIDS are Snort, Cisco Secure IDS, Hogwash and E-Trust IDS.

The operation on a NIDS is essentially based upon the "wiretapping concept" - to gather information from the network traffic stream as data travels. The network interface card (NIC) on a NIDS is made to run in the promiscuous mode – so it can pick up traffic whose destination address is not the IDS [8].

A NIDS can employ signature and/or anomaly based detection techniques.

If a NIDS relies on signature based detection techniques, it maintains a database of known "attack signatures", which are a set of rules to establish upon what constitutes an attack. So, a NIDS compares the signature of network traffic with the database of signatures of known attacks to quickly detect an attack. The demerit of using this technique is that the NIDS is restricted to detecting attacks that have previously occurred. That is, it may not be equipped to identify a unique attack that is occurring for the first time. It is interesting to note that some NIDS allow the user to define his own set of attack signatures, thereby making the functioning of the NIDS more customizable to meet network needs [8].

Alternatively, if a NIDS uses an anomaly based detection technique it generally watches for irregular behaviour by inspecting network connections, content of packet header and payload for malicious content or violation of protocols. Hence, it is fully capable of detecting attacks that have not previously occurred.

For best efficiency, a NIDS that utilizes both signature based and anomaly based detection techniques are employed.

The merits of a Network Intrusion Detection System are as follows [8].

- Reduced management overhead
  Unlike a HIDS, a NIDS is deployed at strategic locations in the network. Hence, the installation of operating system dependent and system configuration dependent software (like a HIDS) in every host is overcome. The greatly plummets the installation and maintenance overhead.
- Operating System Independent
  Since a NIDS is not installed on individual hosts of the network, it is unaffected by the type of operating system running on the individual host. A NIDS listens to attacks irrespective of the destination OS type of the traffic.
- Easier deployment
  Since they are not deployed on individual hosts of the network, the deployment is simplified.
- Detects network based attacks that a HIDS cannot
  One of the ways a NIDS detects an attack is by examining the packet header and packet payload for malicious content. Hence, it is capable of detecting several IP-based denial of service attacks like TCP SYN attack and fragmented packet attack which can be identified only by inspecting the headers and contents of the packets at

real time as they traverse the network. This kind of attack would go unnoticed by a HIDS, which is confined to an individual host.

- Real time intrusion detection and accelerated counteractive response

  Network based IDS examines live network traffic and it performs real time intrusion detection. This makes it nearly impossible for the attacker to remove any evidence of his attack. Also, it detects illicit activity as it occurs on the network. Sometimes, a NIDS can be configured to stop the attack before it reaches the host system and compromises it. On the contrary, a HIDS can detect attacks only after the intruder makes some changes to the system files. By this time, critical systems would have already been compromised to a considerable extent.
- Operating system independent

  Since it is deployed on locations of the network and not the individual hosts, it remains of the type of operating system running on the host. Thus, it becomes portable.

The demerits of Network Intrusion Detection System are as follows [8].

- Scalability

  In high paced network environments, a NIDS finds it difficult to inspect every passing packet.
- Reduced accuracy in detection of attacks

  Since a NIDS detects attacks real time, it generates a large number of false positives.
- Inability to furnish detailed information about an attack

  It cannot provide detailed information about an attack as it employs real time intrusion detection.
- TCP Stream Reassembly/IP Defragmentation

  Special attention has to be paid to attacks involving TCP/IP packets. In a TCP/IP connection, the target has to track incoming packets and recorder them as per the packet sequence numbers is case they arrive out of order. There occur several attacks that intend to “bemuse” the stream assembly of packets. A classic example is the teardrop attack – it resorts to the use of malformed packets to incite buffer overflows. The ultimate danger occurs as - the first packet doesn’t appear distinguishably disparate from an ordinary data packet, so the IDS fails to instantly detect the attack. Sometimes, depending upon the operating system, a single bad packet is sufficient to crash the IDS. The failure of an IDS leads to most NIDS failing open. This enables an intruder to access the entire network after successfully compromising the IDS.
- Incompatible with switched and encrypted environments

  A NIDS cannot scan the protocols or the packet contents if network traffic is encrypted. Also, in switched networks, the monitoring of network traffic is made difficult due to the network isolating properties of a switch. A switch acts to isolate connections between hosts, thereby allowing the IDS to inspect traffic that is explicitly addressed to it. In such instances, the NIDS is reduced to monitoring a single host (like a HIDS), defeating much of its intent. To alleviate this problem, the number of NIDS deployed in a network should be increased significantly.

### *B. Based on Behaviour after an Attack*

Based upon the behaviour after an attack, an IDS can be classified into the following two types [9].

*1) Active Response Intrusion Detection System:* An active response IDS is configured to automatically take counteractive action in response to an intrusion, without requiring any form of intervention by the administrator. Hence, an active response IDS is said to be “proactive” in response.

Some of the types of counteractive action taken by an active response IDS include - resetting the connection, reprogramming of the firewall to block network traffic from the suspected harmful source, gathering more information about the attack as well as the attacker by increasing the sensitivity level of the IDS, blocking the source address of the attacker, restarting of a server or a service, resetting of the TCP sessions, closing of all ports and connections, if an attack is detected from a specific IP address, the IDS may be programmed to automatically rewrite the rules of the network's firewall in order to ensure that future traffic from the attacking IP address is denied, another less commonly employed response that is not advisable from a legal perspective is retaliation – attacking the attacker in turn.

