Article Citation Format
Adenekan, O.A & Durosinmi, A.E (2017):
Security Vulnerabilities of Existing
Distributed Denial of Service (DDoS) Attack & its Mitigation Techniques.
Journal of Advances in Mathematical & Computational Sciences Vol. 5, No. 1.
Pp 41-46. https://www.mathematics-computationaljournal.info

Article Progression Time Stamps

Article Type: Research Article
Manuscript Received 11th February, 2017
Final Acceptance: 16th March, 2017
Article DOI: dx.doi.org/10.22624/AIMS/MATHS/V5N1P5

Security Vulnerabilities of Existing Distributed Denial of Service (DDoS) Attack & its Mitigation Techniques.

[1]Adenekan, O.A[1] & [2]Durosinmi, A.E
[1&2]Department of Computer Engineering
Moshood Abiola Polytechnic
Abeokuta, Ogun State. Nigeria.
E-mails: adenekanolujide@yahoo.com, cunlexie@hotmail.com

ABSTRACT

Distributed Denial of Service (DDoS) attacks have emerged as a popular means of causing mass targeted service disruptions, often for extended periods of time. Traditional architecture of Internet is vulnerable to DDoS attacks and an ongoing cycle of attack & defense is observed. The denial of service (DOS) attack is one of the most powerful attacks used by hackers to harm a company or organization. Don't confuse a DOS attack with DOS, the disc operating system developed by Microsoft. This attack is one of most dangerous cyber attacks. It causes service outages and the loss of millions, depending on the duration of attack. The attacks categories and existing countermeasures based on preventing, detecting, and responding are reviewed. In this paper we have studied DDos Attack in detail (including attack process and classification of Ddos attack) and reviewed some of the existing anti- DDos techniques along with their advantages and disadvantages and also make recommendations on how both can be mitigated.

Keywords: DDoS, Attacks, Detection, Security, Network.

1. INTRODUCTION

A DOS attack is an attempt to make a system or server unavailable for legitimate users and, finally, to take the service down. This is achieved by flooding the server's request queue with fake requests. After this, server will not be able to handle the requests of legitimate users. A denial of service attack happens when an attacker make a website or other internet-based applications or services to be unreachable and unavailable to the legitimate users . Denial of service can also be defined as a malicious attack, whereby an internet-based service becomes unavailable to the users by interrupting the normal functionality of the hosting server of the application. Normally, the denial of service (DoS) attack involves compromising a single instance of a key internet device.

The scenario a hosting server or a network switch that uses a single internet connection and interrupting its normal functioning. A denial of service (DOS) attack involves compromises multiple devices such as servers, network switches, or routers that are located in different geographical locations across the globe. They are using different networks, and as such, the denial of service is distributed in multiple locations and there is no backup (Muharish, 2016). A denial of service attack involves an attacker who exploits a vulnerability in a device such as a hosting server and makes it a denial of service master. This DoS master is infected with malicious software and it infects other devices such as end-user devices with the malware. A denial of service attack involves a number of computing devices that are compromised, also called master-bots or botnets. They consistently send a large amount of requests or data packets to slave-bots or to the internet connection of the slave-bots, which causes the entire system to collapse, making it unavailable or unreachable .

Attackers create many botnets that are also called zombies, which make multiple requests to the servers of an application such as website, jamming the servers, exhausting the computing resources such as RAM or network bandwidth such that legitimate requests form legitimate users cannot be fulfilled making the entire website unavailable . Victims of a denial of service attack usually become overwhelmed by the huge volumes of data packets that are sent from multiple sources, causing congestion in the networks . DDoS attacks are reported as one of the highly occurred attack over a past few decades. Many service providers and legitimated users have undergone a nasty experience from these attacks. DDoS attack is an intruder attempt to make a network services unavailable to the intended user. DDoS have many faces like flooding attack, logic attack and protocol-based attack. Flooding attack is an attack in which it covers the network with unwanted packets, i.e. either the node may send replicated packets or the node may send the unique packets which exceed its rate limit. Logic attack is an attack which has a buffer space limit and it may exceed or overflow when it accepts a large amount of packets beyond its limit. In protocol-based attack attacker does not weakens the TCP/IP functionality instead it take the expected behaviour of this protocol for the requirements of attacker. (Engineering, 2013)

