IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-2, Issue-4 E-ISSN: 2347-2693

# Comparative Study of Intrusion Detection System

Mahak Chowdhary[1], Shrutika Suri[2] and Mansi Bhutani[3*]

*CSE, AP, MRIU, India*

Received: 09/03/2014 Revised: 17/03/2014 Accepted: 15/04/201x4 Published: 30/04/2014

***Abstract-*** In past few decades, there has been rapid progress in internet based technology and application areas for computer networks have emerged. But number of attacks on network has increased dramatically due to which interest of researchers in the network intrusion detection has also increased. Intrusion detection is a type of security management system for computers and networks. An intrusion detection system gathers and analyzes information from various areas within computer or network to identify possible security breaches, which include both intrusion and misuse. Intrusion detection system also helps in detecting anomalies in network traffic. Intrusion Detection system follows a two-step process. The first procedures are host-based and are considered the passive component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the active component: mechanisms are set in place to reenact known methods of attack and to record system responses. Aim of this research paper is to review current trends in intrusion detection system and analyze current problems that exist in this area. Some key features, attacks detected by different types of IDs are explained in this paper.

***Keywords :*** Detection Methods , Intrusion Detection , Types Of Attacks, Mechanism

## I. INTRODUCTION

Increased dependability of our everyday life on network based technology and reliable operation of network based systems has become necessarily important. New application areas for computer network have also emerged. At the same time, wide spread progress in the Local Area Network (LAN) and Wide Area Network (WAN) application areas in business, financial, industry, security and healthcare sectors made us more dependent on the computer networks. All of these application areas made the network an attractive target for the abuse and a big vulnerability for the community.

Consequently, there has been a simultaneous increase in the number of attacks on networks, resulting in an increasing interest in network intrusion detection among the researchers. The threat of a new wave of cyber or network attacks is not just a probability that should be considered, but it is an accepted fact that can occur at any time. In addition to the hacking, new entities like worms, Trojans and viruses introduced more panic into the networked society. As the current situation is relatively weak network defenses, our ever growing dependency on them thus can have devastating consequences. Securing an important infrastructure thus has become the priority one research area for many researchers.

An Intrusion Detection System (IDS) is a device or a software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection systems constantly monitor a given computer network for invasion or abnormal activity. The advantage of this service is the "round-the-clock" aspect, in that the system is protected even while the user is asleep or otherwise away from any computer hooked up to the network. Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. It is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic.

Intrusion Detection Systems (IDS), though a new field of research, has attracted significant attention towards itself and presently almost every day more researchers are engaged in this field of work. The current trend for the IDS is to make it possible to detect novel network attacks. The major concern is to make sure that in case of an intrusion attempt, the system is able to detect and to report it. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

## II. ATTACKS DETECTED BY DIFFERENT TYPES OF INTRUSION DETECTION SYSTEM

*Scanning Attack:* Scanning attacks can be used to assimilate information about the system being attacked. Using scanning techniques, the attacker can gain topology

Corresponding Author: *Manshi Bhutani*
*Department of CSE, AP, MRIU, India*

 

information, types of network traffic allowed through a firewall, active hosts on a network, OS and kernel of hosts on a network, server software running, version numbers of software, etc... Using this information, the attacker may launch attacks aimed at more specific exploits. The above was gathered by launching a stealth SYN scan. This scan is called stealth because it never actually completes TCP connections. This technique is often referred to as half open scanning, because the attacker does not open a full TCP connection. The attacker sends a SYN packet, as though you he were opening up a real TCP connection. If the attacker receives a SYN/ACK, this indicates the port is listening. If no response is received, the attacker may assume that the port is closed [3]

*Denial of Service Attack:* There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.[2]
*Penetration Attack:* Penetration attacks contain all attacks which give the unauthorized attacker the ability to gain access to system resources, privileges, or data. One common way for this to happen is by exploiting a software flaw. This attack would be considered a penetration attack. Being able to arbitrarily execute code as root easily gives an attacker to whatever system resource imaginable. In addition, this could allow the user to launch other types of attack on this system, or even attack other systems from the compromised system.[2]

*B. DIFFERENT PROTOCOL ATTACKS*

*ICMP:* ICMP is used by the IP layer to send one-way informational messages to a host. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets.There are a few types of attacks that are associated with ICMP shown as follows:
*ICMP DOS Attack:* Attacker could use either the ICMP "Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection. An attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating hosts. Their connection will then be broken. The ICMP redirect message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host. [2]
*Ping of death:* An attacker sends an ICMP echo request packet that's larger than the maximum IP packet size. Since the received ICMP echo request packet is larger than the normal IP packet size, it's fragmented. The target can't reassemble the packets, so the OS crashes or reboots.

*ICMP nuke attack:* Nukes send a packet of information that the target OS can't handle, which causes the system to crash.

*ICMP PING flood attack:* A broadcast storm of pings overwhelms the target system so it can't respond to legitimate traffic.

*ARP:* ARP maps any network level address (such as IP Address to its corresponding data link address. Some ARP attack are given below:

*ARP flooding*
Processing ARP packets consumes system resources. Generally, the size of an ARP table is restricted to guarantee sufficient system memory and searching efficiency. An attacker may send a large number of forged ARP packets with various sender IP addresses to cause an overflow of the ARP table on the victim. Then the victim cannot add valid ARP entries and thus fails to communicate .An attacker may also send a large number of packets with irresolvable destination IP addresses. When the victim keeps trying to resolve the destination IP addresses to forward packets, its CPU will be exhausted.

*User spoofing:* An attacker may send a forged ARP packet containing a false IP-to-MAC address binding to a gateway or a host. The forged ARP packet sent from Host A deceives the gateway into adding a false IP-to-MAC address binding of Host B. After that, normal communications between the gateway and Host B are interrupting.
In DoS attack target hosts are denied from communicating with each other, or with the Internet. Connection Hijacking and Interception Packet interception is the act in which client can be victimized into getting their connection manipulated in a way that it is possible to take complete control aver .

UDP: UDP uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagram may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.Some UDP attacks are describe below :

UDP flood attack**:** Similar to ICMP flood attack, UDP flood attack sends a large number of UDP messages to the target in a short time, so that the target gets too busy to transmit the normal network data packets.
*Fraggle* - A fraggle attack is similar to a smurfing attack with the exception that the User Datagram Protocol (UDP) is used instead of ICMP.
*Teardrop* - A teardrop type of DoS attack The attack works by sending messages fragmented into multiple UDP

packages. Ordinarily the operating system is able to reassemble the packets into a complete message by referencing data in each UDP packet. The teardrop attack works by corrupting the offset data in the UDP packets making it impossible for the system to rebuild the original packets. On systems that are unable to handle this corruption a crash is the most likely outcome of a teardrop attack.

## III. MECHANISM OF INTRUSION DETECTION

*Stack-Based:* Stack based intrusion detection system is the latest technology which works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.

*Signature-Based/PatternMatching-Based:* Signature based intrusion detection system use a rule set to identify the intrusions by watching for patterns of the events specific to known and documented attacks. It is typically connected to a large database which houses attack signatures. It compares the information it gathers against those attack signatures to detect a match.

*Anomaly-Based:* Anomaly Based Intrusion Detection System examines ongoing traffic, activity, transactions and behaviour in order to identify intrusions by detecting anomalies.

*Hybrid-Based:* Hybrid based intrusion detection is the combination of stack, signature, anomaly based detection. Because of the difficulties with the anomaly based and signature based detections, a hybrid model is being developed. Much research is now focussing on this hybrid model.

## IV. KEY FEATURES OF INSTRUSION DETECTION SYSTEM

- Key feature of intrusion detection system is ability to provide a view of unusual activity and issue alerts notifying administrators and/or a block suspected connection.
- Prevent intrusion with firewall, network port security, systrace (process jail).
- Simulation software.
- Monitoring data, security logs or action on network.
- Analyze to ascertain whether it is an attack.
- Detect attack or intruder using some scheme.
- Report Intrusion to system Administrator.
- Act on or defend computer system and possibly repel the attack.

A. Host-Based Instrusion Detection

- Specific and have more detailed signatures.
- They can reduce false positive rates.
- They can determine whether or not an alarm may impact that specific system.
- They are application specific.
- Operates in encrypted environment.
- Detects local attacks before they hit the network.
- Powerful tool for analysing a possible attack because of relevant information in database .
- Require no additional hardware.
- Better for detecting attacks from inside and detect attacks that network-based IDS would miss.

B. Network-Based Intrusion Detection

- Can get information quickly without any reconfiguration of computers or need to redirect logging mechanism.
- Does not affect network or data resources.
- Monitor or detects in real time network attacks or misuses.
- Does not create system overhead.
- Broad in scope.
- Examines packet headers and entire packet.
- No overload.
- Lower cost of ownership.
- Better for detecting attacks from outside and detect attacks that host-based Intrusion detection would miss.

## V. CONCLUSION AND FUTURE SCOPE

An intrusion detection system is a crucial part of the defensive operations that complements the static defenses such as firewalls. Essentially, intrusion detection systems search for signs of an attack and flag when an intrusion is detected. In some cases they may take an action to stop the attack by closing the connection or report the incident for further analysis by network administrators. According to the detection methodology, intrusion detection systems are typically categorized as misuse detection and anomaly detection systems. From a deployment perspective, they are be classified as network based or host based although such distinction is coming to an end in today's intrusion detection systems where information is collected from both network and host resources. In terms of performance, an intrusion detection system becomes more accurate as it detects more attacks and raises fewer false alarms. Future advances in IDS are likely to continue to integrate more information from multiple sources (sensor fusion) whilst making further use of artificial intelligence to minimize the size of log files necessary to support signature databases. Human intervention, however, is certainly necessary and set to continue for the foreseeable future.

## VI. ACKNOWLEDGEMENT

We express our deep thanks to Dr. S.S. TYAGI, Head of Department (CSE) for warm hospitality and affection towards us. We thank the anonymous referees for their reviews that significantly improved the presentation of this paper.
We are thankful to Ms. "Shrutika Suri" for their variable advice and support extended to us without which we could not has been able to complete our paper. Words cannot express our gratitude for all those people who helped us directly or indirectly in our endeavour. We take this

  

opportunity to express our sincere thanks to all staff members of CSE department of MRIU for the valuable suggestion.

## VII. REFERENCES

[1] N. Puketza, K. Zhang, M. Chung, B. Mukherjee and R. A. Olsson "A methodology for testing intrusion detection systems," *Proc. IEEE Transactions on Software Engineering*, vol. 22, pp. 719 -729, 1996.

[2] Amrita Anand and Brijesh Patel, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", *Proc. Ijarcsse* Volume2, August2012, pp.310-325.

[3] J. R. Winkler and W. J. Page"Intrusion and Anomaly Detection in Trusted Systems," *Proc. Fifth Annual Computer Security Applications Conference*, 1989.

[4] D. E. Denning "An intrusion-detection model," *IEEE Trans. on Software Engg.*, vol. SE-13, pp.222 -232 1987

[5] F. Cuppens and A. Miege, "Alert Correlation in a Cooperative Intrusion Detection Framework," *Proc. IEEE Symp. Security and Privacy,* pp. 202-215, May 2002.

[6] R. Durst, T. Champion, B. Witten, E. Miller and L. Spagnuolo, "Addendum to Testing and Evaluating Computer Intrusion Detection Systems," *Proc. Comm. ACM,* vol. 42, no. 9, p. 15, Sept. 1999.

[7] R. Lippmann, D. Fried, I. Graf, J. Haines, K. Kendall, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunningham and M. Zissman, "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation," *Proc. DARPA Information Survivability Conf. and Exposition,* vol. 2, pp. 12-26, Jan. 2000.

[8] Karmore, Preetee K.; Bodkhe, Sonali T, "A Survey on Intrusion in Ad Hoc Networks and its Detection Measures," *Proc. International Journal on Computer Science & Engineering*, 2011, vol. 3, Issue 5, pp. 1896-1903.

***Authors Profile***

Mahak Chowdhary persuing B. Tech. in CSE at Manav Rachna International University, Faridabad(India).

Mansi Bhutani persuing B. Tech. in CSE at Manav Rachna International University, Faridabad(India).

  