ISSN:0975-9646

Intrusion Detection

[#]B.KiranKumar, [#]A.Kamala priya,[*]R.Vishnumurthy, [*]Thillai Nayagi
[#]*Pydah College of Engineering & Technology, Visakhapatnam, A.P*
[*]*BVC college of Engineering, Rajahmundry, A.P*

ABSTRACT-*Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. An IPS is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.*

Keywords: DMZ, OSSEC, SNORT, SSL.

1. INTRODUCTION

Although intrusion detection technology is immature and should not be considered as a complete defence, but at the same time it can play a significant role in overall security architecture. If an organization chooses to deploy an IDS, a range of commercial and public domain products are available that offer varying deployment costs and potential to be effective. Because any deployment will incur ongoing operation and maintenance costs, the organization should consider the full IDS life cycle before making its choice. When an IDS is properly deployed, it can provide warnings indicating that a system is under attack, even if the system is not vulnerable to the specific attack. These warnings can help users alter their installation's defensive posture to increase resistance to attack. In addition, an IDS can serve to confirm secure configuration and operation of other security mechanisms such as firewalls. Within its limitations, it is useful as one portion of a defensive posture, but should not be relied upon as a sole means of protection. As e-commerce sites become attractive targets and the emphasis turns from break-ins to denials of service, the situation will likely worsen.

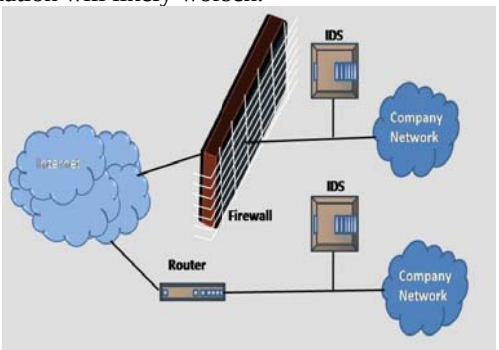
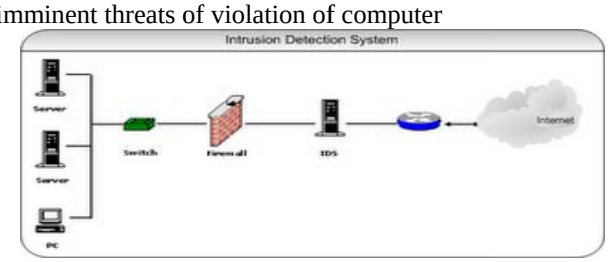


Fig1: Typical locations for an intrusion detection system

Successful IDSs can recognize both intrusions and denial-of-service activities and invoke countermeasures against them in real time. To realize this potential, we'll need more accurate detection and reduced false-alarm rates. In this paper we go through different intrusion detection systems and how to overcome drawbacks in these system by useing DIDS.

Intrusion detection system

An IDS is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer



security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.IDPSs have become a necessary addition to the security infrastructure of nearly every organization.IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content. An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. We'll cover each of these briefly.

Technologies used NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic; however doing so might create a bottleneck that would impair the overall speed of the network. In a network-based intrusion-detection system (NIDS), the sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic. It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected. In a host-based system, the sensor usually consists of a software agent, which monitors all activity of the host on which it is installed, including file system, logs and the kernel. Some application-based IDS are also part of this category. It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state. An example of a HIDS is OSSEC.

Wireless

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyse network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Many previous NIDS tools will include enhancements to support wireless traffic analysis.

2. DETECTION TYPES

Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signature or attributes from known malicious threats. This is similar to the way most antivirus software detects mal-ware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network-what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Passive IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

ReactiveIDS

Reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user.

Limitations

Network intrusion Detection system

NIDS analyze traffic traversing network segments at the network layer. At that level, attacks can be observed when it may be difficult if only observing at an application level. However, there may be traffic passing within the network that may not be fully visible to the NIDS. This happens especially when secure encrypted tunnels and VPNs are deployed. Unless it knows how to decrypt and re-encrypt data, such traffic remains fully opaque to the NIDS. Secure sockets layer (SSL) traffic over hypertext transfer protocol secure *(HTTPS)* connections can be used by attackers to mask intrusions. Another limitation to NIDS manifests as bandwidth rates increase in a network. Especially when the amount of traffic also increases, it becomes a challenge for NIDS to be able to keep up with the rate of traffic and analyze data quickly and sufficiently.Finally, in a large network with many paths of communication, intrusions can bypass NIDS sensors.

