International Conference on Multidisciplinary approaches in Social Sciences, Humanities and Sciences
Sri S.Ramasamy Naidu Memorial College, Sattur, Tamil Nadu, India (MASHS-18)
14th December 2018 www.conferenceworld.in ISBN:978-93-87793-61-3

Application Layer DDOS Attack,Layer 7 DDOS Attack :A Major Threat

[1]Divya Mahajan,

[1]Research Scholar, Bhagwant University,Ajmer

[2]Dr.Kalpana Sharma

[2]Assistant Professor, Department of Computer Sciences, Bhagwant University,Ajmer

[3]Dr. Amit Kumar Chaturvedi

[3]Assistant Professor and Head, MCA Dept, Govt Engineering College, Ajmer

Abstract

Internet was envisioned with functionality and not Security in mind. For this reason, its architecture has some inherent feebleness and bugs called vulnerability which results in fruitful origin of DDOS attacks. The main intention of DoS is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. Over the time, researchers projected many solutions to prevent the DDOS attack from different OSI layers, on the other hand none have seen proper positioning and there were a very small number of researches onSeven layers. This paper presents a wide-ranging study on DDoS attacks on application layer, and the extended incidents of such attacks that are clearly increased recently.

Keywords: DDoS attacks, OSI layer, security,.

Introduction

As the internet advances and computer networks become bigger and bigger, network security has become one of the most important factors for the organizations to consider. The Internet was designed with functionality, not security, in mind. Its design opens several security issues that

can be exploited by attackers. Without security measures and controls in place, networks and data are vulnerable to any of the attack like IP Address Spoofing, Password-Based attack, Sniffer attack Eavesdropping, Denial of Service attack etc. Denial of Service (DoS) attacks constitute one of the major threats and among the hardest security problems in today's Internet. A denial-of-service (DoS) attack is an attempt to make a machine or network resource inaccessible to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service(DDoS) is where the attack source is more than one, often thousands of, unique IP addresses. It is analogous to a group of people flocking the entry door or gate to a shop or business, and not allowing legitimate parties enter into the shop or business, disrupting normal operations. They target a widespread variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.Distributed Denial of Service (DDoS) attacks are a virulent, frequent type of attack on the availability of Internet services and resources. DDoS attackers penetrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks.DDoS attack techniques and vectors targeted at web applications can be broadly grouped into three major classes:

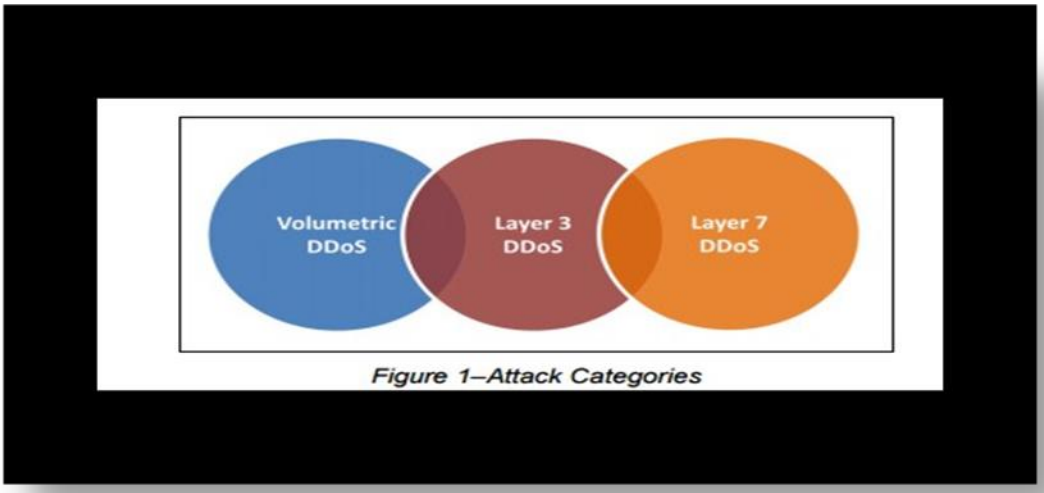


Figure 1–Attack Categories

Volumetric DDoS attacks: Volumetric attacks are tweaked to saturate the bandwidth of the web application‘s hosting infrastructure by directing hefty amounts of network traffic to the target. Volumetric attacks are easy to initiate and do not require identification and supportive exploitation of application weaknesses. These attacks are based on creating blockages in a network or at the target server. It harshly affects the bandwidth of a network causing postponement in serving the genuine request from users. These attacks are merely about theseactivating crowd.

