International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

DOS Attacks

Rushikesh Gawande

Abstract: ***A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.***

Keywords: Denial of service, Distributed Denial of Service, Internet Security

1. Introduction

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management. There are two general forms of DoS attacks: those that crash services and those that flood services. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

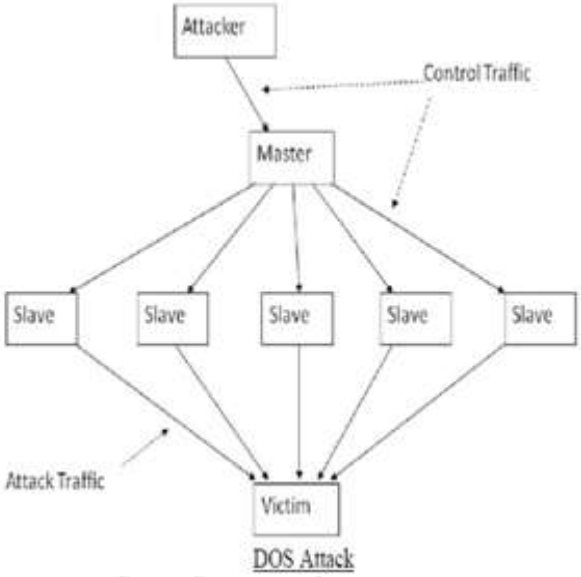

Figure 2.1

2. Symptoms and Manifestations

The United States Computer Emergency Response Team defines symptoms of denial of service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received— (this type of DoS attack is considered an e-mail bomb)

Denial-of-service attacks can also lead to problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by an attack, compromising not only the intended computer, but also the entire network. If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment. Before I go on with DOS attacks, let me explain some vulnerabilities in TCP/IP itself. Some common vulnerabilities are Ping of Death, Teardrop, SYN attacks and Land Attacks.

A. Ping of Death

This vulnerability is quite well known and was earlier commonly used to hang remote systems (or even force them to reboot) so that no users can use its services. This exploit no longer works, as almost all system administrators would have upgraded their systems making them safe from such attacks. In this attack, the target system is pinged with a data packet that exceeds the maximum bytes allowed by TCP/IP, which is 65 536. This would have almost always caused the remote system to hang, reboot or crash. This DOS attack could be carried out even through the command line, in the following manner: The following Ping command creates a giant datagram of the size 65540 for Ping. It might hang the victim's computer:

C:\windows>ping -l 65540

Figure 2.A.1

How to test if you're vulnerable Unfortunately, this bug is really easy to exploit. Users are already trying it out "just to see if it worked". So, to test if your machine is in danger,

find a Windows '95 or NT box (3.51 or 4), and run the following command:
ping -l 65550 your.host.ip.address

3. How to prevent people from breaking your system

If no patch is available, and your main concern are pings from users outside your network, it would seem the best quick-fix solution is to block ping at the firewall. This is not a long-term solution. If you have any services listening on any ports at all, they are vulnerable. Be assured that sooner or later someone will come out with a program which sends invalid packets to a web server, an ftp port. The only solution is to patch your operating system. By blocking ping, you prevent people from pinging you at all. This could possibly break some things that rely on. A better solution than blocking all pings is to block only fragmented pings. This will allow your common-or-garden 64-byte ping through on almost all systems, while blocking any bigger than the MTU size of your link.

B. Ping flood

A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. It only succeeds if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown. There are two general forms of DoS attacks: those that crashes services and those that flood services.

C. Teardrop

The Teardrop attack exploits the vulnerability present in the reassembling of data packets. Whenever data is being sent over the Internet, it is broken down into smaller fragments at the source system and put together at the destination system. Say you need to send 4000 bytes of data from one system to the other, then not all of the 4000 bytes is sent at one go. This entire chunk of data is first broken down into smaller parts and divided into a number of packets, with each packet carrying a specified range of data. For Example, say 4000 bytes is divided into 3 packets, then:

The first Packet will carry data from 1 byte to 1500 bytes. The second Packet will carry data from 1501 bytes to 3000 bytes. The third packet will carry data from 3001 bytes to 4000 bytes. These packets have an OFFSET field in their TCP header part. This Offset field specifies from which byte to which byte does that particular data packet carries data or the range of data that it is carrying. This along with the sequence numbers helps the destination system to reassemble the data packets in the correct order. Now in this attack, a series of data packets are sent to the target system with overlapping Offset field values. As a result, the target system is not able to reassemble the packets and is forced to crash, hang or reboot. Say for example, consider the following scenario-: (Note: _ _ _ = 1 Data Packet) Normally a system receives data packets in the following form, with no overlapping Offset values.
(1 to 1500 bytes)
(1501 to 3000 bytes)
(3001 to 4500 bytes)
Now in a Teardrop attack, the data packets are sent to the target computer in the following format:
(1 to 1500 bytes)
(1500 to 3000 bytes)
(1001 to 3600 bytes)
When the target system receives something like the above, it simply cannot handle it and will crash or hang or reboot.

4. Distributed DOS Attacks

DOS attacks are not new; in fact, they have been around for a long time. However there has been a recent wave of Distributed Denial of Services attacks which pose a great threat to Security and are on the verge of overtaking Viruses/Trojans to become the deadliest threat to Internet Security. Now you see, in almost all of the above TCP/IP vulnerabilities, which are being exploited by hackers, there is a huge chance of the target's system administrator or the authorities tracing the attacks and getting hold of the attacker.

Now what is commonly being done is, say a group of 5 Hackers join and decide to bring a Fortune 500 company's server down. Now each one of them breaks into a smaller less protected network and takes over it. So now they have 5 networks and supposing there are around 20 systems in each network, it gives these Hackers, around 100 systems in all to attack from. So, they sitting on their home computer, connect to the hacked less protected Network, install a Denial of Service Tool on these hacked networks and using these hacked systems in the various networks launch Attacks on the actual Fortune 500 Company. This makes the hackers less easy to detect and helps them to do what they wanted to do without getting caught. As they have full control over the smaller less protected network they can easily remove all traces before the authorities get there. Not even a single system connected to the Internet is safe from such DDOS attacks. All platforms including Unix, Windows NT are vulnerable to such attacks. Even MacOS has not been spared, as some of them are being used to conduct such DDOS attacks.

5. Conclusion

DDoS attack tools are readily available and any internet host is targetable as either a zombie or the ultimate DDoS focus. These attacks can be costly and frustrating and are difficult, if not impossible to eradicate. The best defense is to hinder attackers through vigilant system administration. Applying patches, updating anti-malicious software programs, system monitoring, and reporting incidents go further than retarding DDoS attacks – these defenses also protect against other attacks. The Internet is not stable—it reforms itself rapidly. This means that DDoS countermeasures quickly become obsolete.

References

[1] CIS 659 "Introduction to Network Security – Fall 2003,"http://www.cis.udel.edu/~sunshine/F03/CIS659/class15.pdf
[2] Kevin Tsui, "Tutorial-Virus (Malicious Agents)," University of Calgary, October 2001.
[3] Erickson, Jon (2008). HACKING the art of exploitation (2nd ed.). San Francisco: No Starch Press. p. 256. *ISBN 1-59327-144-1*.
[4] "Microsoft Security Bulletin MS13-065 - Important". *Microsoft. August 13, 2013*. Retrieved February 25, 2017.
[5] Nicholas Weaver, "Warhol Worms: The Potential for Very Fast Internet Plagues," http://www.iwar.org.uk/comsec/resources/worms/warhol-worm.htm
[6] "Understanding Denial-of-Service Attacks". *US-CERT. 6 February 2013*. Retrieved 26 May 2016.
[7] Raghavan, S.V. (2011). An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks. *Springer. ISBN 9788132202776.*
[8] McDowell, Mindi (November 4, 2009). "Cyber Security Tip ST04-015 - Understanding Denial-of-Service Attacks". United States Computer Emergency Readiness Team.
[9] Dhruba Kumar Bhattacharyya (2016), "DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance"