Providing Network Security Against Botnets and SYN Flooding Attack

Nithin Gopal Krishna T P
UG Student
Department of Computer Science and Engineering
Global Academy of Technology

Kiran G
UG Student
Department of Computer Science and Engineering
Global Academy of Technology

Nagendra Prasad P
UG Student
Department of Computer Science and Engineering
Global Academy of Technology

Anvesh P A
UG Student
Department of Computer Science and Engineering
Global Academy of Technology

Shruthi P
Assistant Professor
Department of Computer Science and Engineering
Global Academy of Technology

Abstract

Network security is a big topic and is growing into a high profile in the field of Information Technology, due to its vast growth they are prone to various security concerns. In order to control these security concerns and prevent them this system is proposed. The security breaches of network include Denial of Service attacks. Botnets and SYN flooding attack are two Denial of Service attacks. SYN flood occurs when attackers make half-open connections by not responding to the SYN+ACK packet from server. When the server's SYN buffer is full with these half-open TCP connections, it stops accepting SYN packets, thus resulting in denial of service to legitimate clients. Bots are the malicious scripts that perform automated tasks at a much higher rate than would be possible for a human alone. The SYN flooding and Botnets are detected and addressed before they become an issue and bring down the network service. SYN flooding attack is detected by considering the rate at which the SYN packets are sent, the server will then reject all these suspicious TCP connections, with TCP-RST packets to prevent the potential DOS attack. Later all the connections in the SYN-RECV state will be closed forcibly by the server with the RST packets. Bots usually perform actions faster than humans hence the best way to detect them is by analyzing its behavior. Hence the action time and action frequency considering the number of clicks and the rate at which the form is submitted are determined. The activities which generate abnormal network traffic are detected and the attacker IP is obtained, then the log of these attackers IP are stored in the database so that no further bot activities takes place from the infected client machine.

Keywords- Network Security, Botnets, SYN Flooding, TCP Connections, Dos Attack, Network Traffic

I. INTRODUCTION

Network security is a big topic and is growing into a high profile in the field of Information Technology specialty area. Security-related websites are tremendously popular with savvy Internet users. The popularity of security-related certifications has expanded. Esoteric security measures like biometric identification and authentication, formerly the province of science fiction writers and perhaps a few ultra-secretive government agencies – have become commonplace in corporate America. Yet, with all this focus on security, many organizations still implement security measures in an almost haphazard way, with no well-thought-out plan for making all the parts fit together. Computer security involves many aspects, from protection of the physical equipment to protection of the electronic bits and bytes that make up the information that resides on the network.

A bot, originating from the term 'robot', is an application that can perform and repeat a particular task faster than a human. When a large number of bots spread to several computers and connect to each other through the Internet, they form a group called a botnet, which is a network of bots [1]. Bots are collection of scripts that perform automated tasks in internet. Rather than use a network of infected machines, Bots use Network services to build Botnets. Bot masters registers to the Content Security Policy (CSP) and introduce Bots to the applications and data hosted on network. Bots cannot be noticed easily because they perform tasks as similar to humans but at a higher rate than humans. Hence it is difficult to detect Bots using an Intrusion Detection System (IDS), so it is appropriate to detect Bots based on their behaviour. Bots are frequently used to launch DoS attacks [3]. Bots act safe and are hidden as long as possible and they are easy to establish when compared to the traditional Botnets. Firewalls are inefficient in preventing and detecting Bots. Hence active monitoring of network traffic of anomalous activity is suitable to detect Bots.

The SYN flooding attacks exploit the TCP's three-way handshake mechanism and its limitation in maintaining half-open connections. When a server receives a SYN request, it returns a SYN/ACK packet to the client. Until the SYN/ACK packet is acknowledged by the client, the connection remains in half open state until timeout. The server has built in its system memory a backlog queue to maintain all half-open connections. Since this backlog queue is of finite size, once the backlog queue limit is reached, all connection requests will be dropped [4].

If a SYN request is spoofed, the victim server will never receive the final ACK packet to complete the three-way handshake. Flooding spoofed SYN requests can easily exhaust the victim server's backlog queue, causing all the incoming SYN requests to be dropped. The stateless and destination-based nature of internet routing infrastructure cannot differentiate a legitimate SYN from a spoofed one and TCP does not offer strong authentication on SYN packets. Therefore, under SYN flooding attacks the victim server cannot respond only to legitimate connection requests while ignoring the spoofed requests.

II. SYSTEM ARCHITECTURE

A. Bot Detection

Bots run automated scripts, they enter the cloud/server from client machines and hence continuous monitoring of the network traffic is necessary to detect threats. Bots attack the application by performing fraud activities at a faster rate than humans. Figure 1 shows the architecture of bot detection. The network traffic generated by activities is monitored based on action time and action frequency for parameters like number of clicks, file requests and many more. The activities which generate abnormal network traffic and user agents logged in are joined together to find out the IP address of the client from which bots are trying to entering. The log of IP address is maintained. If a particular IP address is blocked then any number of requests coming from that IP address will be denied.

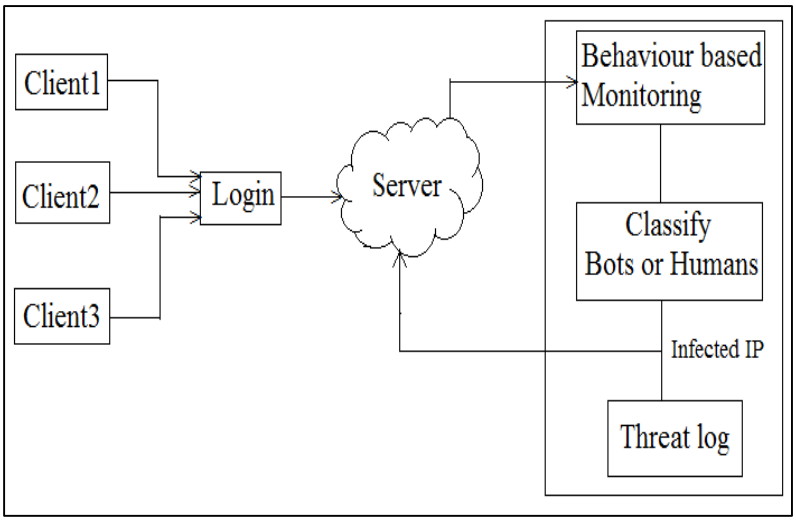

Fig. 1: Bot Detection Architecture

B. SYN Flooding

A SYN queue flood attack takes advantage of the TCP protocol's "three-way handshake". A client sends a TCP SYN (S flag) packet to begin a connection to the server. The target server replies with a TCP SYN-ACK (SA flag) packet, but the client does not respond to the SYN-ACK, leaving the TCP connection "half-open". In normal operation, the client should send an ACK (a flag) packet followed by the data to be transferred, or an RST reply to reset the connection. On the target server, the connection is kept open, in a "SYN_RECV" state, as the ACK packet may have been lost due to network problems. Figure 2 shows the architecture for SYN flooding attack.

In a DDoS, multiple attackers make many such half-connections to the target server, in a storm of requests. When the server's SYN buffer is full with half-open TCP connections, it stops accepting SYN connections, thus resulting in denial of service to legitimate clients. In order to preventive the attack a shell script is written to generate the IPtable rules and to obtain the IP address of the attacker clients. Then the server will reject all these suspicious TCP connections, with TCP-RST packets to prevent the potential DOS attack. Later all the connections in the SYN-RECV state will be closed forcibly by the server with the RST packet.

