BOOK CHAPTER | Hybrid IDS

A Hybrid Intrusion Detection and Prevention System for Cyber Attacks Mitigation

[1]Konyeha S. & [2]Konyeha, C.
[1]Dept of Computer Science, University of Benin, Benin City, Nigeria.
[2]Dept of Electrical/ Electronic Engineering, Benson Idahosa University, Benin City, Nigeria
E-mail: sodirichukwu@gmail.com
Phone: +2348034226244

Abstract

Computer networks have become an essential part of human life. These computer networks are being attacked every day and it is difficult to detect and prevent these attacks by conventional methods such as anti-virus protection, user authentication and use of firewalls only. A radical way of constantly monitoring the network interface for vulnerabilities is needed to detect and respond to these attack events. Intrusion Detection Systems (IDS) have been of interest to researchers for some time now and can provide advance warning against impending attacks due to its in-depth detection and logging of malicious activities. Most of the current intrusion detection systems have mainly concentrated on detection of intrusions with no mechanism incorporated to respond to such intrusions. Also popular intrusion detection systems detect attacks based on policy or signature and hence are able to detect known attacks only. However a hybrid intrusion detection system detects both known and unknown attacks. In this report, a hybrid intrusion detection system that detect known attacks and unknown attacks is presented. The hybrid IDS was trained to detect unknown attacks using a statistical model. The information used for training the hybrid IDS was collected from a business LAN. The performance of the hybrid IDS was tested, under inside and outside attacks. The results were quite encouraging as the hybrid IDS was effective in detecting and preventing attacks from succeeding by automatically reconfiguring firewall rules.

Keywords: Anomaly, signature, hybrid, IDS, NIDS, false positive, false negative, intrusion detection.

Introduction

A network can be considered as an interconnected system based on approved protocols which exchange information (Adat and Gupta, 2018) among the devices operating via the network infrastructure. Digital technology adoption has surged across industries over the past two years, catalyzed by the pandemic. This has helped drive innovation and unlocked new possibilities. However, security and data privacy continue to be the major consideration in the selection and utilization of a network systems for most organizations as more organizational operations are performed using the internet.

BOOK Chapter | Web of Deceit - June 2022 - Creative Research Publishers - Open Access — Distributed Free

Citation Konyeha S. & Konyeha, C. (2022). A Hybrid Intrusion Detection and Prevention System for Cyber Attacks Mitigation. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 179 -184. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P30

Intrusion Detection Systems (IDS) are emerging as a reliable way to detect malicious attacks and reinstate network security in the cloud environment (Raj and Pani (2021).

Related Works

Existing literatures on network security and intrusion detection systems were reviewed. From existing literature we can define Intrusion Detection Systems (IDS) as software/ hardware designed to monitor network traffic or computer activities and alert administrators of suspicious activities (Fung, 2011).

Effectively detecting intrusions in the computer networks still remains problematic. This is because cyber attackers are changing packet contents to confuse the intrusion detection system (IDS). To manage the computer network flows and provide the security in advance; the components of the IDSs, the approaches and technologies that are used, the nature of the attacks, and the tools that are used, need to be examined deeply (Ozkan-Okay et al., 2021).

IDS differ in the ways they detect attacks and handle threats. The most common approaches used to detect attacks include misuse intrusion detection, anomaly intrusion detection, and hybrid intrusion detection (Mgabile et al., 2012). Signature based intrusion detection systems rely on a set of rules (also known as signatures) for detecting intrusion activity. A signature can be described as a conditional rule, which is tested on an instance of activity, identifying a specific type (Cole et al., 2009). Anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior. A wide variety of techniques including data mining, statistical modeling and hidden markov models have been explored as different ways to approach the anomaly detection problem (Nachan, et al., 2021).

