Scientific Journal of Impact Factor (SJIF): 3.134
ISSN (Online): 2348-4470
ISSN (Print) : 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 3, March -2015

HTTP Reverse Proxy Authentication

Avinash.V[1], Sornalakshmi. k[2]

[1]*M.Tech student, Department of Information Technology, SRM University,*
[2]*Asst. Lecturer, Department of Information Technology, SRM University*

Abstract —*Denial of Service (DoS) attack is the attack which occurs very frequently. This attack directly attacks the server and crashes it, thus making it down for certain time which affects the availability of information. And the main aim of this paper is to mitigate http based DOS attacks. For that a reverse proxy authentication need to be done. This http reverse proxy authenticates the users before they access the webserver thoroughly.*

Keywords- *Proxy server, Reverse-Proxy, DDoS, HTTP, Slowloris Attack*

I. INTRODUCTION

Nowadays the world is behind the emerging technologies. A lot of new applications and technologies have been developed, which with the help of internet, aims at easing the lives of people .Each and every organization uses their own infrastructure (network) for providing internet by which it's possible to access any kind of information from anywhere. The information forms the most important asset of any enterprise. Here comes the need to keep it safe from unauthorized access and usage. For that, data-in-rest and data-in-transit need to be secured. Data-in-transit can be secured by securing the network through which it is transmitted. The attacks done on the networks, servers or database can violate the CIA triad of information. Authorized users should be made available with information with full integrity and confidentiality whenever they need.

II. LITERATURE REVIEW

A. Infrastructure of a network

The network infrastructure refers to the hardware and software resources of an entire network that enable network connectivity. Network infrastructure provides the communication path and services between users and external networks.

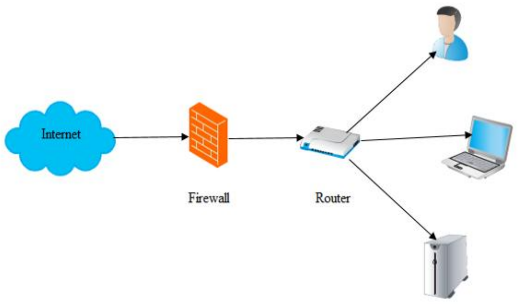

Fig.1. Network Infrastructure

The computer network contains personal computers, servers, switches, cables, routers network interface cards, protocols, applications and so on. The data should flow with sets of rules which is provided by open systems interconnection (OSI).

B. Vulnerabilities and threats

The attackers always want to get into the network and make access. They use the vulnerabilities present in the system and network. The network vulnerability is the weakness available to attack or security breach against the system. The undesirable event will be happen when the system has existence of a weakness, design and implementation error. The network should be trustworthy to keep the data safe and no changes have to be done that in the sense integrity should be there. Also it should be accessible only by the authorized users that in the sense confidentiality should be there. And the data should be available for use whenever it's needed which forms its availability.

C. Security Devices

In network infrastructure many security devices are there like firewall, IDS, IPS, proxy server, SIEM (Security Incident and Event Management), honeypot. These devices work in different layer and either detect or prevent the breaches. But these doesn't provide full assurance. Attacks are still occurring by compromising these system in a different ways. One reason for this is the zero day exploits. A zero-day (or zero-*hour or* day zero) attack or exploit is an attack that exploits a previously unknown vulnerability in a computer application or operating system, for which developers have no time to address and patch. The security devices other than SIEM is not capable of preventing the network from zero day exploit. The SIEM toolkit even can detect the attack after the attack starts and is utilizing some resources. Resources can be database, server, router or anything. The attacker can utilize the database for certain time when the valid user is idle. Once the attacker gets inside the system, the attacker can do whatever he wants. He can load virus or create a backdoor. So it's necessary to build a system which is not comprisable even though has vulnerability present.

D. Proxy Server

A proxy server is a dedicated computer that acts as an intermediary between a devices, such as a computer, smartphones, smart TVs and server .The proxy server may exist in the same machine as a firewall server or it may be a external server, which forwards requests through the firewall. Proxy servers can log interactions. Sites that are frequently requested will be available in it which makes access to them next attempt easy.

