Halmstad University
School of IDE
Network Security 7, 5 p
Networkdesign and Computer Management

DDoS

Distributed Denial of Service

Spring Term 2008

Mattias Holm, 861117-2712
Christian Nilsson, 820309-3532

Supervisor: Yan Wang

Title page: DDOS

1. Introduction
2. DDoS
   2.1 Concept of DDoS
   2.2 DRDoS
   2.3 Examples of known DDoS attacks
   2.4 Prevention and Solutions for DDoS attacks
3. Introduction to TCP
4. Types of Attacks
   4.1 SYN Flood attacks
   4.2 ARP Flood attacks
   4.3 Smurf IP attack
   4.4 Mail bomb
   4.5 SSH process table attack
5. Prevention and solutions
6. Conclusion

1. Introduction

We have chosen to write about DDoS which is a security breach intended to deny legitimate users from services inside their network. The process is simply to take control over computers around the globe to flood the victims' network with traffic to exhaust it. To understand how network DDoS attacks works we have included a short introduction to the TCP three-way handshake which many of the subtypes is using to overwhelm the network. We have also described the concept of DDoS and different kind of attacks. Also we have a page about how to protect your network.

2.DDoS

2.1 Concepts of DDoS

DDoS stands for Distributed Denial of Service. And as you can tell by the name, it is based on Denial of Service. Which is a very basic type of security attack where the intention is to overload a network or a system, so legitimate users cannot access the services. The attack doesn't necessarily have to be digitally implemented. It can also be physically, for example, by cutting wires which also cause the resources to be inaccessible to the users.

This is quite easy to apply to networks, since network resources has finite bandwidth, memory and hardware performance. So by sending the target packets to consume the available resources, the legitimate user requests are rejected and so, the result is that the users will be denied access to the services.

The purpose of Dos attacks is not to "crack" the system and gain access to unauthorized privileges. The meaning is to disrupt the system and the success is measured in how long the system is down.

The essential difference between DDoS and DoS is that the in a DoS the attack is coming from a single source only while an attack from DDoS has multiple sources. A DDoS attack can be defined as an advanced DoS attack. These sources then perform a coordinated attack against the target at the same time.

The DDoS process begins with the attacker looking up vulnerable computers over the internet where he installs the DDoS program. This search is often made by software like 'autorooter'. This program makes the computer a "slave", or "zombie", for the attackers "master device", or "master zombie", which is also an innocent users computer remotely controlled by the attacker. This is what you can call, an attack network. This network often consists of computers that aren't running an anti-virus program or one that is out-of-date. The attacker orders the attack to "master devices", which in turn triggers the "slaves". See figure 2.1 for illustration.

To decrease the risk of being discovered, the attacker distributes the slave computers over several time zones and with different administrators. One way to hide where the attack is coming from is IP Spoofing. This means that the traffic appears to be created from another computer than the true source. As long as the source system is unknown, finding the person who is responsible is highly unlikely.

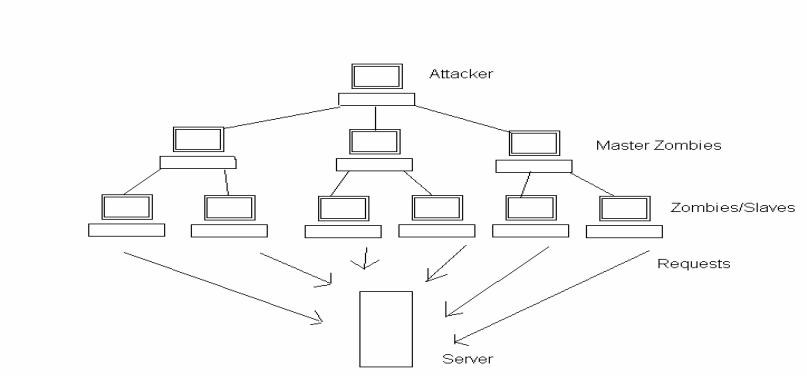

Figure 2.1: DDoS attack

2.2 DRDoS

Distributed Reflection Denial of Service is another type of DDoS. Like DDoS the attacking devices consist of “Master Zombies” and “Slaves”. But in this attack, “Reflectors” are also used. This type of attack uses the TCP handshake process to create traffic towards the intended network. The master zombies order the slaves to send a SYN to other uninfected servers, with the victims IP address as the source. The reflectors will then send a SYN/ACK to the victims system and in that way, overwhelm the network. With this kind of attack you can create more damage because the attacking devices are more distributed.

2.3 Examples of known DDoS attacks.

The first DDoS attack happened in New York September 1996 against the Internet Service Provider Panix. This was a SYN Flood attack with the SMTP ports as targets. The Panix computers were flooded with about 150 SYN packets per second.

Another known DDoS attack took place in June 2006 and it was the Swedish Police Website who was the victim for the attack. The website stayed down for half a day and was probably implemented due to the police raid against The Pirate Bay. The request rate for the website was about half a million every second.

Another more global attack occurred in February 2007, where three of thirteen of the internet root servers where taking out of order with a DDoS attack. These servers are the one managing the Internet Domain Name System. But according to experts regular web users never noticed the attack and they claim this only proof that the Internet is almost invulnerable.

3. Introduction to TCP

To understand the process of some of the attacks a brief introduction to TCP and its three-way handshake is necessary. TCP/IP is an acronym for Transmission Control Protocol / Internet protocol. The protocol is widely used on the internet to establish connection to services. For example HTTP, FTP and SSH uses TCP to establish a connection between server and client.

