Global Information Assurance Certification Paper

Limiting Exposure to Denial of Service Attacks
Heather Alberts
GSEC Practical Assignment, Version 1.4b, Option 1
July 1, 2003

Abstract

Denial of Service (DoS) attacks are attacks against computer systems connected to the internet that block authorized or legitimate access to system's resources or causes a delay in the system's everyday functions. An example of one of the most common denials of service attacks is sending so much traffic (flooding) to a web site that it gets overwhelmed and in turn hinders or disrupts service to the site. In a denial of service attack, the traffic originates from one system and is fairly easy to block by programming the router or firewall to block traffic coming from that single IP address. A distributed denial of service attack (DDoS) uses the same types of attacks as denial of service but is initiated by multiple compromised systems from all over the internet, called zombies. Because this attack is coming from all over the internet, it is much more difficult to stop.

The above example is just one of many types of denial of service of attacks that an attacker might attempt. This paper is oriented to the system administrator of a network to give them general information about denial of service attacks and how to limit the exposure to their network. I will explain the history of denial of service attacks along with some different types of attacks. Next, I will describe some popular tools attackers use and some best practices to use against denial of service attacks. Lastly, I will go into possible legal implications of these attacks.

Introduction

Denials of service attacks are not a new idea and have been around for many years and they weren't always dealing with computers on the internet. On February 1, 1960, four African American college students sat down at the Woolworth's white-only lunch counter asking for service.[1] When asked to leave, the four refused and continued to sit at the counter. Protestors continued the sit-in for 6 months. While these students sat at the lunch counter, they were denying the service of the white patrons wanting lunch.

One of the earliest computer based attacks was in 1988 when Robert T. Morris, Jr., a graduate student from Cornell, wrote a program (worm) that took down most of the internet for two days. A bug in his program caused the worm to be more damaging resulting in victims being infected more than once.

[1] Yeingst, William

In February of 2000, some high profile company's web sites were attacked. Yahoo Inc., Buy.com Inc., eBay Inc., Amazon.com Inc., CNN.com were all victims of a distributed denial of service attack. Some of them lost a considerable amount of money while the sites were down for hours.

A denial of service attack using the flooding technique had caused seven of the thirteen DNS root-name servers in October of 2002 to be unavailable for an hour. These servers are what run domain name services for the internet. This attack was not known to the ordinary user of the internet because their DNS information is cached locally. If this had continued much longer, it could have posed a problem for the entire internet.

Recently, denial of service attacks have been the cause of some web sites being blocked. The SCO Group's web site was taken down for several hours in May of 2003. Al Jazeera, an Arabic news site, was bombarded with a distributed denial of service attack in March.

There is also a worm propagating around Asia and the United States that some experts think could be used for a distributed denial of service attack.[2] The worm, WORM_DELODER.A, leaves two Trojan horse programs on the infected machines. One of them allows an attacker to gain graphical control of the victim machine. What makes this worm dangerous is that it doesn't require any human interaction to spread.

These are just a few of the more well known denial of service attacks that have gained media attention. Most attacks don't get published because the company doesn't want the public to know they were comprised. A study done by researchers at the University of California, San Diego (UCSD) shows that the number of attacks is much larger than people think. During the three week period of the study, they observed 12,000 attacks against more than 5,000 distinct targets.[3]

Specific Types of Denial of Service Attacks

From simple attacks such as a Ping of Death to a more sophisticated as a distributed denial of service attack, there are many types of Denial of service attacks. The following are a few examples:

Smurf Attack

The Smurf Attack is carried out by sending an Internet Control Message Protocol (ICMP) echo request packet to a network with an open broadcast address. The broadcast address is used when a system wants to send information to all hosts on the same network. An attacker will start by sending an echo request from a

[2] Gray, Patrick
[3] Moore, David

spoofed IP address of a victim to an open broadcast address of a network. Spoofing is sending a packet with someone else's return address. All machines on the network will receive this packet. This could cause the systems to send an echo reply to the spoofed IP address, therefore clogging the victim's network with ICMP traffic. Fraggle is another example of an attack and works the same way as Smurf but uses User Datagram Protocol (UDP) echo request and reply packets.