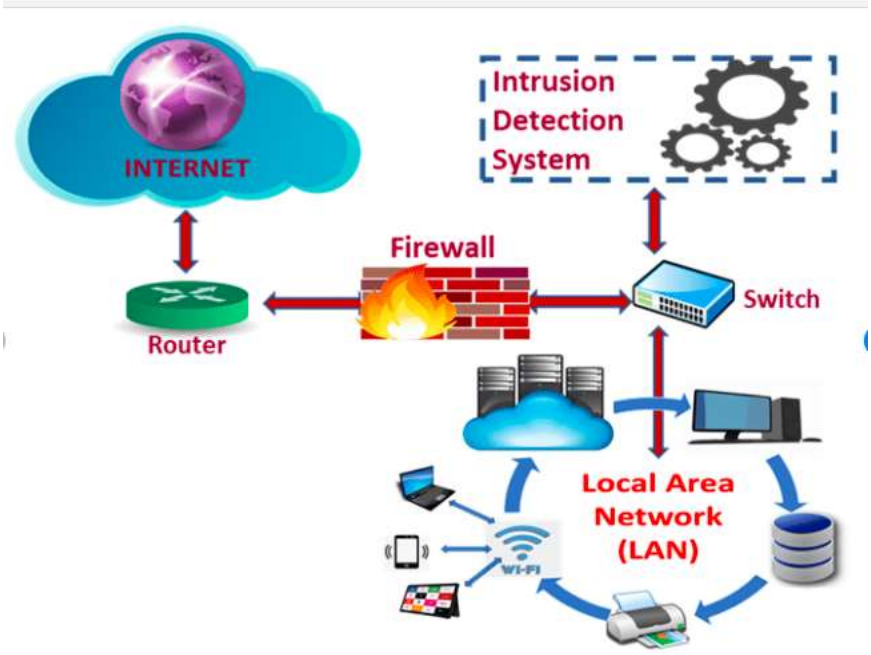

Fig. 1: Intrusion Detection in a LAN Scenario

The hybrid system implemented in this work is a combination of signature based detection using Snort rules to implement signature based detection and a statistical method to implement anomaly detection, We have built a module which can detect unknown attacks and integrated it with Snort (an open source IDS) for signature detection.

Methodology

A local area network (LAN) was configured using static IP addressing for the server and client computers. Several network data traces were collected to use for the demonstration. The normal activity in the business LAN consists of accessing e-mails, browsing, authentication, uploading and downloading of files etc requiring the following network protocols: tcp, http, ack, arp, dns, https, and arp etc. A log or record of this normal data trace was made and kept to be used for the experiments.

The procedure for signature or rule based detection consists of first copying the rules for matching packets, into a rules folder and requiring the IDS it use the rules in the IDS config file. The system when ran, begins to sort the packets and match it against the rules file. It checks for any offending packets. Once there is a match, the system provides an alarm response. If no alarm is raised, the data is simply logged into the database.

In anomaly detection, training and detection are the two processes carried out. The system is trained with data free of attacks in order to learn the normal profile. In the training mode, the system learns and updates the normal profile using a statistical formula which computes a new mean and standard deviation whenever an additional packet is captured at the network interface. The packets that enter the network are stored in a buffer during an analysis cycle and analyzed at the end of the cycle. An anomaly analysis engine checks for anomaly in the network traffic using the sample mean and standard deviation model which is a statistical tool we used for training the anomaly detector in the hybrid IDS. According to Denning(1987), when using the mean and standard deviation model, a new observation is abnormal if it falls outside a confidence interval that is d standard deviations from the mean for some parameter d: mean + d * stdev.

The statistical formula used to update the mean and (estimated) variance of the sequence, for an additional element x_{new}, where, $\bar{x}_n$ denotes the sample mean of the first n samples (x_1, x_2,..... x_{n-1}), s_n^2 their sample variance, and σ_n^2 their population variance is stated in equations (1) - (2):

$$\bar{x}_n = \frac{(n-1)\bar{x}_{n-1} + x_n}{n} = \bar{x}_{n-1} + \frac{x_n - \bar{x}_{n-1}}{n} \qquad (1)$$

$$s_n^2 = \frac{(n-2)s_{n-1}^2 + (x_n - \bar{x}_n)(x_n - \bar{x}_{n-1})}{n-1}, n > 1 \qquad (2)$$

$x < \mu + 3(\sigma) + T$ normal traffic ($T \geq 0$)

Where x_n = Number of packets counted in the cycle (e.g IP:Port combination)
μ = Mean score of packets counted
σ = Standard Deviation
T = Thresholdn = the Cycle no
x = packet count (score)

The anomaly analysis engine uses mean and standard deviation (computed from the variance) rather than variance itself, because the area under the normal distribution curve is obtained using the values of the mean and standard deviation. Figure 1 shows the confidence region for a normal distribution.

