RESEARCH ARTICLE OPEN ACCESS

Identification Of DDoS Attack On Web Servers

Ruchikaa Nayyar [1], Harshita [2]
Department of Information Technology
IGDTUW
New Delhi - India

ABSTRACT

The rapid growth in technology has resulted in more and more people getting online. People, now-a-days are dependent on internet to do most of their jobs like paying bills, shopping, communicating with friends and family, searching Internet for information on various topics, events, conferences etc. However, any disruption to this proves to be disastrous to social and business network. One such disruption can be DOS/DDOS attacks. In modern world of internet and everything getting online, DDOS attack is one of the major problems. It is one the most vulnerable attack that can happen to a web server to crash it or stop from providing services. One of the most recent form of DDOS attack are HTTP flood DDOS attack .Detecting HTTP flood DDOS attack is quite difficult as it uses HTTP protocol to launch the attack, and hence, easily by passes the first line of defence like firewall, IDS etc. Many techniques have been proposed to detect and resolve the attack but it is very difficult to explore and solve every loophole since internet is very vast. DDOS attack on web server can be very disastrous. This paper focuses on a) analysing the raw logs of an APACHE web server and then, b) identifying various parameters from the raw logs that could be used to distinguish incoming request to the web server as being legitimate or malicious. And finally c)validating each incoming request (it's parameters) to the web server against identified parameters from the raw logs . This , thus finally results in identification of malicious request to the web server that could lead to a potential DDOS attack.

Keywords:- Denial-of-Service (DOS), Distributed Denial-of-Service(DDOS), IP Spoofing

I. INTRODUCTION

Information security deals with large number of subjects like spoofed message detection, audio processing, video surveillance and cyber-attack detections. However, the biggest threat for the homeland security is cyber-attacks. One such attack is DDOS (DISTRIBUTED DENIEL-OF-SERVICE) attack. Interconnected systems such as database server, web server, cloud computing server, etc., are now under the threat from network attackers. DDOS attack is a common attack in the internet that causes the problem for both users and service providers.

DOS (DENIEL-OF-SERVICE)ATTACK-A CYBER ATTACK where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. It is achieved by flooding the victim with superfluous request in an attempt to overload the system and prevent it from fulfilling some or legitimate request.

DDOS (DISTRIBUTEDDENIEL-OF-SERVICE) ATTACK-A cyber attack that attempts to make online services unavailable to its legitimate users by flooding the server with traffic from multiple compromised machines (called zombie machines). DDOS attack is very severe when they happen to important server such as banking and government websites. DDOS attacks can be carried out using different methods.

A. DDOS ATTACK METHODS

1. *DIRECT ATTACK*: In this victim is flooded with superfluous request sent from large number of zombie machines. In this, no intermediate machine is being used. This type of attack can be further be classified as

NETWORK LAYER: This involves attacks occurring at network layer such TCP flood, SYN flood, UDP flood and ICMP flood

APPLICATION LAYER: This involves attack occurring at application layer like HTTP flood, FTP flood etc.

2. *REFLECT ATTACK:* In this, the zombie machines firstly send the packets to the reflector to spoof the source IP address of the victim server.

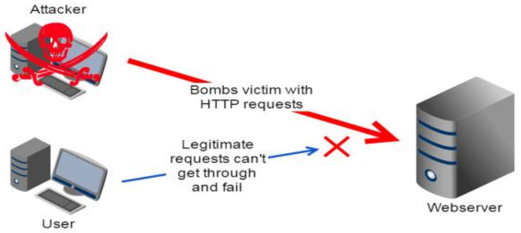

Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

Figure1. Illustrating DDOS ATTACK

B.TYPES OF DDOS ATTACKS:

1. *Volume Based Attacks:*

Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

2. *Protocol Attacks:*

Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in Packets per second.

3. Application Layer Attacks:

Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or Open BSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second.

4. UDP FLOOD:

This types of attack floods the victim machine with UDP packets. In this, attacker sends large number of UDP packets to random ports on the remote machine. causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. Thus, for a large number of UDP packets, the victimized . may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return Packets do not reach them.