Layer 3 DDoS attacks: Layer 3 attacks target’s weaknesses in the TCP stacks that govern how data is transported between a web application‘s infrastructure devices and operating systems. Attackers launch specially crafted packets designed to overflow and disrupt TCP state information, causing additional work for the network processing functions on the target device and slowing down responses. Historically, the most common Layer 3 DDoS vectors have included TCP SYN floods, TCP fragmentation, Teardrop, and other related low-rate attacks. These are also called as “TCP State-Exhaustion Attacks”

Layer 7 DDoS attacks: Layer 7 DDoS attacks target’sexact weaknesses in the configuration of the web application and intermediary supporting services—causing them to slow down, hang, or smash. The deadliest and hard to prevent are on application layer or also called it as a Layer 7 attack.In most cases, Layer 7 attacks manipulate HTTP requests sent to the web server, exploiting susceptibilities within the web server software or the custom code and business logic of the organization‘s application. By targeting the custom code and business logic of the application, attackers seek to cause the application to become slow and indifferent to authentic users and customers. Traditionally, most successful attacks have focused on causing the application to perform intensive processing functions or exhausting memory handlers.

Because they target specific vulnerabilities and weaknesses in the web application‘s logic and code, it is significantly more difficult to combat Layer 7 attacks using filtering technologies. Organizations must focus on both the design of the application architecture and identify and limit

access to critical logic blocks that necessitate intensive processing or system resources. Our main focus under this paper is on application layer DDoS attacks. This layer is also the most accessible and the most exposed to the outside world. For the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS).

In the diagram below, the Web application is entirely exposed to the outside world in spite of network ramparts such as firewalls and intrusion prevention systems:

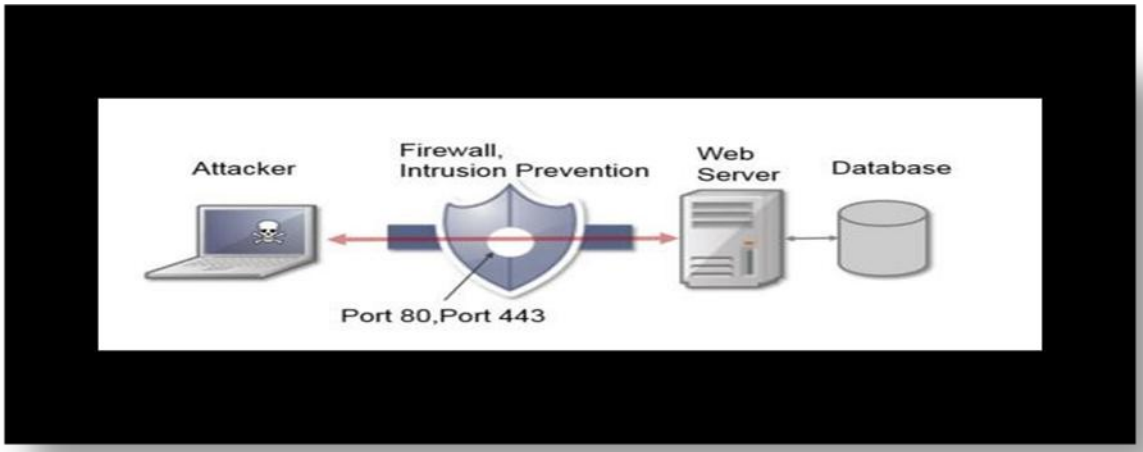


Figure.-2 Application Layer Attack Seven

basic things about layer seven DDoS attacks:

1. Application layer attack the top layer OSI model.
2. They have low bandwidth consumption.
3. They have aauthentic and sneakiness appearance.
4. They‘re mostly non-volumetric.
5. They‘re ever more popular.
6. There are a variety of methods, targets, and open-source tools.
7. They‘re difficult to defend against.

Types of common Layer-7 Attacks: They're divided into four basic categories:

1.Request-Flooding Attacks: High rates of seemingly legitimate(authentic) application requests, such as HTTP GETs, DNS queries and SIP INVITEs), overflow web servers to degrade and disrupt its normal functioning.

2.Asymmetric Attacks: —High-workloadrequests that take a heavy toll of server resources such as CPU, memory or disk space.

3.Repeated Single Attacks: An isolated **—**high-workload request being sent across many TCP sessions, a sneakier way to combine asymmetric and request-flooding layer seven DDoS attacks.

4.Application-Exploit Attacks: The attack vectors here are vulnerabilities in applications, for instance, hidden-field manipulation, buffer overflows, scripting vulnerabilities, crosssite scripting, cookie poisoning, and SQL injection.

Ten Most common Methodologies used by Application Layer attacks:

1. Unvalidated Redirects and Forwards
2. Using Components With Known Vulnerabilities
3. Cross-Site Request Forgery
4. Missing Function Level Access Control
5. Sensitive Data Exposure
6. Security Misconfiguration
7. Insecure Direct Object References
8. Cross-Site Scripting
9. Broken Authentication and Session Management
10. Injections

Review of Literature: This section describes the work done towardsDDoS attacks and the main focus of Literature review is towards Application Layer DDoS attacks.

In 2004, Jelena and Peter et al [1] proposed two taxonomies for classifying attacks and defenses and thus provides us a better understanding of the problem and the current solution space. The attack classification criteria was selected to highlight commonalities and important features of attack strategies and the defense taxonomy classifies the body of existing DDoSdefense based on their design decisions; it then shows how these decisions dictate the advantages and deficiencies of proposed solutions.

In 2004, Stephen M.Specht and Ruby B.Lee[2] describes DDoS attack models and propose taxonomies to characterize the scope of DDoS attacks, the characteristics of the software attacks used and the countermeasures available. These taxonomies illustrates similarities and patterns in different attacks and tools to assist in the development of more generalized solutions to countering DDoS attacks.

In 2000, Felix,Rubin, Smith and Trajkovic [4] describes the methods and techniques used in Denial of service attacks and listed possible defenses. Under this paper simulation is also done using ns-2 simulator.

In 2014, GulshanKumar[3] highlights a structural way to understand DoS attacks with respect to different layers of the OSI reference model. Moreover, various attack vectors, attack tools, trends in detection and mitigation mechanisms are delineated. Several defence mechanisms have been proposed to tackle the problem of DoS attacks.

In 2013, Isha1 ,Arun Malik2 , Gaurav Raj [5] propose some of the security goal for Wireless Sensor Network. To perform any task in WSN, the goal is to ensure the best possible utilization of sensor resources so that the network could be kept functional as long as possible. In contrast to this crucial objective of sensor network management, a Denial of Service (DoS) attack targets to degrade the efficient use of network resources and disrupts the essential services in the network. DoS attack could be considered as one of the major threats against WSN security. And DoS attacks on different layers of OSI are proposed.

In 2009,YiXie and Shun-Zheng Yu[6] proposed a scheme focusing on the detection for application layer attacks . An Access Matrix is defined to capture the spatial-temporal patterns of a normal flash crowd. Principal component analysis and independent component analysis are applied to abstract the multidimensional Access Matrix. A novel anomaly detector based on hidden semi-Markov model is proposed to describe the dynamics of Access Matrix and to detect the attacks. The entropy of document popularity fitting to the model is used to detect the potential application-layer DDoS attacks. Numerical results based on real Web traffic data are presented to demonstrate the effectiveness of the proposed.

