INTRUSION DETECTION SYSTEM

Dheeraj Mishra[1], Pratik Patil[2], Akash Naundla[3], Roshan Shah[4]

[1,2,3,4]*Computer Engineering, Mumbai University (India)*

ABSTRACT

With recent advances in network based technology and increased dependability of our everyday life on this technology, assuring reliable operation of network based systems is very important. During recent years, number of attacks on networks has dramatically increased and consequently interest in network intrusion detection has increased among the researchers. This paper provides a review on current trends in intrusion detection together with a study on technologies implemented by some researchers in this research area. Honey pots are effective detection tools to sense attacks such as port or email scanning activities in the network. Some features and applications of honey pots are explained in this paper.

Index Terms- ADS, Anomaly, Anomaly Detection, Intrusion Detection, , IDS,

I. INTRODUCTION

In the past few decades with the rapid progress in the Internet based technology, new application areas for computer network have emerged. At the same time, wide spread progress in the Local Area Network (LAN) and Wide Area Network (WAN) application areas in business, financial, industry, security and healthcare sectors made us more dependent on the computer networks.

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks.

The remaining portion of the paper is organized as follows. Section 2 tells about the history and the basic concepts of IDS. Section 3 illustrates the IDS functionality.

II. HISTORY

The IDS journey started thirty years ago when increasing enterprise network access spawned a new challenge: the need for user access and user monitoring. As day-to-day operations grew increasingly dependent upon shared use of information systems, levels of access to these systems and clear visibility into user activity was required to operate safely and securely.

Much of the initial headway on IDS was made within the U.S. Air Force. In 1980, James P. Anderson, a pioneer in information security and member of the Defense Science Board Task Force on Computer Security at the U.S. Air Force, produced “Computer Security Threat Monitoring and Surveillance,” a report that is often credited with introducing automated IDS. Soon after this report was released, the first model was built, born out of the same methods used by anti-virus applications: rule-based systems that constantly scanned and compared network traffic against a list of known threats.

During the late 1980's, with a growing number of shared networks, enterprise system administrators all over the world began adopting intrusion detection systems. However, IDS presented a couple problems. First, it could only alert on known issues that had been categorized as threats on a signature list; zero-day attacks could compromise a network's security. Second, the constant scanning and updating of a signature list was cumbersome and significant resource drain.

In the 1990's, IDS technology improved to address the increasing number and sophistication of network attacks. This new method, named anomaly detection, relied on identifying unusual behavioral patterns on the network, and provided alerts for any identified abnormality.

Unfortunately, the inconsistent nature of networks through the 1990's and early 2000's resulted in a high number of false positives, and many administrators thought IDS to be unreliable, and headed for a slow death.

The advent of cloud computing, however, has brought new relevancy to IDS systems, resulting in a surge in the IDS market. An essential component of today's security best practices, IDS systems are designed to detect attacks that may occur, despite preventative measures. In fact, IDS is now one of the top selling security technologies, and predicted to continue to gain momentum. After all, security cloud security in particular is far too complex to be monitored manually.

The logic and tactics IDS uses are more relevant today than ever before. With cloud computing, IDS has truly found an environment where it can thrive and be most effective. With cloud computing, the infrastructure has caught up with the IDS technology.

The consistent nature of servers in the cloud lends itself perfectly to IDS technology. As such, IDS is able to build stronger and more accurate baselines than were possible on the erratic on-premise network infrastructures of the past.

Big data also plays an important role in the growth and importance of intrusion detection today. The world's data doubles every 20 months, and as cloud-hosted databases expand exponentially, it's no wonder IDS is more important than ever

III. INTRUSION DETECTION SYSTEM

An IDS is referred as burglar alarm. For example the lock system in the house protects the house from theft. But if somebody breaks the lock system and tries to enter into the house, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm. Moreover, Firewalls do a very good job of filtering the incoming traffic from the Internet to circumvent the firewall. For example, external users can connect to the Intranet by dialing through a modem installed in the private network of the organization; this kind of access cannot be detected by the firewall. An Intrusion Prevention System (IPS) is a network security/threat prevention technology that audits network traffic flows to detect and prevent vulnerability exploits. There are two types of prevention system they are Network (NIPS) and Host (HIPS). These systems watch the network traffic and automatically take actions to protect networks and systems. IPS issue is false positives and negatives. False positive is defined to be an event which produces an alarm in IDS where there is no attack. False negative is defined to be an event which does not produces an alarm when there is an attacks takes place. Inline operation can create bottlenecks such as single point of failure, signature updates and encrypted traffic. The actions occurring in a system or network is measured by IDS [8].

3.1 Types of IDS

Figure 1 shows the different types of Intrusion detection systems.

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 [9]. 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 [10]. The elementary principle in IDS including Network Based Intrusion Detection System (NIDS) originated from anomaly HIDS research based on Denning's pioneering work [11]. A host-based IDS provides much more relevant information than Network-based IDS. HIDS are used efficiently for analyzing the network attacks, for example, it can sometimes tell exactly what the attacker did, which commands he used, what files he opened, rather than just a vague accusation and there is an attempt to execute a dangerous command [12]. It is less risky to configure.

3.1.1. Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

Network based IDS systems collect information from the network itself rather than from each separate host [13]. 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 [13]. Attack on the 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 [14].

The transparency of the monitors decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without the efforts [10]. Network Node IDS (NNIDS) agents are deployed on every host within the network being protected [2].

3.1.2 Advantages of Network based Intrusion Detection Systems:

- Lower Cost of Ownership
- Easier to deploy
- Detect network based attacks
- Retaining evidence
- Real Time detection and quick response
- Detection of failed attacks

Application based IDS (APIDS) will check the effective behavior and event of the protocol [2]. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices [2]. 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 [2]. There are numerous attacks have taken place in OSI layer

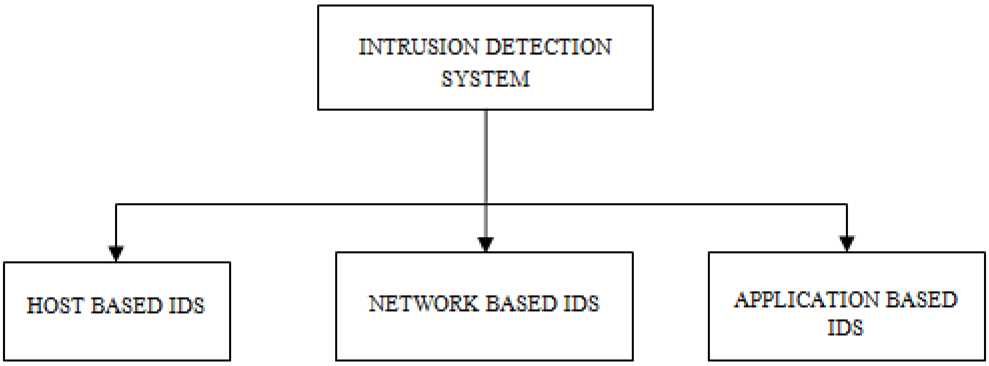

Fig.1. Intrusion Detection System - Types

3.2 Intrusion Detection Attacks

3.2.1 Denial-of-Service (DOS) Attacks

It tries to deny the authorized users from promoting the requested service. An advanced Distributed Denial of Service occurs in a distributed environment that the attacker sends or floods the server with numerous connection that request to knock the target system [2]. Types of DOS attacks are

3.2.1. SYN Attack

SYN attack is also defined as Synchronization attack. Here, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive.

3.2.2. Ping of Death

In this the intruder sends a ping request to the targeted system which is larger than 65,536 bytes which causes the system to crash [2]. The formal size must be 56 bytes or 84 bytes incase of considering Internet protocol header.

3.3. Eavesdropping Attacks

It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines or through email. [2].

3.4. Spoofing Attacks

This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker [2].

3.5. Intrusion attacks or User to Root Attack (U2R)

An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data [2].

3.6. Logon Abuse Attacks

A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages [2].

3.7. Application-Level Attacks

The attacker targets the disabilities of application layer. For example, security weakness in the web server or in faulty controls on the server side [2].

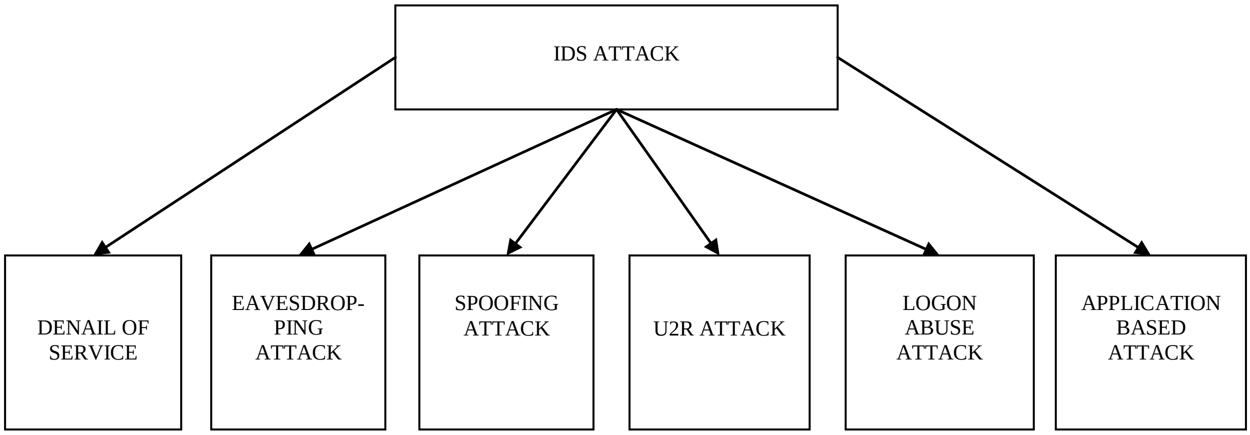

Fig.2. Intrusion Detection Attacks

IV. FUNCTIONS OF IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and action, which is given in Figure 3.

4.1 Data collection

This module passes the data as input to the IDS. The data is recorded into a file and then it is analyzed.
Network based IDS collects and alters the data packets and in host based IDS collects details like usage of the disk and processes of the system**.**

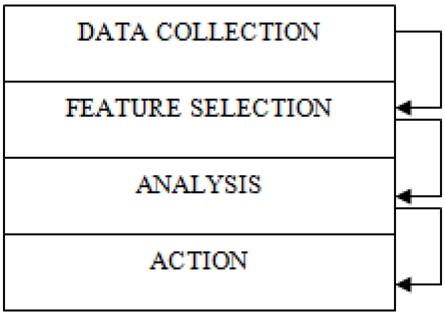

Figure 3. Functionality of IDS

4.2 Feature Selection

To select the particular feature large data is available in the network and they are usually evaluated for intrusion. For example, the Internet Protocol (IP) address of the source and target system, protocol type, header length and size could be taken as a key for intrusion [15].

4.3 Analysis

The data is analyzed to find the correctness. Rule based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern [15]. Another method is anomaly based IDS where the system behavior is studied and mathematical models are employed to it [15].

4.4 Action

It defines about the attack and reaction of the system. It can either inform the system administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports

V. PROPOSED SYSTEM

This paper is mainly focusing on ICMP flooding attack and how to detect the ICMP flooding attack.

5.1 ICMP Flood

ICMP flood is producing a large number of Echo Requests, making flood victim too busy replying to the requests and ending up consuming bandwidth and slowing down the victim.

We can model this attack using either Total Bytes sent or Total Packets sent or both. For now, this app models only the Total Packets sent over the network from one host to another.

Overview of the Triple Exponential Smoothing:

Exponential Smoothing can be used to predict some future values related to some metric.

HoltWinters Forecasting Algorithm uses exponential smoothing technique and considers 3 factors to predict the values: Baseline, Trend factor and Seasonal Index

The basic equations are:

$St = \alpha y_t/I_{tL} + (1\text{-}\alpha)(S_{t-1}+ b_{t-1})$

$bt = \gamma\ (S_t\ S_{t-1}) + (1\text{-}\ \gamma)b_{\ t-1}$

$It = \beta\ y_t/S_t + (1\text{-}\beta)I_{\ t-L}$

$F_{t+m} = (S_t + mb_t)I_{t-L+m}$

where

- y_t is the traffic count in the time t
- S_t is the prediction made for the time t
- b is the trend factor
- I is the seasonal index
- F is the forecast and m periods ahead
- t is the time frame used for collecting and predicting traffic
- αβγ are model parameters

Confidence Bands:

Concept of confidence bands is used to measure the deviation of actual traffic from the predicted value and consider it as anomaly.

The deviation is defined using the equation:

$d_t = | y_t - St\delta |$

where

- d_t is the deviation
- y_t is the actual traffic count
- S_t is the predicted traffic value
- t is the time frame for which the data is used
- δ is known as the scaling factor, also define the width of the confidence band

Anomaly Detection:

The app only considers positive deviation while using the above equation. Thus, if the actual traffic crosses the upper bound of the confidence band only then it is considered an anomaly and recorded in the memory. The upper bound is represented as THRESHOLD variable in the code.

Choosing Model Parameters:

αβγ

When α is close to 1. dampening is quick and the equation responds more to the changes in the current time.

When it is close to 0, this dampening is slow.

We choose α such that MSE (Mean Squared Error) of the actual and predicted value is less.

δ

The reasonable values lies between [2,3] using the statistical distribution theory. For this app,value is 2 to detect anomalies very aggressively for demonstration purposes .

V. CONCLUSION

IDS is a technology that can be use to detect an attack but for future capabilities in IDS can be improved. This System is only detecting ICMP attack and DDOS attack.

VI. ACKNOWLEDGEMENT

We express our gratefulness to our guide, Prof.Dyanaeshwar Dhangar, department of Computer Engineering for all the advice and constant support he has given to us throughout our project work. This job would not have been possible without his support and useful and as well as valuable

REFERENCES

[1] Corinne Lawrence- “IPS – The Future of Intrusion Detection”- University of Auckland - 26th October 2004.

[2] Karthikeyan .K.R and A. Indra- “Intrusion Detection Tools and Techniques a Survey”

[3] Anita K. Jones and Robert S. Sielken –“Computer System Intrusion Detection A Survey “International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010

[4] Vera Marinova-Boncheva-“A Short Survey of Intrusion Detection Systems”-. Bulgarian academy of sciences.

[5] Carl Endorf, Eugene Schultz, Jim Mellander “Intrusion detection & prevention” by Written-published by McGraw-Hill.

[6] “Top 125 Network Security Tools”- SecTools.Org- http://sectools.org/tag/ids/sec

[7] PeymanKabiri and Ali A.Ghorbani-“Research on Intrusion Detection and Response Survey”- International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005

[8] Christopher Low –“Understanding Wireless attacks &detection “-GIAC Security Essentials