CHAPTER-1

INTRODUCTION

DOS Attacks or Denial Of Services Attack have become very common amongst Hackers who use them as a path to fame and respect in the underground groups of the Internet. Denial of Service Attacks basically means denying valid Internet and Network users from using the services of the target network or server. It basically means, launching an attack, which will temporarily make the services, offered by the Network unusable by legitimate users.

In others words one can describe a DOS attack, saying that a DOS attack is one in which you clog up so much memory on the target system that it cannot serve legitimate users. Or you send the target system data packets, which cannot be handled by it and thus causes it to either crash, reboot or more commonly deny services to legitimate users.

DOS Attacks are of the following different types-:

1. Those that exploit vulnerabilities in the TCP/IP protocols suite.
2. Those that exploit vulnerabilities in the Ipv4 implementation.
3. There are also some brute force attacks, which try to use up all resources of the target system and make the services unusable.

Symptoms and Manifestations

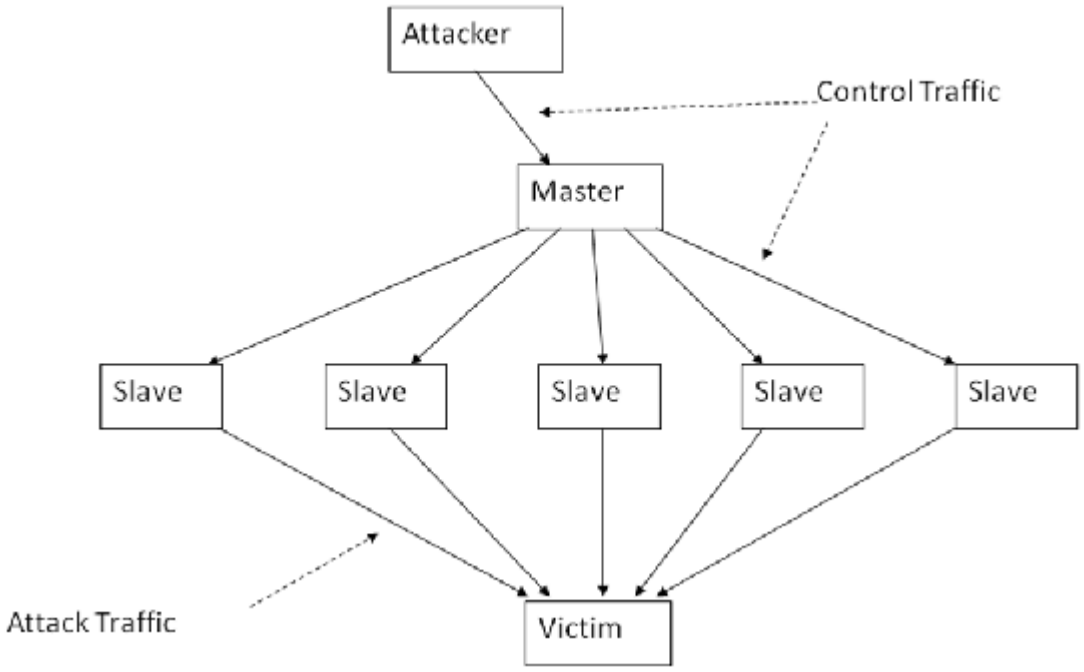
The United States Computer Emergency Response Team defines symptoms of denial-of-service attacks to include:

- 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.



