DDOS and Compilation of Mitigation Techniques

Ayush Goyal
Department of Computer Science & Engineering
Jaipur Engineering College and Research Center
Jaipur, Rajasthan, India

Palak Baid
Department of Computer Science & Engineering
Jaipur Engineering College and Research Center
Jaipur, Rajasthan, India

ABSTRACT
In network communication, attackers often breach the security. Therefore, keeping the data and servers secure is a very crucial task. Among several online attacks, DDOS is the most devastating attack. This attack has the most ravaging effect on the servers. There exists a tremendous pressure on security experts to mitigate the annihilating effects of this attack. In this paper, we have done a comprehensive research on types of DDOS attacks and mitigating its effects. Albeit this attack cannot be fully curbed, it can be extenuated to a certain extent.

General Terms
Attacks, Packets, Filtering, Mitigation Techniques

Keywords
DOS, DDOS, IP Spoofing, Amplification, TCP

1. INTRODUCTION
Internet has become an integral part of our lives. It finds its applications in day to day life such that imagining a life without internet is unfathomable. But on the flip side, there are also some risks accompanied along with the plethora of benefits that internet has to offer. Imagine a scenario when your favorite website stops providing you services, or a scenario when a website on which you are dependent isn't responding to your requests. You are being denied the service by that website. At the same time, millions of users might not be getting a response if the website servers aren't up. But why would a website's servers be down? Why would any website deny services to its users and incur the business loses? A business will never do that, but the attackers will. Attackers might overwhelm the server by a large number of illegitimate requests in order to consume its maximum bandwidth, such that the server slows down and it isn't able to respond to legitimate requests. This is exactly what a DOS (Denial of Service) attack is. In DOS attack, the attacker sends large number of packets to the target server, so that the target's resources are consumed and exhausted, as a result of which it will not be able to respond to new requests and will eventually lead to denial of service to its end users. There can be numerous reasons why an attacker might target a particular server for a DOS attack, some of which can be revenge, animosity, political motivation, or financial benefits such as asking for ransom to stop the attack. But DOS attacks couldn't survive for long, because they are easy to detect and block. So the attackers came up with a new type of attack, abbreviated as DDOS attack (Distributed Denial of Service attack). In DDOS attack, the attackers compromise a large number of computers on the network through the root kits (without the knowledge of the host being compromised), which are also known as botnets, and use these botnets to flood the target server. The requests are reaching the victim (target server) from hundreds or thousands of hosts, and so it becomes difficult to detect and block such attacks. Many big organizations such as Dyn (the company which controls most of the DNS infrastructure), BBC, Twitter, Netflix, PayPal, Visa, StackOverflow and GitHub have been DDOSed in the past. The DDOS attack carried out on GitHub servers on 28th February 2018 was the largest DDOS attack in history of cyber-attacks, with traffic flowing in at the rate 1.35 terabits per second. Virgin Blue airline lost $20 million in 2010 due to such attacks. DDOS attacks are expected to be increased by 260% by 2020. Gaming sector is most susceptible to DDOS attacks, accounting for 50% of all DDOS attacks, according to Akamai's research. Completely protecting and detecting DDOS attacks has been impossible till date, but there are preventive measures which could be taken to prevent the servers from being DDOSed. With the help of counter measures, the effects of DDOS attacks can be mitigated to a particular extent, but one cannot be sure that the server would always sail on a safe harbor.

2. LITERATURE REVIEW
Darshan Lal Meena et al. in their paper [1] have explained various attacks of DOS and DDOS, possibility to eliminate this attack and several defense techniques. Complete strategies are not available both academically and industrially to eradicate this attack. They concluded by explaining the main problem which is that there are many machines over internet that can be undermined to launch DDoS attack. The only solution is to circumscribe the defense activities to curb DDoS attacks.

Qijun Gu et al. in this paper [2] has provided the overview regarding the DOS attacks, protection and it's mitigation techniques. They have explained Network based attacks and Host based attacks. Host based attacks use specific algorithms [3], memory structure, [4], authentication protocols [5], implementation [6]. Also, there is an explanation for different types of DOS/DDOS attacks which are classified based on material presented in [7]. Different attacks and their protection and defense techniques in wireless network are also described. They concluded that only securing the servers is not enough because the DDOS attacks are more complicated. They have addressed one of the various problems i.e. to distinguish legitimate traffic from flooding traffic, and to identify the attacking host, how to control flooding traffic. These results can manage to control the attack to the most extend but cannot completely cease them.

