Anomaly Detection of IP Header Threats

S.H.C. Haris shajar_charis@yahoo.com
School of Computer and Communication Engineering,
University Malaysia Perlis (UniMAP),
Kangar, Perlis

Dr.Ghossoon M.Waleed Al-Saadoon ghowaleed2004@yahoo.com
College of Administrative Sciences,
Applied Science University
Kingdom of Bahrain, Manama, Jufair, P.O.Box:5055
Tel: + (973) 17728777- 149, Fax: + (973)17728915

Ass.Prof.Dr.R.B. Ahmad badli@unimap.edu.my
School of Computer and Communication Engineering,
University Malaysia Perlis (UniMAP),
Kangar, Perlis

M.A.H.A. Ghani alifhasmani@unimap.edu.my
School of Computer and Communication Engineering,
University Malaysia Perlis (UniMAP),
Kangar, Perlis

Abstract

Threats have become a big problem since the past few years as computer viruses are widely recognized as a significant computer threat. However, the role of Information Technology security must be revisit again since it is too often. IT security managers find themselves in the hopeless situation of trying to uphold a maximum of security as requested from management. At the same time they are considered an obstacle in the way of developing and introducing new applications into business and government network environments. This paper will focus on Transmission Control Protocol Synchronize Flooding attack detections using the Internet Protocol header as a platform to detect threats, especially in the IP protocol and TCP protocol, and check packets using anomaly detection system which has many advantages, and applied it under the open source Linux. The problem is to detect TCP SYN Flood attack through internet security. This paper also focusing on detecting threats in the local network by monitoring all the packets that goes through the networks. The results show that the proposed detection method can detect TCP SYN Flooding in both normal and attacked network and alert the user about the attack after sending the report to the administrator. As a conclusion, TCP SYN Flood and other attacks can be detected through the traffic monitoring tools if the abnormal behaviors of the packets are recognized such as incomplete TCP three-way handshake application and IP header length.

Keywords: TCP SYN Flood, Rate-Based Detection, Three-Way Handshake, IP Header, TCP Header

1. INTRODUCTION

Threats have been a big problem to internet security nowadays especially for security management department to maintain the level of their security from being threaten by intruders.

There are many types of threats in the internet such as phishing, hackers, worms, virus that occur every day without being realized by the users. Intruders will do anything to attack and violence the network even though the security management had upgraded their security with the newest defence methods. The intruders target to break all the security especially in government, military, banks and others because whenever the intruders can break in the network, that network might lose data, money or confidential information and documents. The objective of this paper is to detect TCP SYN Flood attack that occurs in TCP protocol before it affects the network system.

TCP SYN Flood is hard to detect and we used anomaly detection because it is the most frequently suggested approach to detect attack variants, which looks for abnormal behavior. This paper focusing on detecting threats in the local network by monitoring all the packets that goes through the networks. This paper is comprised in two main parts. First part, do the monitoring and analysis the normal flow of the network and second part is monitor and analysis the network that had been attack by TCP SYN Flood.

Results show that there are threats in normal traffic without any alarming to the users. The suggested detection method can detect TCP SYN flood and other threats in the normal network and attacked network. Then, the system will send a report to the administration for warning all the users in the network.

2. LITERATURE REVIEW

Several methods for detecting TCP SYN flood attacks have been proposed.In network security architecture, network intrusion detection systems such as SNORT [2] and Bro [3], detect signatures of known attack such as packet payload inspection, buffer overflows according to the rules that had been written in this application. It differs from the anomaly detection system such as Network Traffic Anomaly Detection (NETAD) [4]. NETAD filtered the traffic and examined only the start of incoming server requests. It starts with the IP header, every first 48 bytes is treated as an attribute and do not parse the packet into fields. NETAD used nine separated models corresponding to the most common protocols such as IP, TCP, and UDP. The anomaly score tn/r was modified to scare rare. The t value is the time since the attributes was last anomalous, n is the number of training observations, and r is the size of the set of allowed values. Only the start of incoming server requests are examined after filtered the traffic.