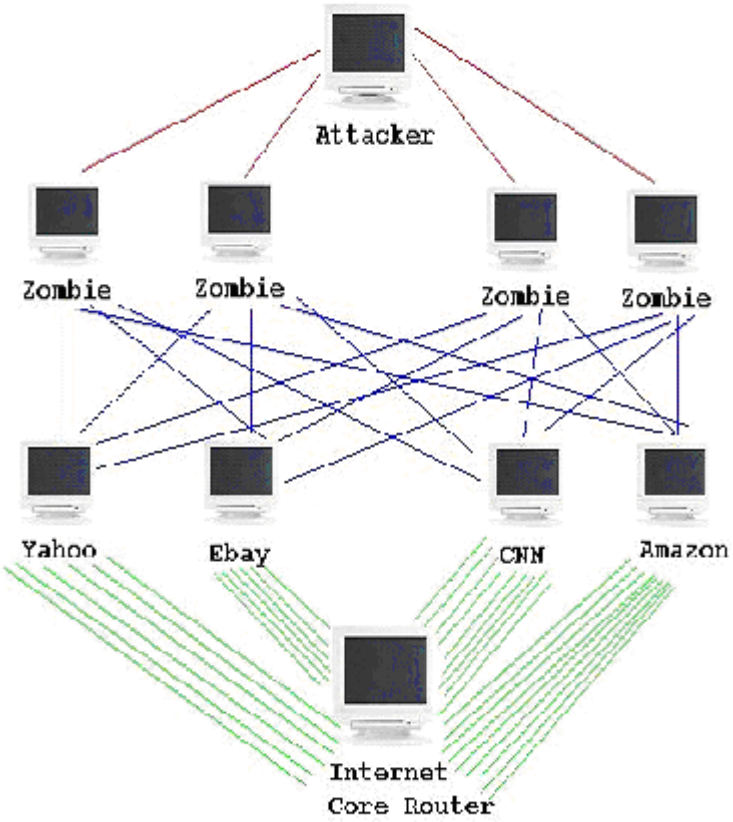
DOS Attack

CHAPTER-2

IP SPOOFING

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Newer routers and firewall arrangements can offer protection against IP spoofing.



IP SPOOFING

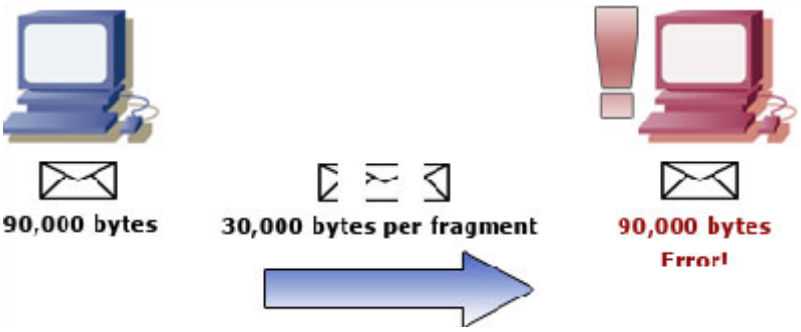
CHAPTER -3

TYPES OF DDOS ATTACK

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



Ping of Death

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

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. (This varies, but about 1k is a good bet).

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.

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:

_ _ _

– – –

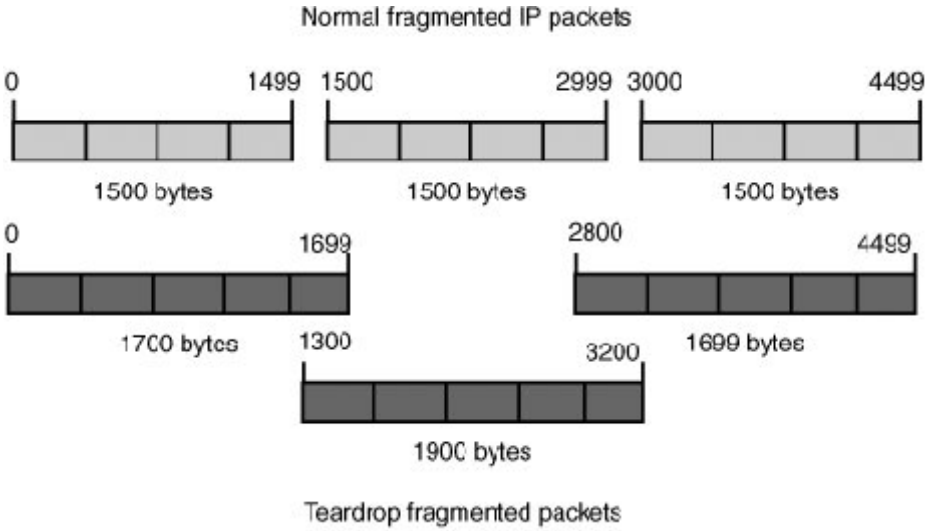
– – –

(1 to 1500 bytes)

