IBM Global Services

Denial-of-Service attacks: Understanding network vulnerabilities.

Key Topics

Placing risk in the proper context

Defining Denial-of-Service methods and remedies

Defending against Distributed Denial-of-Service attacks

Understanding basic Denial-of-Service response methods

Looking to the future: The likelihood of more sophisticated attacks

Introduction

By adopting and employing stable, forward-looking strategies for avoiding and circumventing site intrusions and the resulting disruptions, executives and practitioners can bolster their company's defenses against attacks like those recently highlighted in the media. These incidents, as unfortunate as they may be, emphasize what will soon become a common refrain: Security on the Web requires teamwork and attentiveness by all members of the Internet community.

Denial-of-Service (DoS) attacks is a phenomenon that has recently plagued a number of well-known online companies. This paper will explore DoS attack methods; best practices for implementing sound strategies for risk management; and how best to equip systems and people to recognize and respond to attacks should they occur.

e-business

Placing risk in the proper context

There is no longer any question that the Internet is revolutionizing the way companies communicate and conduct business. Its remarkable growth is already translating into significant business rewards — financial and otherwise — especially for those who are first to implement. At the same time, with every opportunity comes a measure of risk.

By nature, the Web is public, distributed, connected and highly dynamic — subject to phenomenal growth in terms of infrastructure, the number of people online — as well as the sheer volume and types of applications running across and beyond today's complex corporate environments. Security threats and attacks can often be traced to hackers, who enjoy the thrill of pushing security boundaries, pointing out companies' security weaknesses and winning the respect of their peers. These traits are fostering a new generation of skilled hackers armed with sophisticated tools designed to attack the weakest link in a network. DoS attacks point out the heavy price that companies can pay when security is lacking, and underscore the vulnerabilities of the weakest link in a given entity.

Network environments are complicated. Security solutions are most effective when they can be customized to a specific installation. Unfortunately, a high percentage of individuals involved in building and maintaining Web sites and infrastructures for these environments have little knowledge of security protocols. As a result, many of today's Web hosting systems and networks are vulnerable to break-ins and disruptions.

Still, learning to build and maintain secure Web sites is only one piece of the security puzzle. Security gaps must be detected, new technologies implemented, and tools and best practices developed for minimizing risk and avoiding the repercussions of service interruptions — or worse. That said, it is important to note that creating a secure posture for e-business is not a single effort; it is an ongoing *process*. The effort takes time, and must be continually refined to become an integral part of standard business operations. Security approaches that take a holistic view of hardware, software, services and networks have the best chance of succeeding.

To help ensure and manage Internet security, you can begin by following three fundamental guidelines:

- Understand your dependencies on the Internet
- Maintain constant awareness of the status and nature of those dependencies
- Be prepared to react quickly yet thoughtfully to changes in the environment.

Remember, successful online businesses all share a distinguishing characteristic: awareness and effective management of security risks. Although security gaps will continue to emerge, enterprises can mitigate risk by exercising diligence and implementing proactive processes.

DoS attacks: What are they?

When DoS attacks occur, the hacker's objective is to render target systems inaccessible by legitimate users. During a recent spate of incidents, hackers effectively flooded the companies' Web servers and communication links—temporarily halting access.

Fortunately, this type of attack does not threaten credit card information or other corporate data stored on host systems, which could otherwise be vulnerable to viewing, tampering or theft. Nevertheless, DoS occurrences can pose serious problems for companies whose very business depends on their ability to service customers on the Web. For these organizations, downtime constitutes a closed store; customers can shift their allegiance with the click of a mouse.

The nature of DoS attacks can vary—from the more publicized incidents that can be remedied with operating system fixes, to very sophisticated violations that are more difficult to detect and avoid. The following section provides a summary of the types and nature of DoS attacks, as well as their remedies.

DoS attack methods and remedies

Numerous DoS attack methods have been documented. Attacks that directly target host systems can most often be checked with operating system patches. It is much more difficult, however, to defend against attacks that flood networks with data packets.

Network flooding attacks can be categorized as “Smurf,” “TCP SYN,” “UDP,” “TCP” and combinations thereof.

- **Smurf**

  During a Smurf[1] attack, the hacker floods the network with Internet Control Message Protocol (ICMP) ping response messages. Ping is the simplest kind of activity you can have on the Internet, and is routinely employed by hackers to hunt for active servers.

  These requests are forwarded to a directed broadcast address; the source address is set to the address of the target system, which then becomes flooded with ping response packets from all the hosts on the selected network. The attack system can amplify its original ping request hundreds of times. The original address is hidden behind the forged address. Furthermore, by bouncing the attack off a number of networks, effective Smurf attacks make it impossible for the victimized system to filter out the intrusive data.

  Although this scenario is complex, Smurf attacks can be stopped if all leaf routers—the router at the top of an IP subnet that defines the subnet—are configured *not* to forward directed broadcast packets. This is strongly recommended by IETF (Internet Engineering Task Force) and the Computer Emergency Response Team (CERT). Unfortunately, many sites have not implemented this type of filtering.

Smurf attacks can also be handled with upstream rate limiting, which maintains total ICMP traffic to approximately 2.5 percent—high enough to handle expected ICMP traffic, but low enough to keep large attacks at bay.

- **ICMP**

  An ICMP flood attack is similar to Smurf, but without the amplification caused by sending packets to broadcast addresses. Similar remedies apply.

- **TCP SYN**

  A TCP SYN flood[2] sends erroneous Transmission Control Protocol (TCP) requests to the target system, which cannot complete the connections. The hacker hides his or her identity by using the address of an innocent party—further complicating attempts to trace the hacker. Incomplete connection requests fill up the target's request table, preventing it from accepting anymore valid requests.

  These type of attacks can be handled with a defense called "random early drop," which, as the name implies, randomly deletes incomplete connection requests. Today, "patches" are available for most operating systems. Cisco routers have implemented another defense called TCP Intercept,[3] which reportedly helps protect host systems.

- **UDP**

  A UDP flood sends large numbers of User Datagram Protocol (UDP) packets to the target system, effectively tying up available network bandwidth. Packets typically contain forged source addresses to prevent simple filtering.

The best way to deflect UDP attacks is to have all peered boundary routers implement Network Ingress Filtering,[4] which blocks packets with clearly forged source addresses from entering the Internet in the first place. While this method does not prevent UDP floods, it will indicate their source. Upstream rate limiting of UDP traffic is another defensive approach to UDP attacks, and can be achieved in much the same way as ICMP limiting. The problem is that different sites may have different volumes of normal UDP traffic. Limiting should thus be undertaken with care.

- **TCP**

  TCP floods are similar to UDP floods, except the attacker uses TCP packets instead of UDP packets. TCP floods create a problem unlike the UDP case—upstream rate limiting is not an option, since most valid traffic is over TCP. The only defense for TCP floods is to enforce Network Ingress Filtering.

- **Distributed Denial of Service (DDoS)**

  Distributed Denial of Service (DDoS)[5] attacks are harder to remedy than simple DoS attacks, and therefore require a more comprehensive set of approaches. By utilizing DoS building blocks, DDoS takes a more sophisticated approach by replicating the *attacking host* hundreds of times around the Internet. These distributed attack agents are controlled remotely from a central location manned by one or more "handlers." Even if one attack system is traced and shut down, others can continue their assault, making it difficult to eliminate the problem. Nonetheless, defending against each component of these well orchestrated incidents can still help. Most network vulnerability scanners can detect common vulnerabilities, which can be patched to prevent loading of the DDoS agent.

  A number of DDoS programs have been developed by hackers over the past few years. The ones that are most prevalent in widespread attacks include Floodnet, Trinoo, TFN, Stacheldraht and TFN2K.

Floodnet (Netstrike) is a Java™ application that inundates the target host with requests for non-existent pages and queries to the search engines. It uses a form of TCP/IP flooding that attacks inbound and outbound data. This form of TCP/IP flooding saturates not only the CPU, but also the network—filling up disk space used for logging. Floodnet is a cooperative system; the debilitating application is downloaded by a willing perpetrator. In 1998, Floodnet was used for an online sit-in as a political protest called NetStrike. The protests were directed at the Web sites of the Department of Defense, the president of Mexico and the Frankfurt Stock Exchange.

