Intrusion Detection And Prevention System: A Comparative Study

Madhuri Gokhale
Assistant Professor, Dept of Computer Science and Engineering
Jabalpur Engineering College, Jabalpur, Madhya Pradesh

Abstract- *An intrusion Detection System (IDS) is a defensive-aggressive system to protect the information, verifying and responding to occurring attacks on computer systems and networks. It provides an overview of the state of the art in intrusion detection research. Intrusion detection systems are software and/or hardware components that monitor computer systems and analyze events occurring in them for signs of intrusions. Due to the widespread diversity and complexity of computer infrastructures, it is difficult to provide a completely secure computer system. Therefore, there are numerous security systems and intrusion detection systems that address different aspects of computer security. It provides a taxonomy of IDS, along with brief descriptions. Second, a common architecture of intrusion detection prevention systems.*

Keywords- Intrusion detection system (IDS), Intrusion prevention system, security alert, network security.

I. INTRODUCTION

An intrusion detection system (IDS) monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusive events to computer networks are expanding because of the liking of adopting the internet and local area networks be more and more exposed to attack, due to its widespread network connec- tivity. Intrusion Detection Systems (IDS) are primarily focused on identifying probable incidents, monitoring information, trying to stop it, and reporting them to security administrators in a real-time environment, and those that exercise audit data with some delay (non-real-time). An IDS provides around-the- clock network observation and is an additional wall to secure the network.

Intrusion is to violate the security policy of a system. Any kind of malicious activity that attempts to collect, disrupt, an assault on system security that derives from an intelligent threat [1]. An attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroying, or mali- ciously controlling a computing infrastructure; or destroying the integrity of the data or stealing controlled information. The different types of intrusion are as follows:

(i) Password-Based Intrusion: A common denominator of most operating system and network security plans is password-based access control. Your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. If the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time [2]. After gaining access to your network with a valid account, an attacker can do any of the following: Modify server and network configurations, including access controls and routing tables. Modify, reroute, or delete your data.

(ii) Denial-of-Service Intrusion: It is performed on computer or network by valid users. After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion [3].
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services [4]

(iii) Man-in-the-Middle Intrusion: As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently [2]. For example, the at- tacker can re-route a data exchange. When computers are communicating at low levels of the network layer might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assum- ing your identity in order to read your message.

(iv) Compromised-Key Intrusion: A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attackers can and try to use the compromised key to compute additional keys, which might allow the attacker access to data.

(v) Sniffer Intrusion: A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not en- crypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key. Using a sniffer, an attacker can do any of the following: Analyze your network and gain IDS information to eventually cause your network.

II. INTRUSION DETECTION SYSTEM (IDS)

An intrusion-detection system acquires information about an information system to perform a diagnosis on the security status of the latter [5], [6]. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities. An intrusion detection system (IDS) monitors network or system activities for malicious activities or policy violations and produces reports to a management station. These systems are primarily focused on identifying probable incidents, monitor- ing information about them, and tries to stop them.

A. IDS vs. Firewall

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communi- cations, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system and is another form of an application layer firewall [7], [3].

B. Classification of IDS

IDS can be classified by where detection takes place (net- work or host) and the detection method that is employed.

(a) Signature Based IDS: A signature-based IDS monitor’s packets in the network and compares them with pre-configured and pre-determined attack patterns known as signatures. When a new attack is recognized experts or programs have to identify typical patterns in such attacks, which can be made into the signature. Since this process takes time, there will be a lag between the new threat discovered and the signature being applied in IDS for detecting the threat. During this lag time, your IDS will be unable to identify the threat. To reduce further lag, security software using such signatures should be updated as frequently as feasible.

(b) Anomaly Based IDS: Anomaly-based IDSs detect incidents, which show a typical behavior profile or violate thresholds based on statistical analysis. Examples of this are possible masquerade attacks, which are detected in this way, or penetrations of the security control system. Other possible scenarios leakage or denial of service attacks, which are detected by the typical use of sys- tem resources. Other problems include malicious use. It records what sort of bandwidth is generally used, what kind of protocols are used, which ports and devices generally connect, and alert the administrator or user when traffic is detected which is anomalous (not normal).

(c) Host Based IDS: Host-based intrusion detection (HIDS) refers to intrusion detection that takes place on a single host system. The data is collected from an individual host system. By using common hashing tools, file timestamps, system logs, and monitors system calls and the local network interface gives the agent insight into the present state of the local unauthorized change or activity is a host. If there is any detected, it alerts the user by a pop- up, security constraints, or use of special privileges.

(d) Network-Based IDS: A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats where the data is traffic across the network. A NIDS tries to detect malicious activities such as denial-of-service (Dos) attacks, port scans, and monitoring the network traffic attacks. NIDS includes several sensors to monitors packet traffic, one or more servers for NIDS management functions, and one or more management relieves for the human interface NIDS examines the traffic packet by packet in real-time, or near to real-time, for attempting to detect intrusion patterns.

