Cyber Times International Journal of Technology & Management

Vol. 11 Issue 2, April 2018 – September 2018

TABLE OF CONTENTS

MITIGATION OF THE RISK FACTOR ON APACHE WEB SERVER FROM DDoS ATTACK

Rama Bansode
Ph.D. Research Scholar, Tilak Maharashtra Vidyapeeth, Pune,
rama.bansode@yahoomail.com

ABSTRACT

DDoS Attacks also known as **"Distributed Denial-of-Service".** *Attacker use* **zombie computers** *for launch their attacks on a systems or web servers Distributed denial of service (DDoS) is one of the type of attack of computer network and internet today. DDoS attacks are among the most difficult problems to resolve online, especially, when the target is the Web server. Many protocols such as Domain Name System (DNS) have several security vulnerabilities and utilized by Botnet attackers. Botnet - based DDoS attacks that use DNS as a basic infrastructure to launch attack. Each and every organization desire to protect its services and their customer's privacy by protecting them against these attacks, some may be difficult to detect which may bring down the name of the company.*

KEYWORDS: *Apache Web Server, Botnet, DoS, DDoS, DNS.*

I. INTRODUCTION

Distributed Denial of Service attacks are a significant cyber threat; interrupt a web service provided by an organization. The methods of attacks could be choose for various purposes by different entities, for example cyber-criminals conduct a similar attack for hackers could use a similar approach to express social conflict.

Such type of attack used to prevent authorized users from accessing services or resources. It involves multiple connected online devices, collectively known as a botnet, which are used to a target website with fake traffic. [1][2]

By Distributed Denial of Service (DDoS) attack, the website or any online service is overloaded with traffic from multiple sources and thus make the website unavailable.

While Denial of Service (DoS) attack uses one computer and one Internet connection, DDoS attack uses many computers and many Internet connections, to flood a target resource with packets and distributed globally, which is termed as botnet.

DDoS attack generally traffic measured in hundreds of Gigabits per second, which the normal network will not be able to handle.[3]

Types of DDoS Attacks?

DDoS attacks can be broadly classified into three categories;

- Volume-based Attacks
- Protocol Attacks
- Application Layer Attacks

VOLUME-BASED ATTACKS

TCP floods, UDP floods, ICMP floods, and other spoofed packet floods, these are the Volume Based Attack. These are also called Layer 3 & 4 Attacks. The bandwidth of the target size is being saturated by the attacker. The magnitude of the attack is measured in terms of Bits per Second (bps).

- **UDP Flood** – This is used to flood random ports on a remote host with numerous UDP packets on port number 53. To filter out or block malicious UDP packets, specialized firewalls are used.

- **ICMP Flood:** This is same as compared to UDP flood and used to flood a remote host with numerous ICMP Echo Requests. Outgoing and incoming bandwidth is consumed and ends up with overall slowdown of the system due to the high volume of the ping requests.

- **HTTP Flood:** A large volume of HTTP GET and POST requests are sent by the attacker which are not handled by the server and leads to denial of the additional connections from legitimate clients.

- **Amplification Attack:** A request is made by the attacker which generates a large response including DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.

PROTOCOL ATTACKS

Ping of Death, SYN floods, fragmented packet attacks, Smurf DDoS, etc. This type of attack use actual server, firewalls and load balancers. The intensity of the attack is measured in terms of Packets per Second.

- **DNS Flood** – infrastructure and DNS application are attacked by DNS floods to get access to a target system and consume the available network bandwidth.

- **SYN Flood** −TCP connection requests are sent by the attacker faster than the targeted machine can process them, causing network saturation. Controller can improve TCP stacks to moderating the effect of SYN floods. The effect of the SYN floods can be reduced by reducing the timeout or dropping the desired incoming connections using **ip tables**.[5]

- **Ping of Death** − The attacker sends malicious, larger packets using a ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.[4]

APPLICATION LAYER ATTACKS

Application Layer Attacks include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or Open BSD vulnerabilities and more. Here the goal is to crash the web server. The magnitude of the attack is measured in terms of Requests per Second.

Figure 1: Application Attack

- **Application Attack** – In this attacker do extremely log-in, database-lookup, or search requests to overload the application. This is also called Layer 7 Attack, It is difficult to detect Layer 7

attacks because they properly detect website traffic.

- **Slowloris** – Huge number of HTTP headers are sent by the attacker to the targeted web server, never completing the request. Opening false connection by the targeted web server and overflow the maximum concurrent connection pool, and promote to denial of additional connections from legitimate clients.

