Types of Attacks on Web Servers

Newspapers Internet magazines came with cover stories when Denial of service (DoS) attacks assaulted a number of large and very successful companies' websites last year. Those who claim to provide security tools were under attack. If Yahoo, Amazon, CNN and Microsoft feel victim to DoS attacks, can any site-owner feel safe?

In this article we'll try to make site owners understand the "In and Outs" of DoS andDDoS attack methods, vulnerabilities, and potential solutions to these problems. Webmasters are usually seen searching for solutions to new security threats and ways of patching-up before it is too late.

DoS:

In a Denial of Service (DoS) attack, the attacker sends a stream of requests to a service on the server machine in the hope of exhausting all resources like "memory" or consuming all processor capacity.

DoS Attacks Involve:

* Jamming Networks
* Flooding Service Ports
* Misconfiguring Routers
* Flooding Mail Servers

DDoS:

In Distributed DoS (DDoS) attack, a hacker installs an agent or daemon on numerous hosts. The hacker sends a command to the master, which resides in any of the many hosts. The master communicates with the agents residing in other servers to commence the attack. DDoS are harder to combat because blocking a single IP address or network will not stop them. The traffic can derive from hundred or even thousands of individual systems and sometimes the users are not even aware that their computers are part of the attack.

DDoS Attacks Involve:

* FTP Bounce Attacks
* Port Scanning Attack
* Ping Flooding Attack
* Smurf Attack
* SYN Flooding Attack
* IP Fragmentation/Overlapping Fragment Attack
* IP Sequence Prediction Attack
* DNS Cache Poisoning
* SNMP Attack
* Send Mail Attack

Some of the more popular attack methods are described below.

FTP Bounce Attack

FTP (File Transfer Protocol) is used to transfer documents and data anonymously from local machine to the server and vice versa. All administrators of FTP servers should understand how this attack works. The FTP bounce attack is used to slip past application-based firewalls.

In a bounce attack, the hacker uploads a file to the FTP server and then requests this file be sent to an internal server. The file can contain malicious software or a simple script that occupies the internal server and uses up all the memory and CPU resources.

To avoid these attacks, the FTP daemon on the Web servers should be updated regularly. The site FTP should me monitored regularly to check whether any unknown file is transferred to the Web server. Firewalls also help by filtering content and commands. Some firewalls block certain file extensions, a technique that can help block the upload of malicious software.

Port Scanning Attack

A port scan is when someone is using software tosystematically scan the entry points on other person?s machine. There arelegitimate uses for this software in managing a network.

Mosthackers enter another?s computer to leave unidentifiable harassing messages,capture passwords or change the set-up configuration. The defense for this isthrough, consistent network monitoring. There are free tools that monitor forport scans and related activity.

Ping Flooding Attack

Pinging involves one computer sending a signal to anothercomputer expecting a response back. Responsible use of pinging providesinformation on the availability of a particular service. Ping Flooding is theextreme of sending thousands or millions of pings per second. Ping Flooding cancripple a system or even shut down an entire site.

APing Flooding Attack floods the victim?s network or machine with IP Pingpackets. At least 18 operating systems are vulnerable to this attack, but themajority can be patched. There are also numerous routers and printers that arevulnerable. Patches cannot currently be applied throughout a global networkeasily.

Smurf Attack

A Smurf Attack is modification of the "ping attack"and instead of sending pings directly to the attacked system, they are sent to abroadcast address with the victim?s return address. A range of IP addressesfrom the intermediate system will send pings to the victim, bombarding thevictim machine or system with hundreds or thousands of pings.

One solution is to prevent the Web server from being usedas a broadcast. Routers must be configured to deny IP-Directed broadcasts fromother networks into the network. Another helpful measure is to configure therouter to block IP spoofing from the network to be saved. Routers configured assuch will block any packets that donor originate in the Network.To be effective this must be done to all routers on the network.