- The Flood Detection System (FDS), which used Cumulative Sum (CUSUM) that detect the SYN flooding attacks at leaf routers which connect end hosts to the Internet, instead of monitoring the ongoing traffic at the front end (like firewall or proxy) or a victim server itself. The detection utilizes the SYN-FIN pairs' behavior and distinguish features FDS make it immune to SYN flooding attacks, CUSUM method that make the detection robust, and it does not undermine the end-to-end TCP performance. This mechanism not only sets alarms upon detection of ongoing SYN flooding attacks, but also reveals the location of the flooding sources [5].
- Partial Completion Filters (PCF) has an independent interest because they provide a solution to the general problem of detecting imbalanced parentheses in streaming environment. It consists of parallel stages containing buckets that are incremented for a SYN and decremented for a FIN. Thus, if a destination hashes into buckets with large counters in all stages, it seems plausible that the destination is being attacked [6].
- The comparison of three types SYN Flooding detection has been done in this research. Most of the researches used TCP control packets only as an input and each is designed to be deployed at the edge of a leaf network. The results show that FDS has good detection speed but long time to return to non-alert state [7].
- The significantly and negatively affected by attacks that create high variance in the traffic rate, but faster in signaling the end of an attack, and PCF performs well with regards to both detection time and quiescence time[8].
- Architecture of an anomaly detection system is based on the paradigm of Artificial Immune Systems (AISs). Incoming network traffic data are considered by the system as signatures of potential attackers by mapping them into antigens of AISs either using some parameters of network traffic or headers of selected TCP/IP protocols. A number of methods for generation of antibodies (anomaly detectors) were implemented. The way of anomaly detection depends on the method of antibodies generation. The paper presents results of an experimental study

performed with use of real data and shows how the performance of the anomaly detection system depends on traffic data coding and methods of detectors generation [9].

- Packet Header Anomaly Detector (PHAD) learns the normal range of values for 33 fields of the Ethernet, IP, TCP, UDP, and ICMP protocols. On the 1999 DARPA off-line intrusion detection evaluation data set, PHAD detects 72 of 201 instances (29 of 59 types) of attacks, including all but 3 types that exploit the protocols examined, at a rate of 10 false alarms per day after training on 7 days of attack-free internal network traffic. In contrast to most other network intrusion detectors and firewalls, only 8 attacks (6 types) are detected based on anomalous IP addresses, and none by their port numbers. A number of variations of PHAD were studied, and the best results were obtained by examining packets and fields in isolation, and by using simple no stationary models that estimate probabilities based on the time since the last event rather than the average rate of events [10].

3. TCP SYN FLOODING

TCP SYN Flooding are a common form of denial-of-service attacks launched against IP based hosts, designed to incapacitate the target by exhausting its resources with illegitimate TCP connections [1]. A normal TCP connection usually start a transmission from client by sending a SYN to the server, and the server will allocates a buffer for the client and replies with a SYN and ACK packet. At this stage, the connection is in the half-open state, waiting for the ACK reply from the client to complete the connection setup. When the connection is complete, it called 3-way handshake and TCP SYN Flood attack manipulate this 3-way handshake by making the server exhausted with SYN request.

This application is different from TCP SYN Flooding attack which takes an advantage of the half-open state condition by sending multiple SYN packets with spoofed address. Figure 1 shows the TCP SYN Flood happened. An attacker will send multiple SYN requests to the victim server using a spoofed address. A victim server sends back a request SYN and ACK packet to the client or spoofed address and wait for confirmation or timeout expiration of SYN packets. If the client does not send back the final ACK packet, the server's resources can be easily exhausted. At this time the TCP SYN Flood attack occurred because too many SYN packet request from clients.

