A Review on Distributed Denial of Service

Usman Ali1†, Abu ul Hassan††, Dr. Muhammad Sheraz Arshad Malik †††, Syed Kashif Hashmi ††††, Bushra Aslam†††††, Basit Ayub †††††††

†,††,††††,†††††,††††††RIPHAH International University, Islamabad, Pakistan
†††Government College University, Faisalabad, Pakistan

Summary
A denial of service attack consists of sending and requesting a lot of data to a server in a network, thus getting the server saturated and unable to respond to data requests that are legitimately made. This paper will discuss in detail about DDoS and the measures to prevent from it. The paper will also discuss its working phenomenon and some specific terms including botnet, Syn flood, ICMP flood and UDP flood. In the end, the paper will describe the DDoS mitigation services.

Key words:
DDoS, botnet, Syn flood, ICMP flood and UDP flood.

1. Introduction

DDoS stands for Distributed Denial of Service, which translates as a Distributed Interruption of the service, and consists of filling a site with requests until it is knocked out and made unreachable. According to the latest data from the association for information security, it is among the attacks that hit a company every five minutes along with malware and ransomware. Its use has decreased compared to previous years, registering 66.96%, their power has increased: the average occupied band has increased from 11 gigabits per second in 2016 to 59 gigabits per second in 2018 [1].

A DoS (Denial of Service) attack objectives was to stop the usage of a network resource, like the website. When attacking many systems, frequently in the tens of thousands, DDoS (Distributed DoS) is simple to know why it is much more overwhelming and problematic to block.

Participants have usually compromised nodes, which act directly on the main victim (also, of course, they are victims, but secondary) or through badly configured servers: in this case, it is about DRDoS (Distributed Reflected DoS). Just to give an idea of the relevance of the phenomenon, according to Arbor Network [v.gd/ P8MDJE] for the first 9 months of 2013: 54% of the attacks exceeded 1 Gb/s (33% in 2012), 37% was between 2 and 10 Gb/s (15% in 2012), for an average value of 2.64 Gb/s (+78% compared to 2012), with a verified maximum of 191 Gb/s (other sources speak of 300 Gb/s) [2].

2. Literature Review

DDoS means "Distributed Denial of Service", that is, several computers previously infected by hackers are fired remotely against a target determined by the cybercriminal, and from there they start to generate thousands or millions of requests until the service or website goes offline or suffer intermittencies due to overload or over-traffic [3].

These attacks force victims to restart their systems, suspend services temporarily, or obstruct communication between users and the victim. Also, these kinds of attacks are more common than you might think and, far from affecting only large companies, can affect smaller websites and services. In simplest of terms, it means when more clients try to connect to your service than your system or network can handle. Since your system cannot handle any more connections, everyone else is blocked. Under normal loads, the blocks are short and only result in very slow web connections, and in the worst case, this attack can crash a service completely [4].

As DDoS has matured over the years humans have remained susceptible. Since DDoS is typically spread in and social media humans have no idea that they've infected their system and spread the malicious software to other computers. Humans will always be vulnerable to the spread of malicious software [5].

Today, however, there is an even greater threat posed by the Internet of Things (IoT) devices. IoT devices create a massive attack platform. For example, an attacker can chain together thousands of connected cameras and generate one of the largest DDoS attacks the world has ever seen. The same vulnerabilities that make IoT devices susceptible to being a part of a botnet make them excellent entry points into the data center and cloud [6].

Organizations face several types of DDoS threats that are popular today. DNS amplified attacks, NTP reflection based attacks, SYN flood attacks, and Application-layer attacks. A penetration test must be performed to determine the approximate number of vulnerabilities that must be mitigated [7].

The most common vulnerabilities are user computers and portable devices. At this point, we need to ensure that a Security Policy is in place to help prevent a DDoS attack.

Manuscript received August 5, 2018
Manuscript revised August 20, 2018

Proactively monitor network traffic around the clock. overprovide bandwidth to accommodate unexpected surges in network traffic. Defend the organization's network parameter. Discover application layer vulnerabilities. Also, partner with the ISP. There is a 60 percent chance that the organization will be the victim of a DDoS attack. This threat is very common and the impact of the attack can be devastating to the organization. Financial systems and customer information are at the greats risk. These systems must be actively monitored and provided additional security [8].

The proposed security policy for DDoS prevention is not the final draft. It is fully expected the team to discuss the policy and make recommendations. The overall security policy should include an acceptable use policy (AUP) and have an established IRT [9].

The security policy covers monitoring Many large organizations have teams that focus on securing the network. However, in many cases, the IT department is responsible for securing the network. These teams are also responsible for developing and implementing a security policy that will prevent and mitigate DDoS on company assets and customers [10].

3. Working on the DDoS attack

To understand what a DDoS attack is, one must first understand the less sophisticated version: the DoS, i.e. Denial of Service. It is an action whose objective is to flood the resources of an information system that provides a certain service to the connected computers. It succeeds in targeting servers, distribution networks, or data centers that are flooded with false access requests, which they cannot cope with. It is said that the communication band is saturated and websites or web surfers trying to reach that particular online resource have difficulty, or they do not succeed at all [11].

DDoS work the same way, but they occur on a much larger scale. In the case of Dos, users need to defend themselves from a single source of computer traffic: for example, a huge amount of incoming emails at the similar time. While during DDoS attacks, the fake questions come at the same time from multiple sources. All this determines a greater effectiveness of the instrument that needs less time to work. The disastrous effects, however, last longer: from a few hours to several days, depending on the readiness with which users react [12].

4. Use of botnet

In general, the tool with which cybercriminals succeed in their intent is the so-called botnet. This term indicates a group of computers compromised by a malware, that is a computer virus, which allows the bad guys to take control of the PCs and have them perform certain operations. A well-known practical example is Mirai, a botnet created by infecting thousands of devices, which occupied the international chronicles showing what these systems are capable of doing.

On October 21, 2016, the botnet determined the temporary interruption of some services, including Twitter, Amazon and New York Times, on the east coast of the United States. Two weeks later, a variant was used to block the traffic of the largest Liberia provider in Africa. And again, in Germany, it has knocked out the internet and telephone connections of about one million people in November 2016 [13].

5. Types of DDoS attacks

Depending on the methods used and the objectives they propose, DDoS attacks can be grouped into four key groups. There are those who target the TCP connection, focusing all on speed. In this case, the botnet floods the connection request server, without ever coming to an end: so the communication band of the computer system is saturated quickly, making it impossible for any user to access the content. Another type of DDoS is the volumetric attacks in which the volume of traffic created is enormous and unmanageable. As a consequence, the object of the attack uses most of its resources to try to reconstruct the received digital information. Finally, there are application attacks that do not point to the entire infrastructure. But they target an indispensable program, making it unstable and therefore unusable [14].

DDoS attacks are used to distract attention from other simultaneous criminal activities, such as bank scams, or against the government or financial institutions, such as those claimed by Anonymous, or even against e-commerce sites for competition reasons. From a taxonomic point of view, there are three types: volumetric attacks, which try to saturate the victim's band, protocol attacks, which consume server resources and attacks at the application level, for example by saturating requests with a web server. Often the three types are mixed.

Among the most used volumetric attacks are the UDP and ICMP flood, in which a large number of packets UDP or ICMP (usually "ping") are sent, which have the double result of saturating the receiver band and its resources, when trying to process incoming data. The sender is practically always falsified, with the result that completely innocent nodes receive responses to packages that have not been sent. Protocol attacks exploit characteristics of IP protocols. The most used is the SYN flood, in which the target is overawed by a huge amount of requests to open

TCP connections (SYN packets), which are not completed because the reply packet is sent to the falsified sender, thus leaving the resources busy of the server, until it is completely blocked [15].

5.1 Flood Syn or Syn Flood

The machines communicate through TCP/IP, this protocol has a header and in this header, there are some flags, which among other things indicate the priority of the connection or when it ends. The flood consists in the sending of TCP/SYN packets, with falsified IPS connection requests and the target machine tries to respond to each of these connections by sending a TCP/SYN-ACK connection waiting for this origin machine to respond. Since the IP is false and nobody has requested this connection, logically no one responds, pending connections begin to accumulate until the machine becomes saturated when it reaches the limit of connections and stops servicing legitimate requests [16].

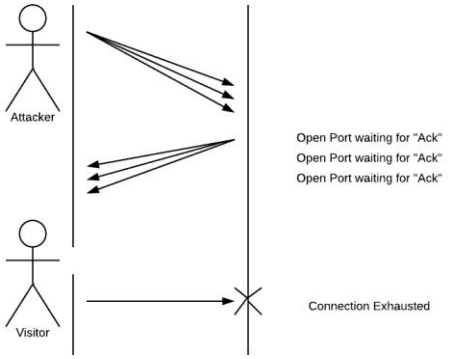

Fig. 1 TCP/Syn Packets Attack

5.2 ICMP Flood

With this option, the Hacker is intended to leave the victim without bandwidth. The best-known variant of this sort of attack is the so-called SMURF. The attacker directs the ICMP intermediaries Echo request with the Ip of the machine that is attacked, when all these intermediaries respond to the objective and an effect similar to the one that is counted in the first part of this point is obtained but without needing so much power of process [17]. Through an ICMP Flood DDoS can be broken with 2 iterating steps:

1. Through too many ICMP echo request packets sending to the targeted server with help of several devices.
2. The under attack server then sends an ICMP echo reply packet to every requesting device's IP address as a reply.

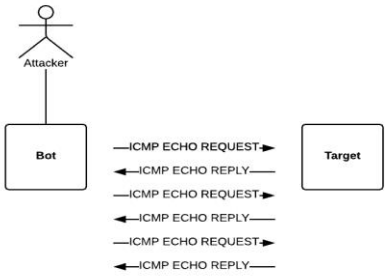

Fig. 1 ICMP Attack

5.3 UDP Flood

It is basically the same as the ICMP flood but using the UDP protocol. It is usually done to machines that run the Echo service waiting for the response of these with large packets. Users cannot ask for freedom of expression because a website is closed and at the same time limit this same freedom attacking other websites even if users disagree with their opinion. The way to solve Wikileaks problems is not to go against Visa or Mastercard, but it is to give all the diffusion to the information that has been published here [18].

Table 1: Attacks and Prevention

Attack Name	Working	How To Prevent From These Attacks
Syn Flood	With an Invalid IP address, several Syn packets send to the server. The server tries to respond to each packet but the source IP address invalid and server go to wait for state.	• Configuring Firewall • Configuring switches • Using Commercial tools or Services
ICMP Flood	In this, the attacker takes down a victim's machine by overwhelming it with ICMP echo requests, also known as pings.	• By controlling or limiting the size of ping requests on targeting router. • Contacting ISP
UDP Flood	In this, a large number of UDP (User datagram protocols) send to victim's machine for stopping it to process and respond	• Configuring Firewall to mitigate UDP packets. • Using online services and tools

6. Evolution and future of DDoS attacks

The latest analysis highlighted two changes in the DDoS world in the last year. First of all, the countries from which the attacks are launched. The United States is still in the lead, but to follow there are nations that until a few years ago were not even taken into consideration in this area, like Egypt. The second change concerns the speed of

DDoS. The cybercriminals seem to have set aside prolonged attacks, preferring instead of frequent and fast: "hit and run" DDoS, which are interrupted after a few minutes. In this way, the companies affected do not even have time to recover before facing a new threat. As already mentioned, moreover, the power has increased: the average occupied band has increased from 11 gigabits per second of 2016 to 59 gigabits per second of 2018. Also because objects connected to the Net, therefore exploitable as botnets, have increased dramatically [19].

7. Defense against DDoS attacks

The defense contrary to DDoS attacks is very difficult and it is better to gear up first. A possible countermove against application attacks is a scalable and resilient infrastructure (web front-end clusters, databases, firewalls, and so on). From the band DDoS, on the other hand, only Internet Service Providers can protect users (Fastweb, for example, has a dedicated paid service). Alternatively, users can contact a specialized market player (like Akamai) who receives all the traffic addressed to the computer system in question, cleans it, and sends only the appropriate one. Then there are the particularly complex targeted attacks that must be managed from time to time [20].

8. DDoS Mitigation Services

One solution advocated by experts is to choose a cloud-based DDoS prevention service. It is important to know the origin of the addresses of cloud mitigation services both in the assessment phase and in the implementation phase, also for a dimensional fact: depending on the size of an organization, in fact, there are several options that can lead to a redirection traffic through a through DNS (Domain Name System) or BGP (Border Gateway Protocol).

A process of verification of the analysis must be established on a periodic basis. There are a number of ways in which the source IP can be violated: a tool like CloudPiercer, for example, is able to verify some of these ways, but users must consider how it cannot always be a malevolent violation (it is the case of a web developer accidentally included in a series of activities and which can alter the pingbacks with information on X.509 certificates with his MX records) [21].

That's why it's critical to include vulnerability scanning tools, application testing tools, DLP tools, or any other tool that can tune into network anomalies or write rules that help find and flag the source violation. The automatic periodic analysis is also important because each evaluation becomes a punctual exercise compared to configurations and updates that can change. The important thing, experts warn, is to see the DDoS Mitigation Services (DDoSMS) a bit like a form of insurance that is always and in any case, but which is evident when needed [22].

The best action to do is to verify the mitigation service similar to how the disaster recovery and similar tests are performed. A quality provider will not be exempt from the request and will not limit itself to checking, taking the opportunity to show all its capabilities, for example by ensuring, in the case of bandwidth saturation, that the service works as intended.

Another important advice is to evaluate the use of filters and detection rules with respect to network traffic trends that do not come from the scrubbing center. Some service providers, in fact, can suggest filtering all traffic: it can be a good approach when possible, but, according to the security consultants, situations that prevent it may exist. This is the case with a broad base of legacy applications, based on very rigid IP coding systems or, in general, difficult to modify and which can make filtering difficult [23].

In other situations where users cannot filter all traffic except the scrubbing center, they can choose other options such as using an IDS or another detection system that alerts the security team to abnormal connections that do not come from the service provider. Although this will not prevent a DDoS attack, it will at least warn the organization of the anomaly generated, for example, by an investigative probe of a hacker who is planning a malicious action.

9. Conclusion

In conclusion, DDoS is a very serious type of attack, dealing with a DDoS mitigation is definitely a challenge, from an implementation point of view there are some steps that companies must take to achieve the protection they want and expect. Certainly going back to the origin of the anomaly and carrying out appropriate tests on the DDoS mitigation service and on the filtering and/or detection mechanisms, the organizations can raise the levels of safety and be extremely more proactive.

References

[1] Kiattikul Treseangrat, Samad Salehi Kolahi, Bahman Sarrafpour, "Analysis of UDP DDoS cyber Flood Attack and Defence Mechanism on Windows Server 2012 and Linux Ubuntu 13", IEEE, 2015.

[2] Rashmi V. Deshmukh, Kailas K. Devadkar, "Understanding the DDoS attack & its Effects In Cloud Environment", ICAC3–15, vol. 49, no. 2015, pp. 202-210.

[3] S. M., & St-Hilaire, M. Mousavi, "Early detection of DDoS attacks against SDN controllers," In Computing, Networking and Communications (ICNC), 2015 International Conference, 2015.

[4] J., Choi, C., Ko, B., & Kim, P. Choi, "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment.A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment.," 2014.
[5] S. T., Joshi, J., & Tipper, D. Zargar, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. ," IEEE communications surveys & tutorials, 2013.
[6] C., Kambourakis, G., Stavrou, A., & Voas, J. Kolias, "DDoS in the IoT: Mirai and other botnets. ," 2017.
[7] [7] Y., Li, K., & Zhou, W. Xiang, "Low-rate DDoS attacks detection and traceback by using new information metrics.," 2011.
[8] B., Vijayan, A. S., & Joshi, B. K. Joshi, "Securing cloud computing environment against DDoS attacks.," 2011.
[9] R., Xu, R., Tang, X., Sheng, V. S., & Cai, C. Cheng, "An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment," 2018.
[10] C., Miu, T. T., Luo, X., & Wang, J Wang, "Skyshield: A sketch-based defense system against application layer DDoS attacks," 2018.
[11] Jisa David, Ciza Thomas, "DDoS Detection using Fast Entropy Approach on Flow Based Network Traffic", 2nd International Symposium on Big Data and cloud computing(ISBCC‘ 15), vol. 50, no. 2015, pp. 30-36.
[12] Istvan Kiss, Piroska Haller, Adela Beres, "Denial of Service attack Detection in case of Tennessee Eastman challenge process" in 8th INTER-ENG 2014, Romania:, vol. 19, pp. 835-841, 2015.
[13] Vijay D. Katkar, Deepti S. Bhatia, "Lightweight approach for the denial of service attacks using numeric to binary preprocessing", International Conference on Circuit System Communication and Information Technology Application(CSCITA) in IEEE, 2014.
[14] Harkeerat Bedi, Sankardas Roy, Sajjan Shiva, "Mitigating Congestion-Based Denial of Service Attacks with Active Queue Management", IEEE 2013, pp. 1440-1445.
[15] Paul c. Hershey, Charles B. Silio, "Procedure for detection of and response to Distributed Denial of Service Cyber-attack on complex enterprise systems", IEEE, 2012.
[16] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, "A System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis", IEEE Transactions on parallel and distributed system, 2013.
[17] Munish Dhar, Rajeshwar Singh, "A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks", International Journal of Computer Science and Information Technology Research, vol. 3, no. 2015, pp. 27-33.
[18] Y. Huang, J. M Pullen, "Countering Denial-of-Service attacks Using Congestion Triggered Packet Sampling and Filtering", Proc. 10 th ICCCN , Oct. 2001.
[19] X. Geng, A. B. Whinston, "Defeating Distributed Denial of Service attacks," IEEE IT Professional 2, july 2000, pp. 36-42.
[20] J. B. D. Cabrera et al., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables - A Feasibility Study", Proc 7 th IFIP/IEEE Int. Symp. On Integrated Network Management , May 2001
[21] J. Ioannidis, S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", Proc. IEEE INFOCOMM, pp. 878-886, Apr. 2001
[22] Gary C. Kessler "Defenses Against Distributed Denial of Service Attacks," 4th edition of the Computer Security Handbook, November 2000.
[23]]Puneet Zaroo," A Survey of DDoS attacks and some DDoS defense mechanisms," Advanced Information Assurance (CS 626), 2003.

Usman Ali is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: r.usmaanali@gmail.com

Abu ul Hassan is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: Hassan.superior1@gmail.com

Muhammad Sheraz Arshad Malik is a professor in RIPHAH international University and GC University Faisalabad E-mail: sheraz_awan@gcuf.edu.pk

Syed Kashif Hashmi is currently pursuing MS degree program in Computer Science in RIPHAH International University, Pakistan, E-mail: mk.hashmi@yahoo.com

Bushra Aslam is currently pursuing MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: bushraa400@gmail.com

Basit Ayub is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: basitayub947@gmail.com