Denial of Service Attacks – Are You Vulnerable?

Mr. Jitu Panesar & Mr. George Goutas

The availability of any e-gaming website is essential to the success of its operations. Website downtime is equivalent to a closed store. Every minute that an e-gaming site is down, revenue losses increase dramatically.

A Denial of Service (DoS) attack affects the availability of an e-gaming system by either interrupting service or by completely denying legitimate customers from accessing needed system resources.

DoS attacks cost businesses millions of dollars each year because of system downtime, lost revenue and productivity, tarnished reputation, and the hours required by technical staff to locate the problem and resolve it. Once customers lose confidence in the security of the systems holding their confidential and financial information, they will often take their business elsewhere.

The type of DoS attacks that have been plaguing many of the well-known e-commerce sites flood the victim's computer or network with apparently valid Internet traffic. This overwhelms the victim's servers, or the link from the victim to the Internet. Some of the more prevalent network flooding DoS attacks include "Smurf", "Fraggle", "ICMP Flood", "TCP SYN Flood", "Teardrop", "Ping-of-Death", and "DDoS".

In a "Smurf" attack, the attacker floods the network with Internet Control Message Protocol (ICMP) ping response messages. ICMP is generally used for diagnostic purposes by administrators to determine the status of network devices. To carry out this attack, the attacker spoofs the source IP address to appear as though it originated from the victim's own systems. Spoofing is a technique whereby the attacker falsifies his own machine's source address, thereby masquerading his/her true identify. An ICMP message with this spoofed address is sent by the attacker to a directed broadcast address at an amplifying network. All the hosts on the amplifying network then send ICMP ping reply messages to the target machine. The victim system and network are overwhelmed.

A "Fraggle" attack is similar to a Smurf attack, but instead of using the ICMP protocol, the User Datagram Protocol (UDP) is used. The attacker broadcasts a spoofed UDP packet to the amplifying network, which replies to the victim's systems.

An "ICMP Flood" attack is similar to a Smurf attack, but does not take advantage of amplification created by sending packets to a broadcast address.

Before two systems can communicate over a network using the TCP protocol, they must establish a virtual connection. This connection is established every time you visit a website or download a file. In a "TCP SYN" flood attack the attacker makes a request to the victim's server to establish one of these virtual connections. The victim's server then responds and awaits a final response from the attacker's computer, in order to complete the virtual circuit. However, the attacker does not respond and as a result the connection is never completed. The victim's server can only handle a limited number of these types of connections and the incomplete connection requests prevent the victim's server from accepting any further valid connection requests.

When you email a file over the Internet, it is often split up into packet fragments that are delivered and transmitted separately, and then these fragments are recombined at the destination. In a "Teardrop" attack, packets are fragmented in such a way that they cannot be properly reassembled by the receiving system, which could freeze or reboot. A "Ping-of-Death" attack uses an oversized ICMP packet to accomplish the same result. Some other DoS attacks include DNS DoS and Timing Attacks.

A more aggressive form of a DoS attack that has been affecting organizations recently is called a Distributed Denial of Service (DDoS) attack. The DDoS uses an array of computers from around the Internet to stage a DoS attack and amplify its effects. The attacker instructs computers that he/she has compromised ("zombies") to work in concert to overwhelm the targeted victim.

Because of flaws inherent in the design of the network stack when the Internet was originally created, it is difficult to completely prevent DoS and DDoS attacks. A preventative plan and an incident response plan are essential to mitigate the effects of DoS and DDoS attacks. Once these plans are established, a comprehensive set of technical controls must follow. Technical countermeasures include: intelligent TCP, UDP and ICMP traffic inspection and filtering; traffic rate limiting and limiting connection-established timeout periods; disabling broadcast functionality at border routers; use of a firewall that provides stateful filtering; increasing the size of the connection queue in the IP stack; implementing and correctly configuring a Network Intrusion Detection System; and keeping up to date with current patch/revisions on your network machines.

DoS attacks should be viewed as a risk management issue that can be effectively dealt with like other business issues. This means minimising exposure where possible and being fully prepared should an attack eventuate.

About the authors:

Mr. Jitu Panesar & Mr. George Goutas are Infrastructure Security Specialists at Technical Systems Testing (TST), one of the world's most experienced testing laboratories that offers a full range of testing and consultation services for Terrestrial (traditional / land-based) and Interactive-based Gaming, Wagering, Lottery, e-Commerce and Information Technology (IT) industries.

TST is a fully independent and internationally accredited laboratory, working with gaming industry regulators, manufacturers and suppliers to ensure that systems comply with legislative, regulatory industry standards.

Contact details:

Office: +1 (604) 873-5833
Email: tstna@tstglobal.com

OFFICES:
Vancouver – Suite #420, 1367 West Broadway, Vancouver, British Columbia, Canada, V6H 4A7 // O: +1 (604) 873-5833 // F: +1 (604) 873-1075
London – Swan Centre, Fishers Lane, Chiswick, London, England, United Kingdom, W4 1RX // O: +44 (0)2087 474 956 // F: +44 (0)2087 427 967
Sydney – Suite #305 / 306, 30 – 40 Harcourt Parade, Rosebery, New South Wales, Australia, 2018 // O: +61(2) 9700 7023 // F: +61(2) 9700 7024
Melbourne – Level 28, 303 Collins Street, Melbourne, Victoria, Australia, 3000 // O: +61 (3) 9678 9095 // F: +61 (2) 9700 7024
Macau – Macau Number 39, 17F Central Plaza, 61 Avenida de Almeida Ribeiro, Macau, China // O: +853 8291 3992 // F: +853 8291 3889