Cybersecurity

Author Name(s), First M. Last, Omit Titles and Degrees

Cybersecurity

**Introduction**

Modern life spins around several elements of technology. Owing to an increase in the use of technology, it has become an indispensable part of our lives. Despite several benefits of technology, it is undeniably true that it poses various threats as well. Many IT firms are struggling to secure their systems and confidential from various attacks and attackers. Thus, cybersecurity has become an essential element for all the IT firms and therefore they take various cybersecurity measures to protect their data. This research paper will focus on various security measures especially, the intrusion detection system, its types, and methods.

**Intrusion Detection System**

Cybersecurity measures have become a necessity for IT firms owing to an increase in cyber-attacks. An intrusion detection system is also one of the well-known software that helps in detecting any security threat. An intrusion detection system (IDS) is a software application monitors not only privacy violations but also oversees any malicious activity (Turban & Wood, 2018). In case of any violation or potential threat, the software directly reports to a network administrator. The malicious activity is also collected centrally by utilizing security information and event management system (SIEM). The main purpose of SIEM is to integrate outputs that are collected from multiple sources and then filter the outputs by utilizing an alarm filtering technique. This aids in differentiating malicious activity or privacy violations from false alarms.

While installing IDS it is necessary to set the system properly as it is inclined to the false alarms so properly setting up the system will facilitate IDS to recognize the difference between the normal activity on the network as compared to the malicious activity. IDS are different from firewalls in a way that IDS unlike firewalls monitors the attacks within the system and signals an alarm in case of any privacy violation. Typically, IDS detect the malicious activities by examining network communications and identifying patterns and heuristics of several computer attacks and then take action by signaling an alarm.

**Types of IDS**

There are a few types that differ from each other due to the method of detection and the place where the detection takes place. The types of IDS are as follows:

**Network intrusion detection system (NIDS)**

NIDS are typically set up at a point present within the network so that it can easily determine traffic to and from all the devices attached to a network. The NIDS system analyzes all the traffic passed to and from the devices on the subnet and then compare it with the traffic that is passed on the subnets to the library of all known attacks (Liao & Tung, 2013). As soon as the system identifies an attack or any violation of privacy it signals an alert to the administrator. NIDS can also be installed on the subnets where firewalls are present. This will facilitate in detecting any intrusion or attacker trying to damage the firewall. Another important feature of NIDS is that it can be combined with various technologies to increase the detection and prediction of any malicious activity.

**Host Intrusion Detection System (HIDS)**

HIDS runs on devices or an individual host that are present on the network. The HIDS monitor both the incoming and outgoing of the packets only from the devices present on the network and will signal an alert in case of any suspicious activity to the administrator or user. Unlike NIDS it takes snapshots of the current traffic and then compares the snapshots with the previous snapshots. If any system file is removed or altered, an alert is sent directly to the administrator so that immediate action can be taken to avoid severe consequences (Liao & Tung, 2013). HIDS can be used in machines that do not require changing in their configuration or layout.

**IDS Detection Methods**

As mentioned earlier IDS can also be classified based on the method of detection. There are two types of IDS detection methods that are as follows:

**Signature Based Method**

A signature-based method is a method detecting attacks by identifying specific patterns such as bytes’ sequence or a number of 1’s and 0’s that are present in the network traffic (Smaha, 1988). This method also helps in detecting the instructions of malicious sequence that is utilized by malware. Another terminology that is used for the detected patterns is known as signatures.

**Anomaly-Based Method**

The anomaly-based method is a method that is used to detect various unknown malware attacks. In this method machine learning is utilized to develop a model of trustworthy activity so that new behavior of the system can be compared against this model. These models can be configured according to the requirement but in general, the model that is based on machine learning are more reliable. Despite facilitating in detecting several unknown attacks it is prone to detect false positives as a previous legitimate activity can also be considered as an unknown attack (Smaha, 1988). Various existing IDSs require a significant amount of time during the detection process. However, the selection algorithm is fast as compared to the typical IDS and is, therefore, more reliable and efficient.

**Conclusion**

Security is one of the major concerns of all IT firms. Many companies are struggling to implement a system or utilize software that can efficiently detect or prevent malicious activity. IDS is a system that facilitates detecting malicious activity. It also provides information based on the addresses of the networks that are associated with IP packets sent to the network. Although, the system is an efficient way to detect intrusions yet it does have some limitations. For instance, various factors such as noise can limit the detection ability of IDS. Thus, it is necessary to install the system carefully to avoid false alarms or alerts.

**References**

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.

Smaha, S. E. (1988, September). Haystack: An intrusion detection system. In *[Proceedings 1988] Fourth Aerospace Computer Security Applications* (pp. 37-44). IEEE.

Turban, E., Pollard, C., & Wood, G. (2018). *Information Technology for Management: On-demand Strategies for Performance, Growth and Sustainability*. John Wiley & Sons.