ORIGINAL RESEARCH PAPER | Computer Science | Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

"Analyzing different types of Intrusion Detection System for e-commerce portal"

KEYWORDS: e-commerce, intrusion detection system.

Poonam Patel
SDJ International College, Surat.

Dr. Kamaljeet Lakhtariya
Department of Computer Science Gujarat University, Ahmedabad.

ABSTRACT

E-Commerce is basically trading in product or services using computer network such as the internet. With the invention of the World Wide Web in 1989, the mere idea of electronic commerce, which takes place through internet, has been transformed into reality. With the rapid development of e-commerce, the security of the transaction is the core and key issues of the development of e-commerce. Therefore e-commerce providers can instigate various security protocols to reduce the risk of attacks. Implementation of various security protocols and practicing of encryption, authentication, and confidentiality will minimize the risk in security. Here in this paper we have discussed the overview of E- Commerce, security issues in ecommerce, threats in e-commerce, key dimensions of ecommerce security, various security protocols. Summary: E-commerce is defined as the buying and selling of products or services over electronic systems. Any secure e-commerce system must meet four integral requirements privacy, integrity, authentication and non-repudiation. This security can be achieved to some extended by applying different Intrusion Detection technique for different circumstances.

I. INTRODUCTION

We human beings are quickly adopting changes in our day to day life. These days we people prefer to go online for buying and selling of goods or services. For availing these facility web is getting bigger and bigger, coming with new and needed goods and services online for their customers. For doing online trading we need to exchange our personal and confidential information online. The most common method of payment for online purchase is credit card. In developed countries and also in developing countries to some extent, credit card is most acceptable payment mode for online and offline transaction. As usage of credit card increases worldwide, chances of attacker to steal credit card details and then, make fraud transaction are also increasing.

These days with increase in online trading, malicious transactions has also increased. Getting open access to internet, computer systems data is at risk. For the protection of such confidential data over internet we need Intrusion Detection System.

II. INTRUSION DETECTION SYSTEM

An intrusion can be defined as "an act of a person of proxy attempting to break into or Misuse a system in violation of an established policy". And intrusion detection system is a system use to detect intrusion. IDS can be a software and/or hardware System for monitoring and detecting data traffic or might be user behavior to identify attempts of illegitimate accessing system manipulation through a network by malware and/or intruders. [1].

The goal of intrusion detection is to monitor the network assets to detect anomalous behavior and misuse in network [2]. Intrusion detection concept was introduced in early 1980's after the evolution of internet with surveillance end monitoring the threat [3]. There was a sudden rise in reputation and incorporation in security infrastructure. Since then, several events in IDS technology have advanced intrusion detection to its current state [2]. James Anderson's wrote a paper for a government organization and imported an approach that audit trails contained important information that could be valuable in tracking misuse and understanding of user behavior [2].

Then the detection appeared and audit data and its importance led to terrific improvements in the subsystems of every operating system [2]. IDS and Host Based Intrusion Detection System (HIDS) were first defined. In 1983, SRI International and Dorothy Denning began working on a government project that launched a new effort into intrusion detection system development [3]. Around 1990s the revenues are generated and intrusion detection market has been raised. Real secure is an intrusion detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection and purchased the Wheel Group for attaining the security solutions [3]. The government actions like Federal Intrusion Detection Networks (FID Net) were designed under Presidential Decision Directive 63 is also adding impulse to the IDS [3].

III. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion Detection System can be classified in many ways. This classification is done on Host, Network and Application based IDS.

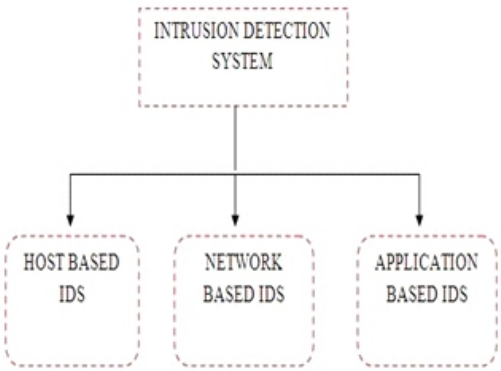

Figure : Classification of IDS

Host based IDS views the sign of intrusion in the local system. For analysis they use host system's logging and other information. Host based handler is referred as sensor. Other sources, from which a host-based sensor can obtain data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms [4]. Host based system trust strongly on audit trail. The information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction [5].

Network based IDS systems collect information from the network itself rather than from each separate host [6]. The NIDS audits the network attacks while packets moving across the network. The network sensors come equipped with attack signatures that are rules on what will constitute an attack and most network-based systems allow advanced users to define their own signatures [6]. Attack on the

Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

sensor is based on signature and they are from the previous attacks and the operation of the monitors will be transparent to the users and this is also significant [7].

Application based IDS (APIDS) will check the effective behavior and event of the protocol [8]. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices [8]. Intentional attacks are the malignant attacks carried out by disgruntled employees to cause harm to the organization and Unintentional attacks causes financial damage to the organization by deleting the important data file [8].

IV. INTRUSION DETECTION TECHNIQUE

There are many intrusion detection techniques has implemented to protect computer systems from network attacks which are increasing now and then. These techniques differ in way of working, their implementation, and many more factors. However these techniques just help to detect intrusion in network, prevention will be carried out when we will have reliable intrusion detection system. [9] The fundamentals of various techniques used to detect intrusions are described below.

Anomaly based Intrusion Detection: Anomaly is indicated as an outlier, peculiarities or exceptions are the data pattern which performs abnormally. Anomaly detection technique is designed to uncover the patterns that are far from the normal and others are flagged as an intrusion [8]. Anomaly detections are categorized into static and dynamic detectors.

Cognition based Detection Technique: Cognition-Based (also called knowledge-based or expert systems) Detection Techniques work on the audit data [15].The set of predefined rules for the classes and attributes are identified from training dataset [15].

a) Boosted Decision Tree or Boosted Tree (BT): It uses ADA Boost (adaptive boosting) algorithm to generate many Decision Trees classifiers trained by different sample which is implemented in IDS [15].

b) Support Vector Machine (SVM): SVM is defined to be the classifiers which are designed for the binary classification. Decision tree based SVM is a techniques which merges the two techniques to solve the problem in an efficient way. The training and testing time can be decreased by using this method.

Signature based Detection Technique: Signature based intrusion detection is termed as misuse detection. Here, the dataset has number of instances and every data must be labeled as normal or intrusive. The machine learning algorithms are used to train the data set according to their label. This technique automatically retains the signature to detect the intruder. Misuse detection technique is created automatically and the works are more complicated and accurate than manually done [10]. Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities [10].

Target Monitoring: Target monitoring is a technique which is used to report if any changes or modifications happen in the system. This is usually done through cryptographic algorithm which computes a crypto checksum for each targeted file [11].If any changes happens in crypto checksum they are reported by IDS. Tripwire checksum is an integrity checker which checks for the changes or modification in the files.

Stealth Probes: A stealth probe is a technique used to collect and associates the data. It tries to find the attacks which has taken long period of time. Attackers will check for the system errors over a period of month, and wait for another two months to launch the attacks and they take a wide-area sampling and attempt to discover any correlating attacks [8].

V. CONCLUSION

The main objective of this research paper is to provide an overview of the necessity and utility of intrusion detection system. This research paper gives complete study about types of IDS and different Intrusion Detection Techniques. IDS are becoming essential for today security in corporate world and for network users.

ACKNOWELDGEMENT

The Author is thankful to Prof. (Dr.) Kamaljeet Lakhtaria for his encouragement, helpful suggestions and supervision throughout the course of this work.

REFERENCES

[1] Khattab M. Alheeti, "Intrusion Detection System and Artificial Intelligent".
[2] Anderson, Ross. 2001a. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons.
[3] Anderson, Ross. 2001b. Why Information Security is Hard - An Economic Perspective.
[4] Adams, Anne, and Martina Angela Sasse. 1999. Users Are Not the Enemy. Communications of the ACM, 42 (12) : 40-46.
[5] Adams, C., and S. Farrell. 1999. Internet X.509 Public Key Infrastructure certificate management protocols. Internet RFC 2510.
[6] Anderson, Ross, and M. Kuhn. 1996. Tamper Resistance - A Cautionary Note. Proceedings of the Second USENIX Workshop on Electronic Commerce : 1-11.
[7] Anderson, Ross, and M. Kuhn. 1997. Low Cost Attacks on Tamper-resistant Devices.
[8] "SANS penetration testing copyright by SANS"-Copyright SANS Institute Author Retains Full Rights.
[9] PeymanKabiri, Ali A. Ghorbani, "Research on Intrusion Detection and Response: A Survey". International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005.
[10] A SENGUPTA, C MAZUMDAR "e-Commerce security – A life cycle approach" Sadhana Vol. 30, Parts 2 & 3, April/June 2005
[11] Abdulghader.A.Ahmed.Moftah. "CHALLENGES OF SECURITY,
[12] Asmaa Shaker Ashoor, Prof. Sharad Gore – "Importance of Intrusion Detection System"-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.
[13] Bace, Rebecca-"An Introduction to Intrusion Detection &Assessment"- Infidel, Inc. for ICSA, Inc.
[14] Bernard, H. Russell. 2000. Social Research Methods: Qualitative and Quantitative Approaches. Newbury Park, CA: Sage.