Signature-Based Detection

A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first. New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.

Challenges with Wireless Technologies

Wireless technologies are becoming increasingly ubiquitous in modern networks; however, this new technolology comes with its own set of challenges. Wireless networks are inherently ‘open’ and viewable by all network scanners. There are no physical barriers between data sent through the air. As such, it is relatively easy to intercept data packets in a wireless network. One of the challenges with wireless is that the new technology comes with its own set of protocols for communication that break the traditional OSI layer model IDS must learn new communication patterns. Also, as open as wireless communication is, devices on such networks rely on established trust relationships between identified systems; however, if one system is already compromised before rejoining a network; it may be difficult for the IDS to detect intrusive activity from a trusted source.

The Need for Multiple IDPS Technologies

To overcome the above mentioned limitations we are going to use Multiple IDPS and DIDS.In many environments, a robust IDPS solution cannot be achieved without using

multiple types of IDPS technologies. For example, network-based IDPSs cannot monitor wireless protocols, and wireless IDPSs cannot monitor application protocol activity. Table 1 provides a high-level comparison of the four primary IDPS technology types.

Comparison of IDPSgy Types IDPS Technology Type	*Types of Malicious Activity Detected*	*Scope per Sensor or Agent*	*Strengths*
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

Table-1

Distributed Intrusion Detection System

Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS's. The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network. The information gathered by these distributed components is transported to, and analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis. This approach is unique among current IDS's. The components of DIDS are the *DIDS director*, a single *host monitor* per host and a single *LAN monitor* for each broadcast LAN segment in the monitored network. A distributed IDS (dIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. By having these co-operative agents distributed across a network, incident analysts, network operations and security personnel are able to get a broader view of what is occurring on their network as a whole.

3. CONCLUSION

In this paper we go through different intrusion detection systems, there advantages and there limitations. To overcome the drawbacks in each of these IDS we are going for integration of different IDS or distributed intrusion detection system. The DIDS uses different components to detect intruders; this approach is unique and quite effective.

ACKNOWLEDGEMENTS

Thanks to my Principal prof.R.P.Das for his guidance and Chairman of our college Pydah Krishna Prasad extended his support in publishing this paper.

REFERENCES

[1]Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.

[2]Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988

[3]Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET 2003

[4]Revision by Tzeyoung Max Wu Information Assurance Technology Analysis Center (IATAC) CONTRACT NUMBER SPO700-98-D-4002 Information Assurance Tools Report – Intrusion Detection Systems. Sixth Edition.

[5]Winkeler, J.R., "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," The Thirteenth National Computer Security Conference, Washington, DC, pages 115–124, 1990

[6]Snapp, Steven R, Brentano, James, Dias, Gihan V., Goan, Terrance L., Heberlein, L. Todd, Ho, Che-Lin, Levitt, Karl N., Mukherjee, Biswanath, Smaha, Stephen E., Grance, Tim, Teal, Daniel M. and Mansur, Doug, "DIDS (Distributed Intrusion Detection System) -- Motivation, Architecture, and An Early Prototype," The 14th National Computer Security Conference, October, 1991, pages 167–176.

[7]Jackson, Kathleen, DuBois, David H., and Stallings, Cathy A., "A Phased Approach to Network Intrusion Detection," 14th National Computing Security Conference, 1991

[8]Distributed Intrusion Detection System, http://www.dshield.com/

ABOUT AUTHORS

Mr.B.kiran kumar working as an Asst.prof in Pydah College of engineering and tech Vishakhapatnam. He completed is Master Degree in Information Technology from Gitam University. He has a good teaching experience and having a good knowledge on Information Security.

Miss A.KamalaPriya working as an Asst.prof in Pydah college of Engineering. She completed her Masters in CSE from Andhra University. She has good teaching experience and has profound knowledge on computer Subjects.

Mr.R.VishnuMurthy working as Asst.Prof in BVC college of engg, Rajahamundry.He completed his M.tech in Information Technology from Gitam University. He has good teaching experience and good knowledge in Computer Subjects.

S.Thillai Nayagi working as an Asst.Prof in Sanketika College of engg &tech, Vishakhapatnam.