In Operating System (OS) level attacks, vulnerabilities of operating system in the victim machine are used to launch DoS attack. In application level attacks, bugs or vulnerabilities in the application are identified to exploit them for DoS attack. Port scanning for identifying open ports of a remote application is very common in this perspective. Such attacks are now getting more popular as they present the traffic to a network and its devices similar to the legitimate traffic. Therefore, in a scenario where most of other attacks are now identifiable, application level attacks offer more success rate to attackers. In data flood attacks, targets are the connection capacity of a remote host or the bandwidth of a network. Heavy traffic is generated by the attacker towards the victim to exhaust connectivity or bandwidth resources so that normal services are denied or degraded for requests of legitimate users.

Even though denial of service attacks have existed for some time, their recent distributed formats have made these attacks more difficult to prevent(Lau, Rubin, & Smith, n.d.). In protocol feature attacks, the weaknesses of some protocol features are used to exploit them for launching a DoS attack. For example, the source IP address of a data packet (which relates to Internet Protocol and is a part of TCP/IP stack) can be spoofed by an attacker to launch a DoS attack which can be harder to trace due to a fake address(Aamir & Zaidi, n.d.) Denial of Service (DOS) attacks are intended to shut down the servers for a period of time. To make site nonfunctional for a time, the main part of attack is DOS attack.(Priyadharshini & Kuppusamy, 2012)

2. RELATED WORKS

A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. This is any type of attack that attempts to make this computer resource unavailable to its users.A DDOS attack is simply a combined effort to prevent computer systems from working as well as they should, typically from a remote location over the internet. A number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. The most common method of attack is to send a mass saturation of incessant requests for external communication to the target. These systems are flooded with requests for information from non-users, and often non-visitors to the website. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed.

If this type of service becomes too slow, time sensitive information such as live video footage may be rendered entirely useless to legitimate end users(Sahu, 2014) . Protection against DoS and DDoS attacks highly depends on the model of the network and the type of attack. Several mechanisms have been proposed to solve the problem. However, most of them have weaknesses and fail under certain scenarios (Ervers, 2011). In this DOS attack, the attacker's goal is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. All the resources of the nodes will continuously busy in message verification, which (messages) is coming from attacker nodes (Raghuwanshi & Jain, 2015). Denial of Service (DoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. DoS attacks vastly focus on degrading the availability of a victim, which can either be host, router, or an entire network. Interconnected systems, cloud computing servers, web servers, so on, are under threads from the network attackers.

Denial-of-service (DoS) attacks cause serious impaction these computing systems. In this paper, a DoS attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. The MCA-based DoS attack detection system employs the principle of anomaly based detection in attack recognition. This makes solution capable of detecting known and unknown DoS attacks effectively by learning only the patterns of legitimate network traffic. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that this system outperforms two other previously developed state-of-the-art approaches in terms of detection. A MCA based analysis DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique.

The former existing technique captures the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and allows space for more accurate characterization for network traffic behaviors. The latter technique facilitates to be able to distinguish both known and unknown DoS attacks from legitimate network traffic (Abliz, 2011). In DDoS attack, when a huge number of queries come to the server, the server increases its computational power and starts to entertain every request. The server system has the limited capacity to entertain the number of user request at a time. So, when a huge a number of fake request or queries come to the server, the server gets busy and the actual user request cannot be entertained in that period. Hence the denial of service occurred(Sattar & Shahid, 2015).

3. DISTRIBUTED DENIAL OF SERVICE ATTACKS TYPES

Next we discuss DDOS typologies

SYN FLOODING

This is the most important attack occur during the three-way handshake. In three-way handshake client request a new connection by sending SYN packet server ACK sends back to client. Finally client acknowledged with ACK.If attack occur numerous SYN packet to victim. It makes open numerous connections and responds to them, and third step of the hank-shake will not perform. That makes unable to open new connections. This Because of queue is filled with full of half-way TCP request. This flooding does not targeting specific operating system. It attacks any system that support TCP connection(Engineering, 2013).

SMURF ATTACK

Cause of smurf attack is flooding of ICMP echo-request echo-reply. Direction of packet is to IP broadcast address from remote location to generate DoS attack. Most of time attacker generate forged echo request using spoofed IP address, i.e. it is intended to victim machine, and attacker hide its identity. The intermediate node can't identify whether it is original or not. So intermediate node immediately reply that make flood on the victim machine.

UDP FLOOD ATTACK

This is the second most popular attack. Main idea of this attack is to exploit UDP services. These attacks slowly down/congested the network. In this attack attacker sends to random port of victim. After receiving that packet victim system is try to find which application is waiting on the destination. But actually no application running on that port.AZ large number of UDP packet are received by the victim, it make infinite number of loop goes between the Two UDP services.

ICMP DOS ATTACK

In this attack Attacker simply forging the notification message. Attacker could use either Time exceed and or Destination unreached that cause immediately drop the connection Eg. Ping of Death, ICMP PING flood attack, ICMP nukes attack.

PING OF DEATH

In this attack, attacker sends large number of malicious ping to computer. In this case large IP packet is split in multiple IP packets. In ping death scenario receiver ends up with packet size greater than 65,535when reassembled and over flow on allocated memory with numerous packets.

LAND ATTACK

It consist stream of the TCP SYN packet both source and destination have same IP address and port number. Some implementations are impossible to handle this type of attacks completly.The main cause of this attack the operating system repeatedly go into the loop try to resolved repeated connection itself.

MAIL BOMB

It is bandwidth-based flood attack. The attacker node sends large volumes of mail to mail-server causing it to deny services to legitimate user.

DNS AMPLIFICATION ATTACK

Attacker use publically accessible open DNS server to flood a target system with DNS response traffic. The crucial technique consists of an attacker sending a DNS name lookup to an open DNS server with source address spoofed to be target's address. Attacker submits more requests to zone as possible to maximize the effect.

IGMP ATTACK.

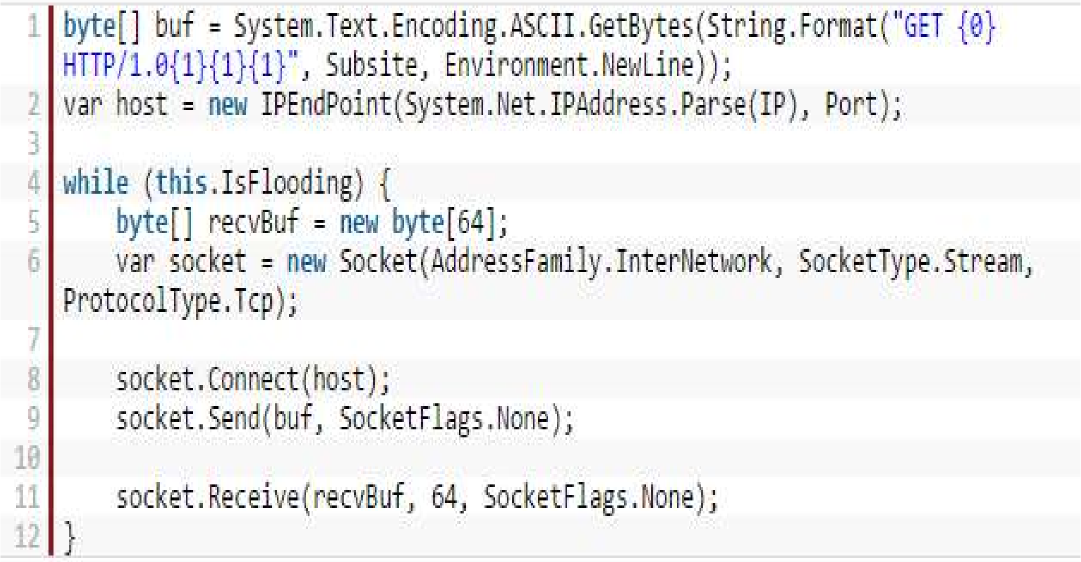
Cause this attack is to Flood the network with random IGMP messages. It makes overload on the network. It is the type of hacking attack. Main idea this attack is to reduced broadband and memory usage. But it is useful for multimedia broadcast application.

SQL SLAMMER

It is one computer worm that causes the denial of service on some internet host. Dramatically slow down internet traffic. It exploits buffer overflow vulnerability in SQL server and MSDE code.

4. DISTRIBUTED DENIAL OF SERVICE ATTACKS TECHNIQUES

Below is a cleaned up and simplified version of the method responsible for carrying out the actual HTTP Denial of Service attack.



```
1  byte[] buf = System.Text.Encoding.ASCII.GetBytes(String.Format("GET {0}
   HTTP/1.0{1}{1}{1}", Subsite, Environment.NewLine));
2  var host = new IPEndPoint(System.Net.IPAddress.Parse(IP), Port);
3
4  while (this.IsFlooding) {
5      byte[] recvBuf = new byte[64];
6      var socket = new Socket(AddressFamily.InterNetwork, SocketType.Stream,
   ProtocolType.Tcp);
7
8      socket.Connect(host);
9      socket.Send(buf, SocketFlags.None);
10
11     socket.Receive(recvBuf, 64, SocketFlags.None);
12 }
```

a. In the first two lines the application prepares the attack's underlying HTTP request and sets the target IP address and the target port.
b. Although it's done in an rather unusual way it's a legitimate implementation for an application requesting data from an external HTTP service.
c. In the following third line the while command tells the system to repeat all enclosed and indented further commands. Within this section the actual attack is launched.

d. However to do so two more things need to be prepared: At first in line 5 a buffer called recvBuf is created that is used to store the subsequential answer from the victim and in line 6 further connection details like the use of the TCP protocol are specified.
e. Finally in line 8 the network connection to the victim's server is established and in line 9 the HTTP request that was created in the beginning is sent.
f. The subsequent receive method call in line 10 stores the first 64 byte of the server's reply in the previously created receive buffer recvBuf. This forces the application to wait for the server to reply before it moves on.
g. Until now we behaved like a normal web browser, however as the last command within the while loop was reached the whole process beginning at line 5 is repeated again and again …
h. What that means is we didn't really use any service and just created unnecessary load on the server and the network connection. As the attack requests are generally repeated as fast as possible and are executed in parallel this load can render services unusable or even bring them down completely.

5. CONCLUSION

Every server should set up a way to detect and block DDOS attacks. DOS attacks are a significant threat to many online services that are used every day and can cost businesses significant amounts in lost revenue. They can often be a cover for a different kind of cyber-attack, most notably theft from networks.

Organisations of all sizes, including small and medium sized enterprises, should take this threat seriously and are recommended to follow the mitigation advice in this paper. With greater cyber awareness and better working practices, the threat from DOS attacks can be reduced.

REFERENCES

1. Aamir, M., & Zaidi, M. A. (n.d.). DDoS Attack and Defense : Review of Some Traditional and Current Techniques, 1–19. http://doi.org/10.4036/iis.2013.173
2. Abliz, M. (2011). Internet Denial of Service Attacks and Defense Mechanisms, (March), 1–50.
3. Engineering, C. (2013). A Survey on DDoS Attacks and Defense Approaches, 1800–1805.
4. Ervers, W. E. B. S. (2011). A Robust Mechanism For Defending Distributed Denial Of Service Attacks on, 3(2), 162–179.
5. Lau, F., Rubin, S. H., & Smith, M. H. (n.d.). Distributed Denial of Service Attacks.
6. Muharish, E. Y. M. (2016). Packet Filter Approach to Detect.
7. Priyadharshini, V., & Kuppusamy, K. (2012). Prevention of DDOS Attacks using New Cracking Algorithm, 2(3), 2263–2267.
8. Raghuwanshi, V., & Jain, S. (2015). Denial of Service Attack in Vanet : A Survey, 28(1), 15–20.
9. Sahu, S. S. (2014). Distributed Denial of Service Attacks : A Review, (January), 65–71. http://doi.org/10.5815/ijmecs.2014.01.07
10. Sattar, I., & Shahid, M. (2015). A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment, 115(8), 23–27.