Network Intrusion Detection and Prevention techniques for DoS attacks

Suchita Patil, Dr. B.B.Meshram
VJTI, Mumbai, India
Suchitapatil26@gmail.com

Abstract: The Intrusion prevention system is the extension of Intrusion detection system. Network Intrusion Detection and Prevention system works on analyzing the packets coming and going through the interface. The paper illustrates the idea of detecting the DoS Attack. There are many methods available to Detect and avoid the DoS attack. On the network there are many types of DoS attack occurs due to which the service gets interrupted. This paper mainly deals with the DoS attacks.

Index Terms- IDS (Intrusion Prevention System), IPS (Intrusion Prevention System), NIDS(Network Intrusion Detection System)

I. INTRODUCTION

An Intrusion Prevention System is extension of Intrusion Detection System which is made by combining the Intrusion Detection System and Firewall.

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis. [3][3][8]

Signature-based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

Statistical Anomaly-based Detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Stateful Protocol Analysis Detection: This method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity."[3]

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories: signature-based intrusion detection systems and anomaly detection systems. Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers.

1.1 Network IDS or NIDS[3,4]

NIDS are intrusion detection systems that capture data packets traveling on the network media (cables, wireless) and match them to a database of signatures. Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database. One major use of Snort is as a NIDS.

1.2 Host IDS or HIDS[3,4]

Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity. Some of these systems are reactive, meaning that they inform you only when something has happened. Some HIDS are proactive; they can sniff the network traffic coming to a particular host on which the HIDS is installed and alert you in real time.

II. RELATED WORK

As mensioned in the paper[1] efficient adaptive sequential and batch-sequential methods for an early detection of attacks that lead to changes in network traffic, such as denial-of-service attacks, worm-based attacks, port scanning, and man-in-the-middle attacks. These methods employ a statistical analysis of data from multiple layers of the network protocol to detect very subtle traffic changes. The algorithms are based on change-point detection theory and utilize a thresholding of test statistics to achieve a fixed rate of false alarms while allowing us to detect changes in statistical models as soon as possible.

Existing intrusion detection systems (IDSs) can be classified as either signature detection systems or anomaly detection systems (see, e.g., [14]). Signature detection systems detect

attacks by comparing the observed patterns of the network traffic with known attack templates (signatures). If the true attack belongs to the class of attacks listed in the database, then it can be successfully detected and, moreover, identified. Examples of signature-based IDSs are Snort [2] and Bro [23]. Anomaly detection systems compare the parameters of the observed traffic with "normal" network traffic. The attack is declared once a deviation from a normal traffic is observed. Examples of ad hoc anomaly IDSs are MULTOPS [11] and D-WARD [19].

A comprehensive security system consists of multiple tools, including:

• Firewalls that are used to block unwanted incoming as well as outgoing traffic of data. There is a range of firewall products available in the market both in Open Source and commercial products. Most popular commercial firewall products are from Checkpoint (http://www.checkpoint.com), Cisco (http://www.cisco.com) and Netscreen (http://www.netscreen.com). The most popular Open Source firewall is the Netfilter/Iptables (http://www.netfilter.org)-based firewall.

• Intrusion detection systems (IDS) that are used to find out if someone has gotten into or is trying to get into your network. The most popular IDS is Snort, which is available at http://www.snort.org.

• Vulnerability assessment tools that are used to find and plug security holes present in your network. Information collected from vulnerability assessment tools is used to set rules on firewalls so that these security holes are safeguarded from malicious Internet users. There are many vulnerability assessment tools including Nmap (http://www.nmap.org) and Nessus (http://www.nessus.org).

These tools can work together and exchange information with each other. Some products provide complete systems consisting of all of these products bundled together. Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network.

There are some known attacks that are undetectable or difficult to detect; those for which signatures cannot be identified. Examples of these attacks are those with encrypted payloads and those that are polymorphic [5]. MDLC may be effective against polymorphic attacks. This needs to be evaluated.

In paper[7], designed an overlay mechanism for the defense of DDoS attack on converged networks. This defense mechanism consists basically of construction of hierarchical overlay, notification of attack detection, judgment of victims and decision of defense nodes, and notification of traffic detour.