(1500 to 3000 bytes)

(1001 to 3600 bytes)

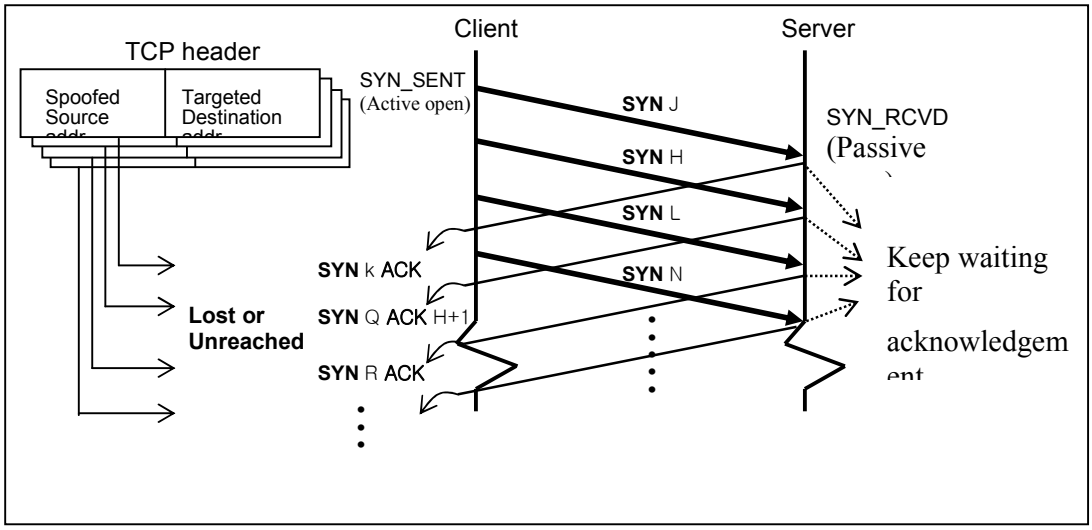
When the target system receives something like the above, it simply cannot handle it and will crash or hang or reboot.



Tear drop Attack

SYN Flooding Attack

The SYN attack exploits TCP/IP's three-way handshake. Thus, in order to understand as to how SYN Attacks works, you need to first know how TCP/IP establishes a connection between two systems. Whenever a client wants to establish a connection with a host, then three steps take place. These three steps are referred to as the three-way handshake. In a normal three way handshake, what happens is that, the client sends a SYN packet to the host, the host replies to this packet with a SYN ACK packet. Then the client responds with a ACK (Acknowledgement) packet. This will be clearer after the following depiction of these steps-:



SYN Flooding Attack

1. Client- - - - - - -SYN Packet----------à Host

   In the first step the client sends a SYN packet to the host, with whom it wants to establish a three-way connection.

   The SYN packet requests the remote system for a connection. It also contains the Initial Sequence Number or ISN of the client, which is needed by the host to put back the fragmented data in the correct sequence.

2. Host- - - - - - - - - - - -SYN/ACK Packet----------à Client
   In the second step, the host replies to the client with a SYN/ACK packet. This packet acknowledges the SYN packet sent by the client and sends the client its own ISN.
3. Clie n t- - - - - - - - - - - - - A C K----------à H o s t

In the last step the client acknowledges the SYN/ACK packet sent by the host by replying with a ACK packet. These three steps together are known as the 3-way handshake and only when they are completed is a complete TCP/IP connection established.

