Information Systems Security Training
DoS Attacks: Instigation and Mitigation

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+
info@infosecprofessionals.com

During the release of a new software product specialized to track spam, ACME Software Inc notice that there was not as much traffic as they hoped to receive. During further investigation, they found that they could not view their own website. At that moment, the VP of sales received a call from the company's broker stating that ACME Software Inc stock fell 4 point due to lack of confidence. Several states away, spammers didn't like the idea of lower profit margins do to an easy to install spam blocking software so they thought they would fight back. Earlier that day, they took control of hundreds of compromised computers and used them as DoS zombies to attack ACME Software Inc's Internet servers in a vicious act of cyber assault. During an emergency press conference the next morning, ACME Software Inc's CIO announced his resignation as a result of a several million dollar corporate loss.

Scenarios like the one above happen a more then people think and are more costly then most will admit. Denial of Service (DoS) attacks are designed to deplete the resources of a target computer system in an attempt to take a node off line by crashing or overloading it. Distributed Denial of Service (DDoS) is a DoS attack that is engaged by many different locations. The most common DDoS attacks are instigated through viruses or zombie machines. There are many reasons that DoS attacks are executed, and most of them are out of malicious intent. DoS attacks are almost impossible to prevent if you are singled out as a target. It's difficult to distinguish the difference between a legitimate packet and one used for a DoS attack.

The purpose of this article is to give the reader with basic network knowledge a better understanding of the challenges presented by *Denial of Service* attacks, how they work, and ways to protect systems and networks from them.

The attendee should have a basic knowledge of computers systems, networking, and familiarity with the Microsoft Windows platforms. Programming knowledge is helpful.

***

Instigation

Spoofing – Falsifying an Internet address (know as spoofing) is the method an attacker uses to fake an IP address. This is used to reroute traffic to a target network node or used to deceive a server into identifying the attacker as a legitimate node. When most of us think of this approach of hacking, we think of someone in another city essentially becoming you. The way TCP/IP is designed, the only way a criminal hacker or cracker can take over your Internet identity in this fashion is to blind spoof. This means that the impostor knows exactly what responses to send to a port, but will not get the corresponding response since the traffic is routed to the original system. If the spoofing is designed around a DoS attack, the internal address becomes the victim. Spoofing is used in most of the well-known DoS attacks. Many attackers will start a DoS attack to drop a node from the network so they can take over the IP address of that device. IP Hijacking is the main method used when attacking a secured network or attempting other attacks like the *Man in the Middle* attack.

SYN Flood - Attackers send a series of SYN requests to a target (victim). The target sends a SYN ACK in response and waits for an ACK to come back to complete the session set up. Instead of responding with an ACK, the attacker responds with another SYN to open up a new connection. This causes the connection queues and memory buffer to fill up, thereby denying service to legitimate TCP users. At this time, the attacker can hijack the system's IP address if that is the end goal. Spoofing the "source" IP address when sending a SYN flood will not only cover the offender's tracks, but is also a method of attack in itself. SYN Floods are the most commonly used DoS in viruses and are easy to write. See http://www.infosecprofessionals.com/code/synflood.c.txt

Smurf Attack- Smurf and Fraggle attacks are the easiest to prevent. A perpetrator sends a large number of ICMP echo (ping) traffic at IP broadcast addresses, using a fake source address. The "source" or spoofed address will be flooded with simultaneous replies (See CERT Advisory: CA-1998-01). This can be prevented by simply blocking broadcast traffic from remote network sources using access control lists.

Fraggle Attack – This types of attack is the same as a Smurf attack except using UDP instead if TCP. By sending an UDP echo (ping) traffic to IP broadcast addresses, the systems on the network will all respond to the spoofed address and affect the target system. This is a simple rewrite of the Smurf code. This can be prevented by simply blocking broadcast traffic from remote IP address.

Ping of Death - An attacker sends illegitimate ICMP (ping) packets larger than 65,536 bytes to a system with the intention of crashing it. These attacks have been outdated since the days of NT4 and Win95.

Teardrop - Otherwise known as an IP fragmentation attack, this DoS attack targets systems that are running Windows NT 4.0, Win95 , Linux up to 2.0.32. Like the Ping of Death, the Teardrop is no longer effective.

