ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Review on Intrusion Detection System

RafatRana S.H. Rizvi[1]
Computer Science and Engineering
H.V.P.M's C.O.E.T
Amravati, India

Ranjit R. Keole[2]
Professor
Information Technology
H.V.P.M's C.O.E.T
Amravati, India

Abstract: ***One of most important existent issues in information security application domain is Intrusion Detection System (IDS); IDS is a defensive-aggressive system to protect information, verifying and responding to occurring attacks on computer systems and networks. This paper provides the 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 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. This paper first provides taxonomy of IDS, along with brief descriptions Second, a common architecture of intrusion detection systems and their basic characteristics are presented. Third, working of intrusion detection systems based on four phases is provided. Finally, intrusion prevention systems are classified according to each of these categories.***

Keywords: Intrusion Detection System, Signature-Based IDS, Anomaly-Based IDS, Host Based IDS, Network IDS.

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 and new automated hacking tools and strategy. Computer systems are evolving to be more and more exposed to attack, due to its wide spread network connectivity.Intrusion Detection Systems (IDS) are primarily focused on identifying probable incidents, monitoring information about them, tries to stop them, and reporting them to security administrators in 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.

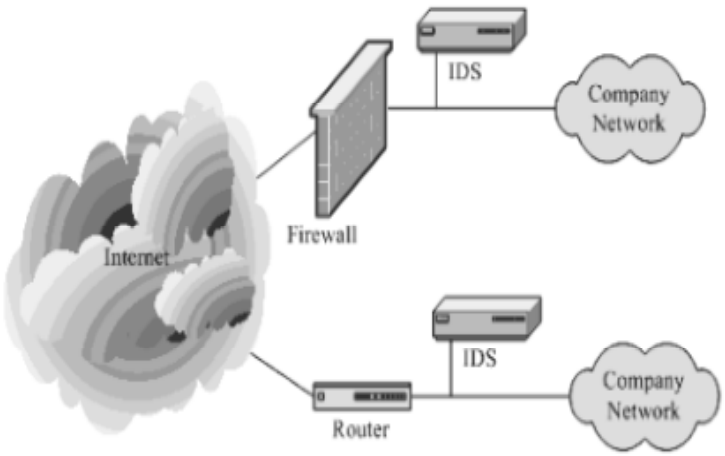


Fig :- IDS

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. Literature Review And Related Work

Several people have reviewed the state of the art James Anderson, 1980 showed that audit records could be used to identify computer misuse and to identify threat classifications, and it offered suggestions to improve auditing of systems to identify misuse. Dr. Dorothy Denning,1986 presents the first intrusion detection model, which has six main components: subjects, objects, audit records, profiles, anomaly records, and activity rules. Haystack, 1988 introduces a combined anomaly detection/misuse detection IDS that models individual users as well as groups of users. Marcus J. Ranum, 1990 presents commercial IDS called Network Flight Recorder (NFR). Sundaram, A., 1996 describes recent developments in conventional intrusion detection: Distributed, modular system which includes both anomaly and misuse detection. Bai, Y., And Kobayashi, H, 2003 presented a survey on major challenges to ID technology Eduardo Mosqueira- Rey et al, 2007 described the design of misuse detection agent which is one of the different agents in a multiagent-based intrusion detection system. Magnus Almgren, Ulf Lindqvist, and Erland Jonsson, 2008 designed a theoretical model for the reason about thealerts from the different sensors through concentrating on the web server attacks.Naeimeh Laleh and Mohammad Abdollahi Azgomi, 2009 propose a new taxonomy and complete review for the different types of fraud and data mining techniques of fraud detection..Yurong Xu, James Ford, and Fillia Makedon, 2010 introduces a distributed wormhole detection algorithm called Wormhole Geographic Distributed Detection (WGDD) that is based on detecting network disorder caused by the existence of a wormhole.

III. Intruder Detection System

An intrusion-detection system acquires information about an information system to perform a diagnosis on the security status of the latter. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. A typical intrusion-detection system is shown in Figure

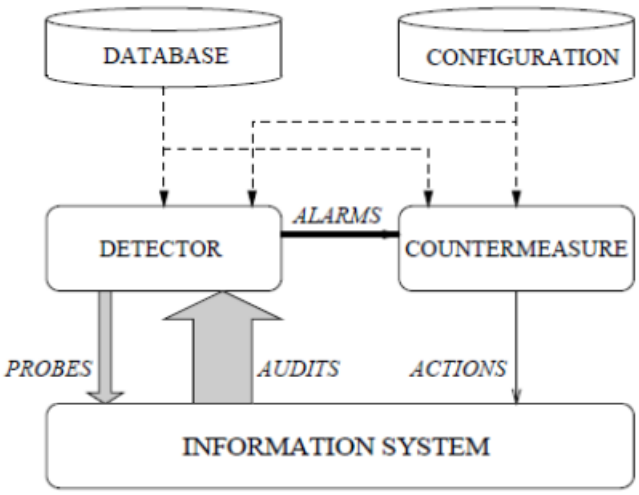


Fig: Very simple intrusion-detection system

An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system to be protected. This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications. It uses three kinds of information: long-term information related to the technique used to detect intrusions (a knowledge base of attacks, for example), configuration information about the current state of the system, and audit information describing the events that are happening on the system.

The role of the detector is to eliminate unneeded information from the audit trail. It then presents either a synthetic view of the security-related actions taken during normal usage of the system, or a synthetic view of the current security state of the system. A decision is then taken to evaluate the probability that these actions or this state can be considered as symptoms of an intrusion or vulnerabilities. A countermeasure component can then take corrective action to either prevent the actions from being executed or change the state of the system back to a secure state.

IV. Working Phases of Intrusion Analysis

Intrusion analysis process is very important for the networks and the system sand can be broadly broken into four phases and the phases are as follows

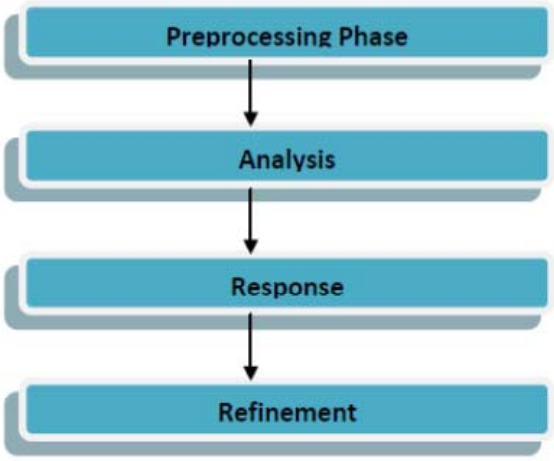


Fig 1: Phases of IDS

a) Preprocessing

It is the first phase of the Intrusion detection system. It collects the activity from an IDs or IPS sensors. In this step, data are organized in some pattern for classification. This stage would help in determine the format the data are put into, which would be a canonical format or a structured database. Once the data are formatted they are further classified, this classifications depends upon the analysis schemas being used.

b) Analysis

After prepocessing, the data record is compared with the Knowledge base. The data record will either be logged as an intrusion event or it will be dropped and next data record is analyzed.

c) Response

In the IDS we get the information passively after the fact, so we would get an alert after the fact. The response can be set to be automatically performed, or can be done manually after someone manually analyzed the situation.

d) Refinement

At this stage fine tunings is done, based on the previous usage and detected intrusions. This helps in reducing false positive levels and to have more security tool. These are tool like CTR (Cisco Threat Response) that helps with the refining stage by

actually making sure that an alert is valid by checking whether you are vulnerable to the attack or not. Rule based detection, even known as signature detection, pattern matching and misuse detection.

V. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

In order to discuss IDS properly it is necessary to distinguish between the different IDS. Therefore the classification of ID systems is very important.

a) Signature-Based IDS

A signature based IDS monitor's packets in the network and compares with preconfigured and predetermined 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 signature. Since this process takes time, there will be a lag between the new threat discovered and signature being applied in IDS for detecting the threat. During this lag time your IDS will be unable to identify the threat.[9]To reduce further lag, security software using such signatures should be updated as frequently as feasible.

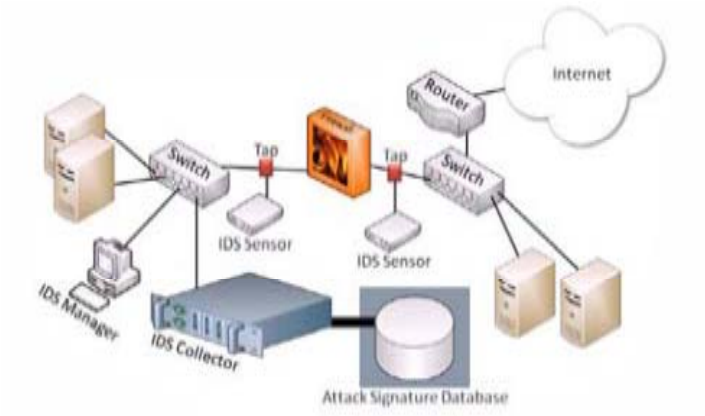


Fig : Signature Based Intrusion Detection System

b) Anomaly-Based Intrusion Detection System:

Anomaly-based IDSs detect incidents, which show atypical behavior profiles or violate thresholds based on statistical analysis. Examples for this are possible masquerade attacks, which are detected in this way or penetrations of the security control system. Another possible scenarios leakage or denial of service attacks, which are detected by atypical use of system resources. Other problems include malicious use, violations of security constraints, or use of special privileges.[8]Therefore, a statistical anomaly-based IDSs determines normal network activity. It records what sort of bandwidth is generally used, what kind of protocols are used, which ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous (not normal).[8] This could include to compare certain traffic indicator value against a threshold, based on their historically determined standard deviation.

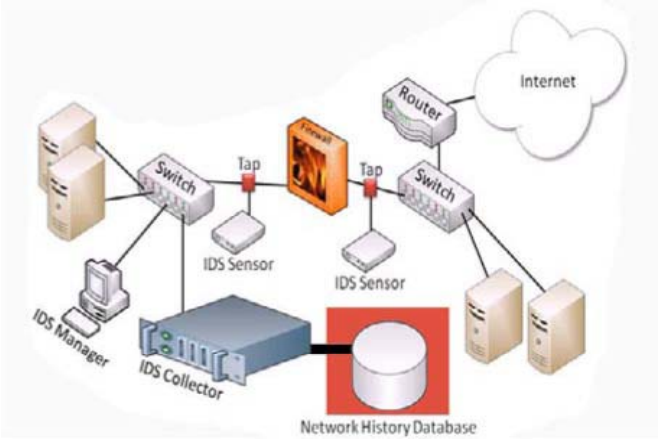


Fig : Example for Statistical Anomaly-based IDS

c) Host Based Intrusion Detection System:

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. The HIDS agent monitors activities such as integrity of system, application action, file changes, host based network traffic, and system logs. By using common hashing tools, file timestamps, system logs, and monitors system calls and the local network interface gives the agent insight to the present state of the local host. If there is any unauthorized change or activity is detected, it alerts the user by a pop-up, it alerts the central management server, blocks the activity, or a combination of the above three. The decision should be based on the policy that is installed on the local system. These host-based procedures are considered the passive component.

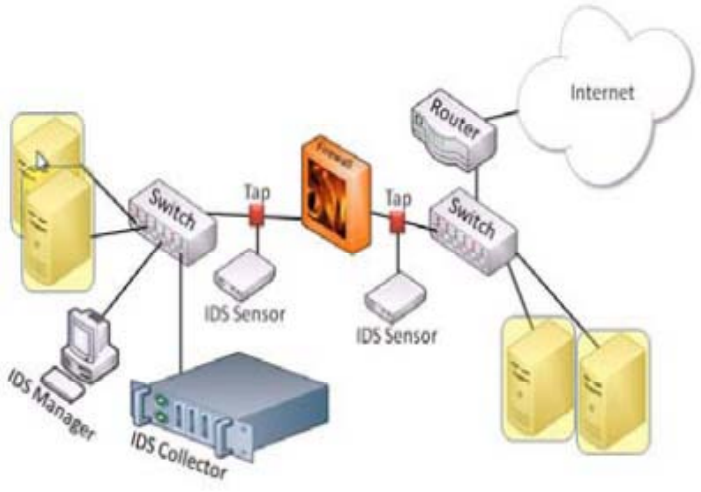


Fig : Host based Intrusion detection system

d) Network Intrusion Detection Systems

A network-based intrusion detection system (NIDS) is used to monitor and analyse 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 a number of sensors to monitors packet traffic, one or more than 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. The analysis of traffic patterns to detect intrusions may be done at the sensors, at the management servers, or combination of the both. These network-based procedures are considered the ***active*** component.

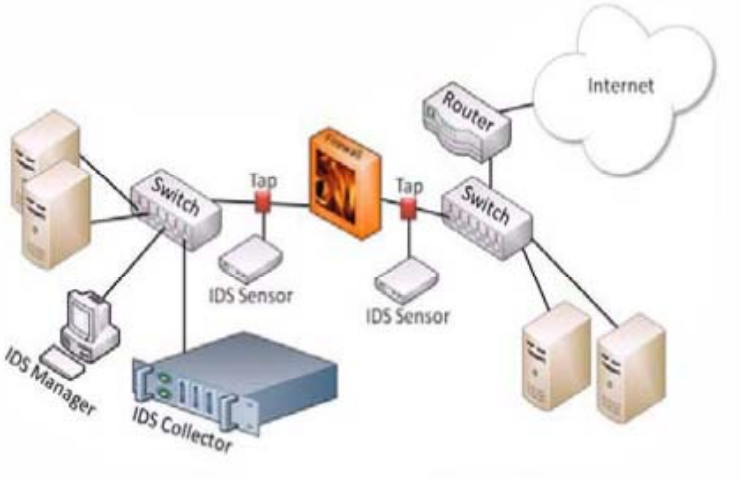


Fig :Network Intrusion Detection System

VI. Intrusion Prevention Systems

Intrusion Prevention Systems (IPSs) also known as Intrusion Detection and Prevention Systems (IDPSs), are network security applications, that monitor and change network and system activities if found suspicious. The main functions of IPSs are, as explained to identify malicious activity, log information about it, and attempt to block or stop and report that activity. Since they are not in the focus of this report, it is necessary to note here, that they are important parts of network security and strongly related to intrusion detection. IPSs can be considered extensions of IDSs. The main differences that should be figured out between them are, that IDPs are placed in-line and are able to actively prevent or block intrusions that are detected. [11][12] To be a little bit more precise it can be declared, that IPSs can take such actions as sending an alarm, dropping the malicious packets, resetting the connection or blocking the traffic from the offending IP address. [13] This might also include other actions like changing or reconfiguring firewall rules. Additional tasks of an IPS are correcting "Cyclic Redundancy Check (CRC) errors, un-fragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options" [10] [13]. For that they are using several response techniques, which involve the IDPS stopping the attack itself.

a) CLASSIFICATIONS OF IDPS

Intrusion Prevention Systems can be classified into four different types

1.Network Based Intrusion Prevention System (NIPS) :-It analysis the traffic of entire network by analyzing protocol activities and take appropriate actions.

2. Wireless Intrusion Prevention System (WIPS) :- This type of IDPS analysis the traffic of Wireless network by analyzing protocol activities and take appropriate actions.

3. Network Behavior Analysis (NBA) :- Network Behavior Analysis examines traffic to identify threats that generate unusual traffic flow, such as DDOS attack, malware and Policy Violation.

4. Host Based Intrusion Prevention (HIPS) :- This type of IDPS monitors single host for suspicious activity by analyzing events occurring within that host .

VII. Conclusion

Intrusion detection currently attracts considerable interest from both the research community and commercial companies. Research prototypes continue to appear, and commercial products based on early research are now available. In this paper, we have discussed different groups of intrusion detection and prevention system to support the security of an organization against threats and attacks.

Some of research topics are as following:

» Presenting some strategies to eliminating the designed defects and preventing from intruders' attack techniques;

» Introducing some methods to tracking intruders and reacting against impersonation (identity forge);

» Presenting the used traffic encryption techniques by intruders;

» Presenting some techniques to detecting attacks of encrypted traffic;

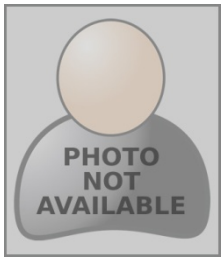
Acknowledgment

My thanks to the Guide, Prof. R.R.Keole and Principal Dr.A.B.Marathe, who provided me constructive and positive feedback during the preparation of this paper.

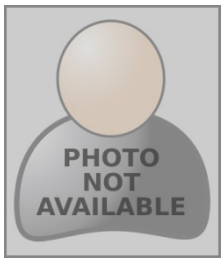
References

1. Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.
2. Garuba, M., Liu, C. & Fraites, D. (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE, 2008
3. Peter Scarf one, Karen; Mell. Guide to intrusion detection and prevention systems (idps).Computer Security Resource Center (National Institute of Standards and Technology), January 2010.
4. Andreas Fuchsberger,"Intrusion Detection Systems and Intrusion Prevention Systems "Information Security Technical Report Elsevier (2005) 10, 134-139.
5. Yogesh Kumar and Swati Dhawan,A REVIEW ON INFORMATION FLOW IN INTRUSION DETECTION SYSTEM, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 1, January 2012ISSN (Online): 2230-7893 p 91-96
6. Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]
7. Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
8. Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference

AUTHOR(S) PROFILE



RafatRana S.H. Rizvi, received the B.E.degree in Computer Science and Engineering from H.V.P.M's College Of Engineering And Technology, Amravati in 2014. She is currently persuing Master's Degree in Computer Science and Engineering from H.V.P.M's College of Engineering And Technology, Amravati.



Prof. Ranjit R.Keole, received the B.E.and M.E degree in Computer Science from Prof. Ram Megha Institute of Technology, Badnera in 1992 and 2008, respectively. His field of specialisation is web Mining. He is currently working as Associate Professor at H.V.P.M's college of Engineering and Technology,Amravati.