SYN Flooding Attack

This attack exploits vulnerability in the TCP/IPcommunications protocol. This attack keeps the victim machine responding back toa non-existent system. The victim is sent packets and asked to response to asystem or machine with an incorrect IP address. As it responds, it is floodedwith the requests. The requests wait for a response until the packets begin totime out and are dropped. During the waiting period, the victim system isconsumed by the request and cannot respond to legitimate requests.

When a normal TCP connection starts, a destination hostreceives a SYN (synchronize/start) packet from a source host and sends back aSYN ACK (synchronize acknowledge) response. The destination host must the hearan acknowledgement, or ACK packet, of the SYN ACK before the connection isestablished. This is referred as the "TCP three-way handshake?.

Decreasingthe time-out waiting period for the three way handshake can help to reduce therisk of SYN flooding attacks, as will increasing the size of the connectionqueue (the SYN ACK queue). Applying service packs to upgrade older operatingsystems is also a good countermeasure. More recent operating systems areresistant to these attacks.

IP Fragmentation/Overlapping Fragment Attack

To facilitate IP transmission over comparatively congestednetworks. IP packets can be reduced in size or broken into smaller packets. Bymaking the packets very small, routers and intrusion detection systems cannotidentify the packets contents and will let them pass through without anyexamination. When a packet is reassembled at the other end, it overflows thebuffer. The machine will hang, reboot or may exhibit no effect at all.

Inan Overlapping Fragment Attack, the reassembled packet starts in the middle ofanother packet. As the operating system receives these invalid packets, itallocates memory to hold them. This eventually uses all the memory resources andcauses the machine to reboot or hang.

IP Sequence Prediction Attack

Usingthe SYN Flood method, a hacker can establish connection with a victim machineand obtain the IP packet sequence number in an IP Sequence Prediction Attack.With this number, the hacker can control the victim machine and fool it intobelieving it?s communicating with another network machines. The victim machinewill provide requested services. Most operating

systems now randomize theirsequence numbers to reduce the possibility of prediction.

DNS Cache Poisoning

DNS provides distributed host information used for mappingdomain names and IP addresses. To improve productivity, the DNS server cachesthe most recent data for quick retrieval. This cache can be attacked and theinformation spoofed to redirect a network connection or block access to the Web sites),a devious tactic called DNS cache poisoning.

The best defense against problems such as DNS cachepoisoning is to run the latest version of the DNS software for the operatingsystem in use. New versions track pending and serialize them to help preventspoofing.

SNMP Attack

Most network devices support SNMP because it is active bydefault. An SNMP Attack can result in the network being mapped, and traffic canbe monitored and redirected.

The best defense against this attack is upgrading toSNMP3, which encrypts passwords and messages. SinceSNMP resides on almost all network devices, routers, hubs, switches, Servers andprinters, the task of upgrading is huge. Some vendors now offer an SNMP Managementtool that includes upgrade distribution for global networks.

UDP Flood Attack

AUDP Flood Attacks links two unsuspecting systems. By Spoofing, the UDP floodhooks up one system?s UDP service (which for testing purposes generates aseries of characters for each packet it receives) with another system?s UDPecho service (which echoes any character it receives in an attempt to testnetwork programs). As a result a non-stop flood of useless data passes betweentwo systems.

Send Mail Attack

In this attack, hundreds of thousands ofmessages are sent in a short period of time; a normal load might only be 100 or1000 messages per hour. Attacks against Send Mail might not make the front page,but downtime on major websites will.

For companies whose reputation dependson the reliability and accuracy of their Web-Based transactions, a DoS attackcan be a major embarrassment and a serious threat to business.

Conclusion

Frequent denial-of-service attacks and achange in strategy by "Black-Hat Hackers" are prompting enterprises todemand technology that proactively blocks malicious traffic.

Tools and services that reflect approaches to combat such DoS attacks have been introduced with time. These arenormally upgrades to what was produced before. No solution is ever said to be anultimate solution to defend DoS attacks. Despite the new technology coming everyday, the attacks are likely to continue.

Source: http://www.go4expert.com/articles/types-attacks-web-servers-t305/