5. ICMP FLOOD:

In this attacker floods the victim machine with the ICMP echo request packet (ping packets). In this, server reply with ICMP echo reply packet and thus, enabling consumption of both incoming and outgoing bandwidth. This thus results in breakdown of the system.

6. SYN FLOOD:

This attack exploits the vulnerability in a 3-way handshake mechanism of TCP protocol. In 3-way handshake mechanism, SYN packets are first sent to establish a connection with the other machine. The other connecting machine then responds with ACK packet if it wants to establish a connection with the first machine. Now, in response to ACK packet first machine needs to send ACK+SYN packet to ensure the other machine that you want to establish a connection with the other machine. In this attack, attacker sends multiple SYN request to the victim using spoofed IP so that the reply doesn't reach his machine and these multiple SYN request flood the victim machine thus preventing the victim from responding to request of genuine clients.

7. PING OF DEATH**:**

In this attack, attacker sends malformed PING packets to the victim. The maximum permissible size of the packet is 65,535 bytes. In this attack, attacker sends ping packets with packet size greater than maximum permissible limit. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

8. HTTP FLOOD

In this attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

C. IP SPOOFING

It is technique by wherein a host creates a IP packet with false IP address in order to hide their identity

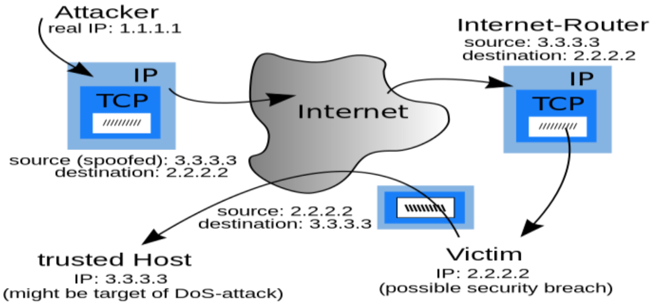


Figure2. IP Address Spoofing

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, attacker sends IP packets with source address of some other machine on the network to hide its identity and carry out a malicious activity. Major use of this IP spoofing is in the DDOS attacks. DDOS attacks floods the victim machine with superfluous request that appears to be legitimate users but are actually IP packets sent by attacker from his machine using the IP address of some other machine in the network as its source address in IP header of the IP packet.

There are two ways in which IP spoofing can be used to flood the target with malicious traffic. One method is to simply flood the target with packets from multiple spoofed address. This method works by sending target machine more amounts of data than the target machine can handle. The second method is to send the IP packets with the address of the target machine as the source address from attacker machine to all other machine in the network. When these machines on the packet will receive the packet they will automatically reply to the source of the packet which in turn will flood the target machine with large number of reply from the various machines in the network.

IP spoofing can also be used to by-pass IP address based authentication mechanism. Many connecting machines depend on IP address for authentication rather than user logins. In such scenario, an attacker perform an IP spoofing attack to hide its malicious packet in the source address of some other machine on the network which can be useful to by-pass the authentication mechanism.

II. RELATED WORK

DDOS attack is one the major security concerns for networks and web servers. It is a most vulnerable attack that can happen to a web server to crash or stop it from providing services to the legitimate request. Many techniques have proposed to identify and mitigate DDOS attack, but all these techniques have resolved these to a certain extend but it is really difficult to explore each vulnerability in the since

Internet is a vast domain. Some of the DDOS attack detection techniques are explained below:

[1],Mohammad Alenezi and Martin J.Reed suggested a technique, Detection using TCP congestion window analysis, this approach is used to detect TCP flood attack by using TCP congestion window which is analyzed using cumulative sum (CUSUM). This approach focuses on various parameters like address, port, protocol etc. It detects two sided function of both positive side and negative side. After analysis of CUSUM value congestion window detection will be used to detect the attack. When an attack occurs, congestion window will be affected and that is analyzed by CUSUM and CUSUM alerts the CUVDT about the attack. By using congestion window value, the DDOS attack is detected.