Need to study Application layer attacks: The number of DDoS (distributed denial-of-service) attacks that targetweak spots in Web applications in addition to network services has risen during the past years and attackers are using increasingly sophisticated methods to bypass defenses, according to DDoS mitigation experts. So researches should be done to make strong defending systems against application layer DDoS attacks or to prevent them.

Statement of problem: The sophistication and volume of complex Layer 7 DDoS attacks is on the rise, according to security researchers from companies like RivalHostand Prolexic. Layer-7 DDoS attack is a vexing threat as unlike other denial of service attacks these attacks requires very little investment by attackers.Slow traffic, legitimate as far as protocol rules and rates are concerned, and normal and complete TCP connections, are the main prerequisites that entail the benign appearance typical of layer seven DDoS attacks. These attacks require limited resources, so limited investment by attackers can result a successful attack. Traffic involved in these attacks seems to be legitimate as it follows the protocol rules, rate and complete TCP handshake process. It follows all the basic requirements that a normal traffic flows The challenge with applicationlayer attacks is to distinguish human traffic from bot traffic.

Objectives: Our main target under this paper is to study the application layer attacks, their types, Methods used by attacks ,some existing methodologies used to detect application layer attacks

so that we have clear depiction about application layer attacks, and we can do more work to proposed some effective defending mechanisms against Application layer DDoS attacks that is layer 7 Ddos attack.

Hypothesis: We can have some strong security mechanism against application layer attack that can differentiate between normal traffic and bot traffic in effective manner using some statistical information of data or using artificial intelligence techniques like fuzzy, neural networks etc.

Methodologies to detect Application Layer Attacks:

DETECTION CATEGORY	APPROACH
Session History	"DDoS- shield" uses session history to detect the attack
Traffic Monitoring/ Web User Behavior	"CALD", "A novel method for detecting application layer DDoS attacks", "An effective approach to counter application layer DDoS attacks", "Cisco Systems Defeating DDoS Attacks "and "Application layer DDoS detection using Clustering analysis" uses Traffic monitoring or Web user behavior.
Clustered User Sessions	"Detection and offense mechanism to defend against application layer DDoS attacks" uses K-means clustering method to detect attacks. "Application layer DDoS detection using Clustering analysis" uses clustered user sessions.
Pattern recognition	"An effective approach to counter application layer DDoS attacks" and "Timeslot monitoring model for application layer DDoS attack detection" uses pattern recognition to detect an attack.
IP address	"A three layer defense mechanism based on web servers against DDoS attacks" uses IP address to detect the attack traffic.
Signature	"A novel framework to detect and block DDoS attack at application layer" uses signature to determine whether the user is suspicious or not.
Packet Marking	"IP Trace back system for network and application layer attacks" uses packet marking method.

Table 1: Classification Based on Detection Categories

Results and discussions: As we can see from the figure3 that application layer attacks go on growing every year with bigger size. Arbor, in their 2015/Q1 Global DDoS Attack Trends Report, revealed that 17% of all attacks they handled were bigger than 1Gbps and the average size of the attacks was 804Mbps / 272K pps. The big ones peaked at 335Gbps.