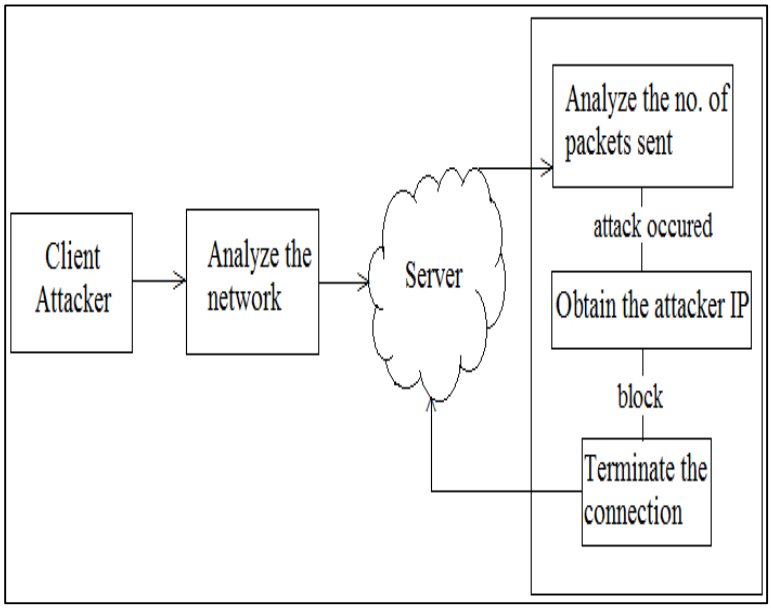

Fig. 2: SYN flooding Architecture

III. EXISTING SYSTEM

CAPTCHA- Computer Automated Public Turing test to tell Computers or Human Apart are used to differentiate between bots and human. They are used to prevent Bots but recent survey states that CAPTCHA's can be easily cracked down by using advanced character and pattern recognition software's.

SYN cookies- It allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue has been enlarged. The server sends back the appropriate SYN+ACK response to the client but discards the SYN queue entry. The two caveats that take effect when SYN cookies are in use are Firstly, the server is limited to only 8 unique Maximum segment size values, as that is all that can be encoded in 3 bits. Secondly, the server must reject all TCP options, because the server discards the SYN queue entry where that information would otherwise be stored.

SYN cache- The SYN cache data structure is robust to attackers attempting to overflow its buckets because it uses the initiator's local port number and some secret bits in the hash value. Because stacks are a more effective data structure to search than a simple linked list, stacks that use a SYN cache can have improved speed, even when not under attack. The disadvantage of using these caches is that every time the backlog queue is full the cache size has to be incremented in order to control this attack which is waste of memory and time.

IV. PROPOSED SYSTEM

Since security is the major concern in networking, the proposed system is intended to solve the network security threat which including SYN flooding attack and Botnets which plague the network and cause Denial of Service for the legitimate users. Bots are the malicious scripts that perform automated tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. When a large number of bots spread to several computers and connect to each other through the Internet, they form a group called a botnet, which is a network of bots. The bots enter the network from any of the client machine, where the bot script from clients machine tries to send the form request multiple times in a very short time interval say less than milliseconds which is impossible by humans so continuous monitoring of the network traffic is dene to detect the bot activity. The network traffic generated by these activities are monitored based on action time and action frequency considering the number of clicks and the rate at which the form is submitted. The activities which generate abnormal network traffic and the user agents logged in are joined together to find out the IP address of the client from which bots are entering. Then the log of these attacker clients are stored in the database so that no further bot activities take place from the infected client machine. The administrator has the full control over the log data where he can view and make necessary changes to it through webpage.

