Intrusion Detection System to Detect Bandwidth Attacks

Sanket Lokhande, Akshay Bhaskarwar,Sujata Bhaskarwar,Sadhana Chidrawar

Hyundai Mobis Research and Development Pvt. Ltd

Hyderabad, India

ABSTRACT

This paper focuses on theoretical and practical methods for detecting bandwidth attacks upon networks and sites. Comparison of existing methods used in traditional networks, as well as discussion of a new method for detecting attacks is presented. Advantages and limitations of few of methods are considered. Attack Detection helps to plan a security monitoring system on Linux based networks that can detect attacks that originate from internal and external sources. The main aim of a security monitoring system is to identify unusual events on the network that indicate malicious activity or procedural errors. Security monitoring provides two primary benefits for organizations of all sizes: the ability to identify attacks as they occur, and the ability to perform forensic analysis on the events that have occurred before, during, and after an attack.

1. DENIAL-OF-SERVICE ATTACK (DOS)

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the IAB's (Internet Architecture Board) Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

2. WHAT IS A DISTRIBUTED DENIAL OF SERVICE ATTACK?

As Defined by the World Wide Web Security FAQ: A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms. Typically a DDoS master program is installed on one computer using a stolen account. The master program, at a designated time, then communicates to any number of "agent" programs, installed on computers anywhere on the internet. The agents, when they receive the command, initiate the attack. Using client/server technology, the master program can initiate hundreds or even thousands of agent programs within seconds.

Figure below depicts the typical DDoS architecture.

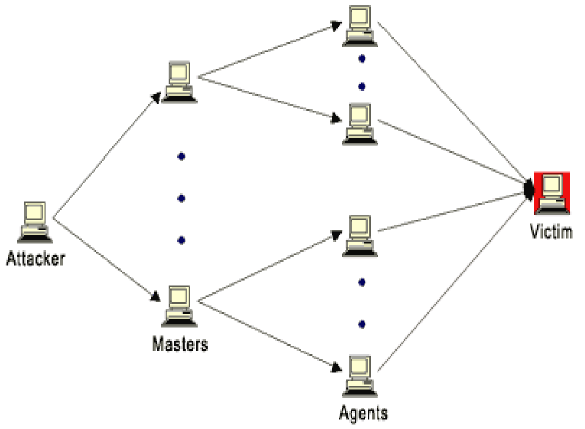

Figure 1: DDoS Architecture

2.1 Types of DDoS Attacks

DoS attacks can be classified into two main categories:

2.1.1 Flood attacks

A remote system is overwhelmed by a continuous flood of traffic designed to consume resources at the targeted server (CPU cycles and memory) and/or in the network (bandwidth and packet buffers). These attacks result in degraded service or a complete site shutdown.

2.1.2 Logic or software attacks

A small number of malformed packets are designed to exploit known software bugs on the target system. These attacks are relatively easy to counter either through the installation of software patches that eliminate the vulnerabilities or by adding specialized firewall rules to filter out malformed packets before they reach the target system.

2.2 DoS Shortfalls

- DoS attacks are unable to attack large bandwidth websites – one upstream client cannot generate enough bandwidth to cripple major megabit websites.
- New distributed server architecture makes it harder for one DoS to take down an entire site.
- New software protections neutralize existing DoS attacks quickly
- Service Providers know how to prevent these attacks from affecting their networks.
- "Old" Internet Technology – something new needs to take its place (Hackers want the challenge of a new technology).

2.3 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

2.3.1 Types of intrusion detection systems

For the purpose of dealing with Intrusion Detection mechanism in IT industries, there are two main types of IDS:

2.4 Network intrusion detection system (NIDS)

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensor captures all network traffic and analyzes the content of individual packets for malicious traffic. An example of a NIDS is Snort.

2.5 Host-based intrusion detection system (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category.

Intrusion detection systems can also be system-specific using custom tools and honeypots. In the case of physical building security, IDS is defined as an alarm system designed to detect unauthorized entry.