3. DOS ATTACK
Cyberspace today is more vulnerable to threats than ever. Attackers are constantly coming up with new attacks to divulge the servers for personal benefits. Even if some attacks are identified and curbed, some attacks are onerous to stop once they have started. One such attack is DOS attack. DOS stands for Denial-of-service, cardinal purpose of which is to flood the server or the network with illegitimate packets, so that the network's resources are consumed and it denies service to legitimate users. The DOS attack generally

originates from a single source, which is used to send copious number of packets. Moreover, the attacker sends the packets with invalid return addresses, so that the server cannot return packets to those addresses, as a result of which the connection is not completed, and the target server keeps on waiting to complete the connection until the connection times out. Meanwhile, attacker floods the victim with more such requests, until the victim is completely taken down. Such attacks might be launched by hackers for personal benefits (financial benefits, revenge, negative publicity), by hacktivists who want to spread a social message, or by the company itself to test its server's ability to respond to such attacks. The attackers identify the IP address of the target server, and launch an attack with the help of tools or online services. The attackers take advantage of vulnerability of TCP/IP protocol, which uses a 3-way handshake technique to open a trusted connection. The attacker sends large number of SYN packets (with invalid return address) to the target server, and the server replies with SYN-ACK response for each SYN packet. Under normal circumstances, an ACK packet would be sent back to the server in response to SYN-ACK packet to complete the three-way handshake and hence making a secure TCP connection. However, under DOS attacks, the ACK packet never actually arrives back at the server. The packet does not arrive because the SYN packet received at first place has an invalid address, so SYN-ACK packet is being reverted to that invalid address which doesn't respond with ACK packet to the server. So, the server keeps on waiting for ACK packet until the time out. This happens for all the packets that the attacker has sent. This is known as SYN-flood attack. Eventually, the bandwidth of the server is consumed, the server is consumed in replying to the new illegitimate requests, as well as in waiting for the older ones to complete the connection. Until then, the new legitimate requests are put in the waiting queue. Thus, in this way a denial of service attack is carried out and the victim ends up denying the service to its actual users. The main aim of this attack is not to steal the sensitive data, but to take down the target server. However, there are certain ways to prevent this attack. The adage "Prevention is better than cure" fits here perfectly. It is always better to make your servers secure beforehand rather than trying to stop the attacks after they have been launched. Preventive measures can be applied at firewall level (deep down the network hierarchy), or at the ISP level. Although DOS attacks can be curbed after they are identified, but if left unidentified it can lead to devastating results. Firewalls or IP tables can be used to block the attacker's IP address if it is not spoofed. When the DOS attacks lost their effectiveness due to security measures taken by companies, the hackers came up with yet another more destructive and perilous attack, known as DDOS or Distributed Denial-of-service attack.

4. DISTRIBUTED DENIAL OF SERVICE (DDOS)

A more devastating form of DOS attack is DDOS (distributed denial of service) attack. The difference between DOS and DDOS is that, in DDOS, the attack is carried out from hundreds or thousands of hosts, unlike DOS, in which the source of attack is a single host. The attacker compromises several number of hosts on the network (without the host's knowledge) with the help of several malwares and malicious links. One such attack happened in January 2012 when some anonymous hacktivists compromised hosts by providing malicious links on social media websites such as twitter. These compromised hosts, collectively known as botnets, are controlled by the hacker remotely. Now these hosts are used to attack the target server and flood it with traffic. What makes DDOS attack difficult to mitigate is the fact that the attack traffic cannot be separated from legitimate traffic, because the attack packets are themselves coming from authentic hosts. Also, when thousands of computers will be sending the requests to the target server, it would become immensely difficult for it to block a particular IP address because the traffic cannot be discerned. Moreover, even if the attack traffic is identified, it can become an arduous task to block it if the source IP address in the packet headers is spoofed. IP spoofing is a technique where the actual source of the packet is hidden, so when the incoming traffic is traced at the target server, it gets wrong information about the packet's origin. IP spoofing technique is used by attackers, to hide the actual source of traffic. As a result of such attacks, the target server ends up denying the service to its actual users. There are many vulnerabilities which have been exploited in order to launch DDOS attacks. There are several types of DDOS attacks which have been described in the following section. The measures to mitigate the DDOS attacks have been comprehensively discussed later in the paper.