- **NTP Amplification** – The Network Time Protocol (NTP), which is accessible publicly is being exploited by the attacker to overcome the server target with User Datagram Protocol (UDP) traffic.[5]

- **Zero-day DDoS Attacks** − It is a system or application flaw previously unknown to the dealer, and has not been fixed.[1]

WEB SERVER DDOS ATTACKS BEST PRACTICES

- Understand your environment and prioritize your assets.
- Apply best practices for the configuration of network devices, systems and services.
- Monitor and log your networks, systems and services.
- Have an incident response plan
- Have business continuity plan.

Attackers can start a volumetric attack on website, can also issue an application or traffic attack. And also the mitigation is most often done on a network level, whereas the application and traffic types have some mitigation on the Web-service level.[4]

PROTECTION FOR APACHE SERVER

Apache Web servers, there are a few mitigation solutions available-

ModSecurity

- Mod_security is an Apache module that detects and prevents intrusion.
- Normally configured such that it is between the client and the web server.
- Analyses network traffic at the HTTP layer.
- Allows the administrator to define custom input and output rules to perform specific actions.
- Offers forensic logging to record a full activity log, including POST-based attacks.
- The sequence of events that happen with mod_security when an HTTP request comes is :
- Parse the request.
- Perform canonization and anti-evasion actions.
- Perform special built-in checks.
- Execute input rules.
- Mod_security also monitors the response:
- Execute output rules
- Log the complete request consisting of input and output headers, and the request body.

mod_evasive

- mod_evasive Apache's module which provides action in the event of an HTTP DoS or DDoS attack or brute-force attack.
- The module tracks HTTP connections and verifies no. of requests for a page are done within a given time frame. If request large then it is blocked. This blocking is done on an application level.
- The configuration and setup (on Ubuntu) is easy. The module is available as a package:

sudo apt-get install libapache2-mod-evasive

You then have to create the log directory. (Note: Make sure the directory is owned by

the Web user; in most cases, this is www-data.)

sudo mkdir /var/log/mod_evasive

Then enable the module for the Apache Web server.

sudo a2enmod evasive

The configuration file

/etc/apache2/modsavailable/evasive.conf

Add your proxy networks to the DOSWhitelist setting so that you do not block your own network. Also make sure you change DOSEmailNotify to a working email address, otherwise you won't get notifications from mod_evasive.

If you're not sure about the correct configuration options, test your setup with a Perl script that's part of the installed package. The script performs a number of concurrent HTTP queries, which should trigger the module.

perl /usr/share/doc/libapache2-mod-evasive/examples/test.pl

Fail2ban

- Fail2ban scans log files and bans IPs that show malicious signs.
- Block SSH knock attempts, we can also use it to block repeated requests to our Web resources.
- Fail2ban uses a list of regular expressions and checks these expressions against a set of log files.
- Matches occur within certain limit, then the source IP of the request is blocked on a network level.

Similar to mod_evasive, the installation on Ubuntu is easy.

sudo apt-get install fail2ban

After installing the package, you have to copy the default configuration file to a working configuration file.

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Add your proxy networks to ignoreip and set a proper destemail email address for block notifications. I also advise you to set usedns to no.

Fail2ban uses jails to describe services that have to be protected. By default, Fail2ban enables the SSH jail. If you don't want this, then disable the SSH jail. apache-ddos jail to hold the configuration settings for protecting your Web server. Note that you can use pattern matching in the log path (**e.g., /var/log/apache*/*access.log**).

```
[apache-ddos]
enabled = true
port = http,https
filter = apache-ddos
logpath = /var/log/apache2/access.log
findtime = 1
maxretry = 1
```

This will start a jail with the filter apache-ddos. The filters are defined in /etc/fail2ban/filter.d/. Add the file apache-ddos.conf to this location.

```
[INCLUDES]
before = apache-common.conf

[Definition]
failregex = ^<HOST>.* "HEAD / .*
            ^<HOST>.* "POST /xmlrpc.php HTTP.*
ignoreregex =
```

This code will block IPs that do repeated request for HEAD or IPs that do repeated POST requests to xmlrpc.php. If you are not sure about the exact configuration or regular expressions, then have a look at the provided examples (e.g., apache-badbots, apache-noscript, etc).If you list the active firewall rules, the list of blocked IPs can be viewed (iptables -L -n). You can remove a blocked IP with:

Fail2ban-client set apache-ddos unbanip 1.2.3.4

The fail2ban-client command is a useful command-line utility to get the status of the current jails, reload configuration, add

individual IPs to the jail or stop and restart the service.