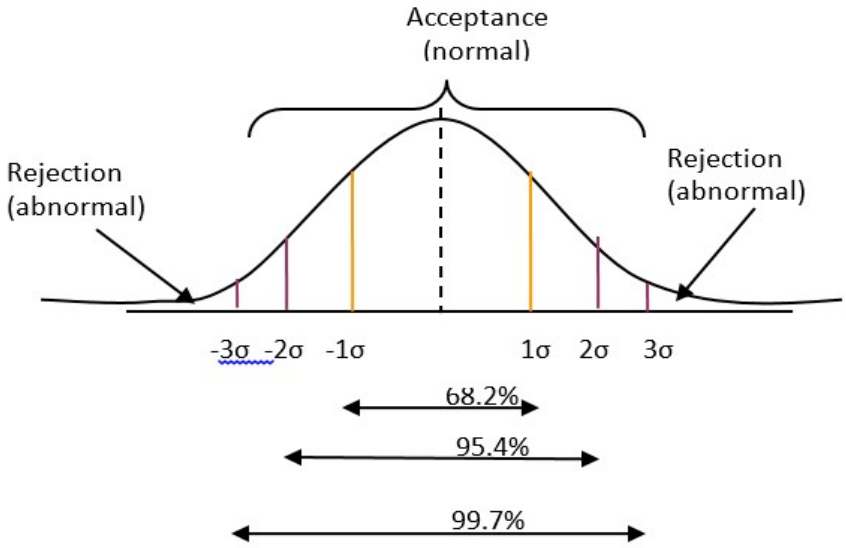

Figure 2: Normal distribution curve

The baseline for a detection event is the upper bound for the third standard deviation from mean plus a pre-assigned threshold value (T). Thus our baseline is given as $x < \mu + 3\sigma + T$, where T is the threshold. The defined upper bound of $x < \mu + 3\sigma + T$ is a normal region, where the proportion of observed packet scores falling in the region is at least 99.7%. Beyond this normal region, the observed packets are anomalous. The graphic user interface (GUI) and anomaly detection engine components of hybrid IDS were developed with Java programming language which is a general purpose, concurrent, class-based, object-oriented programming language. Since JAVA is not native to windows, we used a wrapper for WinPCap called JPCap to capture the packets from the device's network interface card.

After packet capture, the system was required to check if it is operating in learning mode or detection mode. When the system is working in learning mode, it would store the mean score and standard deviations (profiles) of these captured packets in an anomaly profile database. However if the system is working in the detection mode, it will match the captured packets against the normal profiles of packets already recorded in the database during training. This method of detection owes to the fact that: 99.7% of the data falls under three standard deviation of the mean.

Results

A prototype of the hybrid IDS has been implemented and tested for signature based detection and anomaly based detection using real time data collected on a LAN, and the IDEVAL 1999 DARPA dataset. For the demonstration, the hybrid IDS was configured a host computer on the LAN. Wireshark (a network protocol analyzer) was configured on another one of the hosts on the LAN. We also installed Nmap or network mapper (an open source utility for network exploration and security auditing) and NSA's http traffic generator on a computer that would emulate an attacker, attacking from both within the network and from outside the network depending on the attack scenario.

Results for inside attack scenario

A host computer on our LAN performed an intense port scan of the network using Nmap and then sent reassembled packets with a bogus IP address that is classified as a "bogon" using http traffic generator. The hybrid IDS detected a bogon here with IP:PORT 184.168.221.84:80. The bogus packet is destined for the IP:PORT 192.168.0.2:1433.

Results for outside attack scenario

1. The hybrid IDS detecting an instance of crafted packets with bogus IP headers sent to an attacked host (192.168.0.2) on the LAN

Figure 2: Showing attacks detected from Nmap and HTTP traffic generator simulated data

2. The hybrid IDS response mechanism automatically block packets that trigger alerts on the network from further communication on the visited port. Note that the traffic was generated by Nmap and http traffic generator hence the bogus source IPs obtained.

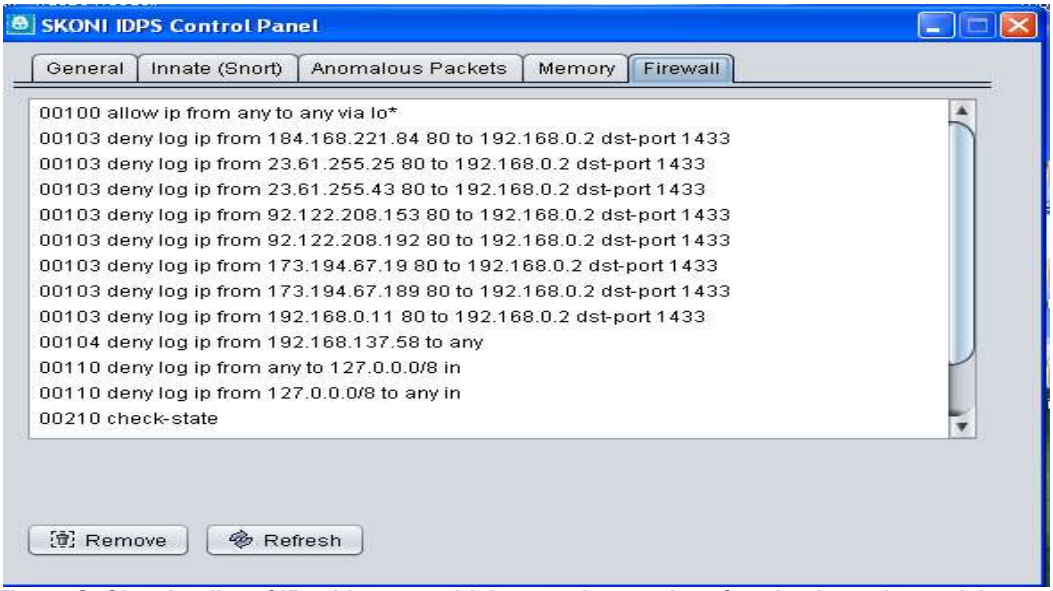

Figure 3: Showing list of IP addresses which were detected performing intrusive activity and hence blocked from further communication on the visited port.

REFERENCES

1. Adat, V., and Gupta, B. (2018). *Security in Internet of Things: Issues, challenges, taxonomy, and architecture*. Model. Anal. Des. Manag. 2018, 67, 423-441.
2. Cole, E., Krutz, R. and Conley, J.W. (2009). *Network Security Bible*, Wiley Publishing Inc.
3. Denning D. E. (1987). *An Intrusion-Detection Model*, IEEE Transaction on Software Engineering, Vol. SE-13, No.2 (Feb), 222-232.
4. Fung Carol (2011). *Collaborative Intrusion Detection Networks and Insider Attacks*. University of Waterloo, Waterloo, ON, Canada. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 1, pp. 63-74.
5. Mgabile T., Msiza S. Ishmael, and Dube Erick (2012). *Anomaly Based Intrusion Detection for a Biometric Identification System using Neural Networks* International Conference on Artificial Intelligence and Image Processing (ICAIIP'2012).
6. Nachan, H., Kumhar, P., Birla, S., Poddar, D., and Sarode, S. (2021). *Intrusion Detection System: A Survey.* International Journal of Engineering Research & Technology (IJERT) Volume 10, Issue 05 (May 2021), pp 1036 – 1047.
7. Ozkan-Okay, M., Samet, R., Aslan, Ö, and Gupta, D. (2021). *A Comprehensive Systematic Literature Review on Intrusion Detection Systems*, in IEEE Access, vol. 9, pp. 157727-157760, 2021, doi: 10.1109/ACCESS.2021.3129336.
8. Raj, M. G., and Pani, S. K. (2021). *A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment*. International Journal of Advanced Computer Science and Applications, 12(10), pp 206 - 217). doi:10.14569/ijacsa.2021.0121023.