In our approach, we consider the intrusion detection as a data analysis process. Network behaviors can be categorized as normal and abnormal. Due to the sheer volume of real network traffic, both in the amount of records and in the number of features, it is extremely difficult to process all the traffic information before making decisions. Data mining is a powerful tool to analyze the enormous data and extract the most relevant information 171. The task of generating cIassifiers based on rules using genetic algorithms and other evolutionary techniques the condition part of a rule has a tree structure, which is hard to represent with a linear structure. Some approaches to deal with the problem of representing the rules condition part as a h e a r string are discussed in [IO, 61. CTree [SI uses linear representation scheme for evolving the fuzzy rules with complete binary tree data structure. The importance of real-time classification is very crucial in network intrusion detection. A faster and correct classifier can dramatically improve the performance of the IDS. In the approach proposed in paper[9] aims at developing an automated approach for building the IDS kernel - feature extraction and classification. It is extremely difficuIt to process in' real time the large amount of network traffic to detect network attacks and take the appropriate actions. To process the network data in real time, we need to extract the most important data lhat can be used to efficiently detect network attacks. they use information theory to identify the most relevant features to be used in our online analysis of the traffic data.

We then apply data mining programs and genetic algorithm to compute linear classifiers that accurately capture the difference between intrusions and normal activities. Finally, we use the linear classifier with the trained thresholds and coefficients to detect a wide range of network attacks. This approach significantly reduces the need to manually analyze and encode normal usage profiles and intrusion models.These classifiers can be more effective because they are computed and validated using large amount of audit data.

Diffeireint types of network attacks are as shown bellow:

Table 1. Classes of Atatcks[9]

Class	Attacks
DoS	Back, land, neptune, pod, smurf, teardrop
U2R(unauthorized access to local superuser (root) privileges)	Buffer-overflow, loadmodule, ped, rootkit
R2L	ftp-write, guess-passad, imap, multihop. phf, spy, warezclient, warezmaster
PROBE	Ipsweep, nmap, portsweep, satan

SVM [10] is a machine learning method based on the statistical learn ing theory , the key point of its is to improve the generation ability of the learning machine according to the Vapnik structural risk minimization principle, namely obtain small err ors according to the limited training sets sample, and ensure the independent test sets keeping small errors. Moreover, the SVM algorithm is a convex optimization problem. Thus the local optimal solution must be the global optimal solution which other algorithms can not achieve. It can also used in the limited sample data and not be sensitive to data dimensions. Therefore, SVM is adapted to the intrusion detection field high dimension heterogeneous imbalance data set character, and it can be applied to intrusion detection.

III. DISCUSSION

For many platforms different firewalls are present like for Linux IPTable firewall is inbuilt firewall present which has to be accordingly by writing rules. It is rule-based Intrusion Prevention System. Same way for windows Net defender, WIPFW (windows firewall) which is based on BSD firewall ipfw. By writing ipfw rules the network or the system can be protected. There are two types of IDS one is Network Intrusion Detection System and other is Host based Intrusion Detection System. Network Intrusion Detection System tries to identify the malicious activity by monitoring the incoming and outgoing network traffic.

The following figure-1 shows the methods to detect the types of DoS attacks. To detect the attacks or malicious traffic on the network first step is to capture the packets. There are two types of mode present to capture the packet one is normal in that the packets intended to the system are only captured by the system. And other is Promiscuous mode in which every packet which is going through the interface is captured by the system. So to monitor the network traffic the system has to be operated in promiscuous mode.

In every NIDS or NIPS the overall architecture contains the following units.

1. Packet Sniffer unit: this unit captures the packet from the interface either in promiscuous mode or in normal mode. Promiscuous mode is explained above.
2. Intrusion Detection or Pre processing engine: in this unit it uses the different approaches to detect the attack depending on flow based analysis or protocol based analysis.
3. Countermeasures : in this the packets which contains the malicious code or if any abnormal flow of packets is observed the the particular action is selected to avoid the intruder to enter in to the network.

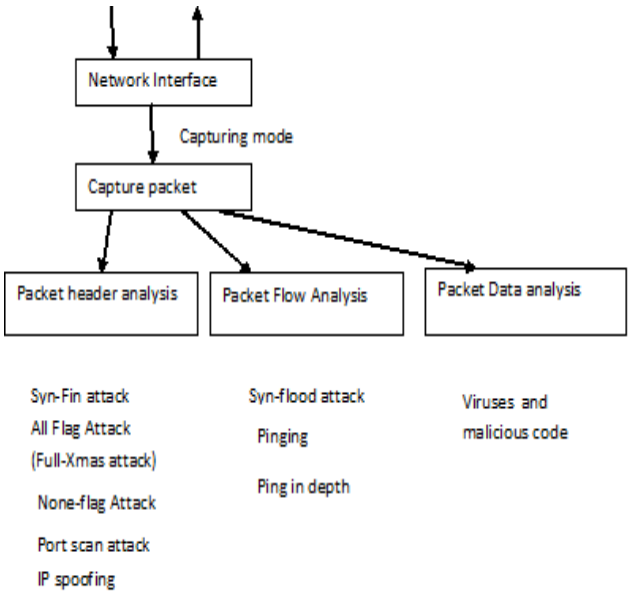

Figure-1 types of DoS attacks.