Floodnet agents can be identified by an intrusion detection system, then filtered based upon the packet content.

Trinoo[6] is the first and simplest of the DDoS systems. In this case, the target and date of the attack is controlled by the master, and contains only the UDP flood package. Its agents are detected with remote scanning.

Tribal Flood Network (TFN)[7] comprises multiple DoS attacks: Smurf, TCP SYN flood, UDP flood, and ICMP flood. Its agents can be detected with remote scanning.

Stacheldraht[8] *(German for "barbed wire")* is based on TFN, and incorporates multiple DoS attacks: Smurf, TCP SYN flood, UDP flood and ICMP flood. Its agents can be detected with remote scanning.

TFN2k[9]–Although similar to TFN, TFN2k attacks are much harder to detect. Communications are encrypted, and there is no default key. Agents can be detected with a remote scanner if a key is known, or with a host-based tool like National Infrastructure Protection Center's (NIPC) find_ddos.

DDoS Defense Planning

This section details additional measures that can be employed to help protect against DoS attacks. It begins by describing general security practices that every organization should have in place, then focuses on intrusion detection—a key factor in defending against DoS attacks. Finally, it provides a detailed description of steps that can help prevent DoS attacks, followed by a discussion of incident management.

e-business security checklist

- *Have you implemented a thorough and aggressive security policy* that is reflected throughout the business — including firewall configurations, access controls and employee communications?

- *Have you received endorsement* by all levels of management and the Board of Directors to implement effective security measures?

- *Have you fully integrated* established security processes and procedures with your organization's systems management software?

- *Do you have operating systems* that are configured to the most secure settings? Are vendor-supplied password default settings replaced with your own secure passwords?[10]

- *Have you installed firewalls on outside borders, as well as internal borders?* Have the default settings on the firewall application been changed?

- *Have you adopted intrusion detection software?* Similar to installing burglar alarms and motion detectors, intrusion detection is equally critical for internal and external networks. Complementary policy-based roles and responsibilities should be assigned and used at the application layer to prevent Trojan horse software.

- *Have you distributed antivirus software?* The best antivirus systems will have easy, effective update mechanisms for thorough, up-to-date implementation.

- *Can you regularly validate installed software inventories?* Software should be obtained from sources that are consistent with corporate security policy.

- *Are clients equipped with enhanced security capabilities for network access?* It is important to establish access rights via hardware-based security elements such as embedded security subsystem, smart-cards and secure access tokens. Usage privileges and access control should be authenticated via Public Key Infrastructure-based credentials.

- *Have you implemented a user administration system?* Enterprise solutions should be established to enable centralized support staff to easily create, modify and delete user accounts that are consistent with the corporation's security policy.

- *Have you established rules for password selection?* Determine very clear guidelines for passwords, e.g., six characters with at least one numeral, and develop an easy way to verify. Passwords should be changed periodically. Users should not store their passwords in their applications, or on or near their systems.

- *Have you conducted a security awareness campaign to regularly remind employees of their security responsibilities* (Web-based certification or regular e-mails, etc.)?

- *Do you perform security audits on a regular basis?* These should be unannounced and random—some electronic, some physical, some concealed and others overt. The purpose of these audits is to test whether policies are being implemented and whether practices are effective. The goal of some audits, for example, may be to attempt to break into a target system, access valuable data if possible, and determine if the intrusion was noticed by those charged with monitoring the systems.

- *Have you designated someone as the main network security contact and determined clear procedures for reporting and responding to security issues?*

- *Do your employees clearly understand that they should report all incidents that seem to breach the security policy? Do they know whom to contact?*

- *Can you ensure that system administrators stay abreast of security advisories and make security-related changes in a timely manner?* These people are your first, best defense; they need to take a proactive role and be ready to react quickly to security issues.

- *Do you have a clear policy for action when an employee leaves the company, regardless of the reason?* Measures should be taken to quickly disable an ex-employee's building and computer access, delete or redistribute computer accounts, and change all passwords and access codes known by the employee.

- **Risk management**
  Companies should deploy a risk-management solution to help centrally manage attacks, threats and exposures by correlating security information from firewalls, intrusion detectors, vulnerability scanning tools and other security check-points. This helps administrators eliminate "clutter" such as false-positives, and respond with adaptive security measures.

  Integrated security management also makes it easier for system administrators—who are not necessarily security experts—to monitor and assess security risks in realtime and with a high degree of integrity and confidence across an organization's multiple security checkpoints. Automated countermeasures help ensure limited access to business partners, customers, suppliers, internal employees and other authorized users. An example of this type of integrated security and risk management solution is Tivoli® SecureWay® Risk Manager. (See reference, page 22).

- **Intrusion detection**
  In matters of network security, corrective actions to intrusions should be taken as soon as possible. Intrusion Detection Systems (IDS) support network managers in two ways: They alert them promptly so that planned responses can be invoked, and help them determine whether an unusual traffic pattern is an attack or a random event caused by non-malicious actions. IDS can detect when malicious users are employing your site to launch attacks against another site. Intrusion detection systems can be designed for network-based and host-based systems.

  Network-based IDS are attached to the network; they detect attacks by analyzing the content of network packets sent over the wire. An unusually high number of TCP, UDP, or ICMP packets sent to a single destination can easily be detected. IDS are configured to determine if these packets should be considered attacks or normal traffic. Tivoli SecureWay Risk Manager [11] is a good example of a product solution capable of recognizing basic attacks (Smurf, TCP SYN flood, UDP flood, TCP flood) and preventing DDoS incidents.

  Host-based IDS are software components that attempt to detect attacks against the computers on which the IDS is installed. Host-based IDS can analyze the network packets received on the network interface, as well as the log files written by the operating system or by applications running on the computer. Typically, a host-based IDS can detect DoS attacks against Web servers by analyzing its log in realtime.

  Sites should install both network and host-based detection systems. Rapid availability of network analyzers must be assured to help determine the nature of an incident, and to help formulate possible filtering/rate limiting responses in the event of an actual DoS or DDoS attack.

Additional DDoS defense planning

The previous sections have outlined sound security and intrusion detection practices that all organizations should implement. Sites more vulnerable to DDoS attacks require additional measures, which can help organizations respond in a calm, prudent manner.

Be prepared: Establish a response plan *before* an attack occurs:

- Develop a documented incident management plan (see p. 11)
- Create a list of the names and numbers of your security team and securing partners who can begin analysis of attacks
- Maintain a list of available emergency response services
- Know the name and number of your Internet Service Provider (ISP) contact, who can provide additional filtering/limiting
- Know the name and number of your law enforcement contact
- Work with your ISP to establish proactive rate limiting of ICMP[12] and define procedures for implementing new filters or rate limits
- Install intrusion detection systems that are capable of recognizing basic attacks (Smurf, TCP SYN flood, UDP flood, ICMP flood)
- Ensure rapid availability of network analyzers to determine the nature of an attack and formulate possible filtering/rate limiting responses should an actual attack occur.

Understand basic DoS response methods

It is important to know how to address each type of DoS attack (see p. 3).

Be a good neighbor

Defending against DDoS attacks is especially challenging; traditional security strategies are simply not sufficient. Defense management requires the cooperation of multiple organizations in the Internet community; organizations experiencing an attack can do little to stop or track these incidents without the help of others. A victimized system is highly dependent upon its ISP and its upstream routers — as well as administrators at remote sites — to help limit and stop such assaults.

Attacks are better controlled if all organizations practice basic “good neighbor” policies that limit the use of their sites as “agents” or “soldiers” in Distributed DoS attacks. These measures require that the company:

- *Implement Network Ingress Filtering.*[16] on all boundary routers. This type of filtering blocks all packets with forged source addresses from moving from the site to the Internet. This filtering stops Smurf attacks, while simplifying attack filtering and tracking. It is important to note that the Internet Engineering Task Force has advanced the network ingress filtering Request for Comment (RFC) to a status of Best Current Practices (BCP).

- *Disable directed broadcast messages at leaf routers.*[17] The routers closest to end-user systems know the broadcast addresses for their subnets. Therefore, they can be configured not to forward packets directed to broadcast addresses. Blocking directed broadcast packets stops the amplification used in Smurf attacks, but does not halt legitimate broadcasts. It prevents only those broadcasts that are going from leaf nodes upwards. In addition, if a broadcast is trying to move up from a leaf and it couldn't possibly have originated on the sub-network that the leaf is on, the packet's origin address was probably forged and should be considered suspect. As with ingress filtering, the IETF has just elevated the directed broadcast filtering RFC to a status of BCP.

- *Scan external hosts for vulnerabilities to prevent installation of new DDoS agents.*[18] Current DDoS installation tools appear to use well-known vulnerabilities in some RPC services; fixing these known weaknesses will help to shield a site's systems from attack.

- *Scan external hosts for the existence of known DDoS agents.*[19, 20] Detecting and removing existing DDoS agents will also help prevent DDoS attacks.

- *Report attacks* to local law enforcement and industry organizations.

A good summary of these and related countermeasures is contained in the IETF working draft, "Security Expectations for Internet Service Providers," by Tom Killalea.[21]

Secure Web site configurations

There are several security practices that, if implemented during a Web site's system configuration, can reduce the likelihood of future attacks. A sound IT security policy should provide guidance to Web masters and Web system administrators during the system setup and subsequent deployment. This policy should entail:

- Guidance on installing and configuring peripheral packet filters and Internet firewalls as a first line of defense
- A list of TCP/IP services that are *not* required for Web site function. These services should be disabled
- Installation of devices to ensure that configured controls do not change; these should include intrusion-detection “health checking” tools
- Application of timely security fixes to the operating system and Web server, including replacement of vendor-supplied default settings for passwords, etc.
- Regular scanning of the Internet/intranets to detect vulnerabilities.

Unless specific traffic is allowed to reach the Web server, no service can be provided. Therefore, you must allow certain TCP/IP traffic to reach the Web server. Generally, this is TCP ports 80 and 443. It is very difficult to defend against a DoS attack on a Web server on one of these ports, since the normal primary defense mechanisms, such as routers and firewalls, are configured to allow traffic through. Hence, special steps are needed.

First, consider where the Web server will reside within the infrastructure. Traditionally, the Web server is located between filtering devices, such as firewalls and routers. This places it in a "demilitarized" zone (DMZ), which offers some protection from Internet intrusions. The internal network receives protection from the Web server. Outside filtering devices permit only ports 80 and 443 to reach the Web server; other potentially dangerous traffic, such as ICMP, is inhibited. The inside filtering device is important, since the Web server itself should not rely on other hosts within the secure LAN. Although you must allow potentially dangerous parties access to your Web server, careful measures should be taken to prevent unwanted entry. (There are many reference books that address the different DMZ methods in more detail).

The second step is to configure these filtering devices to comply with the service you are providing, while restricting everything else. Proper configuration of firewalls and routers can be a complex task, and is often assigned to highly skilled security consultants. Many types of undesirable attacks, such as TCP and UDP, as well as the methods for blocking them, have been described in this paper. It is important to remember that in addition to blocking traffic, attacks can also be directed at your infrastructure. A key consideration of comprehensive intrusion detection can help discover when an unwanted intruder has been attempting unauthorized use.

Deny logs triggered by these filtering devices should be sent to a logging server for analysis and storage. Much like filtering-device logs, Web server logs provide excellent sources for detecting intrusions. Many DoS attacks can be detected by the *signature* they leave in the Web server log files. More sophisticated mechanisms include intrusion detection boxes, which perform network "sniffing" as they seek out suspect signatures.

A simpler technique involves writing a piece of shell code that notices exception patterns like unusual CPU utilization, or a dramatic increase in the number of threads currently running on the Web server. If such patterns are detected, the tools page can alert key personnel. Of course, this method takes some tuning to determine what is *truly* unusual, versus what constitutes a simple increase in normal service requests. Nevertheless, this has proven to be an effective approach for circumventing DoS attacks.

It is critical to develop, document and test a detailed response plan before problems occur. In the case of a prolonged DoS attack, an appropriate response is to continue to keep the problem away from the Web server complex. This would involve pushing the offending traffic away from the Web server and back into the supporting infrastructure network, then pushing it away from the infrastructure and back into the assigned ISP, who would help in the recovery process. Other remedial tactics for deflecting a severe attack include:

- Adding filter rules to the Web server or operating system to block traffic associated with the attack. Not all Web servers or operating systems provide this function, so a deliberate check is recommended
- Adding filter rules to routers and/or firewalls to block undesirable traffic
- Adding rules to divert unwelcome traffic to a nonexistent host IP on the LAN
- Minimizing exposure of IP pool addresses. If there is no route, the packet will collapse at the nearest full routing router.

Incident management

When an incident occurs, security personnel are faced with many different and difficult choices. At the same time, hasty, improper reactions can only make matters worse. Before any actions are taken, several key questions must be answered:

- *Has an incident actually occurred?* Human error or a software failure can sometimes mimic the actions of an intruder.
- *Was any damage really done?* In many incidents, the perpetrator gains unauthorized access, but doesn't actually access privileged information or alter data.
- *Is it important to collect and protect evidence that might be used in an investigation? Is it important to get systems back into normal operation as soon as possible?*
- *Is it acceptable to assume that data has been changed or deleted? How do you determine if changes have been made?*
- *Does it matter if people inside and outside the organization hear about the incident?*
- *Could this event happen again?*

The answers to some of these questions may be contradictory. For example, collecting and protecting evidence may not be possible if the primary goal is to get systems and services back into normal operation immediately. Because such choices must be made quickly—when an incident is actually detected—a well-defined process is vital to helping security personnel take appropriate and necessary actions.

An Internet Security Event Response Process (ISERP) should be designed to help companies react in a rapid, structured, efficient and effective manner. The ISERP should be carried out by a group of people possessing a variety of skills—not only in relevant technologies, but also in non-technical areas such as public relations. This group is referred to as the "Response Team." By effectively organizing responses, the ISERP allows organizations to optimize the protection that technological components provide. This will in turn extend protection to a company's data, systems and services, safeguarding the business's reputation. The ISERP plan comprises four elements, which should be clearly documented:

- *The process description* articulates *what* needs to be done from a high-level operational standpoint—but not *how* it should be done. The process description thus remains independent of the specific technological components and the configuration of a company's current environment, and can be easily adapted to accommodate change. The process description should include—at a minimum—contact information for your security specialists, ISPs and enterprise security vendors.

- *Scope and goals* describes the scope, context, inputs and outputs and external connections, plus required mechanisms and measurements.

- *Functionality* defines diagrams and descriptions of each of the major sub-processes, including Internet security event notification, categorization, investigation, reaction, restoration, defense strengthening and documentation. Process testing, review and updating are also addressed.

- *Staffing and assignments* provide detailed definition on process roles, assignments and associated responsibilities.

In the event of a DoS attack:

- ■ Work with your ISP and emergency response team to perform rate limiting and other steps outlined on pages 4-7. If these do not work, try steps 2 and 3.

- ■ Change the IP address of the target and update the DNS to reflect the new address. Most of these attacks, once initiated, are then left to run. They do not look up the IP address at each attempt and therefore do not go to the correct address. In these cases, an enterprise can block intrusions at the router level. The problem with this approach is caching; in the time it takes for the DNS information to propagate, the attack could be over—before the change is completed.

- ■ Investigate the actual attack by working with the ISP, who can check each router. If the attack spans multiple ISPs, the providers must work together. When severe attacks occur, it may be appropriate to contact federal law enforcement, specifically the FBI, for assistance. In order to trace one connection to the source of the attack, the location of the master station must be known before appropriate actions can be taken.

DDoS attacks have two distinct types of victims: *end targets*—the sites under attack, and *soldiers or agents*—companies whose systems have been compromised and are now controlled by the hacker. Typically, organizations become the hacker's soldier, rather than the end target. Hackers assign soldiers by exploiting weaknesses and defects in networks and operating systems, which gains them root/administrator access. Next, they install software to hide the break-in and all subsequent activities. The software they employ includes a process to remotely control the victimized system and use it for subsequent attacks on others.

DDoS attacks make detective work extremely difficult. Although the packets flooding the network—those with source and destination addresses—must be inspected, this is not really helpful, since a target's IP address is the destination and the source address is random. The only valid information available is the hardware address of the last router the packet passed through before reaching its final destination. Sometimes, this provides insight into the ISP, who may be passing the flood of packets.

The greater the complexity of a company's LAN or WAN, the more steps it will take to access the initial outside router. A company may even have to trace its own internal routers first. Next, a packet from the other side of that outside boundary router must be obtained. Since the enterprise under attack would not own this router, cooperation is required from the network administrator, who can obtain the hardware address of the previous router. Finally, a packet from the other side of that previous router must be found.

These steps must be performed over and over, from network to network, until the hardware address of one soldier machine is determined. Note that the success of DDoS attacks on the scale of a gigabit of packets per second will depend on hundreds of soldier systems. Once one soldier is located, the next effort is to trace it back to the controlling system. There may be information on the soldier system that describes its origin or the original compromise that led to the setup of the soldier system.

Another tactic is to track the controlling system when the controller next deploys the soldier system. This type of tracking can only be done when the controller is active. It may involve multiple intermediate links, limiting its chance of success. Both of these approaches should be done in parallel with tracking down additional soldier systems. Shutting off soldier systems can provide immediate relief from a portion of the attack.

The above tactic is from the point of view of the victim. The owner of the soldier system may have a different objective: to restore their system. Their recovery may remove the chance of examining the compromised system for clues to the origin of the attack; however, their cooperation can still allow placement of a network IDS to deflect attempted contacts by the controlling system. In this event, a request to do a bit-level copy of the system's disk storage might be granted, opening a larger window of time to examine the system for additional evidence (particularly if one "peeks" beneath the file system layer and examines the raw disk blocks to locate intruder data file contents subsequently deleted). Again, knowing your service providers and having the right contact information can speed this process.

If you are looking for a drive's full data forensics, be sure to make a bit-copy of the drive (if possible) and conduct the exam on copies of that mirror. Using monitoring tools to detect active soldiers is easy. An IDS should be able to pick up both incoming and outgoing floods. If an organization's routers are configured properly, outbound traffic should not appear to originate from outside the network. Some new routers provide this capability, but are turned off by default. Also, since the masters of these soldiers (shall we call them "generals"?) can use "connectionless" protocols (udp/icmp), they can also disguise the address of the "generals'" orders. This makes detection much more difficult, and of limited value.

Looking to the future

Over time, the variety and sophistication of network attacks are likely to increase. The Internet technical community has repeatedly risen to the challenge of closing security exposures, and will undoubtedly do the same regarding DDoS attacks.

A promising new approach to blocking and tracking DDoS attacks is the *packet tagging*[22] method. Backbone routers add tagging information to packets to help trace them back to their real source. Another encouraging area involves finding ways to share attack data while removing sensitive packets that might inadvertently disclose private or confidential information. This is referred to as “blinding” the data captured by intrusion detection systems so that details like “who is surfing which Web sites” are hidden from view. If there is a subsequent investigation, the security officer can unlock the relevant records.

System design techniques that appear to be effective for defending against DDoS attacks avoid single points of failure; that is, they have *built-in redundancy*. An example of this method is distributed replication of caching servers, where multiple servers, maintaining similar content, are spread geographically.

Work is also underway to make operating systems more secure. The concepts behind evaluated systems are being adapted for broader use. An area that needs further research is the improvement of forensic tools to apprehend hackers.

Conclusions

DoS attacks should be viewed as a risk management issue — one that can be effectively dealt with like other business issues. Having appropriate plans in place allows organizations to deal with attacks on their systems in a controlled, consistent manner, in an environment where duties and actions are clearly defined and understood by all key players. Two plans are essential:

- A *preventive plan* can help ensure that appropriate measures are taken to maintain business continuity. These include installing software to detect and prevent attacks, as well as software to identify the nature of the attack. Because preventive measures are typically not 100 percent effective, a plan must consider how to deal with security breaches when they do happen.
- The *incident response plan* outlines the steps to take should a security breach event occur, and specifies responsibilities for executing necessary tasks. A clear-cut plan can prevent panic, as well as ineffective or sometimes detrimental actions.

In many parts of the world, neighborhood "watch" programs rely on members of the community to help keep other residents safe. The community of e-business is no different; responsible users of the Internet should adhere to "good neighbor" principles. When a problem does arise, the community should join forces to maintain their collective security.

The principles of being a good neighbor on the Internet include:

- Securing one's own systems to help prevent against them being compromised or used against others
- Conducting regular testing of those systems for vulnerabilities
- Instituting a process to proactively monitor systems activity and take action when any attempt is made to illegally gain access to those systems
- Reporting factual information promptly
- Avoid spreading inaccurate or untrue information that could create or exacerbate a situation.

Cooperation with authorities is essential. Timely responses to law enforcement subpoenas for critical information, for example, can help locate and identify hackers and minimize further disruptions to your business or others on the network.

The collective strength of an informed, responsible and cooperative Internet community is a powerful security tool that can aid in the success of your business, as well as those on whom it depends.

For more information

To learn how the professionals of IBM security and privacy services can help you protect your IT infrastructure, contact your IBM sales representative, or visit:

ibm.com/security/services

References

[1] Smurf
http://www.cert.org/advisories/CA-98.01.smurf.html

[2] TCP-SYN flood Information
ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding

[3] TCP Intercept
http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/intercpt.htm

[4] Network Ingress Filtering RFC 2267 (January 1998)
http://www.ietf.org/rfc/rfc2267.txt

[5] CERT analysis of DDoS
http://www.cert.org/advisories/CA-2000-01.html
http://staff.washington.edu/dittrich/talks/cert/
http://www.cert.org/reports/dsit_workshop.pdf

[6] Trinoo
http://staff.washington.edu/dittrich/misc/trinoo.analysis

[7] Tribe Flood Network (TFN)
http://staff.washington.edu/dittrich/misc/tfn.analysis

[8] Stacheldraht
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

[9] TFN2K
http://packetstorm.securify.com/distributed/TFN2k_Analysis.htm

[10] IBM Server Security
ibm.com/servers/aix/security.html
http://www.as400.ibm.com/tstudio/secure1/sdex_fr.htm
ibm.com/S390/security

[11] Security risk management solutions—Tivoli SecureWay Risk Manager
http://www.tivoli.com/products/index/

[12] ICMP
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart4/qcpolts.htm
http://www.cisco.com/warp/public/707/newsflash.html

[13] Software distribution for compliance with corporate security policies
http://www.tivoli.com/products/index/software_dist/

[14] Disaster recovery solutions
http://www.tivoli.com/products/index/disaster_recover_mgr/

[15] Enterprise management solution to prepare against an attack
http://www.tivoli.com/products/documents/whitepapers/

[16] Network Ingress Filtering RFC 2267 (January 1998)
http://www.ietf.org/rfc/rfc2267.txt

[17] Directed Broadcast Filtering
http://www.cert.org/advisories/CA-98.01.smurf.html
http://www.ietf.org/rfc/rfc2644.txt

[18] NSA Host Vulnerability Scanner
http://dr.watson.ibm.com/nsa

[19] NIPC's find_ddos
http://www.fbi.gov/nipc/trinoo.htm

[20] Agent scanners
dr.watson.ibm.com/nsa
http://staff.washington.edu/dittrich/misc/sickenscan.tar
http://staff.washington.edu/dittrich/misc/ddos_scan.tar

[21] Internet Engineering Task Force working draft,
"Security Expectations for Internet Service Providers"
http://www.ietf.org/internet-drafts/draft-ietf-grip-isp-expectations-03.
Updates will be posted at http://ww.ietf.org/ieft/…abstracts.txt.

[22] Packet tagging
http://www.cs.washington.edu/homes/savage/traceback.html

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
06-00
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.