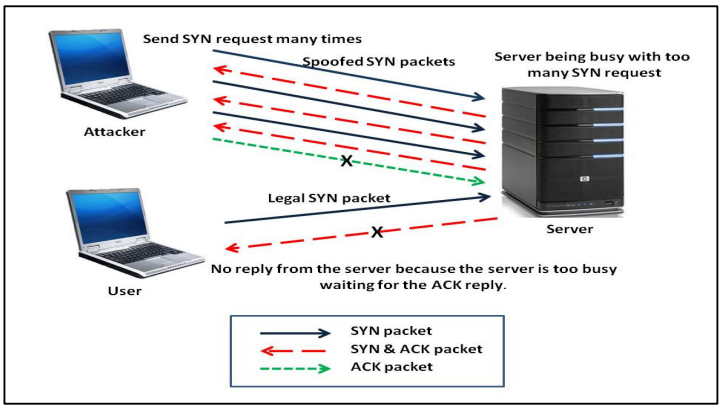

FIGURE 1: TCP SYN Flood Attack

The attack succeeds because the number of half-open connections that can be supported per TCP port is limited. When the number of half-open connections is exceeded the server will reject all subsequent incoming connection requests until the existing requests time out, creating a denial-of-service condition.

4. DETECTION METHODS

There are two types of network intrusion detection system which are signature based detection or anomaly based detection. Signature detection is a technique often used in the Intrusion Detection System (IDS) and many anti-malware systems such as anti-virus and anti-spyware. In the signature detection process, network or system information is scanned against a known attack or malware signature database. If match found, an alert takes place for further actions [10, 11].

In this paper, rate-based detection will be used for anomaly detection. Anomaly detection has three types of detection in network analysis behavior: It used protocol to detect packets that are too short which violate specific application layers protocol, rate-based detection which detects floods in traffic using a time-based model of normal traffic volumes especially Denial of Service (DoS) attacks. Lastly, it detects through the behavioral or relational changes in how individual or groups of hosts interact with one another on a network.

5. METHODOLOGY

In order to perform this research, the network under UniMAP (University Malaysia Perlis) is being used as a platform to capture the packets. The operating system used the open source GNU/Linux -Ubuntu ver. 9.04 and focusing the network inside UniMAP Research Cluster. Linux is used because this operating system is stable and also capable to act as client or server and free to modify the system. In this research, the experiments are divided into two categories which are the normal flow of the network had been monitored to see the data of the packets and checked for the threats. Secondly, the network that had been attacked with TCP SYN Flooding and the data is checked.

In order to evaluate this experiment, a simple networking testbed was constructed. Shown in Figure 2, this essentially consists of three Linux clients and one Linux PC as a traffic monitoring tools. All the data from the client will be monitored by traffic monitoring tool.

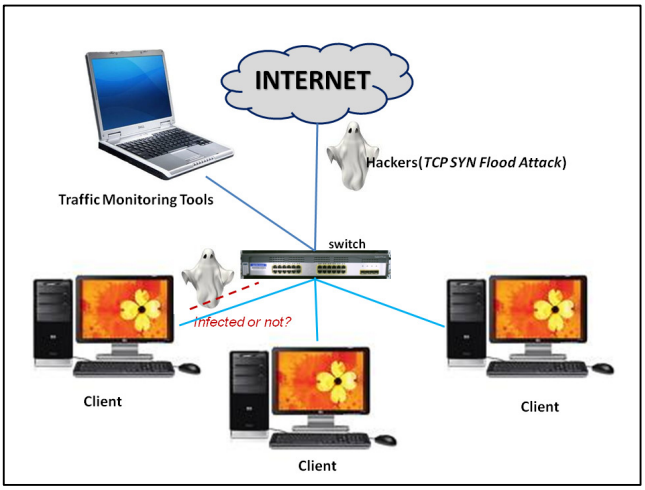

FIGURE 2: Testbed for Traffic Monitoring

This research used tcpdump software to sniff the packet that got through the network and internet in the real time. The data is saved after capturing the packets for the next process, analysis the packets. The captured data will be analyze every 1000 packets and check for threats. These packets that go through the network are analyzed according to the protocols (TCP, UDP and ICMP). The analysis packets based on IP and TCP headers of the packets from the monitored traffic. This analysis was focusing on IP header of the IP packets regardless of their layer protocol such as TCP packets and UDP packets which in transport layer protocol, and ICMP packets in the network layer protocol. UDP, ICMP and other types of packets could also be used in security breaches according on the IP payload and unusable area.

5.1 Algorithm

The algorithm for this paper is illustrated as Figure 3. The packets will go through the anomaly detection software that sniffs using tcpdump. IP Header analysis includes each field such as IP Header Length (IHL), Type of Service (ToS), Identification (ID), Flags and etc. The IP packet header consists of 20 bytes of data and if the length is below than 20 bytes, that packet is assume as abnormal packet and go for analysis before report to administrator. An option exists within the header that allows further optional bytes to be added, but this is not normally used.

The TCP header is analyzed for the next step in this process since TCP SYN Flooding is the main threats. TCP header is built on top of IP header, which is unreliable and connectionless. TCP header occupies 20 bytes and has some limitations in header length. As mentioned, normal TCP header is 20 bytes but TCP can have another 40 bytes for option. So the header size is limited to 60 bytes. TCP Flags have six flags bits namely URG, ACK, PSH, RST, SYN and FIN, each of them has a special use in the connection establishment, connection termination or control purposes. Only few combinations of the six TCP flags can be carried in a TCP packet. URG and PSH flags can be used only when a packet carries data, for instance a combination of SYN and PSH becomes invalid. Since TCP SYN Flooding attack will flood the network with SYN packets, the three-way handshake application is checked in every packet.

At this stage, packets are divided into two groups whether infected packets or normal packets. If the packet is infected, the system will distinguish the packet and go for analysis again to confirm whether the packet is truly comes from attackers. Otherwise, the normal packet will go through the network sending the data to the destination.

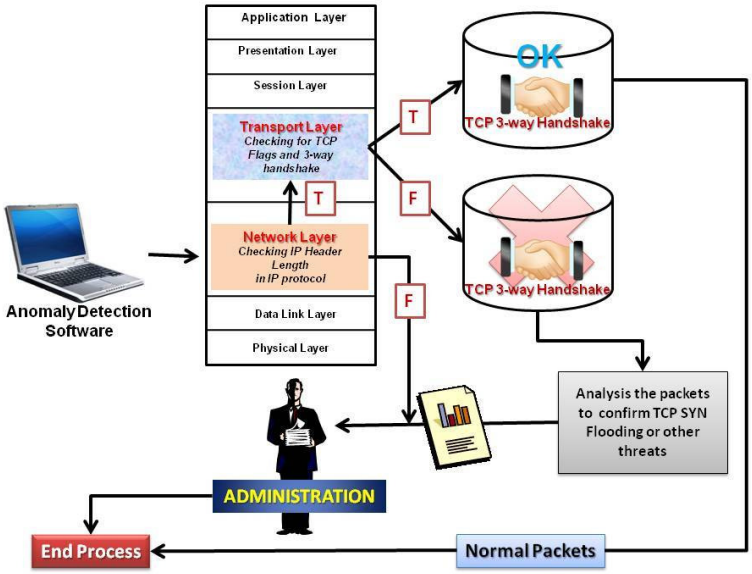

FIGURE 3: Packet Filtering Flowchart

5.2 Packet Filtering

In order to do the packet filtering, many factors will be considered. There are three main factors in this paper:

1. The traffic filtered each packet to each protocol such as TCP, UDP and ICMP.
2. TCP flags SYN, ACK, RST, FIN, are divided to each group to check the three-way handshake is complete or not.
3. IP address is valid and not a spoofed address.

These factors are important for detection method to recognize which packets are the infected packets in order to distinguish the normal packet from abnormal packet. Then the analysis for each packet is done using these factors.

6. EXPERIMENT RESULTS

The experimental result is divided into two parts. First part, monitoring and analysis the normal flow packet in the network. Analysis all the packet header and check for the threats for each packet. The normal packets behaviors are being analyzed according to each protocol and header. Each protocol has header and function according to the TCP/IP protocol.

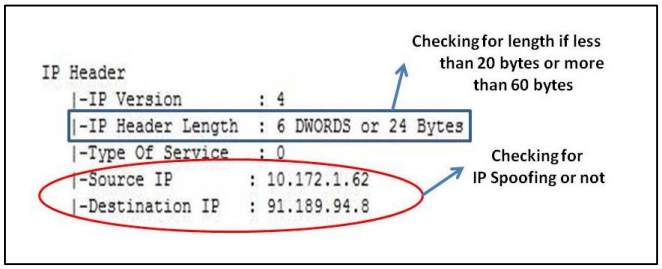

FIGURE 4: Packet Filtering Flowchart

Figure 4 above shows the field that had been observed and analyzed in IP header for the first part experiment. There are five main fields that are important in order to detect threats. This experiment is focusing on Internet Protocol Version 4 (IPV4), so the IPV must be 4 and IP header length must be equal or above than 20 bytes and equal or below than 60 bytes. ToS should be zero for normal packets and the IP address is not the spoofed address because hackers will use IP Spoofing to attack the network. At the same time, TCP three-way handshake application is checked.

The second part is analyzed the packet that been attacked by TCP SYN Flooding. This analysis is focusing in TCP protocol that is in transport layer according to Open System Interconnection (OSI) model by monitoring its behavior such as the flow of the packet, TCP header and flags. The attack had been run for half an hour and at the same time the data (packet) is save in the real time. If the data is not saved after capturing, the data may be flushed away and actual packet contents are no longer available.

In order to detect the SYN flood, the internet must be connected and this detection is focusing on port 80, HTTP. Other port than 80 the packet will be discard. HTTP has been chosen because most of the internet user or web used this port as a platform for communication. It had been reported in 1996 that 65 percent of the web users used HTTP.

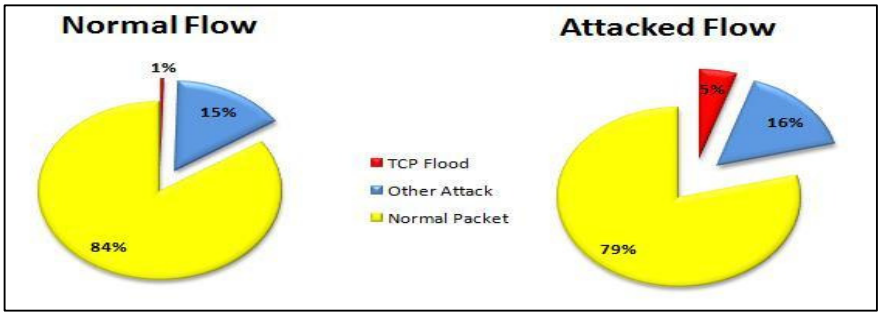

FIGURE 5: Threats in Network

From the experiment, there is SYN flood attack occurred in the normal network in the cluster but it was not much compared to other threat which is more in the network. Figure 5 shows the differences between a normal flow packet and attacked network flow packet. TCP SYN flood attack percentage had been increased after the system had been attack and this detection

method also detected other packets that have an error in the payload and IP header especially. An abnormal behaviour of the packet traffic especially in TCP protocol is important to detect in order to defence the network. Even though, the normal packets for both experiments are showing the highest range, the flooding attack can reduce the normal packets if it the flooding amount is bigger and can make the connection to the internet slower than usual.

From the analyzed packets through the TCP port, there are more threats other than SYN flood attack such as Trojan and backdoor, as shown in Figure 6 below.

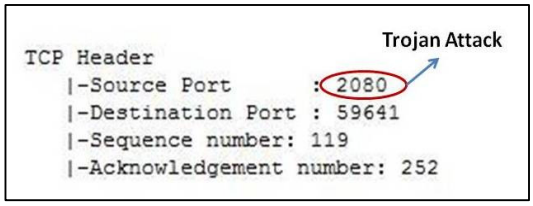

FIGURE 6: Trojan Attack in the Network

7. DISCUSSION

IP header is the main platform for detecting the threats especially in IP protocol and TCP protocol that are applied under open source Linux. Monitoring can detect abnormal behaviour in the network. In military, banking, government and many expertise departments, if SYN flood occurred in the system but there is no monitoring done, and no expertise, the network team will never realize that they had been attacked. In contrast with other work [5], the suggested method is much better because it alarming the administrative department from the start of the attack.