[2] B. Liu, J. Bi, A. V. Vasilakos suggested Mutual egress filtering technique for detecting malicious traffic, this approach provides detection against IP spoofing based DDOS attack using real internet dataset for obtaining simulation results. Since, this approach uses egress filtering so ingress/egress filtering rules are applied using ACL (Access Control List) of autonomous system. This approach however, protects only those systems that deploy this mechanism and prevent other non-deplorers from using this mechanism. By using mutual egress filtering technique, false positive rate reduces.

[3] F. Soldo, K. Argyraki, A. Markopoulou presented Source based filtering approach, in this approach applies ACLs (Access Control List) at the routers. These ACLs uses some predefined rules for blocking IP address of prefixes of predefined type. One major disadvantage with using ACLs is that these ACLs are stored in ternary content addressable memory and that makes accessing ACLs quite expensive and also ACLs consumes more power and space. This problem is resolved by formulating filtering rules as optimization problem for blocking attackers with minimum damage and limited filters.

[4] Archana .S. Pimpalkar, A. R. Bhagat Patil proposed, Hash based cryptographic technique, hashing technique is used for authentication of packets transmitted between clients and servers. In this approach, certain fields of IP header of IP packets are encrypted using a secret key. This secret key is generated using the Type-of-Service field of IP header. Last 2 bits of this field are used for key generation. Different combinations of these 2 bits results in generation of different keys. Secret key is generated by EX-OR of source address with identification filed of packet header if last 2 bits of Type-of-Service field are 10 and if last 2 bits are 11 then source address is EX-ORed with flag field of IP header. HMAC is used for encryption. Border router of clients attaches this secure information to all forwarded packets towards server which is verified by border router of receiving network. Based on this verification packets are classified as attack packets or genuine packets.

[5] Stavros N.Shiaeles, Vasilios Katos, Alexandros S.Karakros, Basil K.Papadopoulos, Fuzzy estimator approach, in this approach the DDOS attack is identified during the run time. In earlier derived techniques a DDOS attack is identified after its effect are felt, but using this approach a DDOS attack is identified at the time it is happening and before it affects the system. This approach uses fuzzy estimator to identify a DDOS attack and also the suspect host that is participating in the attack. Attack is identified by packet arrival interval and number of packets sent. In this approach the maximum number of packets that the server or the machine will accept will be set prior. Now, if the amount of packets reaching the server or the machine exceeds the maximum permissible limit then it is identified as attack. And such packets will be dropped immediately. Major disadvantage of this approach is identification of false positive, this means when a genuine user also sends large number of packets more than the permissible amount of packets then that user will also be considered as an attacker his packets will be dropped and he will not be provided any servicers.

[10]K.Narasimha Malliarjunan, K.Muthipriya, Dr. S.Mercy Shalinie, suggested Detection using fast entropy approach, in this approach ADAPTIVE algorithm is used to detect a DOS attack. This technique focuses on continuously monitoring the incoming traffic flow and notes the traffic count value at particular time interval. The DOS attack is identified by high traffic count value and thus resulting in drastic drop in entropy because there is one flow count that is dominating. However, there will be a consistent entropy value in case of normal traffic flow. This technique is based on IP header information. This technique does not care about the data in the flow, rather focuses on the IP header information like IP address of source and destination and also the traffic flow details. There is one major disadvantage about this technique, attacker can send packets from different sources with less traffic flow so that this technique does not detect sudden increase in the traffic flow count value and entropy remains consistent.

III. METHODOLOGY

The strategy adopted in this research paper is bifurcated into different modules. These modules are

A. Collection of Logs

Collect the raw logs of an APACHE web server and analyse those logs to identify various parameters that can be used to identify a potential DDOS attack on web server.

B. Identification of Parameters

Identify various parameters from the raw logs such as

Different IP address

Counter hits from each IP address

Browsing length Ratio (how quickly client browses through different urls)

Average stay time on each web page

Bandwidth utilization by each client

Most commonly used operating system by client

Timestamp of each request made by the client

C. Validation of Incoming HTTP Request

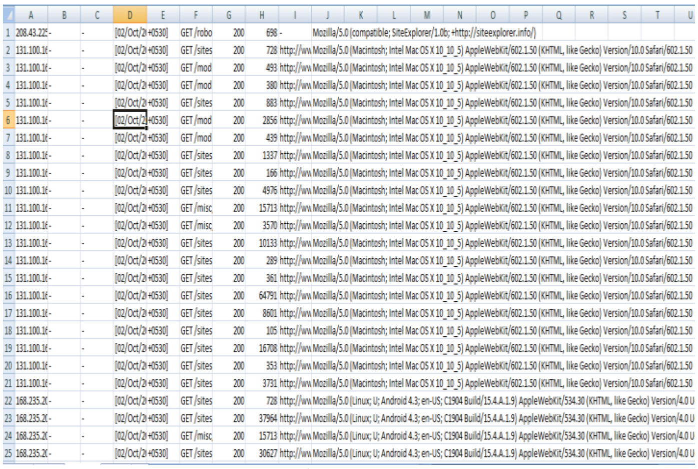
For each incoming request to the web server, compare this request and its various parameters with the threshold value of parameters identified above.
If for any request, the parameters values exceeds the threshold value then categorize those request made by the client and its IP address as being malicious.

D. Conclusion

By validating each request made to the web server, we identified those IP address which could lead to a potential DDOS attack on the web server.

IV. INDENTIFICATION

Raw logs of an APACHE web server are analysed to identify various parameters that can be used to detect a potential DDOS attack to the web server.



	A	B	C	D	E	F	G	H	I	J
1	208.43.22	-	-	[02/Oct/2	+0530]	GET /robo	200	698	-	Mozilla/5.0 (compatible; SiteExplorer/1.0b; +http://siteexplorer.info/)
2	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	728	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
3	131.100.16	-	-	[02/Oct/2	+0530]	GET /mod	200	493	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
4	131.100.16	-	-	[02/Oct/2	+0530]	GET /mod	200	380	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
5	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	883	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
6	131.100.16	-	-	[02/Oct/2	+0530]	GET /mod	200	2856	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
7	131.100.16	-	-	[02/Oct/2	+0530]	GET /mod	200	439	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
8	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	1337	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
9	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	166	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
10	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	4976	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
11	131.100.16	-	-	[02/Oct/2	+0530]	GET /misc	200	15713	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
12	131.100.16	-	-	[02/Oct/2	+0530]	GET /misc	200	3570	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
13	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	10133	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
14	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	289	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
15	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	361	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
16	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	64791	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
17	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	8601	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
18	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	105	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
19	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	16708	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
20	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	353	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
21	131.100.16	-	-	[02/Oct/2	+0530]	GET /sites	200	3731	http://ww	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50
22	168.235.20	-	-	[02/Oct/2	+0530]	GET /sites	200	728	http://ww	Mozilla/5.0 (Linux; U; Android 4.3; en-US; C1904 Build/15.4.A.1.9) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 U
23	168.235.20	-	-	[02/Oct/2	+0530]	GET /sites	200	37964	http://ww	Mozilla/5.0 (Linux; U; Android 4.3; en-US; C1904 Build/15.4.A.1.9) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 U
24	168.235.20	-	-	[02/Oct/2	+0530]	GET /misc	200	15713	http://ww	Mozilla/5.0 (Linux; U; Android 4.3; en-US; C1904 Build/15.4.A.1.9) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 U
25	168.235.20	-	-	[02/Oct/2	+0530]	GET /sites	200	30627	http://ww	Mozilla/5.0 (Linux; U; Android 4.3; en-US; C1904 Build/15.4.A.1.9) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 U

Figure 3. Raw logs of an APACHE web server

Below shown are the various parameters identified from the raw logs of an APACHE web server along with their values for various request made to the web server.