C. Advantages of IDS

- Visibility: An IDS provides a clear view of what’s going on within your network. It is a valuable source of information about suspicious or malicious network traffic. There are a few practical to an IDS that allow you to track network traffic in depth.
- Defense: An IDS adds a layer of defense to your security profile, providing a useful backstop to some of

your other security measures. Properly configured IDS can produce data that can form the basis for a civil or criminal case against someone who misuses your network.

- Response capability: Although they probably will be of limited use, you may want to enable some of the response features of the IDS. For instance, they can be configured to terminate a user session that violates policy. You must consider the risks of taking this step, since you may accidentally terminate a valid user session.
- Tracking of virus propagation: When a virus first hits your network, an IDS can tell you which machines is compromised, as well as how it is propagating through the network to infect other machines. This can be a great help in slowing or stopping a virus's progress and making sure you remove it.

D. Limitations of IDS

- False alarm rate: It is not uncommon for the number of real attacks to be far below the number of false alarms. The number of real attacks is often so far below the number of false-alarms that the real attacks are often missed and ignored [8].
- Lag Time: For signature-based IDS there will be a lag between a new threat discovery and its signature being applied to the IDS. During this lag time, the IDS will be unable to identify the threat. It cannot compensate for weak identification and authentication mechanisms or weaknesses in network protocols
- Does not protect from encryption: Encrypted packets are not processed by the intrusion detection software. Therefore, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred [2]. Intrusion detection software provides information based on the network address that is associated with the IP packet that is sent into the network.

III. INTRUSION PREVENTION SYSTEM (IPS)

Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. IDPs have become a necessary addition to the secu- rity infrastructure of nearly every organization [8]. Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it [9]. Intrusion preven- tion 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 can actively prevent or block intrusions that are detected [10]. An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted trans- port and network layer options.

A. Classification of IPS

Intrusion prevention systems can be classified into four different types:

(i) Network-based IPS (NIPS): It monitors the entire network for suspicious traffic by analyzing protocol activity network-based intrusion prevention system (NIPS) is a system used to monitor a network as well as protect the confidentiality, integrity, and availability of a network. Its main functions include protecting the network from threats, such as a denial of service (DOS) and unautho- rized usage. The NIPS monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity [3]. In other words, the NIPS becomes like a prison for hostile traffic such as Trojans, worms, viruses, and polymorphic threats.

(ii) Wireless IPS (WIPS): It monitors a wireless network for suspicious traffic by analyzing wireless networking proto- cols. A wireless intrusion prevention system (WIPS) is a dedicated security device or integrated software applica- tion that monitors a wireless LAN network's radio spec- trum for rogue access points and other wireless threats. A WIPS compares the MAC addresses of all wireless access points on a network against the known signatures of pre-authorized, known wireless access points and alerts an administrator when a discrepancy is found [10], [11]. To circumvent MAC address spoofing, some higher-end WIPS can analyze the unique radio frequency signatures that wireless devices generate and block unknown radio fingerprints.

(iii) Network behavior analysis (NBA): It 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.Network behavior analysis (NBA) is a network monitoring program that ensures the security of a proprietary network [7]. Network behavior analysis monitors the inside happenings of an active network by collecting data from many data points and devices [4].A network behavior analysis program must reduce the labor and time expended by network administrators in detecting and resolving network issues. It is thus an enhancement to protect the network along with firewalls, antivirus software, and spyware detection tools.

(iv) Host-based IPS (HIPS): It is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host. A host-based intrusion prevention system (HIPS) is a system or a program employed to protect critical computer systems containing crucial data against viruses and other Internet malware. Starting from the network layer up to the application layer, HIPS protects from known and unknown malicious attacks [2]. HIPS regularly checks the characteristics of a single host and the various events that occur within the host for suspicious activities.HIPS can be implemented on various types of machines, in- cluding servers, workstations, and computers. HIPS uses a database of system objects monitored to identify intru- sions by analyzing system calls, application logs, and file-system modifications binaries, password files, capability databases, and access control lists) [2].

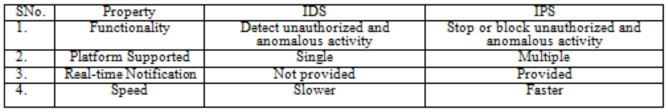
B. Advantages of IPS

- The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack.
- Protect host after decryption: HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in decrypted form [3].
- Operating system independent: A network-based monitoring system has the benefit of easily seeing attacks that are occurring across the entire network. Furthermore, because the monitoring system is examining only traffic from the network, it does not have to support every type of operating system that is used on the network [7].

C. Limitations of IPS

- Does not provide a complete network picture: Because IPS examines information only at the local host level, IPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network [10].
- IPS has a requirement to support multiple operating systems: IPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network [10].

TABLE I
COMPARISON OF IDS AND IPS



SNo.	Property	IDS	IPS
1.	Functionality	Detect unauthorized and anomalous activity	Stop or block unauthorized and anomalous activity
2.	Platform Supported	Single	Multiple
3.	Real-time Notification	Not provided	Provided
4.	Speed	Slower	Faster

- The host is visible to attackers: In IPS during an attack, the host is visible to attackers. It becomes more difficult to place network IPS at a single location in the network and successfully capture all the traffic [10].

IV. DETECTION METHODS

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

(a) Signature-Based Detection: Signature-based IDS monitor packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures. Examples of this are possible masquerade attacks, which are detected in this way, or penetrations of the security control system. Other possible scenarios leakage or denial of service attacks, which are detected by atypical use of system resources.

(b) Statistical anomaly-based detection: An IDS which is an anomaly-based will monitor network traffic and compare it against an established baseline. The baseline will iden- tify what is ”normal” for that network – what sort of bandwidth is generally used, what protocols are used that it may raise a False Positive alarm for legitimate use of bandwidth if the baselines are not intelligently configured [3].

(c) Stateful Protocol Analysis Detection: This method identi- fies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity. The program also checks and accounts for a change in bandwidth and protocol being used during communication. A network behav- ior analysis program must reduce the labor and time expended by network administrators in detecting and resolving network issues.

V. COMPARISON OF IDS AND IPS

The main difference between IDS and IPS is the action that they take when an attack is detected in its initial phases that are network scanning and port scanning. The difference is given in table I.

When you are using IDS instead of IPS, you are in what is called Promiscuous Mode. Your IDS system is working with a copy of packets that are attempting to enter the network segment being protected. To prevent the attack perhaps the device will drop packets or reset TCP connections [9]. The IPS device can perform a variety of actions to try and ensure your network is safe. When you are using IPS instead of IDS, you are in what is called Inline Mode. An Intrusion Prevention System (IPS) can detect the attack, notify the administrators, and also attempt attempting to enter the protected segment. It is not working with a copy of the packets, but instead, it is working with the very packets themselves. Here we are providing a comparative study of Intrusion detection systems and intrusion prevention systems that helps us in understanding which one is better to protect our system from attacks and intrusion [4].

VII. CONCLUSION

Intrusion detection currently attracts considerable interest from both the research community and commercial compa- nies. Research prototypes continue to appear, and commercial products based on early research are now available. In this paper, we have discussed different types of intrusion detection and prevention systems. And how they contribute to securing our data in computer networking. It supports the security of an organization against threats and attacks. The purpose of the classification of intrusion detection and prevention systems is to get a better idea about every class of it. We have different techniques to protect our system from intrusion but the attacker always tries to find new techniques to hack our system or network resource that is why IDS and IPS are of great importance. A lot of work can be done in this field to develop more enhanced and efficient network security systems.

REFERENCES

[1] Cuppens, A. Miege, Alert correlation in a cooperative intrusion detection framework, in: Proceedings 2002 IEEE symposium on security and privacy, IEEE, 2002, pp. 202–215.

[2] Fuchsberger, Intrusion detection systems and intrusion prevention systems, Information Security Technical Report 10 (3) (2005) 134–139.

[3] Ossec, Ossec - world’s most widely used intrusion detection system (2017). URL https://www.ossec.net/

[4] P. security, Panda security - a watch guard brand (2017). URL http://www.pandasecurity.com

[5] U. Bashir, M. Chachoo, Intrusion detection and prevention system: Chal- lenges & opportunities, in: 2014 International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2014, pp. 806–809.

[6] U. A. Sandhu, S. Haider, S. Naseer, O. U. Ateeb, A survey of intrusion detection & prevention techniques, in: 2011 International Conference on Information Communication and Management, IPCSIT, Vol. 16, 2011, pp. 66–71.

[7] M. Beigh, M. Peer, Intrusion detection and prevention system: Classification and quick (2011).

[8] Y. Kumar, S. Dhawan, A review on information flow in intrusion detection system, International Journal of Computational Engineering and Management 15 (1) (2012) 91–96.

[9] K. Levitt, Intrusion detection: current capabilities and future directions, in: 18th Annual Computer Security Applications Conference, 2002. Proceedings., IEEE, 2002, pp. 365–367.

[10] K. Scarfone, P. Mell, Guide to intrusion detection and prevention systems (idps), NIST special publication 800 (2007) (2007) 94.

[11] M. Garuba, C. Liu, D. Fraites, Intrusion techniques: Comparative study of network intrusion detection systems, in: Fifth International Conference on Information Technology: New Generations (itng 2008), IEEE, 2008, pp. 592–598.