E. Working of Proxy Server

When a proxy server receives a request for an Internet (Web page), it looks in its local cache. If it finds the page in the cache, it returns it to the user without forwarding the request to the Internet. If the page is not to be found in the local cache, the proxy server, uses one of its own IP addresses to request the page from the server on the Internet. Once the page requested for is returned, the proxy server relates the page returned to the original request and forwards it the user. In an enterprise, proxy server is used for channel security, administrative control and caching services. In a personal computing context, proxy servers are used to achieve user privacy and anonymous surfing. Proxy servers can also be used for monitoring traffic and undermine user privacy. The proxy server is invisible to users, Internet requests and responses directly appear to be with addressed Internet server. (Actually the proxy is not actually invisible, its IP address has to be made as configuration option to the browser or other protocol program.)

F. Reverse Proxy Server

The reverse proxy is nothing but each request will be validated and see whether it can fulfil the request by itself. For example if a genuine user downloads a file and another user later gives request to download same file, the file will be retrieved from cache.

III. RESEARCH GAP

A lot of attacks is happening on network infrastructure. In that DDoS (Distributed Denial of Service) attack is unique and it happens frequently. In this paper we discussing about the flaws that is present in the network and prevention mechanism to be followed to prevent attacks making use of these flaws. It is a proof of concept. We are designing a proxy server which should protect from DDoS attack. The design of it is a testing module which can be incorporated to IDS or IPS in future. If we inherit to IDS or IPS, the packet entering in a network will be validated thoroughly immediately and if any signature is matched, it will detect and block it.

IV. OBJECTIVE

The objectives of this paper are:

- To understand the basic architecture and working procedure of the network.
- To study how DDoS attack happen and ways to detect it.
- To analyse how proxy server works.

V. SCOPE AND LIMITATION

The scope of the paper is to build a proxy server which will prevent the server or database from DDOS attack. The limitation that it is just a proof of concept which need to tested in industrial environment and check its capability of preventing attacks other than DDoS.

VI. METHODOLOGY

The denial of service (DoS) attack is an attempt to make a server unavailable to the users in a right time and it's usually done by temporarily interrupting the services. The most common DoS attack is to flood the target with

communication requests, when it overloads it will stop the resource from communicating to the legitimate traffic and it makes it unavailable. The target can be a ports, services, or any component of a network. The DoS attack makes the system unstable and it will exploit the operating system vulnerability and crashes the operating system. The vulnerability like SQL injection can lead to tremendous threats. , specific string given to database takes the user to enter the database without proper validation. SQL injection means In DoS attack we use one system with one internet connection to flood a server with packets to overload the target server resources and bandwidth. But in DDoS, uses many devices with multiple internet connections. Many devices are connected via botnet and this DDoS is very difficult to deflect, because there is no single attacker to defend. The target will be flooded from many requests from multiple sources. In order to prevent this attack, we should be quick and effective in identifying a DoS attack- absorb the attack and block the source. Proper validation of requests need to be done.

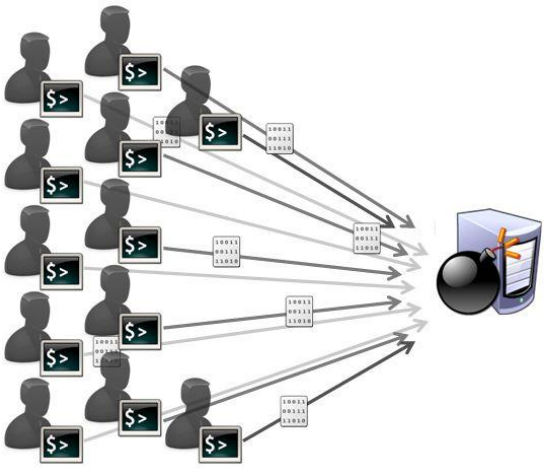

Fig. 2. DDoS Attack

For that a proxy server is built and it alone cannot assure that we can prevent DDoS attack. The main idea of building a proxy server is each and every request to the server will send through it and a validation is done.

VII. ANALYSIS AND DESIGN

A. Vulnerability existing

In network infrastructure, there is an inbuilt and default vulnerability. There are many possible attacks like SQL injection, virus attack etc. But DDoS attack is unique, will affect the availability of the data. The DDoS and DoS attack has many attacking techniques and here we concentrate more on slowloris attack and http flood attack. This attack is much concentrated, because it happens through http protocol. The major advantage of DDoS attack is, the firewall can't filter as it does by checking the headers of the packet. Once the packet enters the network, the server will engage itself with the client. This forms the vulnerability of the networks. To make understand, imagine a network which is connected to database containing user's information. Any user who wants to check his information can do it, his information may be in 100th position, which throws a complexity of '100' to the server. Now just imagine the client giving false information about position; then the complexity of the server is 'n'. This is the case for a serial request accepted server. Similarly, imagine 100 user's giving false information parallel, then how the server will respond? Still the server reply with a response, which will take time thus making server idle or busy, which forms the foundation of DoS attack.

Below are some http based DDoS attacks.

1. Slowloris Attack

The slowloris attack is a piece of software written by Robert 'RSnake' Hansen. This attack allows to take control on another machine or web server with minimal bandwidth which will cause side-effects on unrelated services and ports. The slowloris is an exotic animal of south-eastAsia it has special qualities like its movements are slow and deliberate.

The attack will enable the TCP connection and opens as much as connections possible in a low bandwidth to target the web server. Has another behaviour that will send only partial http header and makes the server to wait long for rest of headers. By doing it, the server will not be able to terminate the connection and accept new. The attacked server and websites will have a high amount of traffic in it. The slowloris attack is such a kind which even IDS cannot detect. This attack uses the buffer and sliding window very efficiently.

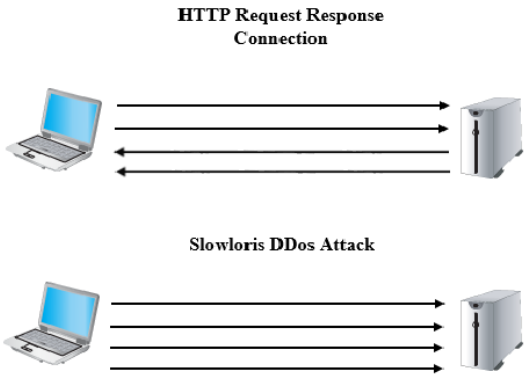

Fig.3. Slowloris attack

Mitigating Slowloris

There are some ways to mitigate the slowloris attack - we have to increase the number of clients the web server allows. By doing this, we will get a chance in between, for some legitimate users to communicate. Care to be taken that only limited connections have to provide via single IP address. We can use IP-tables to limit the connections from particular host. Configuring the time-out in effective manner also solve the attack. The length of the time which makes the server engaged and stay connected should be decreased. We can use load balancers which will allow only full http request. These all mitigations cannot prevent slowloris attack completely but has some possibilities to limit the attack.

2. Http Flood Attack

Http flood attack attacks the server and make the server to come down by its size and complexity. This attack is an application layer attack which uses mostly GET/POST request to attack the server. This attack consumes low bandwidth. The attack can be done using botnet which is called ‘zombie army ‘- which is connected systems using internet also by using Trojan horse. This attack won’t use malformed packets so it’s very difficult to validate and more often it will not spoof so it’s difficult to find whether it is a trusted one. This attack will look in a normal way like, when the client starts to communicate to a server it sends a request, the request is of two types they are GET or POST. The GET method is used to retrieve static content and POST is used to access dynamic resources. This attack will be more effective when it forces the server to allocate maximum resources for a request. The HTTP GET is effective when we use botnet and it's simple to create.