5. TYPES OF DDOS

There ca n be boundless types of DDOS attacks, because attackers always find new ways to breach the security and launch the attacks by exploiting any new vulnerability in any service or software that might still be unknown to the vendor. However, major types are discussed in the following subsections.

5.1 DNS Amplification Attacks

The attackers use amplification technique to send a larger amount of traffic towards the victim with substantially lesser number of requests via UDP. This attack comes under the category of reflection attacks. The attackers primarily use DNS amplification technique in which they send requests to publically accessible DNS servers for the address look up of the victim server, with the source address spoofed as the target address in the packet header. As a result, the DNS servers send the response to the target instead of the requestor. The attacker structures the request query by passing arguments such as "ANY", so that the size of the response is as large as possible, thus creating an amplification effect. Attackers employ botnets to send queries and to remain undetected. The amplification factors have only gone up with time, with more and more number of DNS servers being used for the attack. For example, a DNS request of 10 bytes can be configured to generate a response of over 700 bytes, resulting in an amplification factor of 70:1.

5.2 NTP Amplification Attacks

This attack is similar to DNS amplification attack. In this case, the attackers send requests to open NTP servers, with the requestor's IP spoofed to be the IP of the victim server, such that the response from the NTP server is sent to the target server itself. Since the IP is spoofed to be that of target server, this attack is a type of reflection attack. The requests are sent to the NTP server's port number 123 via UDP. When any device sends a command "monlist" to get a response from the NTP server, the server sends the list of last 600 hosts that connected to it. Attackers continuously send this command to the server, generating a much larger response with respect to the query, thus creating the amplification effect. Amplification factors can be as high as 200:1.

5.3 HTTP Flood

These are the form application layer DDOS attacks or Layer 7 attacks. HTTP flood attacks require less efforts at attacker's

end. The attacker is able to overwhelm the server and its resources with little effort, all that is needed is a smartly crafted HTTP request to be sent to the server with the help of zombie army. When any web browser tries to interact with the server, it sends HTTP requests to the server. The request can either be a GET or POST request. The GET requests are used to retrieve static data such as images and text, while POST requests are used to retrieve dynamic data which requires complex operations, such as interacting with the database. Attackers structure the request in a way that asks the server to do as much processing as possible to give a response to the request. Since these requests are sent by botnets, the server gets overwhelmed with plenitude of requests which inundate the server, each requesting substantial amount of information, which can exhaust the available resources. HTTP flood attack remains much difficult to detect and block, because the requests are sent from authentic devices, which have been compromised by the attacker. Moreover, the IPs used in such an attack are not spoofed, making it more grueling to distinguish the illegitimate requests from the legitimate ones.

5.4 Syn Attack

This attack [9] exploits the vulnerabilities of TCP three-way handshake protocol. As the name suggests, three-way handshake requires exchange of three packets – SYN, SYN-ACK and ACK packet. The requestor first sends SYN packet to the server, the server responds with SYN-ACK packet and expects ACK back from the requestor in order to complete the connection. The attacker sends the SYN packet to the server, and the server sends back the SYN-ACK packet, but the attacker doesn't send back the ACK packet, which results in half-open connections at the server's end. Attackers achieve this either by manually avoiding sending the ACK packets or by falsifying the IP address in the packet headers. The IP which receives the SYN-ACK packet does not respond to this packet, because it never sent SYN packet at first place. Thus there are numerous half-open connections at the server, which devour the resources resulting in denial of service for the legitimate users. This attack is also known as SYN flood attack.

5.5 Zero Day Attack

As DDOS attacks are growing in size and becoming more and more convoluted, so are the efforts to alleviate them. But mitigation efforts won't stop attackers. They can always find new vulnerabilities in softwares to exploit them. Zero day DDOS attacks refer to exploiting the vulnerability which was previously unknown to the software vendor or the company. The vulnerability exploited has never been seen before, hence the name "Zero-day DDOS". It becomes even more difficult to mitigate such attacks, because the type of vulnerability has not been known before, and hence it can take too much time to actually find what was exploited and solve it. The attackers can use such attacks to steal information and to cause denial of service. Therefore, it is more secure to prevent the servers from such an attack, rather than trying to cure it after the attack has been launched. In recent past, many vulnerabilities have been observed in Windows, Java and Adobe which have been used for zero day DDOS attacks.

5.6 Ping Attack

This attack uses the ICMP protocol. Ping command is used to check the connectivity to the server, which first sends echo_request packet and awaits an echo_reply packet in return. The packet is sent using ICMP (Internet Control Message Protocol) via port number 88. The default packet size is 64 bytes, but it can be converted to as large as 65,535 bytes. The bandwidth will be consumed in both receiving the request and sending a reply back to the requestor. When such packets are sent continuously to the target server from thousands of devices, the bandwidth of the server will be totally consumed and the server can be crashed in as less as 10 seconds. This attack is usually successful when the attacker has more bandwidth than the target server. Another similar attack is Slowloris attack, in which attacker keeps the target server busy by sending data bit by bit and as slowly as possible so as to keep the connection open for a longer period of time.

We have used two machines in our private network. The attacking machine has the private IP 192.168.43.22 while the victim machine has private IP 192.168.43.50.

The software used is Low Orbit Ion Canon (LOIC) which is a network penetration testing tool. The victim machine when pings www.google.com gets the response in less than 120ms when there is no network congestion. However, after the UDP flood attack has been launched on the victim machine on port number 80, the response time increased to 800ms. As the number of requests keep increasing, the response time keeps dallying. The machine saw 58% packet loss within 2 minutes of the attack. Eventually the server stops responding to legitimate traffic. Company networks have larger bandwidths, but the attacks are also much larger and amplified which use thousands of compromised hosts.

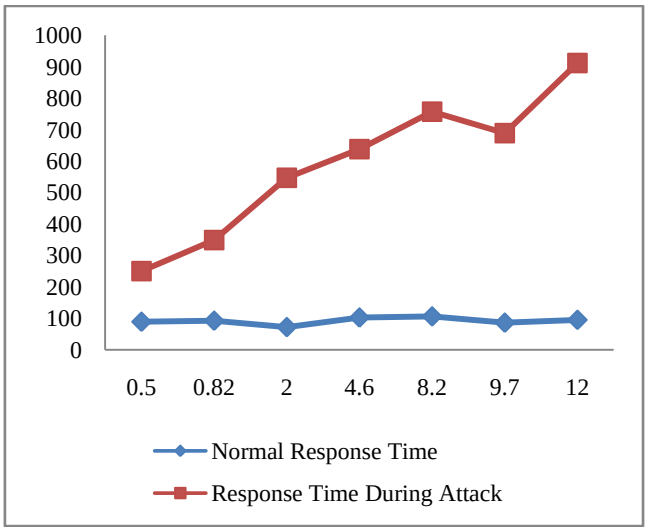

Figure 1 : Response time in DOS attack

6. MITIGATION OF DDOS

Though it cannot be guaranteed that these efforts will certainly prevent your servers from DDOS, but preventing the servers is much more feasible than trying to mitigate the attack after it has been launched. Some solutions exist which have been discussed below:

6.1 Reverse Path Forwarding (Rpf)

It was invented to prevent IP spoofing which is the main problem. The router checks that the address mentioned in the source packet is reachable or not. If it is reachable, then packet is forwarded otherwise it is dropped. Unicast RPF can be configured in 2 modes – Strict Mode and Loose Mode.

6.1.1 Strict Mode

It checks two things – Does the source address of the packet has its entry in the routing table, and is the router using same interface to reach that source which was used to receive the

packet. If a packet passes both these checks, then the packet is forwarded, otherwise it is dropped. Strict mode can drop legitimate traffic too if asymmetric routing paths are present. It can be configured by running following commands on the router:

int fa0/1

Ip verify unicast source reachable-via rx

6.1.2 Loose Mode

It checks only if the source address is present in the routing table. If it is, then the packet is passed else it is dropped. It can be configured in a similar manner with a slight change:

int fa0/0

ip verify unicast source reachable-via any

Here fa0/1 and fa0/0 are the interfaces which the router uses to receive the packets. uRPF is disabled by default on all the routers and switches. Limitation is that when one enables uRPF, it automatically gets enabled on all switch interfaces including LAGs(link aggregation groups), Integrated routing and bridging and all others. So it should be used only when there are untrusted interfaces which might be used to receive the packets.

6.2 Rate Limiting

Rate limiting [10] means limiting the number of connections in order to prevent DDOS attacks which continuously send request packets to make connections with the target server. Rate limiting makes use of leaky bucket and token bucket algorithms. It is implemented with the help of iptables. It can be implemented in either of 2 ways-

- First way is to limit the number of connections per IP. Let's say if the server wants to protect itself from http flood which receives default requests on port number 80, and if it wants to limit the number of connections per ip to 12, it can be done with the help of following command iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 12 --connlimit-mask 32 -j REJECT --reject-with tcp-reset
- Another way is to limit number of new connections to the server per second. If a server wants to limit the number of new connections per second to 125, it can be implemented with the help of following command – iptables -A INPUT -m conntrack --ctstate NEW,RELATED,ESTABLISHED -m limit --limit 125/second --limit-burst 135 -j ACCEPT

6.3 Syn Cookies

When a server receives SYN packet, it makes it entry in the TCP stack and sends SYN-ACK packet back to the client and waits for ACK packet. Many clients do not reply back with the ACK packets, and this results in half open connections. The TCP stack has finite capacity and thus becomes unable to handle any more requests since it keeps on waiting for ACK packets, thus resulting in Denial of Service. SYN cookies help to resolve this problem. When the server sends back SYN-ACK packet, it adds a hash value with the packet which is of 32 bits. It has 5 bits for time, 3 bits for Maximum Segment Size (MSS), and remaining 24 bits consist of MD5 hash which is computed using Initial sequence number(ISN), IPs of both source and destinations, both ports, and the timestamp. The server then drops the packet. The client has to reply ACK with cookies+1. The server subtracts one, computes the hash again and if it matches with the original cookie, the server makes it entry in the TCP stack. Thus server isn't required to remember cookies value because it appends all it needs to remember in the packet itself. Although the computing power required to produce such hashes has always been in question, but a basic core2 x86 CPU can compute 8 million of MD5 hashes per second using a single core. To enable SYN cookies, open /etc/sysctl.conf file and make following entries:

```
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 3
```

6.4 Ingress & Egress Filtering [11]

Egress is the term used to define the outgoing packets from a network. Ingress is the term used to define incoming packets. Egress filtering is used to prevent malicious traffic from going out of a network. It might be possible that filters allow only particular nodes to send data outside of the network. Likewise, ingress filtering is done to prevent malicious traffic to enter a network. These filtering are done on the basis of packet headers and these filters are implemented on routers or firewalls. Simply stated, it consists of ACL which contains list of permitted IP addresses to enter the network. It makes decision based on packet header whether it meets the defined criteria. Admins can whitelist or blacklist certain IP addresses. Checks might include –

- IP addresses which are already in use in internal network. Such checks can be used to prevent smurf attacks.
- In egress filtering, no outbound traffic should have a private IP address and no IP address should have a source IP which is not in the internal network.

6.5 Bogon Filtering

Bogon addresses must never appear in routing tables because these addresses are not allowed for public internet use they and have never been publically assigned by Internet Assigned Numbers Authority (IANA). In one study conducted by Rob Thomas, the attack packets consisted of 60% bogon addresses. So filtering these packets by adding them in router rules can be a major part of preventing DDOS attacks. These addresses are sometimes also known as Martian packets. Some ranges are 10.0.0.0/8 172.16.0.0/12, 192.1680.0/16 169.254.0.0/16. In 2011, IETF recommended that IPv4 bogon filters be removed because all the addresses IPv4/8 addresses have been assigned, except the reserved ones. However filters can be used to check Martians. The updated bogon filters are required to check the bogon list and update the bogon filters according to the updated lists. The new bogon filters must be able to filter IPv6 packets according to the updated IPv6 bogon addresses list. The list can be found at http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt. These filters can be setup with peering with Team Cymru. However, implementing Bogon requires atleast 4,500 rules for IPv4 and atleast 65,000 rules for IPv6. Moreover, bogon addresses are not static because addresses get assigned and unassigned. So it affects the computing power. Only RuleGate is the server capable of adding most of these rules to handle bogon addresses and update them regularly.

6.6 Blackhole Routing

Black hole – the term means that whatever goes in doesn't come out. Same applies with network packets. A black hole means if a packet goes there it will simply get discarded. YouTube saw 2 hours of downtime because an ISP accidently distributed black hole routes. Cisco routers come with a null0 interface, and if a packet goes to this interface then the packet gets discarded. These are useful in case the server is under

DDOS attack. This can discard illegitimate traffic without impacting the performance. Once the attack is detected, black holing can be used to drop all attack traffic at the ISP edge. It is also known as null routing. It can be configured on Cisco router by command –

```
ip route <Destination-IP> 255.255.255.255 null0
```

The ip packets which were to be delivered to <destination IP> will get discarded.

6.7 Other Solutions

Other solutions might include increasing the bandwidths so that the resources don't get overwhelmed, using TCP keepalive messages technique to prevent from attacks like Slowloris(attacks in which attacker sends data very slowly, such as character by character in order to maintain the connection for a long time) attacks, analyzing the traffic patterns and taking measures accordingly, using load balancers, using DDOS protection services provided by the ISPs, and looking if the traffic is behaving unexpectedly and triggering an alert on that basis.

7. COMPILATION OF MITIGATION TECHNIQUES

The best way to stop a DDOS attack is to stop the malicious traffic within its originating network. It becomes arduous to stop the traffic if it reaches near the target server. A compilation of all the above discussed mitigation techniques can prove to be helpful in mitigating th DDOS attacks. We have defined three layers of security. First layer of security is to apply egress filtering at the malicious packet's originating network's router. Attacker might have control over it's router so the packet might pass this layer of security. Then comes the second layer of security, which is applied at target network's edge router. Ingress filtering is applied to the edge router such that if the packet bypasses it's own network, it cannot enter the target network. Furthermore, to prevent packets which have spoofed IP addresses, the routers must be configured with uRPF. After these router configurations, there comes layer 3 security which is applied at the server level. The server must itself be configured with rate limiting on firewalls and IPtables to control number of connections per IP and to control number of connections per second to the server which shall depend on the resources that are available to the server. Also to prevent TCP half open connections and to prevent TCP stacks being exhausted, the server must make use of SYN cookies. The packet must be stopped as soon as it originates, but multiple layer protection at every layer in hierarchy shall definitely help in preventing these attacks to a large extent. This compilation are not limited to these techniques and can be enhanced with more preventive measures.

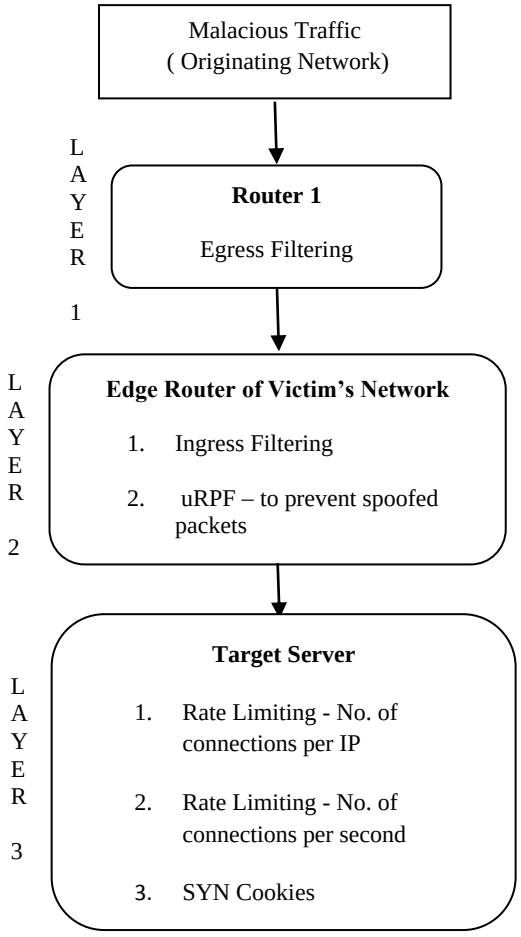

Figure 2 : Compilation of Mitigation Techniques

8. CONCLUSION AND FUTURE SCOPE

DDOS attacks and their devastating effects are not going away soon and are here to stay. These attacks are only expected to grow bigger with time. They have devastating effect on the business and servers which can cause loss of millions. These attacks are carried out on a large scale, and are a big problem for all the servers. These attacks make it difficult for legitimate traffic to access the server, because the resources get overwhelmed by a large number of illegitimate traffic. The various types of DDOS attacks can cause downtime for a server, such as HTTP flood, DNS amplification, Ping Flood, Zero day DDOS etc. These attacks are big problem for businesses, as well for nation's security. The effects of such attacks are annihilating and a cause of worry. Thoroughly analyzing how an attacker is able to carry out several attacks, what vulnerabilities do cyber criminals exploit in order to carry out these attacks, understanding the behavior of attack and what attackers can exploit is a crucial step towards preventing any kind of DDOS attack. In this paper, we tried to explain the various taxonomies related to DDOS attacks, and then we looked at what goes behind the scenes in carrying out such attacks. We tried to integrate several possible solutions which could prove to be effective in mitigating the effects of DDOS, and in some cases these methods might also prove to be useful in preventing DDOS attacks. Though no amount of security can ever ensure that the server is extremely secure, these techniques can be incorporated to achieve a greater level of protection. The attackers use techniques like IP spoofing and amplification, and they do so with the help of botnets. The attacks carried

out using these techniques can never be fully curbed, but they can be mitigated to a great extent. The mitigation technique Unicast Reverse Path Forwarding (uRPF) can be helpful in detecting packets with spoofed IP addresses. Ingress and egress filtering can also help in preventing malicious traffic from entering the network. The server administrators might also be required to aggressively monitor half open connections and analyze the traffic pattern with the help of some script. In future, we plan to write a script which can monitor traffic and generate some alerts if the traffic is increasing abruptly, so that the server administrators have ample amount of time to act before the situation gets out of control. We also plan to analyze traffic patterns by thoroughly observing them, and making the system learn about traffic pattern with the help of artificial intelligence, so that the server knows what it needs to do if it detects that it is under DDOS attack.

9. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

10. REFERENCES

[1] Darshan Lal Meena, Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches, 2014, International Journal of Advance Research in Computer Science and Management Studies, Vol 2, Issue 4

[2] Qijun Gu and Peng Liu. Denial of Service Attacks, February, 2008

[3] Crosby, S. A., and Wallach, D. S. (2003). Denial of Service via Algorithmic Complexity Attacks. Proceedings of the 12th USENIX Security Symposium, 29-44. USENIX Press, Berkeley, CA.

[4] Cowan, C., Beattie, S., Johansen, J., and Wagle. P. (2003). PointGuard: Protecting pointers from buffer overflow vulnerabilities. Proceedings of the 12th USENIX Security.

[5] Dean, D., and Stubblefield, A. (2001). Using client puzzles to protect TLS. Proceedings of the 10th Annual USENIX Security Symposium. USENIX Press, Berkeley, CA.

[6] CERT (1997). CERT Advisory CA-1997-28 IP Denial-of-Service Attacks. Available at: http://www.cert.org/advisories/CA-1997-28.html. (Date of access: August 20, 2006)

[7] Li, J., Mirkovic, J., Wang, M., Reiher, P., and Zhang, L. (2002). Save: source address validity enforcement protocol. Proceedings of IEEE Infocom, 3, 1557-1566. IEEE Press, New York.

[8] Boris Sieklik, Richard J Macfarlane, William J Buchanan, Evaluation of TFTP DDoS amplification attack, Research Gate, October 2015.

[9] Akash Mittal, Prof. Ajit Kumar Shrivastava, Prof. Ajit Kumar Shrivastava , A Review of DDOS Attack and its Countermeasures in TCP Based Networks, 2011, International Journal of Computer Science & Engineering Survey, Vol. 2, No. 4, November 2011.

[10] Dibajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, A Study on Recent Approaches in Handling DDoS Attacks, December 2010.

[11] Saravanan kumarasamy, Dr.R.Asokan, Distributed Denial of Service (DDoS) Attacks Detection Mechanism, International Journal of Computer Science, Engineering and Information Technology, Vol. 1, No. 5, December 2011.