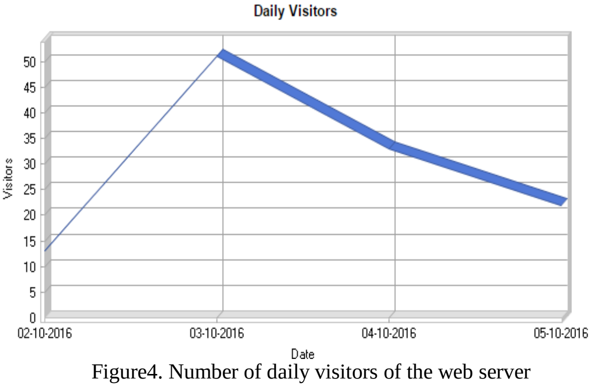


Figure4. Number of daily visitors of the web server

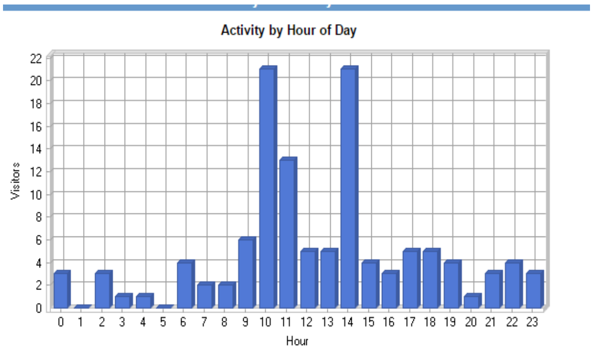
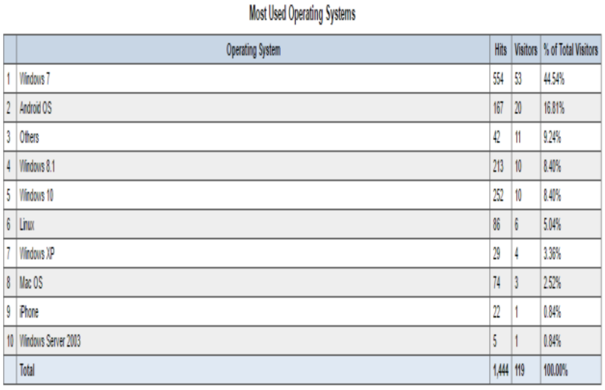


Figure 5. Number of hourly visitors to the web server



Most Used Operating Systems

	Operating System	Hits	Visitors	% of Total Visitors
1	Windows 7	554	53	44.54%
2	Android OS	167	20	16.81%
3	Others	42	11	9.24%
4	Windows 8.1	213	10	8.40%
5	Windows 10	252	10	8.40%
6	Linux	86	6	5.04%
7	Windows XP	29	4	3.36%
8	Mac OS	74	3	2.52%
9	iPhone	22	1	0.84%
10	Windows Server 2003	5	1	0.84%
	Total	1,444	119	100.00%

Figure 6. operating system used by visitor along with their counter hits

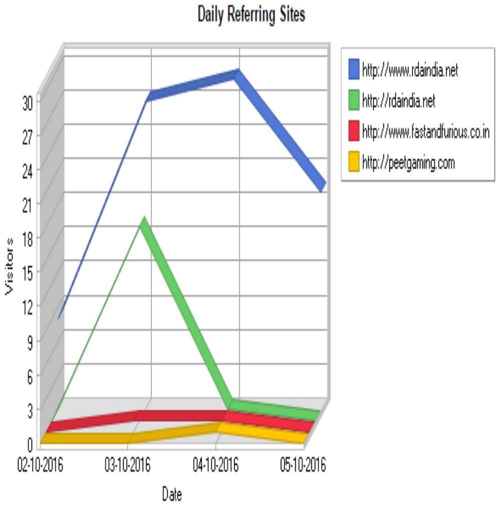


Figure 7. Daily referring sites by visitors(Browsing length Ratio)

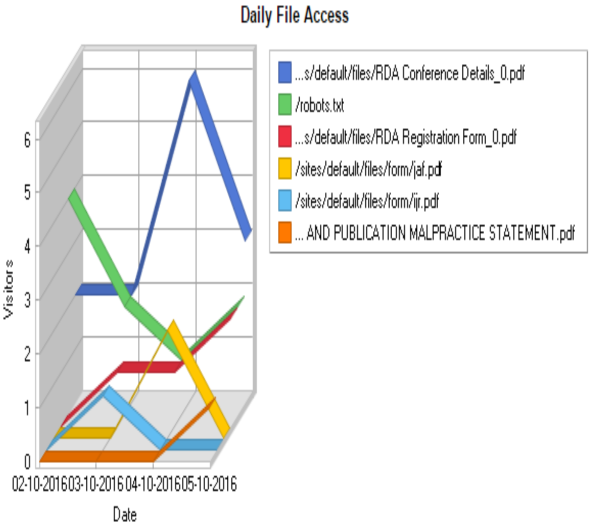


Figure 8. Daily file access by visitors

Using various parameters identified from the raw logs of an APACHE web server, each incoming request to the web server is validated against each of these identified parameters and their threshold value , so as to identify each request(s) made to the web server that could result in a potential DDOS attack.

V. RESULTS

By analysing raw logs of an APACHE web server we identified various parameters that are used to validate each incoming request to the web server. The parameters that can be considered for this purpose are packet size, packet type, operating system, time duration of each request, time difference between consecutive requests, error codes, average stay time, browsing length ratio, bandwidth utilization by each request etc.

VI. CONCLUSION

DDOS attacks are one of the major security concerns. They have the potential to crash a web server and cause severe damages to business and reputation of the organization. Not only detecting these attacks is important but also certain mitigation policies must be developed so as to prevent them from damaging any web server or its business. In this project, based upon the various parameters of the web server logs and their threshold value, each incoming request to the web server is validated against each of these parameters and their threshold value. And if for any request, it's parameter(s) values exceeds the threshold value then those request along with their IP address(s) are categorized as being malicious and could be responsible for a potential DDOS ATTACK

REFRENCES

[1] Mohammad Alenezi, Martin J.Reed, "Deniel Of Service Through Tcp Congestion Window Analysis", "In World Congress On Internet Security, 2013"

[2] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti-Spoofing Deployment", Ieee Transactions On Information Forensics And Security, 2014

[3] F. Soldo, K. Argyraki, A. Markopoulou, "Optimal Source-Based Filtering Of Malicious Traffic", Ieee/Acm Transactions On Networking, 2012.

[4] Archana .S. Pimpalkar, A. R. Bhagat Patil, "Defense Against Ddos Attacks Using Ip Address Spoofing", International Journal Of Innovative Research In Computer And Communication Engineering ,2015

[5] Starvos N.Shiaeles, Vasilios Katos, Alexandros S.Karakros, Basil K.Papadopoulos, "Real Time Ddos Detection Using Fuzzy Estimators", "Eslevier Computer And Security", 2012

[6] Darshan Lal Meena, Dr.R.S Jadon, "Distributed Denial Of Service Attacks And Their Suggested Defense Remedial Approaches", International Journal Of Advance Research In Computer Science And Management Studies, Volume 2, Issue 4, April 2014

[7] G. Usha Devi*, M. K. Priyan, E. Vishnu Balan, C. Gokul Nath And M. Chandrasekhar, "Detection Of Ddos Attack Using Optimized Hop Count Filtering Technique", Indian Journal Of Science And Technology, October 2015

[8] Mandeep Pannu, Bob Gill, Robert Bird, Kia Yang, Ben Farrel, "Exploring Proxy Detection Methodology", 2016 Ieee

[9] Ann Mary Jacob1, Saritha, "Survey On Various Ip Spoofing Detection Techniques", International Journal Of Science And Research (Ijsr), Volume 2 Issue 11, November 2013

[10]K.Narasimha Malliarjunan, K.Muthipriya, Dr. S.Mercy Shalinie, "A Survey Of Distributed Deniel Of Service Attack", Ieee,2015

[11] Saman Taghavi Zargar James Joshi, David Tipper, "A Survey Of Defense Mechanisms Against Distributed Denial Of Service (Ddos) Flooding Attacks", Ieee Vol. 15, No. 4, Fourth Quater, 2013