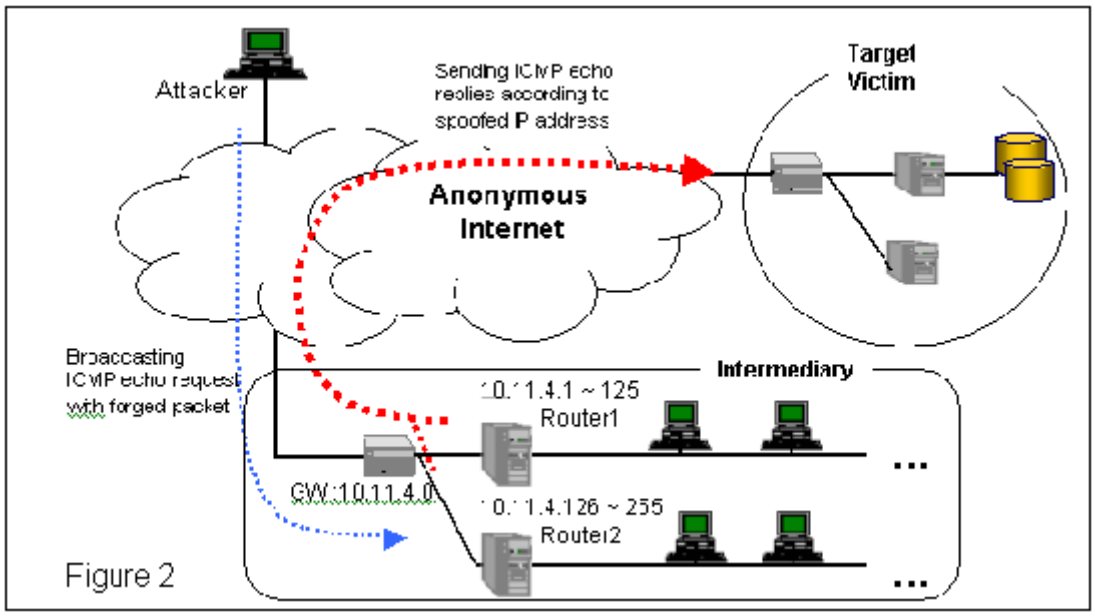
In a SYN attack, several SYN packets are sent to the server but all these SYN packets have a bad source IP Address. When the target system receives these SYN Packets with Bad IP Addresses (spoofed ip), it tries to respond to each one of them with a SYN ACK packet. But the reply goes to the spoofed ip not at all to the attacker ip. Now the target system waits for an ACK message to come from the bad IP address. However, as the bad IP does not actually exist, the target system never actually receives the ACK packet. It thus queues up all these requests until it receives an ACK message. The requests are not removed unless and until, the remote target system gets an ACK message. Thus in all cases only 2 steps is executed not the 3rd process at all. Hence these requests take up or occupy valuable resources of the target machine. To actually affect the target system, a large number of SYN bad IP packets have to be sent. As these packets have a Bad Source IP, they queue up, use up resources and memory or the target system and eventually crash, hang or reboot the system.

But since these spoofed ip might not exist and the hence the packets is likely to move through the network until its TTL values.

Land Attacks

A Land attack is similar to a SYN attack, the only difference being that instead of a bad IP Address, the IP address of the target system itself is used. This creates an infinite loop between the target system and the target system itself. However, almost all systems have filters or firewalls against such attacks.

Smurf Attacks



Smurf Attack

A Smurf attack is a sort of Brute Force DOS Attack, in which a huge number of Ping Requests are sent to a system (normally the router) in the Target Network, using Spoofed IP Addresses from within the target network. As and when the router gets a PING message, it will route it or echo it back, in turn flooding the Network with Packets, and jamming the traffic. If there are a large number of nodes, hosts etc in the Network, then it can easily clog the entire network and prevent any use of the services provided by it.

The two main components to the smurf denial-of-service attack are the use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses.

The Internet Control Message Protocol (ICMP) is used to handle errors and exchange control messages. ICMP can be used to determine if a machine on the Internet is responding. To do this, an ICMP echo request packet is sent to a machine. If a machine receives that packet, that machine will return an ICMP echo reply packet. A common implementation of this process is the "ping" command, which is included with many operating systems and network software packages. ICMP is used to convey status and error information including notification of network congestion and of other network transport problems. ICMP can also be a valuable tool in diagnosing host or network problems.