For the purpose of protecting perimeters of critical infrastructures and high risk assets, there is a primary type of IDS:

2.6 Perimeter Intrusion Detection System (PIDS)

Detects and pinpoints the location of intrusion attempts on perimeter fences of critical infrastructures. Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence, and this signal is monitored and if an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.

2.7 Statistical anomaly and signature based IDS

All Intrusion Detection Systems use one of two detection techniques:

2.8 Statistical anomaly-based IDS

A statistical anomaly-based ID establishes a performance baseline based on normal network traffic evaluations. It will then sample current network traffic activity to this baseline in order to detect whether or not it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm will be triggered.

2.9 Misuse or Signature-based IDS

Network traffic is examined for preconfigured and predetermined attack patterns known as signatures. Many attacks today have distinct signatures. In good security practice, a collection of these signatures must be constantly updated to mitigate emerging threats.

There are actually two main intrusion detection approaches for attack: the behavioral approach (also called anomaly detection) and the signature analysis (also called misuse detection).

Both misuse detection and anomaly detection have advantages and disadvantages. At present, the intrusion detection system is developed by using these two technologies in conjunction with one another, but there is not an effective method to evaluate the intrusion detection systems collaborative detection's performance. It is necessary to analyze it by establishing a strictly mathematical assessment equation. Considering the information theory method to analysis this problem, the intrusion detection capability can be used to analysis and evaluation. By contrast two intrusion detection systems, it turns out, the system that based on misuse and anomaly collaborative detection has the better detection effects.

Anomaly detection is based on statistical description of the normal behavior of users or applications. The misuse detection is based on collecting attack signatures in order to store them in a database. The intrusion detection system (IDS) then parses audit files to find patterns that match the description of an attack stored in the database. The main goal of intrusion detection system is to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. At present, the intrusion detection system has the high false negative rate; this has always been a major problem to the IDS user. The intrusion detection system mainly has two detection technologies: misuse detection and anomaly detection. Can collaborative detection improve the performance of IDS? Such as, raise the detection rate, reduce the false positive rate. I also want to know how to evaluate two intrusion detection system collaborative detection's performance? [15] [16] [17] [18] [19].

2.9.1 Misuse detection:

use patterns of well-known attacks to identify intrusions

- Record the specific patterns of intrusions
- Monitor current audit trails (event sequences) and pattern matching
- Report the matched events as intrusions
- Representation models: expert rules, Colored Petri Net, and state transition diagrams, etc.

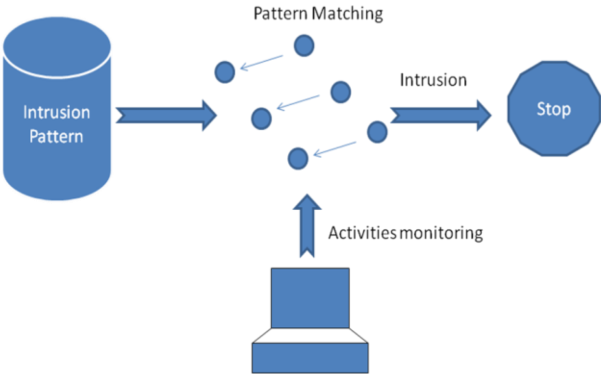

Fig.5. Misuse Detection

2.9.2 Anomaly detection:

use deviation from normal usage patterns to identify intrusions

- Establishing the normal behavior profiles
- Observing and comparing current activities with the (normal) profiles
- Reporting significant deviations as intrusions
- Statistical measures as behavior profiles: ordinal and categorical (binary and linear)

