International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Overview of Denial-of-Service Attack and Statistical Detection Techniques

Sanjivani Sumant [1]
[1] ME (II[nd] year), Department of IT,
R. M. D. Sinhgad School of Engineering,
Maharashtra, India

Prof. Sweta Kale[2]
[2] Assist. Professor, Department of IT,
R. M. D. Sinhgad School of Engineering,
Maharashtra, India

Abstract:- **Network Security plays a vital role in the field of Information Security. The number of attacks like Denial-Of-Service, Spoofing, Phishing, and Man-in-Middle violate the information security of the organisation. CIA Triangle-Confidentiality, integrity & availability are the important aspects in the network security. Denials of Service (DoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. These different types of DoS attacks severely degrade the availability of a victim, which can be a host, a server, a router, or an entire network. They impose exhaustive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. The victim can be forced out of service from a few minutes to even several days. This results in serious damages to the services running on the victim. Effective detection of DoS attacks is essential to the protection of online servers. Work on DoS attack detection mainly focuses on the development of network-based detection mechanisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. The Intrusion detection system monitors the network traffic and extract the features which are directly associated with DoS attacks. Based on these features, the statistical traffic Analysis has been done to detect and prevent the attack. There are different Statistical analysis methods which are discussed in this paper. The statistical analysis helps to detect the DoS attacks on real time traffic and thus can save the online servers from various types of DoS attacks.**

Key Words: Security, CIA triangle, DoS, victim, vulnerability, attack, statistical techniques

1. INTRODUCTION

Network Security plays an important role in the field of Information Security. There are many types of Network attacks which can violate the security of the servers which are attached to the network. The most important type of attack is the DoS i.e Denial of Service attack and DDoS i.e. Distributed Denial of Service attack. It is one type of aggressive attack which can severely degrade the performance and availability of the system which can further stops the working of the host, Server or entire network. In this type of attack , an attacker floods the large amount of useless packets or can impose the exhaustive computational tasks by exploiting the system's vulnerability.
This can force the system out of service for several days.

To detect the DoS attack is the major challenge. There exists different Network Intrusion detection system which can detect the intrusions in the network .
Generally, network-based detection systems can be classified into two main categories, namely, misuse-based detection systems [1] and anomaly based detection systems [2] .
Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. Misuse-based detection system have high detection rates to known attacks and low false-positive rates and are easily evaded by any new attacks and even variants of the existing attacks. In addition, it is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise.
Anomaly-based detection system monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects. Anomaly-based detection systems are capable of detecting zero-day intrusion that can exploit the system vulnerabilities. Also this system need not be updated regularly as misuse- based detection system.
These anomaly-based IDS are also known as behavioural based IDS or statistical based IDS. Statistical analysis observes the packets on the network and based on the analysis detect the attack.
This paper concentrates on different statistical approaches used in Network Intrusion Detection System.

2. ATTACK RECOGNITION

There are various common attacks such as brute force attacks, spoofing, phishing, denial Of Service, and man-in-the–middle attack [7]. Some of them are discussed below:

2.1 Brute force attack

It can be defined as trying every possible combination until the correct one is identified. The attacker usually tries handful number of combinations possible to exploit or to gain access into a system or a network. To overcome this, one can deploy IDS to watch the suspicious activity or set a lockout threshold [7].

2.2 Phishing

Phishing is a more popular type of social engineering attack through which attacker can obtain personal information, credentials, credit card no., or financial data. The attacker, thus phishes for sensitive data through different methods. With this personal information, phisher can create new accounts in the victim's name, gain authorized access to bank accounts and make illegal credit card transactions [7].

2.3 Man-in-the-Middle attack

In Man-in-the–Middle attack, attackers monitor the packet from network, modify it and insert them back into the network. It allows the attacker to eavesdrop as well as to change, delete, add and divert data[8].

2.4 Spoofing

Spoofing is a technique used to gain unauthorized access to computers where in truder sends a message with a source IP address that has been forged to indicate that the message are coming from a trusted host. In IP spoofing hackers use variety of techniques to obtain trusted IP address and then modify the packet headers to insert the forged IP address [8].

2.5 DoS

It is Denial of Service attack, in which the attacker continuously try to access the information through the particular service or port until it gets blocked [8]. Due to DoS attacks the system can become unavailable for a specific period of time. This is dangerous for the critical online servers like web servers, production and application servers. Alternately, servers could also be space-attacked by exhausting their bandwidth or connection buffers with lot of bogus packets/requests.

Distributed Denial of Service (DDoS) attacks are a scaled form of DoS attacks where multiple attacks are employed in a coordinated fashion to form an attack network for attacking a specific target.

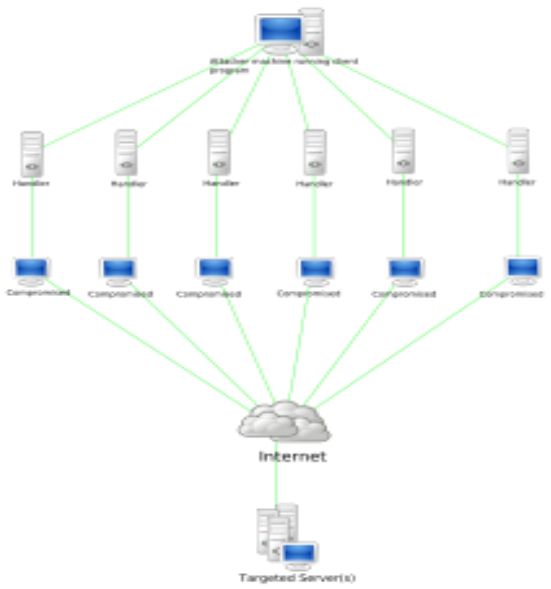

Fig -1: Distributed Denial Of Service Attack

Different types of DoS attacks are discussed below [6]:

1. Teardrop – It is a program which sends IP fragments to the machine over the internet or Network.

2. Smurf Attack – It is a distributed DoS attack in which large number of ICMP packet are generated by Victim's spoofed source IP . Most of the devices on the network respond to this source IP . If number of machines In the network which will respond to these packet is large then Victim's machine will be flooded with the traffic.

3. POD (Ping Of Death) – This type of attack involves malicious ping to the computer. This attack occurs because of large sized ping packet. Because of Ping flooding victim floods so much of ping traffic such that normal traffic fails to reach the system.

4. SYN Flood or Neptune Attack – TCP performs three way handshaking for connection establishment between client and Server. For this TCP will exchange SYN,SYN-ACK and ACK messages between client and server. If one of the system is compromised, then there can be a possibility of half open TCP connection. Usually there is a timeout associated with a pending connection, there can be half-open connections will eventually expire and the victim server system will recover. Still, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections. Within some cases, the system may exhaust memory or crash.

5. LAND (Local Area Network Denial) – This attack sends a special poison spoofed packet to a computer, causing it to lock up. The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. This forces the machine to reply to itself continuously.

6. Internet Worms – The automated scripts are propagated through internet and the effect of such high rate of scanning and propagation caused a DoS effect to many network devices and consumed high bandwidth. As the source came from various IP addresses, it was impossible to prevent the packets by analyzing only the header . Some form of content filtering was necessary to stop the traffic from further penetrating in or out of networks.

3. PREVENTION OF ATTACKS

To secure our network from such kind of attacks, certain skills must be practiced:

3.1 Hardening of Network Devices

Network devices deployed in the network must be hardened to prevent them an unauthorized access the routers, switches, and firewalls must be configured in such a way that intruder or hacker could not able to access these devices.

1. Default user names and passwords must be disabled
2. Telnet access should be allowed from authorized machines only otherwise denied.
3. Access control list –routers and firewalls should be configured to filter the packets accurately and efficiently by passing or dropping packets based on IP address and port address.
4. Unused services must be blocked.
5. Access through AAA- AAA stands for Authentication, Authorization & Accounting which must be configured in network so that each network device can be accessed through Tacacs or Radius servers so that proper authentication and authorization takes place and accounting of the network devices can be obtained which can be useful as a audit trail. Password management can be achieved through AAA server.

3.2 Firewall

Firewalls are used to restrict access to one network to another. Most companies use firewalls to restrict access to their network from internet or to restrict one internal segment from accessing another network segments. The firewall can give more defined and granual security policy through which the services are allowed to be accessed from the systems with authorized IP addresses. Ideally communication should flow through the firewall where traffic is inspected and restricted.

Firewall may be a router, server or specialized hardware device. Special skills are needed to configure the firewall according to requirements of security policy. Access –lists are needed to configure to allow or to restrict the access. Network address Translation can configured on the firewall to hide the internal IP addresses through outside.

3.3 High redundancy and High availability

In order to prevent a network from falling trap into a DoS attack it is crucial to design the network as such that there is not a single point of failure. However, such high availability will incur additional cost, especially in maintaining dual connection to the Internet. It is also required that ISPs provide load balancing on the upstream router to load share the redundant link.

3.4 IDS/IPS

IDS (Intrusion Detection System) are designed to the security bridge. It is the system that takes care of detecting an unauthorized use of, attack upon a computer, network or telecommunication infrastructure. IDS are designed to mitigate the damage that can be caused by hacking. There are two types of IDS: Network based , which monitors network communication and Host based, which can analyze the activity within a computer system.IDS can be configured to watch the attacks, update the administrators for the attacks, protect the system files [7].

IPS(Intrusion Prevention System) which not only detects that something bad is taking place but also prevents the traffic to gain access to the target. So, IPS is the preventive and proactive technology and IDS is a detective and after the fact technology [7].

The ideal solution with respect to DoS and DDoS attacks would be to differentiate between good and bad packets (alternately, connections, sessions, flows, etc.,) in a network.

Some techniques should be there to differentiate between the normal packet and attacked packet. Certain characteristics of normal traffic can be tapped to differentiate them from attack traffic, in this manner letting us differentiate between attack and normal "states" of the network (rather than differentiating packets). For instance, a well researched result suggests that incoming source IP addresses could be a good candidate for detecting normal traffic and attack traffic respectively. But in case of DDoS attacks scanning of source IP address is not sufficient, other parameters like port number can also be traced.

4. DOS ATTACK DETECTION TECHNIQUES

DoS attack detection techniques are basically of two types, Signature based IDS and Statistical based IDS.

Signature based IDS contains the signatures which can be used to detect the malicious traffic. There is administrative overhead as these signatures need to be updated regularly to detect latest attacks.

Statistical based IDS monitors the packets in the network. It captures variety of possible patterns for the legitimate traffic. Any deviation from these patterns can help to detect the attack.

Some of the classification models are discussed below:

4.1 Hidden Marcov Model (HMM)

This has been used for modeling the network traffic for TCP, for detecting intrusions in the form of anomalies.

The HMM is represented with the help of two components – number of states (N), and the number of observables (M) at each state. The HMM starts with a finite number of states. Transitions among states are managed by a set of probabilities called transition probabilities, which are linked with each state. In a particular state, an outcome or observation can be generated according to a state probability distribution associated with the state. It is only the result, not the state, which is noticeable to the observer. As the states are hidden to the outside world, the name Hidden Markov Models.

The Markov model used here is a first layer model, which means that the probability of being in a state depends on the previous state. One of the goals of using an HMM is to deduce from the set of emitted observables the most likely path in state space that was followed by the system.

4.2 Multivariate Correlation Analysis

The idea is to differentiate between normal and attack traffic by considering the correlation between possible pairs of chosen features among a set of features f1 . . . fp at different intervals, and the distance of the formed correlation matrix with the average of correlation matrices seen during training. The features can be separated in the TCP field and show the effectiveness of the method under these conditions. The solution is a target end solution [4].

4.3 Markov Models (MM)
Simpler models with lesser number of computations in comparison with HMMs. However, an optimal number of states has to be developed on the fly per user site, which makes it unsuitable for practical implementation.

4.4 Natıve Bayes (NB) Classifiers
Simplest of the models and ideally suited for the DoS problem, given it's nature of allowing for simplified independence assumptions and the inherent nature of the DoS detection problem, which lets us make such assumptions.
It works on the basis of Bay's theorem which is used find the probability of the unknown things from certain known parameters. A Natıve Bayes classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature. This Natıve Bay's classifier works with small amounts of training data, and can also accommodate a large number of attributes makes them a good choice for network modelling for DoS attacks.

4.5 C4.5 Decision Tree Classifier
C4.5 generates decision tree from the set of training data on the concept of information entropy. At each node of the tree, C4.5 chooses one attribute of the data that most effectively splits it from one class to other [3].

4.6 Decision Table Classifier
This classifier belongs to the category of deterministic classifiers. This method simplifies the training set and creates a set of logic decision over the attributes to determine the class [3].

5. TRAFFIC ANALYSIS

The behavior of different classifiers can be analyzed by using the Training data sets which are publically available. Some of the datasets are

5.1 Datasets
Weka (Waikato Environment for Knowledge Analysis)
Weka is a data mining software that is written in Java and developed at University of Waikato, New Zealand. The software is open source available.

DARPA 98
DARPA evaluation dataset is used for the purpose of training as well as testing the intrusion detectors. The attacks fall into five main classes, Probe, Denial of Service (DoS), Remote to Local(R2L),User to Remote(U2R) and the Data attacks. The DARPA 1999 test data consisted of 190 instances of 57 attacks which integrated 37 Probes, 63 DoS attacks, 53 R2L attacks, 37 U2R/Data attacks [5].

KDD Cup 99
KDD'99 has been the most wildly used data set for the evaluation of anomaly detection methods. It contains both train and test sets. In this dataset three types of legitimate traffic (TCP, UDP and ICMP) and six different types of DoS attacks (Teardrop, Smurf, Pod, Neptune, Land and Back) are available [5].

5.2 Application Classes
The data sets have been divided into a number of application classes.
For the TCP data set, a total of 13 application classes are present.

1. ADMIN
2. ATTACK
3. BULK
4. CHAT
5. DATABASE
6. GAMES
7. INTERACTIVE
8. MAIL
9. MULTIMEDIA
10. P2P
11. SERVICES
12. VOIP
13. WWW

5.3 Statistical Analysis of Packet Behavior
Statistical Analysis has been performed over the training data sets. The analysis extracts the key statistical properties of the training data set [3].
For analysis the packet attributes need to be considered. Some of the attributes are

1. Port Number (Server)
2. Port Number (Client)
3. Data Packets in the Flow
4. Pushed Data Packets (Client)
5. Pushed Data Packets (Server)
6. Minimum Segment Size
7. Average Segment Size
8. Initial Window (Client)
9. Initial Window (Server)
10. Total Number of RTT Samples
11. Median of bytes in IP packet
12. Variance of bytes in Ethernet packet
13. Application Class

5.4 Efficiency Analysis
The classifier efficiency is evaluated against the parameters which are mentioned below [3].

1. True Positive Rate (TPR)
True Positive Rate (TPR) is defined as the rate at which the flow is correctly classified as an application class.

2. True Negative Rate (TNR)
True Negative Rate (TNR) is defined as the rate at which the flow is correctly classified as not an application class.

3. False Positive Rate (FPR)

False Positive Rate (FPR) is defined as the rate at which the flow is incorrectly classified as an application class.

4. False Negative Rate (FNR)

False Negative Rate **(**FNR) is defined as the rate at which the flow is incorrectly classified as not an application class.

All these four factors together determine the accuracy of the classification algorithm.

CONCLUSION

As Denial Of Service attack one type of aggressive and menacing intrusive behavior to online servers. These different types of DoS attacks severely degrade the availability of a victim, which can be a host, a server, a router, or an entire network. We have studied and taken an overview of different types of DoS attacks, prevention techniques used for mitigating DoS attacks, the availability of the datasets for testing and analyzing DoS attacks

ACKNOWLEDGEMENT

We would like to thank our H.O.D. Prof. Dhara T. Kurian for her precious contribution and extended support.

REFERENCES

[1] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, pp. 2435-2463, 1999.
[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques,Systems and Challenges," Computers and Security, vol. 28, pp. 18-28, 2009.
[3] Muzammil, M.J.; Qazi, S.; Ali, T., "Comparative analysis of classification algorithms performance for statistical based intrusion detection system," Computer, Control & Communication (IC4), 2013 3rd International Conference on , vol., no., pp.1,6, 25-26 Sept. 2013
[4] Zhiyuan Tan; Jamdagni, A.; Xiangjian He; Nanda, P.; Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, pp.447,456, Feb. 2014
[5] M. Tavallaee, E. Bagheri, L. Wei, and A.A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," Proc. IEEE Second Int'l Conf. Computational Intelligence for Security and Defense Applications,pp. 1-6, 2009.
[6] http://en.wikipedia.org/wiki/Denial-of-service_attack
[7] CISSP All in one study Guide, 6th Edition ,Shon Harris, Publisher: McGraw-Hill Osborne Media Date: 2012
[8] Principles of information security, 4th Edition, Michael E. Whitman, Herbert J. Mattord

BIOGRAPHIES

Completed B.E.(Elect.) from Shivaji University. Pursuing M.E.in Information Technology from Savitribai Phule Pune University.Having 15 years of experience in Networking and security. Working in CMC Ltd, Pune.

Completed B.Tech.(CSE) from SNDT ,Mumbai and completed M.Tech.(CSE) from University of Nagpur. Currently working as Assistant Professor at R.M.D.Sinhgad College Of Engineering.