On IP networks, a packet can be directed to an individual machine or broadcast to an entire network. When a packet is sent to an IP broadcast address from a machine on the local network, that packet is delivered to all machines on that network. When a packet is sent to that IP broadcast address from a machine outside of the local network, it is broadcast to all machines on the target network (as long as routers are configured to pass along that traffic).

IP broadcast addresses are usually network addresses with the host portion of the address having all one bits. For example, the IP broadcast address for the network 10.0.0.0 is 10.255.255.255. If you have subnetted your class A network into 256 subnets, the IP broadcast address for the 10.50 subnet would be 10.50.255.255. Network addresses with all zeros in the host portion, such as 10.50.0.0, can also produce a broadcast response.

In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. There are three parties in these attacks: the attacker, the intermediary, and the victim (note that the intermediary can also be a victim).

The intermediary receives an ICMP echo request packet directed to the IP broadcast address of their network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, many of the machines on the network will receive this ICMP echo request packet and send an ICMP echo reply packet back. When (potentially) all the

machines on a network respond to this ICMP echo request, the result can be severe network congestion or outages.

When the attackers create these packets, they do not use the IP address of their own machine as the source address. Instead, they create forged packets that contain the spoofed source address of the attacker's intended victim. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. The victim is subjected to network congestion that could potentially make the network unusable. Even though we have not labeled the intermediary as a "victim," the intermediary can be victimized by suffering the same types of problem that the "victim" does in these attacks.

Attackers have developed automated tools that enable them to send these attacks to multiple intermediaries at the same time, causing all of the intermediaries to direct their responses to the same victim. Attackers have also developed tools to look for network routers that do not filter broadcast traffic and networks where multiple hosts respond. These networks can the subsequently be used as intermediaries in attacks.

Solution

Disable IP-directed broadcasts at your router.

One solution to prevent your site from being used as an intermediary in this attack is to disable IP-directed broadcasts at your router. By disabling these broadcasts, you configure your router to deny IP broadcast traffic onto your network from other networks. In almost all cases, IP-directed broadcast functionality is not needed.

This network management best practice is described in more detail in the following document authored by Daniel Senie of Amaranth Networks Inc.:

You should disable IP-directed broadcasts on all of your routers. It is not sufficient to disable IP-directed broadcasts only on the router(s) used for your external network connectivity. For example, if you have five routers connecting ten LANs at your site, you should turn off IP-directed broadcasts on all five routers.

1. **Configure your operating system to prevent the machine from responding to ICMP packets sent to IP broadcast addresses.**

   If an intruder compromises a machine on your network, the intruder may try to launch a smurf attack from your network using you as an intermediary. In this case, the intruder would use the compromised machine to send the ICMP echo request packet to the IP broadcast address of the local network. Since this traffic does not travel through a router to reach the machines on the local network, disabling IP-directed broadcasts on your routers is not sufficient to prevent this attack.

   Some operating systems can be configured to prevent the machine from responding to ICMP packets sent to IP broadcast addresses. Configuring machines so that they do not respond to these packets can prevent your machines from being used as intermediaries in this type of attack.

UDP Flooding

This kind of flooding is done against two target systems and can be used to stop the services offered by any of the two systems. Both of the target systems are connected to each other, one generating a series of characters for each packet received or in other words, requesting UDP character generating service while the other system, echoes all characters it receives. This creates an infinite non-stopping loop between the two systems, making them useless for any data exchange or service provision.

Loop back flooding attack

It is one of oldest type of dos attack.

CHAPTER-4

REAL LIFE EXAMPLES

Updates on the status of the Twitter service on Aug 6, 2009

Thursday August 6

Ongoing denial-of-service attack *1 year ago*

We are defending against a denial-of-service attack, and will update status again shortly.

Update: the site is back up, but we are continuing to defend against and recover from this attack.

Update (9:46a): As we recover, users will experience some longer load times and slowness. This includes timeouts to API clients. We're working to get back to 100% as quickly as we can.

Update (4:14p): Site latency has continued to improve, however some web requests continue to fail. This means that some people may be unable to post or follow from the website.