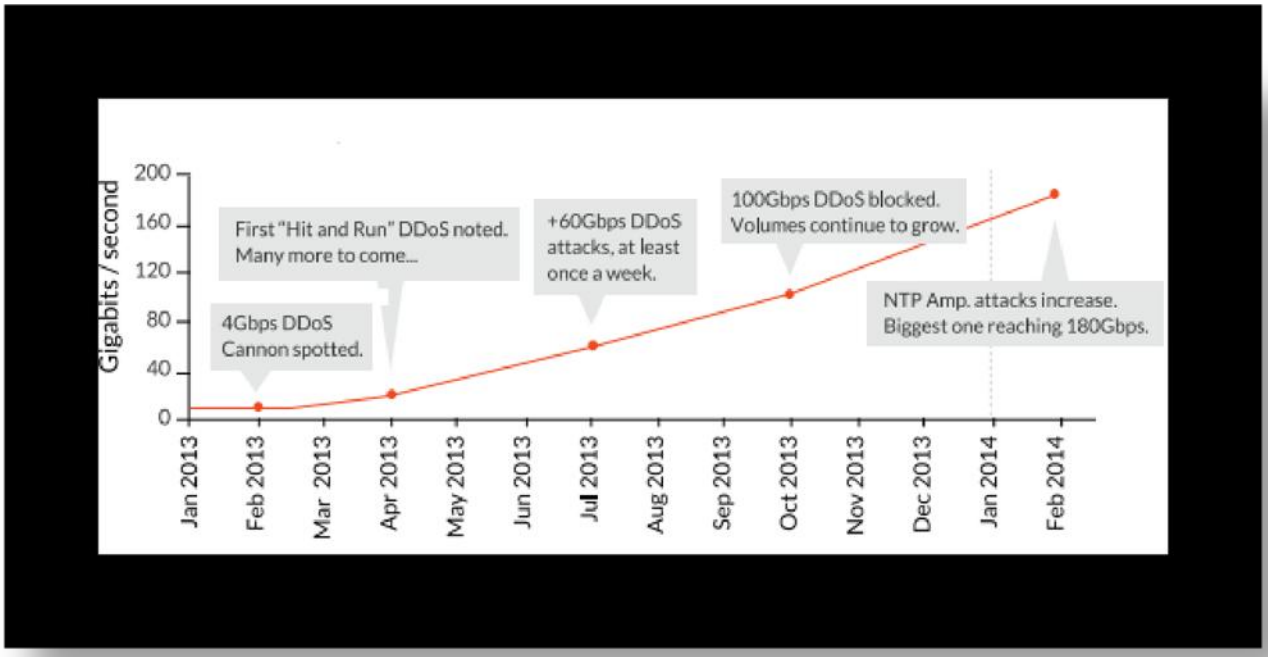


Figure 3: Application Layer attacks overview

Web application attack metrics:

Compared with Q2 2015

- 96.36% increase in HTTP web application attacks
- 79.02% decrease in HTTPS web application attacks
- 21.64% increase in SQLi attacks
- 204.73% increase in LFI attacks
- 57.55% increase in RFI attacks
- 238.98% increase in PHPi attacks

Comparison with other types of DDoS attacks Compared to Q2 2014

- 132.43% increase in total DDoS attacks
- 122.22% increase in application layer (Layer 7) DDoS attacks
- 133.66% increase in infrastructure layer (Layer 3 & 4) attacks
- 18.99% increase in the average attack duration: 20.64 vs. 17.35 hours
- 11.47% decrease in average peak bandwidth
- 77.26% decrease in average peak volume