Since an active response IDS is capable of detecting and preventing an attack, it is also termed as Intrusion Detection and Prevention System (IDPS).

*3) Passive Response Intrusion Detection System:* A passive response IDS is configured detect a latent security breach and issue an alert to the administrator. The administrator has to respond to the alarm and take appropriate corrective action. The corrective action may either be halt the attack or try to determine the intruder. Passive response IDS may utilize pagers, cell phones, email, SNMP trap messages or simply a message box on the administrator’s PC to convey intrusion notifications. Since it in incapable of executing a counteractive action without the intervention of the administrator, it is said to be merely “reactive in response” and can be termed as Intrusion Detection System (IDS).

## VI. COMPONENTS OF AN INTRUSION DETECTION SYSTEM

There are three basic components of an IDS – Sensor (Activity or packet capture engine, Behavioural or signature detection engine), Backend (Event recording database, Alerting engine) and the Frontend (User interface, Command & control).

A sensor forms the primary component of an IDS for detecting intrusions on a computer or in a network. It houses a packet capture or an activity capture engine to perform detection activities. It can employ the signature based or anomaly based intrusion detection techniques [10].

The backend of the IDS is concerned with logging of events detected by the sensors. Additionally, it performs the function of alerting. The backend can alert the administrator in multiple ways – logging events in the database, sending an e-mail, block a connection, reset a TCP connection, and display the alert on the administrator's console. Apart from these two functions, the backend also enables IDS setup and configuration of storage [10].

The frontend forms the IDS's direct user interface. The user can view events that the sensor has detected, configure the IDS, update the signature database and behavioural detection engine [10].

## VII. WORKING OF AN INTRUSION DETECTION SYSTEM

The components of an IDS work in structured co-ordination with each other to alert the administrator of an intrusion [10].

### *A. Sensor - Detect and Report*

It has two interfaces – the capture network interface and the management network interface. As the sensor listens to network traffic by tapping into the network, the capture interface passes on all the captured data into a buffer. The detection engine then examines the buffer contents and executes network protocol analysis. Signature based and anomaly based intrusion detection also happen here [10].

### *B. Backend - Collect and Alert*

The backend is also termed as the nub of an IDS. The events detected by the sensor are recorded in the event repository database. The backend then determines how each event has to be responded to. E-mails, displays, blocking are used to respond to critical events. The non-significant ones are simply logged [10].

### *C. Frontend- Command and Control*

The IDS can be setup, configured and updated from the frontend by the user. All events collected by the backend are presented by the frontend. Thus, the frontend furnishes a convenient interface through which the user can now manage these logged events.

It is not uncommon for an IDS to get extremely event-noisy. That is, it may report an overabundance of events, causing the user to get complacent and ignore a few of them. To derive maximum benefit from an IDS, it has to be fine-tuned to report only significant events. Hence, the user can fine-tune the detection and response of an IDS through this console. If done accurately, the IDS will provide the user with a sufficiently early warning from any intrusion [10].

## VIII. CONCLUSION

The inclusion of IDS into the security infrastructure of an organization is needed. There has been a considerable increase in awareness of computer security threats and its implications in industries. There is a heavy demand for security products to safeguard resources from the industry. Vendors (such as Sourcefire and ISS) in response to these demands are working to make the future IDS, firewalls, and routers to be able to seamlessly interoperate with each other. Having firewall and router functionality incorporated with the IDS will provide extreme flexibility to secure a network. Aligning all devices to transport logs to a database that can incorporate the formats into one that is viewable to the IDS management console will aid in correlating alerts. In fact, Cisco was the first company to release into the market the Cisco SA500 Series Security Appliances that can provide a firewall, VPN, wireless, email and web threat protections and an intrusion prevention system (IPS) all in a single device.

## ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Mrs Sanjeetha. R, Assistant Professor of Computer Science Department of M.S.Ramaiah Institute of Technology, for giving me the much needed encouragement to translate my in-depth research into a survey paper.

## REFERENCES

[1] Ajith Abraham and Mario Koeppen, *Hybrid Information Systems*, 1st ed., Ed. New York, USA: Springer-Verlag, 2002.

[2] (2002) The Wikipedia website. [Online]. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system.

[3] Kevin Grey. (2014) [Online]. Available: http://blog.envisionitsolutions.com/test-your-knowledge-8-common-misconceptions-about-cyber-security.

[4] Ajay Yadav. (2013) [Online]. Available: http://resources.infosecinstitute.com/network-design-firewall-idsips.

[5] Aparna Bhadran. (2014) [Online]. Available: http://www.slideshare.net/aparnacbhadran/intrusion-detection-system-32609044.

[6] Przemyslaw Kazienko & Piotr Dorosz. (2004) [Online]. Available: http://www.slideshare.net/aparnacbhadran/intrusion-detection-system-32609044.

[7] Wikipedia. (2004) [Online]. Available: https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system.

[8] Sans Institute Infosec Reading Room, "Intrusion Detection Systems: Definition, Need and Challenges", 2001.

[9] Vangie Beal. (2005) [Online]. Available: http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp.

[10] J. Forlanda. (2010) [Online]. Available: http://www.brighthub.com/computing/smb-security/articles/65416.aspx.

[11] Wikipedia. (2002) [Online]. Available: https://en.wikipedia.org/wiki/Audit_trail.