It had been reported that a virus called Agent.btz, variation of the "SillyFDC" worm, which spreads by copying itself to thumb drives had attack U.S. military network. When that drive or disk is plugged into a second computer, the worm replicates itself again. The attack struck hard at networks within U.S. Central Command, the headquarters that oversees U.S. involvement in Iraq and Afghanistan, and affected computers in combat zones. The attack also penetrated at least one highly protected classified network and this will affect all the network system at the same time. Such important information must be send immediately to top management as an example, terrorist is trying to ambush an army camp but the information is not sent because of the flooding. The suggested method detects through the behavioral and relational changes in how individual or groups of hosts interact with one another on a network. Comparing the suggested method with other suggested method such as [5] which detects attacks at leaf routers, variance in traffic rate as in [8], detectors generation and antibodies as in [9], or a range of values in a certain number of fields for different protocols, you will see that the suggested method has the comprehensively solution to meet the requirements for such type of attack.

Anomaly detection is important to detect SYN flood and other flooding attacks in huge network system as well to prevent the data loss and traffic jam since it will create Denial of Service (DoS) if it is uncontrolled.

8. CONCLUSION

The analysis for the packets is to detect threats that attack through the network. These threats are detected due to the IP Header (payload and unusable area). These detections are not only for TCP, but include the IGMP, ICMP and UDP. Receiving some numbers of duplicate ACKs means that the network congestion has been occurred.

In the experiment, the main threats in this paper, SYN Flood attack had been traced in a small amount. It is because the Linux operating system is stable and it is very hard to attack by the hackers.

The analysis for the packets is to detect threats that attack through the network. Threats are

detected due to the IP Header (payload and unusable area). This detection is not focusing only for TCP, but others protocol such as IGMP, ICMP and UDP also being examined.

By analyzed every packet to each category in TCP protocol (port, flags, and TCP three-way handshake) and IP header, the threats are easier to detect once we know the behavior of an attack.

In the experiment, the main threats in this paper, SYN Flood attack had been traced even in a normal network. The detection method of attacks can be improve in order to make the detection faster and effective, and alarming the security administration department whenever there is an attack or abnormal behavior in the flow of the traffic.

9. REFERENCES

1. *"Using SYN Flood Protection in SonicOS Enhanced"*,[online] available at: http://www.sonicwall.com/us/support/2134_3480.html

2. Roesch, Martin, *"Snort - Lightweight Intrusion Detection for Networks"*, Proc. USENIX Lisa '99, Seattle: Nov. 7-12, 1999.

3. Paxson, Vern, *"Bro: A System for Detecting Network Intruders in Real-Time",* Lawrence Berkeley National Laboratory Proceedings, 7'Th USENIX Security Symposium, Jan. 26-29, 1998, San Antonio TX.

4. Mahoney, M, *"Network Traffic Anomaly Detection Based on Packet",* ACM (2003).

5. H. Wang, D. Zhang, K. G. Shin, *"Detecting SYN Flooding Attacks ",* Proc. INFOCOM IEEE Communications Society, (2002).

6. R. Rao, K., Sumeet, S., & V. George, "*On Scalable Attack Detection in the Network",* Networking, IEEE/ACM Transactions on, 15(1):14-25.

7. Beaumont-Gay, M, *"A Comparison of SYN Flood Detection Algorithms",* Internet Monitoring and Protection, 2007. ICIMP 2007.

8. V.A. Siris, F.Papagalou. *"Application of anomaly detection algorithms for detecting SYN flooding attacks"*, Proc. of Globecom, IEEE Communications Society, 2004.

9. "*Signature Detection*", [online] available at: http://www.javvin.com/networksecurity/SignatureDetection.html

10. Franciszek, Seredynski & Pascal Bouvry "*Anomaly detection in TCP/IP networks using immune systems paradigm*", ELSEVER , Computer Communications 30 (2007) 740–749, _ 2006 Elsevier B.V. All rights reserved.

11. Matthew V. Mahoney and Philip K. Chan, *"PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic"*, Florida Institute of Technology Technical Report CS-2001-04

12. *Signature Detection",* [online] available at: http://www.javvin.com/networksecurity/SignatureDetection.html

13. M. Bykova, S. Ostermann, *"Statistical Analysis of Malformed Packets and Their Origins in the Modern Internet",* 2nd Internet Measurent Workshop (IMW 2002), Nov. 2002.