Application Attack **-** Thess are DoS attacks that involve exploiting an application vulnerability causing the target program to crash or restart the system.

Kazaa and Morpheus have a known flaw that will allow an attacker to consume all available bandwidth without being logged.
See http://www.infosecprofessionals.com/code/kazaa.pl.txt

Microsoft's IIS 5 SSL also has an easy way to exploit vulnerability. Most exploits like these are easy to find on the Internet and can be copied and pasted as working code. There are thousands of exploits that can be used to DoS a target system/application. *See http://www.infosecprofessionals.com/code/IIS5SSL.c.txt*

Viruses, Worms, and Antivirus **–** Yes, Antivirus. Too many cases where the antivirus configuration is wrong or the wrong edition is installed. This lack of foresight causes an unintentional DDoS attack on the network by taking up valuable CPU resources and bandwidth. Viruses and worms also cause DDoS attacks by the nature of how they spread. Some purposefully attack an individual target after a system has been infected. The Blaster worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135 is a great example of this. The Blaster targeted Microsoft's windows update site by initiating a SYN FLOOD. Because of this, Microsoft decided to no longer resolve the DNS for 'windowsupdate.com'.

DoS attacks are impossible to stop. However, there are things you can do to mitigate potential damages they may cause to your environment. The main thing to remember is that you always need to keep up-to-date on the newest threats.

Mitigation

Antivirus software – Installing an antivirus software with the latest virus definitions will help prevent your system from becoming a DoS zombie. Now, more then ever, this is an important feature that you must have. With lawsuits so prevalent, not having the proper protection can leave you open for downstream liability.

Software updates **-** Keep your software up to date at all times. This includes antivirus, email clients, and network servers. You also need to keep all network Operating Systems installed with the latest security patches. Microsoft has done a great job with making these patches available for their Windows distributions. Linux has been said to be more secure, but the patches are far more scarce. RedHat is planning on incorporating the NSA's SE Linux kernel into future releases. This will give Mandatory Access Control (MAC) capabilities to the Linux community.

Network protection - Using a combination of firewalls and Intrusion Detection Systems (IDS) can cut down on suspicious traffic and can make the difference between logged annoyance and your job. Firewalls should be set to deny all traffic that is not specifically designed to pass through. Integrating an IDS will warn you when strange traffic is present on your network. This will assist you in finding and stopping attacks.

Network device configuration – Configuring perimeter devices like routers can detect and in some cases prevent DoS attacks. Cisco routers can be configured to actively prevent SYN attacks starting in Cisco IOS 11.3 and higher using the TCP intercept command in global configuration mode.

access-list number {deny | permit} tcp any destination destination-wildcard
ip tcp intercept list access-list-number
*ip tcp intercept ? (*will give you a good list of other options.)

Cisco routers can prevent Smurf and Fraggle attacks by blocking broadcast traffic. Since Cisco IOS 12.0, this is the default configuration. ACLs or access control lists should also be configured on all interfaces.

no ip directed-broadcast

The Cisco router can also be used to prevent IP spoofing.

ip access-group list in interface
access-list number deny icmp any any redirect
access-list number deny ip 127.0.0.0 0.255.255.255 any
access-list number deny ip 224.0.0.0 31.255.255.255 any
access-list number deny ip host 0.0.0.0 any
See Improving Security on Cisco Routers - www.cisco.com/warp/public/707/21.html

Old Cisco IOS versions are vulnerable to several DoS attacks. The "*Black Angels*" wrote a program called *Cisco Global Exploite*r. This is a great software to use when testing the security of your Cisco router version and configuration and can be found at http://www.blackangels.it/Projects/cge.htm

Security is not as mystical as people believe. DoS attacks come in many different types and can be devastating if you don't take the proper precautions. Keep up to date and take steps to secure network nodes. Keeping security in mind can minimize damages, downtime, and save your career.

Resources

Security Resources

Black Angels: http://www.blackangels.it/
Cisco: http://www.cisco.com
Microsoft: http://www.microsoft.com/technet/security/current.aspx
Forum of Incident Response and Security Teams: http://www.first.org/
SANS Institute: http://www.sans.org/resources/