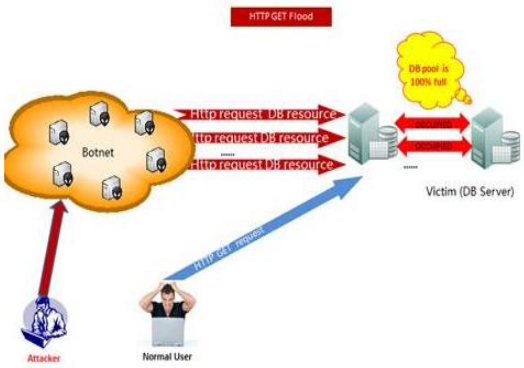

Fig.4. Http Flood Attack

Mitigation of Http Flood Attack

This attack is very difficult to mitigate because it's difficult to differentiate from valid traffic because this attack also uses standard URL requests. Many security applications and devices have failed and become ineffective in detecting this http flood attack. The way to detect the attack efficiently is to identify IP reputation. Keep tracking the abnormal activity and traffic profiling can be done to prevent this active inspection on each packet.

VIII. PROPOSED SYSTEM

The main concept of the paper is to prevent the network infrastructure from DDoS attack which is very unique and very difficult to mitigate. This attack can be launched by anyone easily, compared to other attacks, because of large number of botnets which are available in market. So in security we can't assure that we can protect the things to the fullest. Only way is to make the attacker, perform operations which are difficult and time consuming.

Thus for mitigating DDOS attack, we are building a proxy server which will hide the server, thereby we protect the server from being attacked. If an intruder attempts to compromise the proxy server using various resources, the enterprise network will be having IDS/IPS installed which will be monitoring the proxy server and collects the log files through which the security of total system can be ensured.

The proxy we are building should have load balancing technique, IP reputation and strong ACL rules. The access control list is designed with a set of complicated rules, using such ACL if a malicious packet is detected then all such packets will be compromised. So it should be designed in such a way that malicious packets are only trapped and blocked. Using load balancing techniques packet flooding could be avoided and sends packet in accordance with its throughput. IP Reputation used in our proxy validates an IP address and blocks out unwanted spam messages thereby wastage of resources can be prevented.

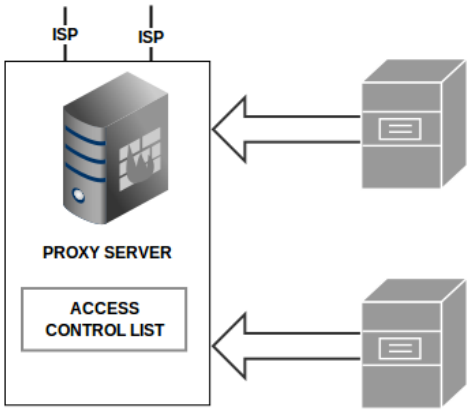

Fig.5. Proposed System

IX. CONCLUSON

The proxy server we have built will protect server from DDos attack. The proxy server monitors the network and mitigates DDos attack thereby availability of information is ensured. Hence the enterprise network is protected from malicious user. Future work of our proposal is to authenticate all incoming packets so as to provide an enhanced secure network.

REFERENCES

[1] Danai Chasaki, Qiang Wu and Tilman Wolf, "Attacks on Network Infrastructure", University of Massachusetts, Amherst, MA, USA.
[2] Brough Davis, "Leveraging the Load Balancer to Fight DDos, SANS Institute InfoSec Reading Room.

[3] Subramani rao Sridhar rao,"Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis", SANS Institute InfoSec Reading Room.
[4] Michael Glenn, "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment", SANS Institute InfoSec Reading Room.
[5] Oludele Awodele, Ernest Enyinnaya Onuiri and Samuel O. Okolie, "Vulnerabilities in Network Infrastructures and Prevention/Containment Measures", Proceedings of Informing Science & IT Education Conference (InSITE) 2012.

WEB REFERENCES

[1] http://www.slashroot.in/slowloris-http-dosdenial-serviceattack-and-prevention
[2] http://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html
[3] http://www.slashroot.in/httphypertext-transfer-protocol-request-and-response
[4] http://security.radware.com/knowledge-center/DDoSPedia/http-flood/
[5] http://blog.sucuri.net/2014/02/layer-7-ddos-blocking-http-flood-attacks.html
[6] http://www.incapsula.com/ddos/attack-glossary/http-flood.html