II. NEED OF STUDY

DDoS attacks, attackers and their campaigns are becoming sophisticated. Attackers are using techniques stalling volume-based attacks to avoid detection and mitigation. They are deploying multi vulnerability attack campaigns that target every layer of the victim's infrastructure, including the network infrastructure devices, firewalls, servers, and applications.

In the following points, we cover the types of DDoS attacks, common methodologies and tools used, of each attack.

III. PROBLEM STATEMENT

DDoS attacks is on the rise, according to security researchers from DDoS attack is a exasperate, threat as unlike other denial of service attacks these attacks requires very some investment by attackers. Slow traffic, legitimate as far as protocol rules and rates are concerned, and normal and complete TCP(Transmission Control Protocol) connections, are the main prerequisites that require the benign appearance typical of DDoS attacks. These attacks require limited resources, so limited investment by attackers can result a successful attack. Traffic in this attack follows the protocol rules, rate and complete TCP handshake process. It follows all the basic requirements that a normal traffic flows The challenge with DDoS attacks is to distinguish human traffic from bot traffic.

IV. HYPOTHESIS

DDoS attacks we can provide their defence method with this DDoS attack that can differentiate between normal traffic and botnet traffic in effective manner using some statistical information of data.

V. RESEARCH METHODOLOGY

CALD: A novel method for detecting Application Layer DDoS attacks
CISCO: Cisco Systems defeating DDoS attack.
CLUSTERING ANALYSIS: Clustering Analysis uses traffic monitoring or web user behavior.
IP ADDRESS: IP Address to detect the attack traffic
DDoS attacks go on increasing every year with bigger size.

VI. RECOMMENDATIONS

- Limit numbers of concurrent connections per source IP.
- Filter foreign TCP packets
- Do not forward packets with header anomalies.
- Monitor self-similarity in traffic.
- Keep unwanted guests away.
- Use specialized DDoS mitigation equipment.
    - Block spoofed TCP attacks before they enter your network.
    - Block unused protocols and ports.
    - Limit the number of access per second per source IP. [1]

VII. CONCLUSION

DDoS attacks become quite common and there is no specific quick fix for it. However, if the system gets DDoS attack, look into the matter and resolve it. DDoS attacks are destructive weapons that hamper business; these attacks are largely adopted cyber warfare to hit the critical infrastructures. DDoS attack targets Organization such as banks, financial institutions, and private businesses. The spreading of botnets, and also the introduction of IPv6, represent a further factor that could raise the important of the cyber threats and the frequency of this type of attacks.

Our dependency on the Internet continues to grow, and the threat of DDoS attacks continues to expand.

- DDoS attacks are very hard to fight, at time of volumetric attack. There are a couple of solutions for Apache Web servers that can limit the harm done by excess traffic and application attacks. Some of these, such as ModSecurity, will filter malicious traffic, whereas other solutions will block traffic on a network level or application level (mod_evasive).

VIII. FUTURE SCOPE

It is clear that one of the major security threats today comes from DDoS attacks. Detection and prevention of DDoS attacks is still an ongoing research. We can see that it is a task to distinguish legitimate traffic from that of the bad traffic. It is very difficult to block the attack traffic without having any impact on the performance of server in providing services to the legitimate users.

In future work we will try to make some effective detection or preventive technique against DDoS attacks.

REFERENCES

[1] Jelena Mirkovic and Reither., April 2004, ”A Taxonomy of DDoS attack and DDoS Defense Mechanisms‖, ACM SIGCOMM Computer Communication” Vol. 34, Issue 2, pp. 39-53.

[2] Stephen M. Specht and Ruby B.Lee, September 2004 “Distributed Denial-of-Service: Taxonomies of Attacks, Tools and Countermeasures‖, Proceedings “17th International Conference on Parallel and Distributed Computing Systems pp. 543-550.

[3] Gulshan Kumar, October-2014, "Understanding Denial of Service (Dos) Attacks Using OSI Reference Model , International Journal of Education and Science Research ,Vol.1,Issue -5.

[4] Isha, Arun and Gaurav raj, JULY 2013 “DOS Attacks on TCP/IP Layers in WSN “, International Journal of Computer Networks and Communications Security VOL. 1, No. 2, 40–45

[5] H.M David, Feb 23, 2004 “Three Different Shades of Ethical Hacking: Black, White and Gray,” in GSEC Practical Assignment, Version 1.4b, Option 1.