100% increase in attacks > 100 Gbps: 12 vs. 6

Compared to Q1 2015

7.13% increase in total DDoS attacks

17.65% increase in application layer (Layer 7) DDoS attacks

6.04% increase in Infrastructure layer (Layer 3 & 4) attacks

16.85% decrease in the average attack duration: 20.64 vs. 24.82 hours

15.46 increase in average peak bandwidth

23.98% increase in average peak volume

50% increase in attacks > 100 Gbps: 12 vs. 8

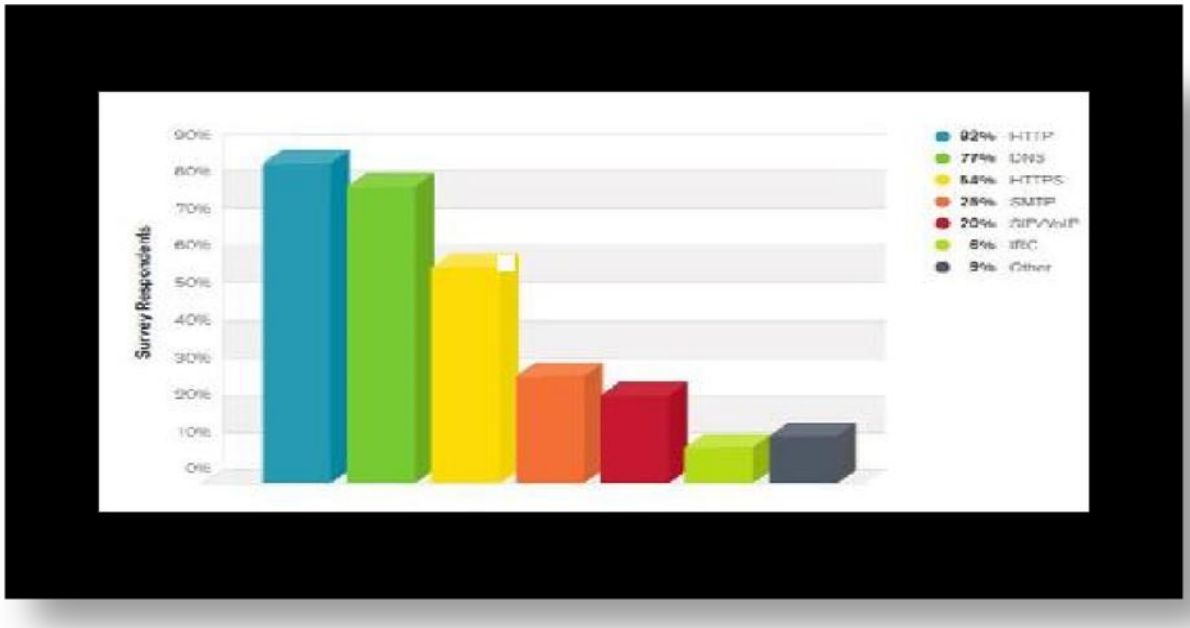


Figure 4-Targets of application layer attacks(Arbor reports)

In Q2 2015, we saw approximately 15 percent of all application layer DDoS traffic evolving from

China—followed by Vietnam, US, Brazil and Thailand. The final was home for most of the MrBlack-infected routers, used in a mass-scale DDoS campaign we reported about one month ago.

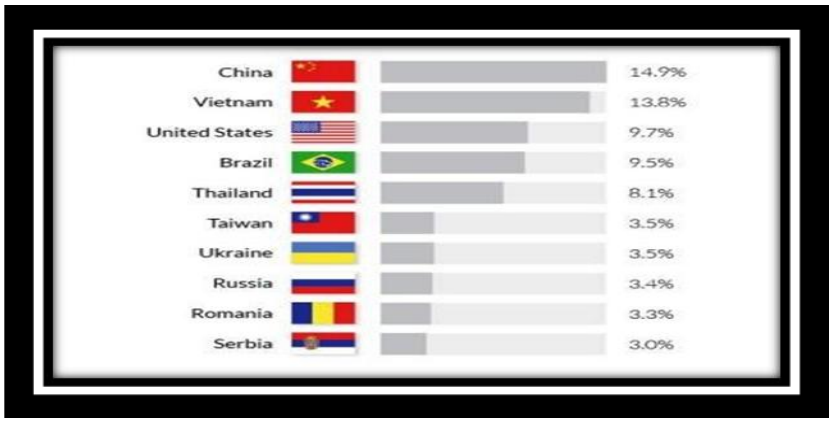
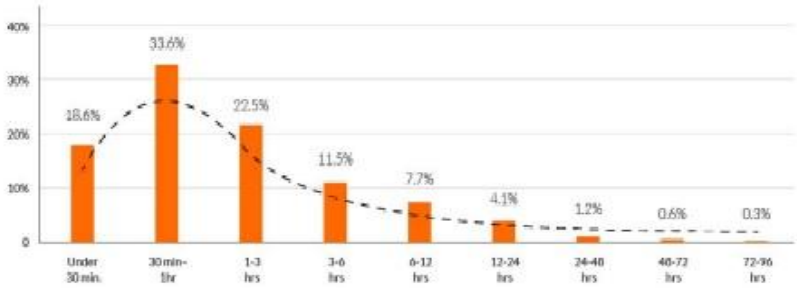


Figure 5-Top 10 Source Countries For Application Layer attacks according to Q1 2015

The lengthiest application layer attack lasted for eight straight days, with the average duration stretching for just over two and a half hours. Once initially targeted, a website will be hit again every ten days on average.

Figure 6- Largest Application Layer attack this past quarter peaing at 179,747 RPS



Illustrated in the Figure 7 below, most application layer attacks (just under 98 percent) lasted under 24 hours, with 52 percent being no more than one

Figure 7-Distribution of application layer attacks by duration

Application Layer Attacks with Possible Defenses		
Name	Categories	Possible Defenses
HTTP	Viruses and Worms	
	SQL injections	• Parametrized queries • Stored procedure • Vulnerability Scanning & Penetration testing
	Cross-site Scripting	• Web developers can implement filtering code for all user input to remove potentially noxious characters, or convert them to something that a browser will not run • Secure Coding Practice • Penetration testing /
		Ethical Hacking
FTP	Directory Traversal Attack	• Web Vulnerability Scanners • Patching Browsers
SMTP	SMTP Worm	Configure your routers and switches to reject packets originating from outside your

	Email Spoofing IP Spoofing	local network that claim to originate from within	
DNS	Man-in-the-Middle Attack		

Table 2: Defense mechanism of application layer attacks

As the number of DDoS attacks increasing over the past year, it is important that network engineers, designers, and operators build services and monitor networks in the context of defending against DDoS attacks.

Conclusions:DDoS attacks pose a severe problem on the Internet and challenge its rate of growth. We hope we were able to provide some insights on the size and types of the Application layer (Layer-7) attacks we are seeing in the wild and help bring more attention to this type of threat. In this paper, we attempted to attain a clear view of the DDoS attack problem, and presented an updated perspective of the problem in respect to different layers of the OSI reference model. Having, this clear view of the problem, our understanding about the problem is clarified and this way we can discover more effective solutions against application layer DDoS attack.

Recommendations/suggestion

- 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.
- Don‘t let dark address packets pass your perimeter.
- Block unused protocols and ports.
- Limit the number of access per second per source IP.

Scope for further study:It is clear that one of the major hazardous security threats today comes from DDoS attacks. Detection and prevention of DDoS attacks is still an ongoingresearch.We can see that it is a tedious task to distinguish legitimate traffic from that of the bad traffic. It is even more difficult to block the attack traffic without having any impact on the performance of server in providing services to the legitimate users. In Our future work we will try to make some effective detection or preventive technique against DDoS attacks.

Acknowledgment: I would like to thank the anonymous referees for their helpful comments and suggestions to improve this work. I would also like to thank Prof. Dinesh Grover and Prof. AbhinavBhandari for his careful reading and valuable suggestions for the improvement of the paper‘s presentation.

References

[1] JelenaMirkovic and Reither.—A Taxonomy of DDoS attack and DDoSDefense Mechanisms‖ ,*ACM SIGCOMM Computer Communication,*Vol. 34, Issue 2, pp. 39-53, April 2004.

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

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

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

[5] Yi Xie and Shun-Zheng . ―Monitoring the Application-Layer DDoS Attacks for Popular Websites ‖ IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 17, NO. 1, FEBRUARY 2009

[6] http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

[7] http://www.digitalattackmap.com/understanding-ddos/

[8] http://ce.sharif.edu/~baki/Monitoring%20the%20Application-Layer%20DDoS%20Attacks%20for%20Popular%20Websites.pdf

[9] http//blog.sucuri.net/2015/09/analyzing-popular-layer-7-application-ddos-attacks

[10] http//www.morningstar.com/pr-news-wire/PRNews20151208NE75270/alkai-releases-q3-2015-state-of-internet-security-report.print.html