The SYN flooding attack takes advantage of the TCP protocol's "three-way handshake". A client sends a TCP SYN (S flag) packet to begin a connection to the server. The target server replies with a TCP SYN-ACK (SA flag) packet, but the client does not respond to the SYN-ACK packet, leaving the TCP connection "half-open". In SYN flood attack, multiple attackers make many such half-open connections to the target server, in a storm of requests. When the server's SYN buffer is full with half-open TCP connections, it stops accepting SYN packets, thus resulting in denial of service to legitimate clients. To simulate the SYN flood attack the attacker first make use of the nmap to get the IP address of the target server and once the IP is obtained attacker use the scapy tool in order to generate multiple SYN request packets and attacks the target server with these storm of SYN request packets. As a preventive measure a shell script is written to generate the IPtable rules and to obtain the IP address of the attacker

clients. Then the server will reject all these suspicious TCP connections, with TCP-RST packets to prevent the potential DOS attack. Later all the connections in the SYN-RECV state will be closed forcibly by the server with the RST packet. Here it allows 25 attempts from a single IP address to take care of packet loss which sometimes happen due to network errors. After 25 attempts from the same IP address, SYN packets from that IP address will be rejected as intentional flooding and an IPtables rule entry is added for the malicious IP addresses and this IP is later rejected by the server with the TCP-RST packet so that it terminates the TCP connection with the attacker machine in order to prevent further possible attacks. If the attacker tries to send the packets again after its blocked by the server then the packet sending fails since the server does not responds to that IP address in order to establish the TCP connection.

V. CONCLUSION

The proposed system detects the two Denial of Service (DoS) attacks, Botnets and SYN flooding that occurs in the network. Bots are automated scripts run on any system which is detected based on action time and action frequency, whenever the behaviour is detected as bots the IP address of the client system which acts as bot is retrieved, blocked and stored in the database so that the attacker does not perform the bot activity again on the targeted host.

The SYN flooding attack occurs during TCP connection between the client and the server the main aim of the attacker is to consume entire server resources making it unavailable for the users. So to detect the attack it considers the number of packets transmitted between the client and server analyse them and if any abnormal activity is observed then the attacker IP is copied and blocked. The connection is terminated and the server is restarted allowing it to respond to the legitimate users.

VI. RESULTS

In bot detection the attacker runs the botscript by providing IP address of the target host, figure 3 shows the attack action. The network is then monitored to detect bots by studying their behavior, figure 4 shows the screenshot where the attacker IP address is logged and blocked due to bot activity to prevent potential DoS attack.

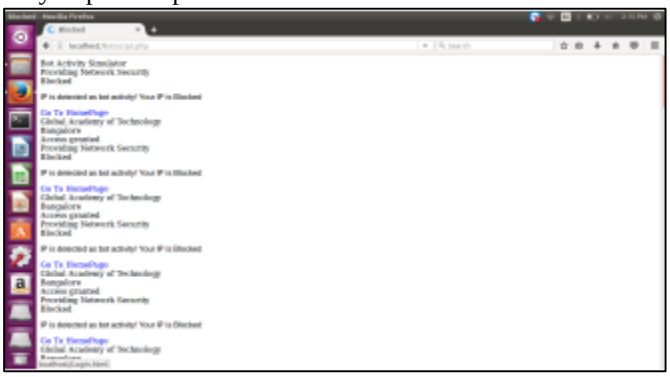

Fig. 3: Botscript running in attacker system

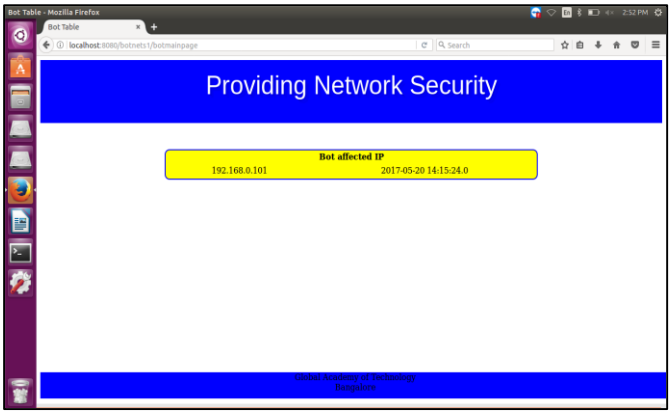

Fig. 4: Attacker IP address is blocked due to bot activity

In SYN flooding attack the attacker sends flood of SYN packets to the target host and does not respond to the SYN+ACK packets send from host, which is shown in figure 5. In figure 6 the IP address of the attacker is detected and blocked by analyzing the number of SYN packets to prevent DoS attack thereby allowing legitimate connections.

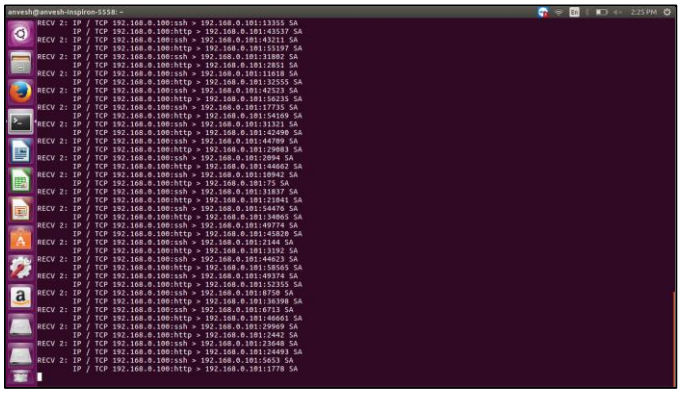

Fig. 5: Attacker sending flood of SYN packets

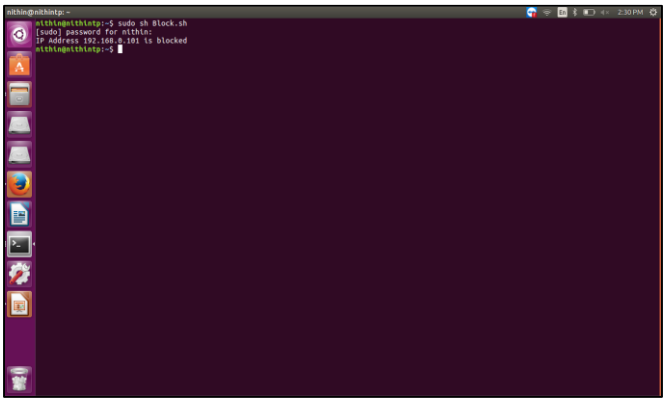

Fig. 6: Attacker IP address is blocked

ACKNOWLEDGMENT

During the entire period of this research, our research paper would not have been materialized without the help of many people, who made our work so easier. It gives us proud privilege to complete this research paper working under valuable guidance of Prof. Shruthi P. She has been very supportive and patient throughout the process. We are also thankful to all staff members for providing all facilities and every help for smooth progress of paper work. We thank our friends and family members who in one way or another helped us in the successful completion of this work.

REFERENCES

[1] 2012 IEEE International Conference on Control System, Computing and Engineering, 23-25 Nov. 2012, Penang, Malaysia, "Bots and Botnets: An Overview of Characteristics,Detection and Challenges", Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar, 978-1-4673-31432/12/$31.00 ©2012 IEEE.

[2] "Analysis of the SYN Flood DoS Attack", 2013, 8, 1-11 Published Online June 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.08.01 Copyright © 2013 MECS I.J. Computer Network and Information Security, 2013, 8, 1-11, Mitko Bogdanoski , Tomislav Shuminoski and Aleksandar Risteski.

[3] Usha L, Chidananda Murthy P, "Securing Data Against Botnets and IP Spoofing", in International Journal of Engineering Research & technology, ISSN : 2278-0181, pp 81-84 July 2014.

[4] "Detection of SYN Flooding Attacks Using Linear Prediction Analysis" Dinil Mon Divakaran, Hema A. Murthy and Timothy A. Gonsalves Department of Computer Science and Engineering Indian Institute of Technology, Madras, 0-7803-9746-0/06/$20.00(2006) IEEE.