1. The client sends a SYN “Synchronize” packet to the receiver.
2. The receiver responds back with an SYN/ACK “Synchronize/Acknowledgement“-packet back to client.
3. And finally the client responds with an ACK “Acknowledgement” back to the receiver.

See figure 3.1 for illustration

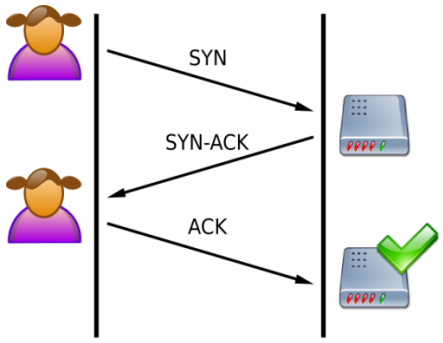

Figure3.1 Illustration of a normal TCP three-way handshake connection.

The sender and receiver have now established a TCP-connection between them, and they will be able to communicate.

4. Types of attacks

4.1 SYN Flood attack

One type of denial-of-service is the SYN Flood attack. It takes advantage of the three-way handshake model described in previous page.

1. The attacker creates packets that contain spoofed IP-addresses[1], with every packet has a SYN flag set meaning it would like to open a new connection to the Server.

2. The Server receives the spoofed packets and is sending back ACK packets back to the spoofed IP-addresses. The Server will wait for an ACK coming back from the attacker, but since the IP-addresses where spoofed it will never get any packets back.

3. During this process the server connection table will be full, and all new connections will be ignored. This will affect all users how wants to make a connection to the Server.

4. After the attacker had his share of fun and stops flooding the Server, the Server normally goes back to its normal state.

See figure 3.2 for illustration

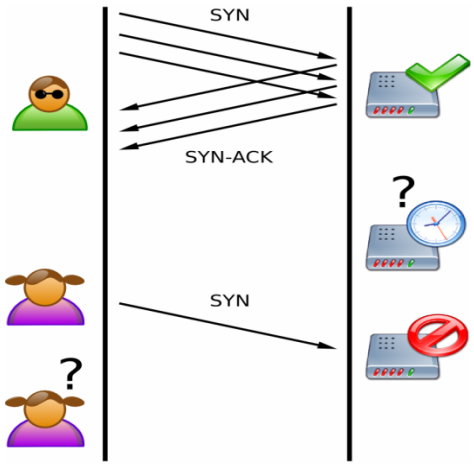

Figure 3.2 Illustration SYN Flood attack

[1]Spoofed IP-address when the attacker fake his IP-address, and is believed coming from that fake IP-address.

4.2 ARP poison

This is an attack against the Address Resolution Protocol. To achieve this kind of attack the attacker must be able to access the intended victims LAN. The purpose of the attack is to trick the hosts in a LAN by giving them the wrong MAC address for already known IP addresses. The process to complete this attack is to listen to the networks “Who has” requests and as quickly as possible respond to the request from the host.

4.3 Smurf IP attack

The attacker sends an ICMP packet to the broadcast address of many vulnerable networks with the victims IP address as the source. These networks then respond to this ICMP packet and flood the intended network to deny the service to legitimate users.

4.4 Mailbomb

In this attack you simply overwhelm the victims' mail with messages to force the system to fail.

4.5 SSH process table attack

In this attack the attacker uses the Secure Shell Protocol to overwhelm the system with connections without finishing the login. The daemon that is contacted by the SSH have to start so many connections until it crashes.

5. Prevention and solutions of DDoS Attacks

To protect your system from not being a victim of a DDoS attack can be very difficult if not impossible. It´s all about trying to determine which traffic is genuine and what is not. But there are a few things you can do to make your system a bit more secure.

IDS or Intrusion detection System is one way to analyze traffic on the system. If the IDS detects suspicious or malicious traffic it can drop that traffic, or it can block a user from accessing the network.

Firewalls are also a way to make the system a bit more secure. Firewalls look at inbound and outbound traffic and filters according to the rules you set up. For example you can drop packets that are coming from the outside of the network with a private IP address. Because no Private ip-addresses should be coming from the outside it is possible spoofed.

7. Conclusion

We have understood that this is a very widespread type of attack that is kind of easy to implement. Also it is very difficult to prevent or protect your network against a DDoS attack. And if so, the chance of catch the attacker is almost impossible since the IP is Spoofed and the slave devices comes from all around the world. This is a very simple and effective way to put a network out of balance or shutdown a specific service for the users.

References

"IDG", http://www.idg.se/2.1085/1.106987

"SecurityFocus", http://www.securityfocus.com/infocus/1647

"CERT", http://www.cert.org/homeusers/ddos.html

"Cisco", http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

"Dagens Nyheter", http://www.dn.se/DNet/jsp/polopoly.jsp?a=615150

"Palisade", http://palisade.plynt.com/issues/2006Apr/ddos-reflection/

"Pervasive Technology Labs", http://anml.iu.edu/ddos/types.html

TCP/IP references

http://www.cbronline.com/article_news.asp?guid=D137B95B-B05A-4838-A584-CD1DD71DDE26

http://www.3wayhandshake.com/images/3way.JPG

http://www.pccitizen.com/threewayhandshake.htm

TCP SYN Flood attack

http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm

http://tools.ietf.org/html/rfc4987

Prevention and solution DDoS attacks

http://www10.org/cdrom/papers/409/

http://www.securitypronews.com/2003/0925.html