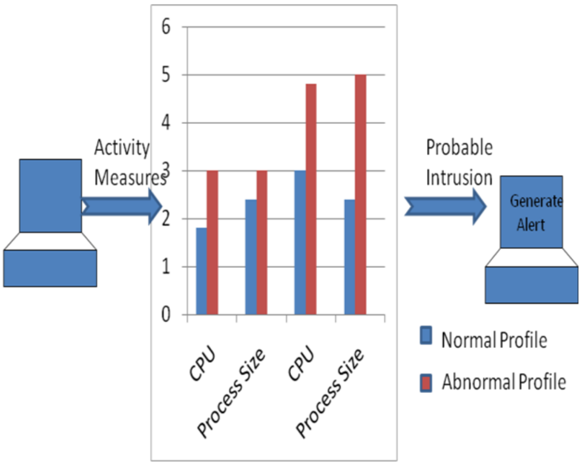

Fig.6. Anomaly Detection

3. Detecting DoS Attack: IP Traceback

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for Denial Of Service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack. The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path.

3.1 Packet-to-reply ratio for TCP, UDP and ICMP:

Many network communications exhibit two-way communication patterns. Aggressive one-way traffic on a protocol or application that is expected to exhibit two-way communication pattern is regarded as a sign of an attack. For example, legitimate TCP traffic should invoke acknowledgments every few packets. If the flow of acknowledgments subsides (e.g., because the destination is under a DoS attack) legitimate traffic will take this as indication of congestion and will reduce its sending rate. Persistent one-way TCP traffic is thus anomalous and regarded as a sign of an attack. To detect aggressive one-way traffic we count the number of TCP, ICMP or UDP (DNS) packets sent and received on a connection and calculate their ratio. We smooth this ratio by calculating its weighted average over time to produce a stable measure that does not oscillate with short traffic bursts. If the increase in the ratio is consistent, it will exceed some given threshold in the end and we will detect the attack. Otherwise, it is only one-time fluctuation; exponentially weighted average will smooth this anomaly and will not produce false alarms. A connection whose ratio exceeded the threshold is considered malicious and all its packets are classified as attack.

3.2 Algorithm:

We harvest traffic traces and look for particular combinations according to the signature based attack detection and find relative impact on the bandwidth for specified amount of time for each packet combinations. Mathematical equations we considered as follows

```
if [Source ip ($\beta$) ] € (completed tcp connection table)
        discard $\beta$
      elseif
              for all same source ip ($\beta$)  Є packet (p)

                $\alpha = \frac{\Sigma \text{ icmp / udp / tcp-syn}}{\Delta}$

              where $\Delta$= time duration

        $\alpha > \theta$    $\theta$ =  threshold

      update attack table with p Є attack packet
```

4. CONCLUSION

In this paper, implementation of Attack Detection Algorithm based on the Decision Tree Algorithm on node computer of the network is shown. In it we have implanted the joined efforts of Signature based and Anomaly based feature selection called as Hybrid Algorithm in real time monitoring and the results were better than using single algorithm based IDS.

5. REFERENCES

[1] Matthew V. Mahoney and Philip K. Chan, “PHAD: A Packet Header Anomaly Detection for Identifying Hostile Network Traffic”, Department of Computer Science Florida Institute of Technology Melbourne, Technical Report # CS-2001-04

[2] S.Karthik, Dr. V.P.Arunachalam, and Dr. T.Ravichandran, “An Analysis of DDoS Attack Methods, Threats, Tools and Defense Mechanisms”

[3] Krishnamurthy, B., Sen, S., Zhang, Y., and Chen, Y. “Sketch-based change detection: methods, evaluation, and applications”, In Proceedings of the conference on Internet measurement conference (2003), ACM Press, pp. 234{247.

[4] Barford, P., Kline, J., Plonka, D., and Ron. A. A; “Signal analysis of network traffic anomalies”, In Proceedings of ACM SIGCOMM Internet Measurement Workshop (Nov. 2002).

