A Survey of Intrusion Detection Techniques in Computer Network

Miss Vinita R. Shewale[1], Dr. Hitendra D.Patil[2]
[1]Master Student, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India
[2]Professor and Head, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India
[1]vinitashewale@gmail.com; [2]hitendradpatil@gmail.com

***Abstract*—** As advances in the networking technology help to connect distant corners of the globe and as the Internet continues to expand its influence as a medium for communication, the threat from attackers and criminal enterprises has also grown accordingly. The increasing occurrence of network attacks is a very big issue to the network services. So, Intrusion Detection System has become a necessary component of network security. It is used for detection of many known and unknown network vulnerabilities in wired networks. While the Internet service for any purpose is used, normally who are attacking on the computer network is not known by us. Those network attacks can cause network services slow, temporarily unavailable, or down for a long period of time. The concern on this work is to perusal various methods of networking attacks detection and compare them against these methods by considering their pros and cons.

Keywords- *Intrusion Detection Systems, signature based detection, anomaly based detection, hybrid; attack; snort*

*****

I. INTRODUCTION

The computer networks expand day by day and number of internet users also increases. Sharing of information and resources among different devices and organizations, make the world become like a small village. Although exchanging information across computer network had improve the efficiency, it is also had given an opportunity of cyber-attack. The vast amount of attacks over the Internet make computer users and many organizations under potential violation of security as a result it is strongly required to protect network systems, organizations and government agencies from intrusions.

A. *Networking Attacks*

This is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groups

1. *Denial of Service (DoS):* A DoS attack is a type of attack in which the hacker makes a computing resources or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a particular machine e.g. apache, smurf, neptune, ping of death, back, mail bomb, UDP storm etc. are all the DoS attacks .
2. *Remote to User Attacks (R2L):* It is an attack in which a user sends packets to a machine over the internet, which he or she does not have access to in order to expose the machines vulnerabilities and exploit permissions which a local user can have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.
3. *User to Root Attacks (U2R):* These attacks are the exploitations in which the hacker starts off on the system with a normal user account behaving as a normal user and attempts to grab vulnerabilities in the system in order to gain privileges of super user e.g. perl, xterm.
4. *Probing:* It is is an attack in which hacker scans a machine or a networking device in such a way that hacker can determine weaknesses or vulnerabilities occurring in the system that may later be misused so as to compromise the system. This technique is commonly used in area of data mining e.g. saint, portsweep, mscan, nmap etc.[1].

B. *Intrusion Detection System*

Intrusion Detection System (IDS) plays a very essential role for detecting different kinds of attacks. It is a device (or the software application) that monitors the network (and system) for detecting malicious activities (that affect the confidentiality, integrity and availability of resources and services) and generating appropriate alerts.

As shown in Fig. 1, IDS involves mainly components which are Data pre-processor, Detection algorithm and Alert filter.

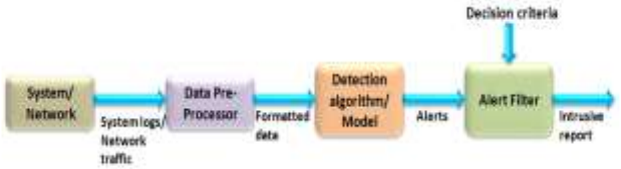

Figure 1. **Intrusion Detection System Components**

- *System/Network:* It is a system that will be monitored and data will be captured for inspection.
- *Data pre-processor:* It collects and formats the data (network traffic/log data) that will be later analyzed by the detection algorithm. In case of network traffic, data involve packets having headers (routing information) and contents (payloads) that are useful for detecting intrusions. Data from system log includes an ordered set of system activities.
- *Detection algorithm (model):* Using detection algorithm/model, IDS detects the distinction between "normal" and "intrusive" traffic.

- *Alert filter***:** This always estimates the severity of the detected intrusions (based on decision criteria) and alerts the operator or manages responsive activities. Filtering is normally done by a set of thresholds that should be set in such a way that IDS can maintain a high level of accuracy and system performance.

There are mainly two techniques used in IDS: Signature based and Anomaly based.

a. *Signature based detection:* It monitors packets on the network and compare them against the database of signatures or attributes from known malicious threats. As a result, signature based systems are capable of attaining high level of accuracy and minimal number of false positives in identifying known intrusions. However, little variation in known attacks may affect the analysis, if detection system is not properly configured [7].

b. *Anomaly detection:* Anomaly based approach collects the data relating to the behavior of user/system/application over a period of time, and then it applies statistical tests to the behavior which is observed, which determines whether that behavior or action is legitimate or not. A large variety of techniques including data mining, statistical modeling and machine learning have been explored as anomaly detection.

II. Literature Survey

After observed limitation of both approaches misuse and anomaly detection such as in the first approach it cannot detect novel attacks and often fail to detect light modifications to existing attacks and the second method anomaly based detectors suffer from a high false alarm rate. Various methods has been proposed in different researches to overcome the above problems with intrusion detection based system in both approaches misuse and anomaly detection based on hybrid anomaly detection.

Another research for this had been devoted, to hybrid IDS by gathering misuse and anomaly detection, using data mining algorithms as the data processing for vast amounts of security audit data, and generates detection models and test models separately from the network data.

A. Hybrid Anomaly Detection Based Methodology

J. Marin et al. [2] described some preliminary results considering the robustness and also the generalization capabilities of the machine learning techniques in making user profiles based on the selection and subsequent classification of command line arguments. The method is based on the assumption that legitimate users can be categorized based on the percentage of commands they use in a specified period of time.

The hybrid approach they employed starts with the application of expert rules for reducing the dimensionality of the data, followed by the initial clustering of the data and then it does subsequent refinement of the cluster locations using the competitive network called Learning Vector Quantization.

B. Anomaly Detection Sceheme based on Principle Component Classifier

M. Shyu et al. [3] proposed Principal Component Anomaly based detection scheme. It uses principal component analysis as an outlier detection scheme to detect intrusions. This scheme is only based on detecting anomalies. They proposed a novel technique that uses robust principal component classifier in intrusion detection issues where the training data may be unsupervised one. Assuming that anomalies can be treated as the outliers, an intrusion predictive model is built from the principal components which can be major or minor of the normal instances. A measure of difference of intrusive from the normal instance is the distance between the principal component spaces.

To establish a detection algorithm, they performed PCA on the correlation matrix of normal group. The correlation matrix is needed to be used because each feature is measured in different levels. It is very important that the training data should be outliers free before they are used and it is used to determine the detection criteria since outliers can bring increase in variance, covariance and correlations.

C. Combining PHAD and NETAD to signature based IDS Snort

M. Aydin et al. [4] discussed a hybrid IDS by combining the two approaches in one system. The hybrid IDS is obtained by combination of packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the signature-based IDS Snort that is an open-source project. Snort's preprocessor design has been used to combine PHAD and NETAD with Snort. It is determined that number of attacks detected will increase as much more with the hybrid IDS. As a result it can be found that combining PHAD and NETAD as a preprocessor which are anomaly-based systems with the misuse-based IDS Snort, contributes to intrusion detection positively or completely [4].

D. Hybrid Approach based on Pattern Matching Engine and Neural Network

C. Amza et al. [5] planned a unique Intrusion Detection System that uses a hybrid approach supported a pattern matching engine and a neural network functioning in parallel to boost the detection potency. This approach relies on the Netpy traffic observance and analysis tool that they developed. Netpy is a network traffic analysis tool using Netflow knowledge. Existing features are used to develop a complex IDS supported pattern matching, as well as anomaly detection.

Netpy is an associate degree application that involves the help of the administrator by observing the state of a network. It can be used to notice if there are any unauthorized open ports, interior worms or viruses, external applications scanning the network systems and many of alternative issues. This novel approach is ready to efficiently detect known classes of attacks, as well as unknown ones. Since the two detection solutions run in parallel it additionally offer a way to filter and group the security alerts to attenuate the number of notifications which is able to be sent to the network administrator.

E. A serial Combination of Anomaly and Misuse IDSes Applied to HTTP Traffic

E. Tombini [6] et al. described in their paper regarding combining an anomaly and a misuse IDSes that offers the benefit of separating the monitored events between intrusive, normal or unqualified classes (i.e. not known as an attack, however not acknowledged as safe either). They provided a framework to systematically reason regarding the mix of anomaly and misuse components. This framework applied to internet servers leads to a serial architecture, using anomaly component which is drastic with a sensitive misuse component.

This design provides the operator with higher qualification of the detection results, raises lower quantity of false alarms and unqualified events. Analyzing web server log files is a vital issue, as web servers and proxies offer a universal gateway to the information system. They have been employing a web intrusion detection system (WIDS) to research in batch mode web server log files to detect compromise attempts and the worm infections. Table 1 shows the comparison of different attack detection techniques used.

III. Comparison of Techniques

TABLE I. **Comparison of Attack Detection Techniques**

Basic Concept	**Technique**	**Advantage**	**Limitation**
Hybrid anomaly detection based methodology	Initial clustering of data using “K-Means” and refined cluster locations with use of a competitive network referred as “Learning Vector Quantization”	Reduce dimensionality of the data using Genetic Algorithm	Less classification rate
Anomaly detection technique based on Principal Component Classifier	Principal component analysis based anomaly detection technique	Exhibits better detection rate than other well-known outlier based anomaly detection algorithms	Covariance matrix is difficult to be evaluated in an accurate manner
Combining PHAD and NETAD to signature-based IDS Snort	Combination of each Snort with Packet Header Anomaly Detection (PHAD) and Network Traffic Anomaly Detection	Number of attacks detected increases much more with the hybrid IDS	Suffer from high false alarm rate
Hybrid approach based on pattern matching engine and neural network	Combined a basic pattern matching engine with a neural network detection component to detect anomalies in the network traffic.	Increase Efficiency and produce few false positives	Not able to detect large number of attacks
A Serial Combination of Anomaly and Misuse based IDSes Applied to HTTP Traffic	A framework with combination of anomaly and misuse components(WIDS) applied to web servers	More Accuracy and less time consuming, low rate of false negatives	The unqualified events require further investigation in order to be qualified as safe or intrusive

IV. Conclusion

In this paper we have described the different networking attacks in wired network and intrusion detection system. This paper presents review of various attack detection techniques and how they are used for detecting number of attacks in wired network. In literature survey we have described the attack detection techniques, and various issues involved in the process. In tabular form we summarized the attack detection techniques for wired network. The limitation of previous techniques in intrusion detection system in term of detected new attacks and false alarm rate respectively had motivated to come up with the idea to integrate them referred to as Hybrid IDS. Hence the aim is to combine both algorithms that are misuse based and anomaly based in order to enhance system security and help IDS user to decide about detected attacks by the system.

References

[1] G M. S. Hoque, M. A. Mukit and M. A. N. Bikas, "An implementation of Intrusion Detection System using Genetic Algorithm," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 4, no. 2, March 2012.

[2] J. Marin, D. Ragsdale and J. Surdu, "A Hybrid Approach to the Profile Creation and Intrusion Detection," in *DARPA Information Survivability Conference and Exposition* , 2001.

[3] M. L. Shyu, S. C. Chen, K. Sarinnapakorn and L. Chang, "A novel anomaly detection scheme based on principal component classifier," in *Proceedings of the IEEE Foundations and New Directions of Data Mining Workshop*, Melbourne, FL, USA, 2003.

[4] M. A. Aydin, A. H. Zaim and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers & Electrical Engineering*, vol. 35, pp. 517-526, May 2009.

[5] C. Amza, C. Leordeanu and V. Cristea, "Hybrid Network Intrusion Detection," in *IEEE International Conference on Intelligent Computer Communication and*, 2011.

[6] E. Tombini, H. Debar, L. Me and M. Ducasse, "A Serial Combination of Anomaly and Misuse IDSes Applied to HTTP Traffic," in *Proceedings of the 20th Annual Computer Security Applications Conference*, 2004.

[7] D. J. Brown, B. Suckow and T. Wang, *A Survey of Intrusion Detection Systems*, Department of Computer Science, University of California, San Diego, 2002.