Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.482 – 485

A Review of Intrusion Detection System Basic Concepts

Ms. Rohini A. Naphade, Ms. Pooja D. Raut, (B.E. Final Year CSE student, AEC Chikhli)
Prof. Abhay A Dande, Asst. Professor (CSE Department, AEC Chikhli)

poojadraut21@gmail.com, rohininaphade06@gmail.com, dandeabhay@gmail.com

Abstract--- Intrusion detection on the internet is a most interesting in computer science today, where much work has been done in the last two decades and still it has a great scope. To have sound understanding of the intrusion detection system concepts, the basic related terms need to be clearly understood. The paper here mainly has its focus on the terminologies used in intrusion detection system and its general architecture. The paper mainly deals with architecture definition of the Intrusion Detection System

Keywords: Intrusion, Intruder, Intrusion Detection System, Security Policy, Vulnerability

I. INTRODUCTION

An intrusion is defined as any set of unauthorized actions that tries to create security threat to the integrity, confidentiality, or availability of resources of the system. It can be defined as the potential possibility of a careful unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable from its security point of view.

An intrusion detection system (IDS) inspects all inside and outside network activities and identifies suspicious traffic patterns that may indicate a network or system attack from someone attempting to compromise a security system. An intrusion detection system attempts to detect these intrusions. In case of, network intrusion detection

systems (NIDS), the primary source of data to be analyzed is network traffic while a host intrusion detection system (HIDS) depends on information collected on individual hosts. Host-based IDS utilizes various collected audit data of the target host machine. It has an advantage that the information provided by the audit data can be helpful to draw the right conclusions about possible intrusion. Network-based IDS makes use of the IP package information collected by network hardware such as switches and routers.

II. BASIC TERMS

Attack: It is defined as action conducted by one opponent, the intruder, against another the victim system. The intruder carries out an attack with a specific defined objective in mind. It is a set of one or more events that may have one or more security consequences over the system. An attack is a mechanism to fulfill its defined objective for an intruder.

Intrusion: It is a similar word for the "attack". It is also called as successful attack.

Intruder: Intruder is a person who does an attack. Attacker is a common word for intruder.
Incident: Data representing one or more related attacks are collectively called as Incident.
True Positive: It is known as an authentic attack which triggers IDS to produce an alarm.
True Negative: It is when no attack has taken place and no alarm is raised.
False negative: It is an event that the IDS fail to detect as an intrusion when one has in fact occurred in reality.
False positive: It is an event, wrongly detected by the IDS as being an intrusion when no intrusion has occurred in reality.
Confidence value: It is defined as a value an organization puts on an IDS based on previous performance and analysis to determine its ability to effectively identify future attack.
Alarm filtering: The process of categorizing attack alerts produced from IDS in order to distinguish false positives from actual attacks is called as alarm filtering.
Burglar Alert/Alarm: It is a signal suggesting that a system has been or is being attacked
Detection Rate: The detection rate is defined as the number of intrusion instances detected by the system divided by the total number of intrusion instances present in the test set.
Vulnerability: A feature or a combination of features of a system that allows an intruder to place the system in unsafe state and increases the probability of undesirable activities in security of the system.
Exploit: It is the process of using a vulnerability to violate a security policy.
Trust: The degree of the confidence in which the system behaves as expected well as IDS is called as trust. Threat: A threat is any event with the potential to harm any essential element of the system.
Site policy: These are instruction sets about the rules and configurations of IDS of an organization.
Site policy awareness: It is defined as IDS's ability to dynamically upgrade its rules and configurations in response to changing environmental activity to give the best results.

Security Policy: A security policy deals with the procedures or models necessary to ensure the security requirements.

III. General architecture of intrusion detection system.

In general any intrusion detection system consists of the following components. These interact with each other via suitable input and output communication messages in order to collect, store, process, analyze the data and then to draw the conclusions.. These components perform the following functions.

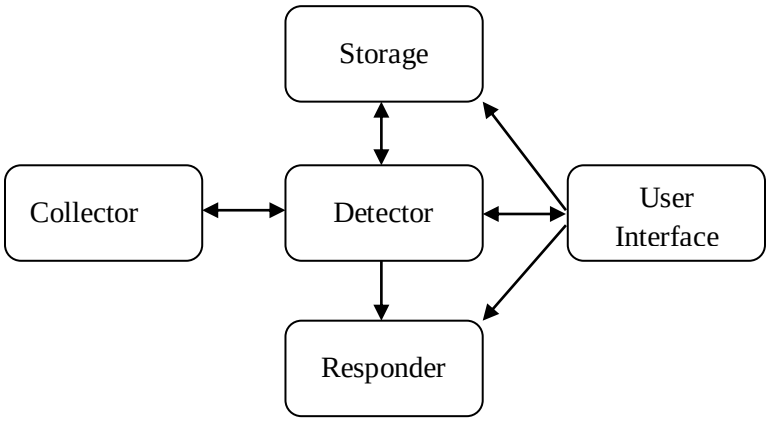

Fig: General components of an Intrusion Detection System

Collector: It provides an interface for accessing data that is used by the detection process. Network tap is most widely used as data collector. It provides access to all raw network packets which cross a particular position of a network. Interfaces to host-based data or external databases are also used as collectors.

Detector: It carries out the actual detection process. It acts as a core part of the. It accesses data provided by collector and storage and it decides what should be triggered as an alert.

User Interface: It is used for reporting results to the user, and enables the user to control the IDS. It has the simultaneous access to storage, detector and responder.

Storage: It stores persistent data required by the detector or the user interface. Such data is either derived by the detector itself or can be provided externally. Storage controls the database system.

Responder: It reacts to detected intrusions in order to prevent future damage to the security of the system. A response can be triggered automatically or manually via the user interface.

IV. CONCLUSION

The paper here mainly discussed the basic terminologies of the Intrusion Detection system. It also gave a brief outline about the general architecture of the basic intrusion system. It can act a well informative document of the beginners who are trying to get hands on the concept of Intrusion Detection. As a future scope of this paper the

various methods that are available for intrusion detection can be discussed with their comparative performance analysis.

REFERENCES

[1] J.P. Anderson, *"Computer Security Threat Monitoring and Surveillance"* Tech. report, 1980.
[2] Karen Scarfone , Peter Mell, *" Guide to Intrusion Detection and Prevention Systems (IDPS)",* National Institute of Standards and Technology,2007.
[3] Paul Helman, Gunar Liepins, and Wynette Richards, Foundations of intrusion detection, in Proceedings of the Fifth Computer Security Foundations Workshop, Franconic, NH, June 1992
[4] Jan Vykopal*, "Security Analysis of a Computer Network",* Masaryk University Brno, master thesis, 2008.
[5] Charlie Kaufman and Mike Speciner; Network Security; Private Communication in a PublicWorld, 2nd Edition, Prentice Hall of India
[6] William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4th Edition, 2011.
[7] *"Understanding Intrusion Detection System",* Internet, sans institute, 2001.
[8] Corinne Lawrence *"IPS – The Future of Intrusion Detection"* University of Auckland October 2004.
[9] Karthikeyan .K.R and A. Indra- *"Intrusion Detection Tools and Techniques a Survey"*
[10] Prof. S. Gore – *"Importance of Intrusion Detection System"*-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.