[5] Jelena Mirkovic, Janice Martin and Peter Reiher, “A taxonomy of DDoS Attacks and DDoS Defense Mechanisms”, Computer Science Department, University of California, Los Angles, Technical Report #020018

[6] Tao Peng, Christopher Leckie and Kotagiri Tamamohanarao, “Survey of Network-Based Defence Mechanisms Countering the DoS and DDoS Problems”, Department of Computer Science and Software Engineering, The University of Melbourne, Australia.

[7] C. Chen, S. Mabu, C. Yue, K. Shimada and K. Hirasawa; “Network Intrusion Detection using Fuzzy lass Association Rule Mining Based on Genetic Network Programming”, In Proc. of the IEEE InternatinalConference on Systems, Man and Cybernetics, 2009 (Submitted).

[8] Gaojun; “Artificial neural network theory and simulation test”, Beijing Machinery Industry Press 2003.

[9] Y. Wang, X. Wang, D. Wang, and D. P. Agrawal; "Localization algorithm using expected hop progress in wireless sensor networks", in the Third IEEE International Conference on Mobile Ad hoc and Sensor Systems (Mass), October 2006.

[10] YU-XIN DING, MIN XIAO, AI-WU LIU Key Laboratory of Network Oriented Intelligent Computation; “RESEARCH AND IMPLEMENTATION ON SNORT-BASED HYBRID INTRUSION DETECTION SYSTEM”, Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009.

[11] Thomer M. Gil and Massimiliano Poletto, “MULTOPS: A Data structure for bandwidth attack Detection” , Vrije University, Amsterdam, The Netherlands and M.I.T., Cambridge, MA, USA

[12] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Network Support for IP Traceback”, IEEE/ACM Trans. Net., vol. 9, no. 3, June 2001, pp.22637.

[13] A. Belenky and N. Ansari, “On IP Traceback”, IEEE Communication Magazine, July 2003, pp.142-153.

[14] J. Mirkovic and P. Reiher, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”, ACM SIGCOMM Computer Communications Review (CCR), vol. 34, no. 2, April 2004, pp.39-54.

[15] Rocky K. C. Chang, “Defending against Flooding-Based Distributed Denial-od-Service Attacks”, A Tutorial, IEEE Communication Magazine, Oct. 2002, pp.42-51.

[16] Min Cai, Kai Hwang, Yu-Kwong Kwok, Shanshan Song, and Yu Chen, “Collaborative Internet Worm Containment”, IEEE Security and Privacy, May/June, 2005, pp. 25.-33.

[17] M. E. Locasto, J. J. Parekh, A. D. Keromytis, and S. J. Stolfo, “Toward Collaborative Security and P2P Intrusion Detection”, IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2005, pp. 333-339 http://www.tcpdump.org/tcpdump_man.html

[18] Saad, Radwane; Nait-Abdesselam, Farid; Serhrouchni, Ahmed, “A collaborative peer-to-peer architecture to defend against DDoS attacks Local Computer Networks”, 2008. LCN 2008. 33rd IEEE Conference on 14-17 Oct. 2008 Page(s):427 - 434.

[19] I. Stoica, R. Morris, D. Nowell, D. Karger, M. Kaashoek, F. Dabek and H.Balakrkshnan, “Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications”, IEEE/ACM Transactions on Networking, Vol.11, No. 1, February 2003.

[20] http://www.snort.org

[21] http://bro-ids.org

[22] S. Roberison. E. Siegel, M. Miller, and S. Stolfo, “Surveillance Detection in High Bandwidth Environments”, in 2003 DARPA DISCEX III Conference, April 2003.

[23] B. H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communication of ACM, Vol. 13, pp. 422-426, July 1970.

[24] Erinc Arikan, "Attack Profiling for DDOS Benchmarks" A thesis submitted to the Computer and Information Sciences Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science with a major in Computer Science : Summer 2006.

[25] http://netdefender.codeplex.com/

[26] http://www.grc.com/securitynow.htm

[27] http://www.caida.org.

[28] http://sourceforge.net/projects/barnyard/

[29] Martin Roesch "Snort Documentation" Official Documentation of snort by its author for its use as a Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS)