ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/388427620

A Study on DDOS Attacks, Its Types and Prevention Methods

Conference Paper · October 2021

CITATIONS
0

READS
8

2 authors:

Syed Ibrahim
VIT University , Chennai Campus
57 PUBLICATIONS **260** CITATIONS
SEE PROFILE

Saumya Singh
Vellore Institute of Technology University
5 PUBLICATIONS **3** CITATIONS
SEE PROFILE

All content following this page was uploaded by Saumya Singh on 28 January 2025.

The user has requested enhancement of the downloaded file.

A Study on DDOS Attacks, Its Types and Prevention Methods

Saumya Singh[1], S. P. Syed Ibrahim[2]

[1]Undergraduate Student, School of Electronics and Computer Engineering, Vellore Institute of Technology

[2]Professor, School of Computer Science and Engineering, Vellore Institute of Technology

ABSTRACT -A cyber attack is an attack on a victim's network with the intention of disruption. There are many types such as man in the middle, SQL injection, DNS Tunneling, etc. Distributed Denial of Service or DDoS is a type of cyber-attack on a network so that the server cannot provide service to its clients and disrupt its normal operation. It is basically flooding the victim host with a constant flood of traffic. There are many types of attacks that can be implemented to deny the service such as ping of death, TCP SYN flood attack, etc. Since DDoS attack pose a great threat to business as well as the security of an individual or an organization, it is crucial to prevent those attacks. This paper focuses on different types of attacks and solution to bandwidth flooding attack. The solution is based on the verification of the user upon which the request will be accepted or they will be put in the block list till the attack does not stop.

KEYWORDS -Dos, DDos, Bandwidth flooding, Captcha, Servers, Username, Password.

I. INTRODUCTION

When the cyber-attack is done by a single source, it is termed as DOS (Denial of Service). Whereas, when the cyber-attack is done by multiple sources headed by a master program, it is termed as DDOS (Distributive Denial of Service). DDOS is the advanced attack form of DOS. The attacker uses malicious software to create his army of infected computers which will help him to attack the target. The attacker develops a malware program and distributes it over the internet by adding it to websites and email attachments. Whenever a computer that is vulnerable, visits these infected websites or opens the infected email attachments, the malware is installed on that computer without permission. Thus, the owner usually doesn't know that their computer has been infected.

Now, this computer is recruited in the army of infected computers to perform a DDOS attack. This army of infected computers is called a BOTNET. This botnet could be millions of computers scattered all over the world. The attacker is the centralized and control center for the botnet. It sends out specific instructions to all these infected computers to attack at the set date and time and once it is reached, the attack begins. The attack can continue for seconds or minutes or even for days, it all depends on the attacker's intent refer fig. 1. An attack can happen for different reasons such as financial issues, political issues, hatred for targeted organizations or just for fun.

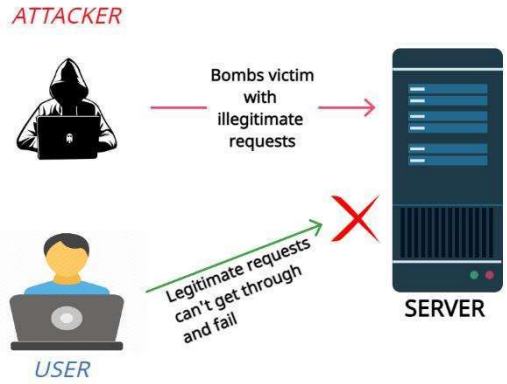

Figure 1: Describes simple working of DDOS

The objective of this paper is to:

- Introduce and analyze DDoS attack.
- Discuss on different types of DDoS attack.
- Observe existing solutions for DDoS attack.
- Propose a new solution for bandwidth flooding attack.

II TYPES OF ATTACK

1. Bandwidth Flood

The attacker implements resource exhaustion by exhausting the bandwidth of the target computer. It sends a lot of network trafficwhich overloads the network. This is the most common type of attack. It is the easiest for hackers to implement and the most difficult to predict and protect without human intervention refer fig. 2.

Denial of service (DoS) attacks on network bandwidth is designed to use available bandwidth in such a way that legitimate traffic cannot reach

the destination. This is achieved by sending large amounts of data that basically crashes the server.

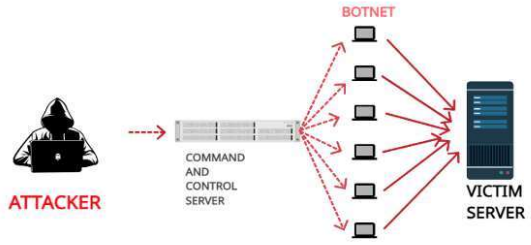

Figure 2: Bandwidth flood.

2. Service request Flood

Service request attacks are more accurate than the garbage heap of network traffic. It sends specific service requests to the target in extremely high amounts. These requests can be such as:

- VPN connection building
- HTTP requests
- DNS queries
- TCP connection requests
- HTTPS session establishment

These service requests do not necessarily have to succeed, they just have to consume resources. This flood attack as shown in fig, 3 is based on sending unlimited syn packets. Usually, service requests are flooded by establishing repeated TCP connections with the system.

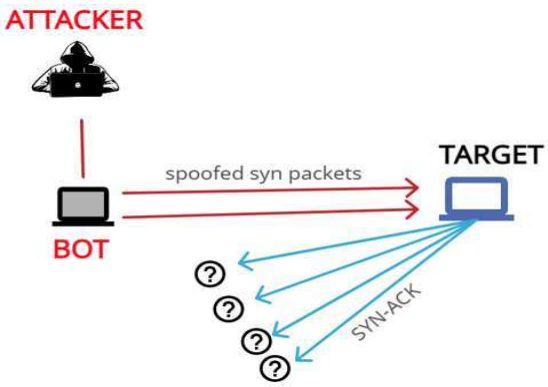

Figure 3: Service request flood

3. ICMP or SYN Flood

ICMP's full form is Internet Control Message Protocol. This type of attack is also called a ping flood attack. Here, the attacker tries to flood the target device with an ICMP echo request (pings). By using request packets to attack the target, the network is forced to respond with the same number of reply packets.

This attack exploits limitation of TCP/IP stack in many devices. Only a limited number of ICMP or SYN requests can be processed at the same time. Outstanding SYN requests are held, which consumes memory. Due to the limited size of the ICMP table, it is easy to overwhelm. As a result, the ICMP table is reset. The router becomes a hub for 1 or 2 seconds. The SYN capacity is emptied after being idle for 75 seconds.

4. Application Flood

It is specifically targeted at known application-level services such as:

- Email
- Database
- Web applications
- Custom applications
- The only limit is the coder's imagination and his exploitable code

This attack basically has same architecture as DOS and DDOS. It exploits the particular port that has been targeted which results in breaking the service from that particular port. In fig. 5 the firewall is exploited by the attacker resulting in damage to the network. In this attack, the application itself, focuses on the vulnerability or issues in the application, resulting in the application not being used by the user when needed. The attacks are usually low to mid volume since the application involves handshakes and compliance, meaning these are primarily launched using intelligent clients like Internet of Things (IoT) devices.

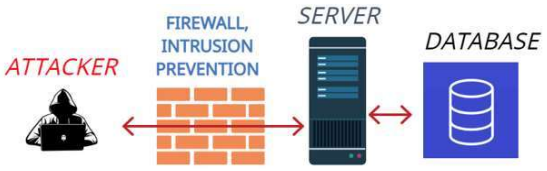

Figure 5: Application flood

III. PREVENTION MECHANISMS

Some basic precautions are:

- Stop using **standard/universal** passwords.

- Disable remote access (WAN) to the device. To ensure that your device is not open for remote access, you can use the following site to scan the following ports: SSH (22), Telnet (23), and HTTP / HTTPS (80/443).

https://www.yougetsignal.com/tools/open-ports/

IV. LITERATURE SURVEY

1. Backward Traffic Throttling (BTT) to Mitigate Bandwidth Flood[1]

Yehoshua Gev, Moti Geva and Amir Herzberg'sBackward Traffic Throttling is one of the prevention methods for congestion and bandwidth flooding DDOS attacks. In this method three basic mechanisms are used that are:

- Prioritize valid flows
- Traffic shaping
- Request the upstream BTT node to determine and configure the priority of traffic

DRAWBACK: Detection of legitimate flow is exceedingly difficult and costly, so this method is not economical.

2. A Mechanism for Prevention of Flooding based DDoS Attack[2]

In this method either the time period or frequency of packets is fixed. That is considered as the threshold for further calculations.

If any amount exceeds the threshold, then the service request is verified by use of a captcha. A captcha is sent to the source and only if the correct response is sent back, the further request is serviced. Again, the traffic is observed for the next time period slot.

DRAWBACK: The attacker can detect the threshold and send the packets accordingly.

3. New cracking algorithm[3]

In this method message authentication code (MAC) is used. Here if a user requests for services for more than 5 times, mac is sent to the IP and the source.

Then mac of server and client are confirmed. If they are same, then the services are provided or else that IP address is put into the blocked list. Thus, it can never further attack the server.

DRAWBACK: If the attacker uses many IPs to send the request instead of just sending many requests to be sent by a single IP, then, this method fails.

4. Integrated DDoS Attack Defense InfrastructureforEffective Attack Prevention[4]

This paper discusses the methodology adopted by the attackers generally. Then in the next part it discusses the prevention methods that people can follow to avoid DDoS. First step is making the malicious software, which cannot be avoided. Second step is installing the software into vulnerable PC's. Here, we can avoid visiting or downloading files from unknown sites. Third step is protection from agent control i.e. to avoid the communication between the software and attacker. Fourth is, prevention during the attack. Fifth is, to remove the zombie PCs after the attack because even if the attack is finished, the PCs are still a potential threat.

DRAWBACK: All the above methods require the victim to manually act and take the prevention measures.

5. A study on DDos attacks, danger, and its prevention[5]

This paper starts with explanation of DDoS and ISP. It further explains different types of DDoS attacks and shows reports on the types of attacks. Then it discusses various defense mechanisms and their drawbacks for ex. Monitoring (which is developed by CISCO that monitors traffic at all points), Ingress/Egress filtering (this method allows only IPs within a certain range, so the drawback is, not all IPs are allowed to access the site), black holing (which tells the upstream network to discard excess traffic that is exactly what the attackers want) and scrubbing (which filters the traffic but is very costly and not affordable by everyone). Their suggestions are to set up security labs, provide every router with username and password, team up with other ISPs for leasing scrubbing center at affordable price etc.

DRAWBACK: This method also requires manual intervention to protect the victim from the attack.

6. A Multi-Criteria-based DDoS-Attack PreventionSolution using Software Defined Networking[6]

This paper suggests the use of software defined networking (SDN) to prevent DDoS. This method first analyses the traffic on the site. They first observed the traffic on 26th March 2015 for 10 minutes, measured inter-arrival time (IAT), analyzed packet quantity per flow, number of source IP, number of flows, addresses and total traffic volume to a same server. Now they compare the nature of traffic every time and know when the traffic is legitimate and when an attack is taking place. If DDoS attack is taking place then IAT will not lie within the parameter range thus it will drop 100% of incoming traffic and when it lies within the parameter range, it will forward the traffic and if no condition is satisfied then it transfers the control to fuzzylogic(). fuzzylogic() is a function which computes using various mathematical formula the amount of traffic flow to be dropped in order to save the server from crashing.

DRAWBACK: If the function fuzzylogic() decides to drop legitimate traffic then, the attacker's main objective, that is, to stop the service to actual legitimate users is a success.

V. PROPOSED SOLUTION FOR BANDWIDTH FLOODING ATTACK

The solution proposed for DDoS bandwidth flooding attack is by placing a shield before the original site is loaded, only when the attack is detected or else it would work normally. A shield is basically a verification step before the request is executed.

The verification step can include:

- entering a captcha
- clicking 'yes' or 'no' for the dialog box that appears
- providing a username and password for the users, etc.

If the response is not given to us within a stipulated time, then we discard the particular request and put the IP in the blocked list. That IP is blocked till the attack is still on. After the attack, we could get in touch with the IP owners and tell them that their device is infected and working in a botnet. In this way we could take care of the botnet after the attack has taken place.

Suppose we are the owner of a site and we use first verification step i.e., the captcha. When there is no attack, i.e., normal traffic, the users do not have to enter the captcha when they use the site (figure 6). But when the detection methods inform that there is an attack taking place, then we put the captcha phase before entering the site (figure 7). So, if a user is entering my site during the attack, he will be asked to put a captcha. If an actual user is using, he can easily put the captcha and then use the site normally, but if it's a bot, then he cannot enter the captcha and thus the stipulated time will be over and his request will be discarded and he will be put in the blocked list (figure 8).

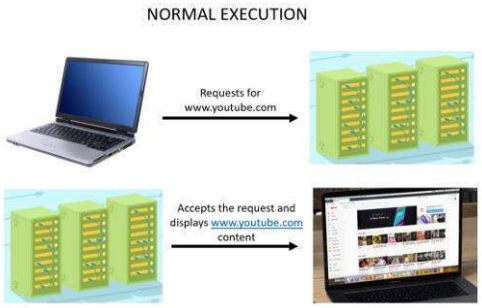

Figure 6: Shows execution when there is no attack

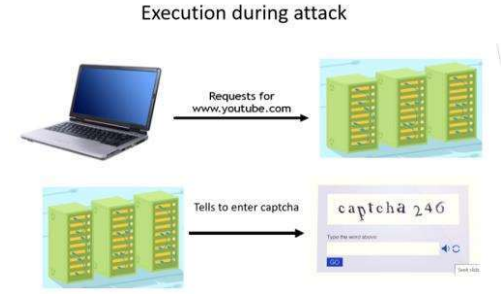

Figure 7: Shows execution when there is bandwidth flooding attack. (Asking to enter captcha)

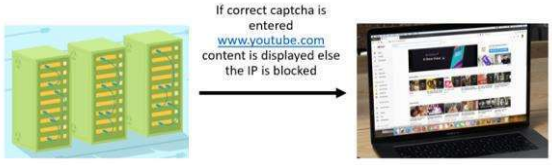

Figure 8: Shows execution when there is bandwidth flooding attack. (If the captcha is correct then displays the content else the IP is put in the blocked list)

VI. CONCLUSION

Distributed Denial of Services attack pose a major security threat to the developers and users online. Attacks on an exceptionally large scale have already taken place in the past and it was almost impossible to stop the attack. There are approaches discovered in the past, but they were either insufficient or easy to crack or were expensive which were not affordable by small website owners. So, in this paper, I have presented how we can save the servers from the attackers in an affordable way and which is easy to implement. The approach is easy, transparent, practical, and easily executable by the servers and the website hosts. It is also compatible with the current network protocols.

VII. REFERENCES

[1] Y. Gev, M. Geva and A. Herzberg, "Backward traffic throttling to mitigate bandwidth floods," 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 904-910, doi: 10.1109/GLOCOM.2012.6503228. Nipa Patani and Rajan Patel, "A Mechanism for Prevention of Flooding based DDoS Attack," in International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 1 (2017), pp. 101-111.

[2] Patani, Nirav P. and R. Patel. "A Mechanism for Prevention of Flooding based DDoS Attack." (2017).

[3] V.Priyadharshini and Dr.K.Kuppusamy. "Prevention of DDOS Attacks using New Cracking Algorithm," in International Journal of Engineering Research and Applications(IJERA)Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

[4] Y. Choi, J. Oh, J. Jang and J. Ryou, "Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention," 2010 2nd International Conference on Information Technology Convergence and Services, 2010, pp. 1-6, doi: 10.1109/ITCS.2010.5581263.

[5] Chakraborty, Sushmita & Kumar, Praveen & Sinha, Bhawna & Professor, Assistnat &Head, (2019). A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION. 10.1729/Journal.20847.

[6] P. Van Trung, T. T. Huong, D. Van Tuyen, D. M. Duc, N. H. Thanh and A. Marshall, "A multi-criteria-based DDoS-attack prevention solution using software defined networking," 2015 International Conference on Advanced Technologies for Communications (ATC), 2015, pp. 308-313, doi: 10.1109/ATC.2015.7388340.

[7] Mukhopadhyay, Debajyoti & Oh, Byung-Jun & Shim, Sang-Heon & Kim, Young-Chon. (2010). A Study on Recent Approaches in Handling DDoS Attacks.

[8] Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," 2011 International Conference on Intelligence Science and Information Engineering, 2011, pp. 426-429, doi: 10.1109/ISIE.2011.66.

[9] Elleithy, Khaled & Blagovic, Drazen & Cheng, Wang & Sideleau, Paul. (2006). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. Journal of Systemics, Cybernetics and Informatics. 3. 66-71.

[10] Smith, Jason & Nieto, Juan & Boyd, Colin. (2006). Modelling Denial of Service Attacks on JFK with Meadows's Cost-Based Framework. 54. 125-134. 10.1145/1151828.1151844.

[11] Udaya Kiran Tupakula and Vijay Varadharajan. 2003. A practical method to counteract denial of service attacks. In Proceedings of the 26th Australasian computer science conference - Volume 16 (ACSC '03). Australian Computer Society, Inc., AUS, 275–284.

[12] Mirkovic, Jelena & Reiher, Peter. (2004). A taxonomy of DDoS attack and DDoS Defense mechanisms. ACM SIGCOMM Computer Communication Review. 34. 10.1145/997150.997156.