Flow based Analysis: A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties.

The common properties are like Source IP address, destination Ip address, Source port and Destination port, and protocol. Using these common properties the flow direction can be determined and type of protocol it can be determined whether the traffic is normal or abnormal traffic.

the FIN or RST flags have been seen in a TCP flow. The packets which are coming and going for them the information related to sampling is stored and using probabilistic approach and the threshold the DoS attack is detected. For example the no of Syn packets are counted and if the number of syn packets are more than 20 per second then the Syn flood Attack is detected, 20 is the threshold value. and all the packets are dropped for the src_ip. Combination of random sampling and normal sampling is used to detect the flood attack.

The techniques which are used to detect the attacks in NIDS uses statistical approach and probabilistic approach and Information theory. Probabilistic approach is easy to implement because in the firewall rules itself we can specify the probability and threshold for dropping that packet or allowing that packets in the network. Like in ipfw rules we can mention the probability eg. *ipfw 0.5 deny from any to any TCP*

In the above rule it checks the probability 0.5 if it is greater than that then perform the action deny(drop) TCP packets coming from any to any.

IV. CONCLUSION

The Network Intrusion System Based on Dataminning takes the time to train the system and Also It does lot of processing to be performed backend to detect the attack and prevent it. The Signature based method are effective but it can not detect the new attacks. Main source of attack on the network is DoS attacks and then gather the required information form the network. The DoS attack can be detected by analysing of incoming packet and outgoing packets. Data mining approach requires lot of processing on the data where as the statistical and probability approach requires less processing than the data mining approach. the intrusion prevention module of network intrusion prevention system which bases on intrusion detection system Snort_inline and Netfilter firewall of IPtables and improved the possibility of its function Intrusion prevention system provides real time and active prevention ability, prevents the attack effectively and assures the normal data stream. Because of the character of intrusion prevention system, it could only be connected in the network is series. This kind of connection position could lead to potential problems. Utilizing SVM in Snort intrusion detection system, reduces the rate of miss and error report, and needs little rules. Which makes Snort combines with firewall can improve the defensive ability of the system, and makes the IPS very intelligent.

To execute the firewall on windows the WIPFW can be used at the place of netfilter. IPFW is same as iptable in linux.

REFERENCES

[1] A Alexander G. Tartakovsky, Boris L. Rozovskii, Rudolf B. Bla˘zek, and Hongjoong Kim, "A Novel Approach to Detection of Intrusions in Computer Networks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 54, NO. 9, SEPTEMBER 2006

[2] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th Syst. Admin. Conf. (LISA), 1999, pp. 229–238.

[3] Rafeeq Ur Rehman, "Intrusion Detection Systems

[4] with Snort", 2003 Pearson Education, Inc. Publishing as Prentice Hall PTR Upper Saddle River, New Jersey 07458 pp 2-3,7-8

[5] Kai Hwang,, Min Cai, Ying Chen, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 4, NO. 1, JANUARY-MARCH 2007

[6] E. Earl Eiland, Scott C. Evans, T. Stephen Markham, Bruce Barnett, "NETWORK INTRUSION DETECTION: USING MDLCOMPRESS FOR DEEP PACKET INSPECTION", 978-1-4244-2677-5/08/$25.00 ©20081EEE

[7] Karen Scarfone Peter Mell ,"Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007)

[8] Mihui Kim, Inshil Doh and Kijoon Chae , "Defense Mechanism using Overlay against DDoS Attacks on Converged Networks", Feb. 12-14, 2007 ICACT2007

[9] Shikha Goel , Sudesh Kumar , "An Improved Method of Detecting Spoofed Attack in Wireless LAN", 2009 First International Conference on Networks & Communications 2009 IEEE

[10] Tao Xia, Guangzhi Qu, Salim Hariri , Mazin Yousif , "An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm", 0-7803-8991-3l051$20.00 0 2005 IEEE

[11] Hui Li, Dihua Liu , "Research on Intelligent Intrusion Prevention System Based on Snort", 2010 Intern ational Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE)