Xournals

Academic Journal of Information Security

ISSN UA | Volume 01 | Issue 01 | May-2018

Detection techniques for Intrusion Detection System (IDS)

Rohit Gaharwal[1], Pawan Kumar[1] and Umakant Dwivedi[1]

Available online at: www.xournals.com

Received 18th January 2017 | Revised 15th February 2018 | Accepted 19th March 2018

Abstract:

A device or software that monitor or identify the network for malicious or unauthorized activities is called as Intrusion Detection System (IDS). An intrusion attempt may be stopped by some systems but this is neither expected nor required of monitoring system. The recognizing possible events, cataloging information about them and reporting attempts are contents that is focused by the Intrusion Detection and Prevention systems (IDPS). Intrusion Detection systems detects any of unauthorized or misuse access by monitoring the network and computer resources and it is essentially an attack on these resources. Consumers should be concern from malicious attack which is increase tremendous and known that how to protect and communicate the digital information in safe manner. For getting valuable information, hackers use altered types of attacks which is detected by many intrusion detection techniques, algorithms and methods. In this paper, discussed about the intrusion detection system, its classification or types, its detection techniques that are frequently used.

Keywords: *Intrusion Detection System, malicious attack, hackers*

Authors:

1. *Department of Information Technology, Bharat Institute of Technology, Meerut, Uttar Pradesh Technical University, INDIA*

Introduction

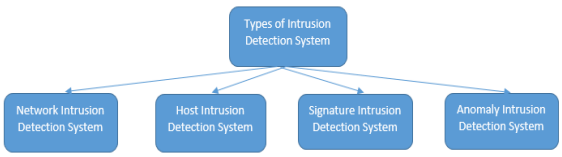
The term intrusion is refer as an malicious entry to another's property or region but these activities are used to compromise the basic computer networks security goals in term of computer science which is confidentiality, integrity and privacy. Computer system or network resources examining the process of events which is analyzing them for indication of intrusion and probable incidents that causes extortions to security measures is called detection of intrusion. It is mainly caused by intruders or attackers, who want to gain unauthorized and additional access to particular network or system for their own resolutions.

Intrusion Detection System is an application that are used for protecting it from intruder and monitoring the network. With internet based technology, it is rapid progress with new application regions for computer system that have occurred. It is software and hardware which focuses and recognizes the probable incidents that caused by attackers, tries to dismiss them, monitors information about those intrusions and produces a report for security managers in real-time environment. It is consider as security operation that complements protection such as firewalls (it is a network security device that monitors the incoming and outgoing network traffic). Intrusion detection system contain many IDS tools that will store a detected incidents in a record form or will combine events with other data which make decisions regarding to policies or damage control. IDS contain some key functionalities that is as follows:

- Recording information relating to observed events.
- Notifying administrators of important observed events.
- Producing reports

Types of Intrusion Detection System

IDS is classified into different ways, the major classifications are Network Intrusion Detection systems (NIDS), Host Intrusion detection system (HIDS), signature based intrusion detection system and anomaly based intrusion detection system.



Network-based Intrusion Detection system (NIDS)

NIDS include network intrusion detection abilities that are standalone hardware appliances. On strategic point, they are mostly arranged in network infrastructure such as at a boundary between systems, remote access servers, virtual private network servers, and wireless networks. This type of network are traffic network which is going through specific network segments or devices. NIDS are detect known attacks or illegal activities or analyze network and application protocol activity to identify anomalous and suspicious activity by scanning which can capture and analyze data. It is also referred to as "packet-sniffers" because it collect and captures the data in the form of internet packets that is passing through communication mediums. It contains some advantages:

- Ownership has lower cost
- Its easily deploy
- Based attacks are detect network
- Retaining evidence
- Quick response and real-time detection
- Failed attacks has been detected

Host-based Intrusion Detection System (HIDS)

For any malicious activity, the characteristics of a single host are monitored and the events of that host are observed in this detection system. They can monitor network traffic, processes, operations performed by applications, logs, file system and modification and any configuration change in this system. On critical hosts, placement of HIDS is usually done and these critical host includes servers or systems that are publicly accessible and have some sensitive information. Where data is collected from different resources there they are placed on one server and workstation and machine analyze the data locally. It contain some advantages:

- The success or failure of an attack is verified
- Monitors system activities
- Network based IDS fail to detect attacks
- Near real time detection and response
- It does not require additional hardware
- Lower entry cost

Signature-based Intrusion Detection System

Signatures is defined as the signature based IDS monitor's packets in network that is compare with preconfigured and predetermined attack patterns. In such attacks, new attack is recognized experts or

programs that have to identify typical patterns which can be made into signature. For detecting threat, there will be a lag between new threats discovered and signature being applied in IDS and this process continue take place. IDS will not be identify the threats during this lag time. By reducing this lag, identify the threats and security software using such signatures should be updated as frequently as feasible.

Anomaly-Based Intrusion Detection System

This type of IDSs detect events which show violate thresholds or atypical behavior profiles that is based on statistical analysis. It contain example that is masquerade attacks which are detected in this way or penetrations of security control system. It also contain another attacks that is leakage or denial of service attacks which are detected by atypical use of system resources and some another problems include malicious use, violations of security constraints, or use of special privileges. Normal network activity is determined by the statistical anomaly-based IDSs which records what kinds of protocols are used, what sort of bandwidth is generally used, which ports and devices generally connect to each other and alert the administrator or user when traffic is detected which is anomalous.

Techniques of Intrusion Detection System

Here, we will discuss many of techniques to detect intrusion system that are given in below:

Artificial Neural Networks (ANNs): This networks are recognized capabilities and provide flexible pattern. In this network, recognize various arbitrary patterns that are provided to it as input data by given some special kind of training to the system. After fully recognize the patterns by system, it is matched these patterns with output produced. It is detected that intrusion has occurred or not by matching various input and output arbitrary patterns.

State Transition Tables: In this table, intruder performed the sequence of actions which is described in the form of a state transition diagram and behavior of system is observed. An intrusion is detected by matches it with identifiable compromise state and penetrated state.

Genetic Algorithms (GAs): It has function that imitate or mimic the natural reproduction system in nature. Only fittest individual will be reproduced in subsequent generations after undergoing recombination and various random changes. Its application has been appeared in IDS research in 1995 and it involves evolving a signature that indicates intrusion. It contain related technique which is Learning Classifier System (LCS) in which binary rules are evolved and collectively recognizes patterns of intrusion.

Bayesian Network: Graphical model have been introduced in Bayesian network. These graphical models are defined by a set of transition rules that are represented as probabilistic interdependencies. In each node, described a conditional probability table and state of random variable in this model. The probabilities of node in a state is determined by the conditional probability table. This approach contain advantage that can deal with incomplete data.

Fuzzy Logic: It is handle vagueness and imprecision that is designed by a set of concepts and approaches. To describe the relationship between input variables and output variables that is the set of rule in which intrusion occurred. This logic uses membership functions to evaluate the degree of truthfulness.

Review of Literature

Nazer and Selvakumar 2011, stated that many commercial companies and research community pay more interest in Intrusion Detection area. In this paper, given the overview of current state of art of Intrusion detection that is based on proposed taxonomy illustrated. In this, protect the infrastructure, end-user station and paradigm by current focus of research prototypes as well as products that has introduced the usage of network sniffers that analyze packets. Now, signature analysis is clearly in commercial domain but it is shown to be detect insufficient all attacks.

Ashoor and Gore 2011, stated that Intrusion Detection system is a defensive operation system that complements the defense such as firewalls and UTM etc. This system basically detects attack signs and then alerts. According to this paper, detection methodologies are typically categorized into two systems such as misuse detection and anomaly detection systems. It can be classified into in network based or host based IDS in deployment perspective and collect the information from both IDS.

Chakraborty 2013, dictated that companies fight the inevitable network and system attack by available many technologies in market. It can be deployed to increase visibility and control within a corporate computing environment by using two technologies IDS and IPS. Both technologies provide a foundation of technology that meets the requirement of tracking and through logs of IDS systems, identifying network attacks to which detect. Host is great to use of IDS, IPS or both in network environment, if the host is with critical systems, confidential data and strict compliance regulations.

Chowdhary, Suri and Bhutani 2014, concluded that Intrusion detection System is crucial part of defensive operations that complements the static defense such as firewalls. When intrusion is deleted, intrusion detection systems search for signs of an attack and flag. By closing the connection or report the incident for further analysis by network administrators, stop the attack. Intrusion detection systems are typically categorized into misuse detection and anomaly detection systems according to detection methodology. An intrusion detection system develop more accurate as it detect more attacks and raises fewer false alarms in term of performance.

Vichare 2017, in this paper, two systems are constructed for security of systems and studies of what is firewall and Intrusion Detection System, their basic working and types and difference between them. In network topology, firewall is placed at different layer and intrusion system at different layer. Both firewall and Intrusion Detection System are active systems for security and equally important.

Conclusion

Intrusion Detection System play an important role in detect an attack on commercial network and companies. It is the important part of defensive system of computer and network resources. This system detect an attack and intrusion more accurately than other system which increases fewer false positive results. At preliminary stages, it is an important security measure in which need for organization to implements this to detect the attacks and other malicious activities. By using the detection technologies, identifying the attack that was occur on network and computer resources.

References:

Analysis of Intrusion Detection Systems and Effective Intrusion Detection Mechanism. Available at: www.ijmer.com

Ashoor, Asmaa Shaker, and Sharad Gore. "Importance of Intrusion Detection System (IDS)." *International Journal of Scientific & Engineering Research,* vol. 2, no. 1, Jan. 2011, pp. 1–4.

Chakraborty, Nilotpal. "Intrusion Detection System and Intrusion Prevention System: A Comparative Study." *International Journal of Computing and Business Research (IJCBR),* vol. 4, no. 2, May 2013.

Chowdhary, Mahak, et al. "Comparative Study of Intrusion Detection System." *International Journal of Computer Sciences and Engineering,* vol. 2, no. 4, 30 Apr. 2014, pp. 197–200.

H., RafatRana S. "A Review on Intrusion Detection System." *International Journal of Advance Research in Computer Science and Management Studies,* vol. 3, no. 3, Mar. 2015, pp. 22–28.

Kumar,, Amit, et al. "A Research Paper on Hybrid Intrusion Detection System." *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 2, no. 4, Apr. 2013, pp. 294–297.

Madni, Hussain Ahmad, et al. "An Overview of Intrusion Detection System (IDS) along with Its Commonly Used Techniques and Classifications." *International Journal of Computer Science and Telecommunications,* vol. 5, no. 2, Feb. 2014, pp. 20–24.

Mukhopadhyay, Indraneel, et al. "A Comparative Study of Related Technologies of Intrusion Detection &Amp; Prevention Systems." *Journal of Information Security,* vol. 02, no. 01, 2011, pp. 28–38.

Nazer, G. Mohammed, and A. Arul Lawrence. "Current Intrusion Detection Techniques in Information Technology - A Detailed Analysis." *European Journal of Scientific Research,* vol. 65, no. 4, 2011, pp. 611–624.

S., Depak, et al. "Comparative Analysis of Different Techniques Used In Anomaly-Based Intrusion Detection." *International Journal of Pure and Applied Mathematics,* vol. 115, no. 7, 2017, pp. 175–182.

Vichare, Shardul Sharad. "Comparative Study on Firewall and Intrusion Detection System." *International Journal of Engineering Science and Computing,* vol. 7, no. 6, June 2017, pp. 13716–13718.

Vijayarani, S., and Maria Sylviaa S. . "Intrusion Detection System – A Study." *International Journal of Security, Privacy and Trust Management (IJSPTM),* vol. 4, no. 1, Feb. 2015, pp. 31–44.