TCP/IP SYN Flood Attack

TCP/IP uses a three-way handshake to establish a communication link. For example: Computer A wants to communicate with a server, so it sends an SYN packet to Server B. Server B acknowledges with a SYN-ACK packet back to Computer A. Then Computer A completes the handshake with a SYN packet. The SYN-ACK or TCP-SYN Flooding uses part of this process for the attack. If the original SYN packet that starts the handshake had a fake return IP address that was unreachable, Server B would try to send the acknowledgement to the spoofed IP address but would never make it to the destination. Server B will store large numbers of acknowledgement packets in it's queue. With it's queue flooded with packets that don't get acknowledged, Server B can't establish links with other systems.

Teardrop Attack

IP specifications allow packets to disassemble into fragments as they are sent across a network if the destination system is unable to receive large packets. IP will reassemble these packet fragments as they arrive at their destination. An offset field in the fragments allows IP to reassemble the packet in the proper sequence. The Teardrop Attack will send fragments with overlapping or confusing offset fields. With these offset fields, IP can not reassemble the packets, disabling the system and possibly causing the system to crash or reboot.

Ping of Death

A flaw in some implementations of TCP/IP allows the possibility to send packets that exceed the maximum 65,536 bytes of data.[4] The Ping of Death attack exploits this bug by sending packets that exceed this maximum packet size causing the targeted victim to crash or reboot. Ping of Death attack one of the earliest denial of service attacks and most operating system vendors have since addressed this particular bug.

UDP Attack

The UDP Flood Attack creates fake UPD connections between two systems. By connecting to a host's chargen service to the echo service on the same or another machine, all affected machines may be effectively taken out of service because of the excessively high number of packets produced.[5] Chargen, short

[4] Extreme Networks

[5] CERT Coordination Center

for character generator, is a service that is used to generate a stream of characters for testing purposes.

Distributed Denial of Service Attacks

Distributed denial of service attacks (DDoS) will use the same types of attacks as the above examples, but uses multiple sources to attack an unsuspecting system. An attacker will gain access to a host, called an agent or zombie, and install software that places services or daemons on the host systems. These agents will wait until a specific date, time or command from an attacker or master system to run a denial of service attack on a victim. A single denial of service attack, such as the types indicated above, may not overwhelm a system or network but if the attack is orchestrated from multiple sources, the system is likely to crash or the network will become unavailable to other users.

Distributed denials of service attacks have become prevalent in IRC networks. IRC, internet relay chat, is a system that allows users to meet in 'rooms' to talk about certain topics. The users install a client, or bot, on their systems that connects to an IRC server. This server could be connected to other servers which could be connected to hundreds of clients. An IRC Botnet is a network of these clients that have been comprised by attackers. Officials at the CERT Coordination Center have been aware of several large botnets, one of which contained more than 140,000 computers.[6]

Attack Tools

There are several attack tools available to attackers on the internet. One doesn't have to be a very experience attacker to use some of these tools; many have been automated to allow for easy implementation. Some distributed denial of service tools running on compromised systems will forge the IP address and sometimes randomly change the addresses, which makes it difficult to trace. Some of the more popular tools that are being used for denial of service attacks are TFN, TFN2K, Trinoo, and Stacheldraht. Attackers use these tools to create a network of comprised systems to use for a denial of service attack.

The Tribe Flood Network or TFN and TFN2K are two different versions of one tool. The attacks available in these tools are SYNflood, PingFlood, UDP bomb and Smurf attacks. They both are able to spoof packets. The TFN2K version has more tools available to it as well as the ability to encrypt the traffic between server and agent. Both networks are made up of a client application on a server and daemons running on agents. An attacker has command line control of a client of which has control of many daemons that run the distributed denial of service attack. Communications between server and agent in the TFN network

[6] Fisher, Dennis

uses ICMP ECHO and ICMP ECHO REPLY. The TFN2K network uses a combination of UDP, ICMP and TCP which are supplied at run time or can be chosen randomly by the program.[7]

The Trinoo is also used for DDoS attacks. Trinoo coordinates a small number of masters and a large number a clients to initiate an attack. A attacker will send a packet on port 27665 to a master, who then sends a UDP packet to the clients using port 27444. The clients then run a "broadcast" program that sends a UDP Flood to a victim. Communication between attacker, masters and clients by default use ports 1524 tcp, 27665 tcp, 27444 udp and 31335 udp. These are default ports for the tools, ports can be changed.

Stacheldraht has the same attacks as TFN, but adds encrypted master/client communications. In addition, the agents are able to download and install newer versions of the agent program. Communication between clients and agents are by default using ports 16660 tcp, 65000 tcp, ICMP ECHO and ICMP ECHO REPLY. These are default ports for the tools, ports can be changed.

Best Practices to limit exposure of DoS attacks

It's not as simply as implementing a firewall to defend against denial of service attacks by stopping certain packets entering your network. You must take a defense in depth approach to defend against these attacks. Your defense should begin at the point where your network connects to the internet and continue all the way down to the PCs, implementing an Incident Response Team and insisting that your security personnel stay current with security issues.

Following certain preventive measures should limit your exposure to denial of service attacks on your network.

Your first line of defense against denial of service attacks should be to implement a good firewall. The firewall should be kept up-to-date with all the latest security patches and be as secure as possible. Follow the recommended hardening steps for your hardware; many of which are found on the internet. Block inbound packets that don't go to permitted ports.

You should turn logging on your routers. Router logging will track down where the attack is coming from and help you give your ISP specific information so they can filter traffic. Another step to take with your routers is to implement ingress filtering. Ingress filtering is the filtering of packets coming from the internet. It is recommended that all private and reserved addresses not be allowed to enter your router.[8] Here is a table of those addresses:

[7] Cisco Systems
[8] SANS Institute

0.0.0.0/8	Historical Broadcast
10.0.0.0/8	RFC 1918 Private Network
127.0.0.0/8	Loopback
169.254.0.0/16	Link Local Networks
172.16.0.0/12	RFC 1918 Private Network
192.0.2.0/24	TEST-NET
192.168.0.0/16	RFC 1918 Private Network
224.0.0.0/4	Class D Multicast
240.0.0.0/5	Class E Reserved
248.0.0.0/5	Unallocated
255.255.255.255/32	Broadcast

While you should never allow packets from the IP addresses above, you should also take into effect the type of traffic. Start by blocking all traffic coming from the internet and then determine what really needs to cross your firewall.

Implement an intrusion detection system (IDS) on your network. An IDS system watches the network traffic and will notify you if there is something out of the ordinary. This is called network-based IDS, but implementing host-based IDS on your essential systems (email, web, DNS) is also recommended. Most IDS systems can be setup to notify someone on an Incident Response Team if it sees something not normal.

Running scanners/tools on your network can help you find if there are any denial of service applications on your systems. Scanners can examine the network for vulnerabilities and some can tell you how to fix them. They look for backdoors and denial of service agents. One such security scanner is called Nessus. Nessus will scan your systems for problems such as default accounts, SMTP problems, useless services and many more. Tripwire is another tool that system administrators should consider running on the network. Tripwire will alert you to a possible comprise of a system by examining changes in configurations.

You may also want to think about installing a product to aid in the detection and prevention of denial of service attacks on your network. These products can be installed between your firewall and the internet, between your firewall and internal network or be used as a scanner and watches the traffic. There are many products available. Network World Fusion has done an extensive test on seven of these types of products. The study found that the seven products worked the same in detecting attacks, most of them detecting 95% of the attacks that were launched. [9]

The PCs and servers on your network should be running the latest anti-virus

[9] Andress, Mandy

software and virus definitions. Think of implementing a centralized virus server that 'pushes' the latest updates to the PCs and servers. Keep browsers, operating systems and products on PCs up-to-date and with the latest security patches. Secure your servers by making sure they are up-to-date with the latest patches and unnecessary services are stopped. You should only have the necessary services running on servers – don't have SMTP running on your web server for example. Some services have bugs that can be exploited and if those services are not running then they can't be comprised.

An Incident Response Team should be established to handle incidents, such as a denial of service attack. Defining an Incident Handling Plan and defining who will be on the Team will make it easier to manage a denial of service attack on your system or network. Your plan should include procedures and policies to follow when a denial of service attack occurs. If you have a plan and team in place, there is no question who or what has to get done to stop the denial of service attack.

And lastly, stay current on security issues by joining mail lists such as CERT Advisory Mailing list (http://www.cert.org/contact_cert/certmaillist.html) and Bugtraq (http://www.securityfocus.com/archive/1). You should also frequently visit the web pages of your operating systems, routers and firewalls for new updates and security patches.

Protect Others from You

"Security is not just protecting yourself from others, you must protect others from yourself"[10]

One of the ways to prevent attacks from leaving your network is to implement egress filtering on your border routers or firewalls. Egress filtering is much like ingress filtering but going in the opposite direction - the checking of packets leaving your network. Use the same table of IP addresses used in implementing ingress filtering to prevent packets from IP addresses that aren't on the internal subnet to leave your network. If the address originates from inside the network, the packet is forwarded. Not only should you not allow traffic from spoofed IP addresses, but you should also look at the type of traffic leaving the network. Let us assume that one of your servers or PCs did in fact get compromised. You want to make that the system doesn't participate in an attack. By allowing only legitimate traffic out your firewall, you can stop the attacks from leaving your network and saving someone else's network.

Another way to protect others from your systems is to not be a broadcast amplifier network. Configure servers, routers and PCs so they don't receive or

[10] Hatch, Brian

forward directed broadcast traffic. At the very least make sure your border router has this disabled.

You can test your network to see if you are acting as a broadcast amplifier network by using the ping utility on the outside. From a system on the internet side of your router, ping your network's broadcast address, x.x.x.255 for a class C, and the base IP address, x.x.x.0 for a class C. If you receive ping replies from the same number of systems behind your firewall, your network is acting as an amplification network. If this is the case, you need to check with your router vendor and disable directed broadcast. Most vendors currently ship equipment with directed broadcast disabled by default which is specified in RFC 2644.

Legal Implications

Not only are attackers liable (if they can be caught) by launching denial of service attacks, but companies that don't put into place preventive measures to protect others from them, could be liable in the future. A consortium established in 2000 would like to do just that. The RFC 2267-plus Working Group, named after the RFC 2267, would like to develop a body of accepted safe practices that companies would have to comply with or risk liability if their computers are comprised and carry out a distributed denial of service attacks.[11]

Organizations that suffer from a loss of money or productivity may go looking for responsible parties to recoup the costs.

There has also been an organization created earlier this year to bring a lawsuit against router and operating system vendors. The ddos-ca.org group wants vendors to change the default settings on hardware and software to safe or benign settings. The current default settings are widely known and unfortunately sometimes the people that install the equipment forget to change these settings allowing access by anyone, including attackers.

Conclusion

Denial of service attacks can range from exploiting a software bug to consuming server memory to cause a crash, to flooding traffic to tie up a web server. All this can lead to companies loosing a great deal of time and money.

It's not just the system administrators of companies that have to worry about denial of service attacks. While attackers might not want to bother with attacking a small home user, there is the possibility that the user's system could become one of many systems used in a distributed denial of service attack.

---

[11] Greene, Tim

With cable modems and DSL connections, more home users are establishing permanent connections to the internet. With this connection, comes needed security and most home users don't take or don't know how to take the added precaution to protect their systems.

System administrators should take a proactive approach to stop the denial of service attacks. While networks, PCs and servers remain unprotected and unpatched there will always be the possibility denial of service attacks. Within this paper I have described some denial of service attacks and listed some approaches to try and limit your exposure to such attacks. You could be saving yourself a headache, money loss or liability.

Additional Resources

Below is a list of additional resources that will be beneficial in your fight against denial of service attacks:

CERT Coordination Center is a research and development center on internet security - http://www.cert.org/nav/index_main.html

Denial of service tools used by hackers - http://packetstormsecurity.nl/distributed/

Cisco Strategies - http://www.cisco.com/warp/public/707/newsflash.html

Cisco ACL and Tracing DoS - http://www.cisco.com/warp/public/707/22.html

Dave Dittrich DDoS page - http://staff.washington.edu/dittrich/misc/ddos/

References

Andress, Mandy. “Denial of service: Fighting back”. Network World. September 2, 2002. http://www.nwfusion.com/reviews/2002/0902rev.html (May 8, 2003)

CERT Coordination Center. Denial of Service Attacks. June 4, 2001. http://www.cert.org/tech_tips/denial_of_service.html (May 8, 2003)

Chapple, Mike. “Egress filtering”. SearchSecurity.com March 4, 2003. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci883409,00.html (May 9, 2003)

CIAC. Computer Incident Advisory Capability. U.S. Department of Energy. K-032: DDoS Mediation Action List. April 3, 2000 http://www.ciac.org/ciac/bulletins/k-032.shtml (May 9, 2003)

Cisco Systems. “Strategies to Protect Against Distributed Denial of Service(DDoS) Attacks”. April 29, 2003. http://www.cisco.com/warp/public/707/newsflash.html (May 9, 2003)

Extreme Networks. “Security on IP Networks. Countering Denial of Service (DoS) Attacks”. http://www.extremenetworks.com/libraries/whitepapers/technology/Security_WP.pdf (May 8, 2003)

Fisher, Dennis. “Thwarting the Zombies”. EWeek.com March 31, 2003. http://www.eweek.com/print_article/0,3668,a=39472,00.asp (June 27, 2003)

Gray, Patrick. “Al-Jazeera Web site suffers denial of service attack”. March 27, 2003. http://zdnet.com.com/2100-1105-994357.html (May 9, 2003)

Gray, Patrick. “Deloder worm threaten DDos attack”. March 10, 2003. http://zdnet.com.com/2100-1105-991712.html (May 9, 2003)

Greene, Tim. “Forum warns of hidden DDoS legal liability”. Network World. October 2, 2000. http://www.nwfusion.com/archive/2000/108677_10-02-2000.html (May 8, 2003)

HackWatch. “DoS Attacks Cripple Yaho, CNN, Amazon and Buy.com”. February 9, 2000. http://www.hackwatch.com/~kooltek/dosattacks.html (May 8, 2003)

Hatch, Brian. “Egress filtering for a healthier Internet”. 2003. http://lwn.net/Articles/23148 (May 9, 2003)

Infosyssec. “Denial of Service Attacks – DDOS, SMURF, FRAGGLE, TRINOO.” 1998-2000. http://www.infosyssec.com/infosyssec/secdos1.htm (May 8, 2003)

Internet Security Systems. Denial of Service FAQ. http://www.iss.net/news/denialfaq.php (May 9, 2003)

Mockapetris, Paul. ZDNet. “Keeping ahead of DNS attacks.” January 8, 2003. http://zdnet.com.com/2100-1107-979650.html (May 8, 2003)

Moore, David. Voelker, Geoffrey M. Savage, Stefan. “Inferring Internet Denial-of-Service Activity”. 2001. http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf (July 9, 2003)

The SANS Institute. “Help Defeat Denial of Service Attacks: Step-by-Step”. March 3, 2000. http://www.sans.org/dosstep/index.php (May 9, 2003)

Shankland, Stephan. “SCO Web site slammed by Net Attack” May 5, 2003. http://zdnet.com.com/2102-1105_2-999584.html (May 9, 2003)

Yeingst, William. Bunch, Lonnie. “Sitting For Justice”. http://www.si.edu/i+d/sitins.arc.html (July 15, 2003)