Other examples are following

- The first major attack involving DNS servers as reflectors occurred in January 2001. The target was Register.com. This attack, which forged requests for the MX records of AOL.com (to amplify the attack) lasted about a week before it could be traced back to all attacking hosts and shut off. It used a list of tens of thousands of DNS records that were a year old at the time of the attack.

- In February, 2001, the Irish Government's Department of Finance server was hit by a denial of service attack carried out as part of a student campaign from NUI Maynooth. The Department officially complained to the University authorities and a number of students were disciplined.

- In July 2002, the Honeynet Project Reverse Challenge was issued. The binary that was analyzed turned out to be yet another DDoS agent, which implemented several DNS related attacks, including an optimized form of a reflection attack.

- On two occasions to date, attackers have performed DNS Backbone DDoS Attacks on the DNS root servers. Since these machines are intended to provide service to all Internet users, these two denial of service attacks might be classified as attempts to take down the entire Internet, though it is unclear what the attackers' true motivations were. The first occurred in October 2002 and disrupted service at 9 of the 13 root servers. The second occurred in February 2007 and caused disruptions at two of the root servers.

- In February 2007, more than 10,000 online game servers in games such as Return to Castle Wolfenstein, Halo, Counter-Strike and many others were attacked by the hacker group RUS. The DDoS attack was made from more than a thousand computer units located in the republics of the former Soviet Union, mostly from Russia, Uzbekistan and Belarus. Minor attacks are still continuing to be made today.

- In the weeks leading up to the five-day 2008 South Ossetia war, a DDoS attack directed at Georgian government sites containing the message: "win+love+in+Rusia" effectively overloaded and shut down multiple Georgian servers. Websites targeted included the Web site of the Georgian president, Mikhail Saakashvili, rendered inoperable for 24 hours, and the National Bank of Georgia. While heavy suspicion was placed on Russia for orchestrating the attack through a proxy, the St. Petersburg-based criminal gang known as the Russian Business Network, or R.B.N, the Russian government denied the allegations, stating that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.

- During the 2009 Iranian election protests, foreign activists seeking to help the opposition engaged in DDoS attacks against Iran's government. The official website of the Iranian government (ahmedinejad.ir) was rendered inaccessible on several occasions. Critics claimed that the DDoS attacks also cut off internet access for protesters inside Iran; activists countered that, while this may have been true, the

attacks still hindered President Mahmoud Ahmadinejad's government enough to aid the opposition.

- On June 25, 2009, the day Michael Jackson died, the spike in searches related to Michael Jackson was so big that Google News initially mistook it for an automated attack. As a result, for about 25 minutes, when some people searched Google News they saw a "We're sorry" page before finding the articles they were looking for.

- June 2009 the P2P site The Pirate Bay was rendered inaccessible due to a DDoS attack. This was most likely provoked by the recent sellout to Global Gaming Factory X AB, which was seen as a "take the money and run" solution to the website's legal issues. In the end, due to the buyers' financial troubles, the site was not sold.

- Multiple waves of July 2009 cyber attacks targeted a number of major websites in South Korea and the United States. The attacker used botnet and file update through internet is known to assist its spread. As it turns out, a computer trojan was coded to scan for existing MyDoom bots. MyDoom was a worm in 2004, and in July around 20,000-50,000 were present. MyDoom has a backdoor, which the DDoS bot could exploit. Since then, the DDoS bot removed itself, and completely formatted the hard drives. Most of the bots originated from China, and North Korea.

- On August 6, 2009 several social networking sites, including Twitter, Facebook, Livejournal, and Google blogging pages were hit by DDoS attacks, apparently aimed at Georgian blogger "Cyxymu". Although Google came through with only minor set-backs, these attacks left Twitter crippled for hours and Facebook did eventually restore service although some users still experienced trouble. Twitter's Site latency has continued to improve, however some web requests continue to fail.

- In July and August, 2010, the Irish Central Applications Office server was hit by a denial of service attack on four separate occasions, causing difficulties for thousands of Second Level students who are required to use the CAO to apply for University and College places. The attack is currently subject to a Garda investigation.