УДК 004.056

Alshati Ahmed Salim, T.A. Prykhodko
Donetsk national technical university

STUDY AND ANALYSIS OF DOS BASICS

Abstract

Alshati Ahmed Salim, Prykhodko T.A. Study and analysis of dos basics. The purpose of this article is to do an observe and comparing characteristic of different kinds of network Denial of Service attacks. This paper gives an understanding the meaning and the mechanism of the Denial of Service attacks, deferent types and tips for prevent these attacks.

Key words: Denial of Service attacks **(DoS),** Distributed Denial of Service **(DDoS)**, Flood attacks.

Introduction.A Denial of Service, or DoS as it is often abbreviated, is a malicious attack on a network. This type of attack is essentially designed to bring a network to its knees by flooding it with useless traffic. Many DoS attacks work by exploiting limitations in the TCP/IP protocols. The threats of flood attacks to the individuals are severe. For instance, any denial of service of a bank server implies a loss of money, disgruntling or losing customers.

Categories of DDoS. While the DDoS threat landscape is constantly evolving, now attacks continue to fall within four attack types: volumetric, asymmetric, computational, and vulnerability-based [3].

- Volumetric—Flood-based attacks that can be at layer 3, 4, or 7.
- Asymmetric—Attacks designed to invoke timeouts or session-state changes.
- Computational—Attacks designed to consume CPU and memory.
- Vulnerability-based—Attacks that exploit software vulnerabilities.

This paper considers flood attacking.

Denial-of-service (DoS) attack. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

4. Political reasons (a country at war could perpetrate attacks against its enemy's critical resources, potentially enlisting a significant portion of the entire country's computing power for this action).

Distributed denial-of-service (DDoS) attack In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack, and of course this type is the most dangerous types of attacks (fig.1).

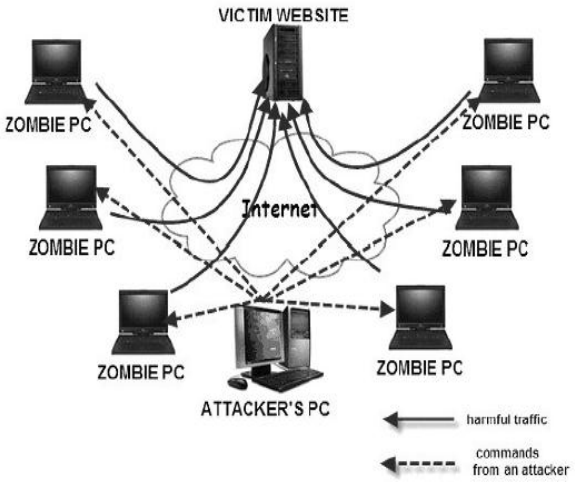

Figure 1 - DDoS mechanism.

Difference between DoS and DDoS attack. It is important to differentiate between Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server's bandwidth and resources. DDoS attack, uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet. A DDoS attack is, therefore, much harder to deflect, simply because there is no single attacker to defend from, as the targeted resource will be flooded with requests from many hundreds and thousands of multiple sources.

Reasons for a DDoS attacks.1. The ulterior motives are personal reasons; a significant number of DDoS attacks are perpetrated against home computers, presumably for purposes of revenge (Expression of anger and criticism).

2. Prestige, a successful attack on popular Web servers gains the respect of the hacker community.

3. However, some DDoS attacks are performed for material gain (damaging a competitor's resources or blackmailing companies)

How to inflict a DDoS attack. To launch a DDoS attack, intruder first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users (Fig 1.). To create attacks, attackers, discover vulnerable sites or hosts on the network. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date antivirus software, or those that have not been properly patched. Then attackers who use their vulnerability to gain access to these hosts exploit vulnerable hosts. The next step for the intruder is to install new programs (attack tools) on the compromised hosts of the attack network. The hosts that are running these attack tools are known as Masters or Handlers, and they can carry out any attack under the control of the attacker. After that, the systems that have been infected by the malicious code look for other vulnerable computers and install on them the same malicious code. Because of that widespread scanning to identify victim systems, it is possible that large attack networks can be built very quickly. The result of this automated process is the creation of a DDoS attack network that consists of masters and slaves (Zombie PC) machines. It can be inferred from this process that another DDoS attack takes place while the attack network is being built, because the process itself creates a significant amount of traffic.

Zombie machines are commonly external to the victim's own network, to avoid efficient response from the victim, and external to the network of the attacker, to avoid liability if the attack is traced back.

Common Dos & DDoS Attacks.*Ping of Death.* A type of DoS attack in which the attacker sends a ping request that is larger than 65,536 bytes, which is the maximum size that IP allows. While a ping larger than 65,536 bytes is too large to fit in one packet that can be transmitted, TCP/IP allows a packet to be fragmented, essentially splitting the packet into smaller segments that are eventually reassembled. Attacks took advantage of this flaw by fragmenting packets that when received would total more than the allowed number of bytes and would effectively cause a buffer overload on the operating system at the receiving end, crashing the system.

Smurf Attack. In a "smurf" attack, the victim is flooded with Internet Control Message Protocol (ICMP) "echo-reply" packets. The attacker sends numerous ICMP "echo-request" packets to the broadcast address of many subnets. These packets

contain the victim's address as the source IP address. Every machine that belongs to any of these subnets responds by sending ICMP "echo-reply" packets to the victim. Smurf attacks are very dangerous, because they are strongly distributed attacks.

TCP SYN Attack. A SYN flood attack occurs during the three-way handshake that marks the onset of a TCP connection. In the three-way handshake, a client requests a new connection by sending a TCP SYN packet to a server. After that, the server sends a SYN/ACK packet back to the client and places the connection request in a queue. Finally, the client acknowledges the SYN/ACK packet. If an attack occurs, however, the attacker sends an abundance of TCP SYN packets to the victim, obliging it both to open a lot of TCP connections and to respond to them. Then the attacker does not execute the third step of the three-way handshake that follows.

Teardrop. While a packet is traveling from the source machine to the destination machine, it may be broken up into smaller fragments, through the process of fragmentation. A Teardrop attack creates a stream of IP fragments with their offset field overloaded. The destination host that tries to reassemble these malformed fragments eventually crashes or reboots.

There are many more types developed every day by hackers…

Conclusions. Undoubtedly, DoS & DDoS attacks present a serious problem in the Internet and challenge its rate of growth and wide acceptance by the general public, skeptical government and businesses. As we understand in this paper that the DoS can avoid or manage because who launch it is one person or a very small number of computers. Now we know more about this problem, architecture, types and tips to avoid being under attack. DDoS attack is the biggest problem in the communication world now.

Perspective. Authors are going to study the quantitative behaviors of attacking under different protocols of transport OSI layer using NS2 simulation tool. The first step is to study statistical properties of legitimate traffic and then flood traffic.

List of references

1. http://www.webopedia.com/DidYouKnow/Internet/DoS_attack.aspb
2. White PaPer. "The F5 DDoS Protection Reference Architecture" http://interact.f5.com/rs/f5/images/ddos-protection-reference-architecture-wp.pdf
3. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html?referring_site=smartnavRD
4. http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html