2.1 Denial of Service Attacks

The first type of attack we should examine is the denial of service (DoS). A denial of service attack is any attack that aims to deny legitimate users the use of the target system. This class of attack does not actually aim to infiltrate a system or to obtain sensitive information. It simply aims to prevent legitimate users from accessing a given system.

This type of attack is one of the most common categories of attack. Many experts feel that it is so common due to the fact that most forms of denying a service attack can be fairly easy to execute. These attacks can be executed with ease, meaning that even attackers with minimal technical skills can often successfully perform a denial of service.

The concept underlying the denial of service attack is based on the fact that any device has operational limits. This fact applies to all devices, not just computer systems. For example, bridges are designed to hold weight up to a certain limit, aircraft have limits on how far they can travel without refuelling, and automobiles can accelerate until a certain point. All of these various devices share a common trait: They have set limitations to their capacity in order to perform work. Computers are no different from these, or any other machine; they too also have limits. Any computer system, web server, or network can only handle a finite load.

How a workload (and its limits) can be defined depends on the machine. A workload for a computer system might be defined in a number of different ways, including the number of simultaneous users, the size of files, the speed of data transmission, or the amount of data stored. Exceeding any of these limits will stop the system from responding. For example, if you can flood a web server with more requests than it can process, it will overload and will no longer be able to respond to further requests. This reality underlies the DoS attack. Simply overload the system with requests, and it will no longer be able to respond to legitimate users attempting to access the web server.

2.1.1 SYN Flood

Sending a flood of pings is the most primitive method of performing a DoS. More sophisticated methods use specific types of packets. One very popular version of the DoS attack is the SYN flood. This particular attack depends on the hacker’s knowledge of how connections are made to a server. When a session is initiated between the client and server in a network using the TCP protocol, a small buffer space in memory is set aside on the server to handle the “hand-shaking” exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange.

A SYN flood attempts to disrupt this process. In this attack, the attacker sends a number of connection requests very rapidly and then fails to respond to the reply that is sent back by the server. In other words, the attacker requests connections, and then never follows through with the rest of the connection sequence. This effect leaves connections on the server half open, and reserves the buffer memory allocated, making it not available to other applications. Although the packet in the buffer is dropped after a certain period of time (usually about three minutes) without a reply, the effect of these false connection requests makes it difficult for legitimate requests to be established within a session.

2.1.2 Smurf Attack

The Smurf attack is a popular type of DoS attack. It was named after the application first used to execute this type of attack. In the Smurf attack, an ICMP packet is sent out to the broadcast address of a network, but its return address has been altered to match one of the computers on that network, most likely a key server. All the computers on the network will then respond by pinging the target computer.

ICMP packets use the Internet Control Message Protocol to send error messages on the Internet. As the address of packets are sent to a broadcast address, that address responds by echoing the packet out to all hosts on the network, that then sends it to the spoofed source address.

Continually sending such packets will cause the network to perform a DoS attack on one or more of its member servers. This attack is both clever and simple. The greatest difficulty here is to get the packets to start on the target network. This can be accomplished via certain software such as a virus or Trojan horse that will begin sending the packets.

2.1.3 Ping of Death

The Ping of Death (PoD), is perhaps the simplest and most primitive form of DoS attack. It is based on overloading the target system. TCP packets have limited size. In some cases, by simply sending a packet that is too large, it can shut down a target machine.

The aim of this attack is to overload the target system and to cause it to quit responding. The PoD works to compromise systems that cannot deal with extremely large packet sizes. If successful, the server will actually shut down. It can, of course, be rebooted.

The only real safeguard against this type of attack is to ensure that all operating systems and software are routinely patched. This attack relies on vulnerabilities in the way a particular operating system or application handles abnormally large TCP packets. When such vulnerabilities are discovered, the vendor customarily releases a patch. The possibility of PoD is amongst one of many reasons why you must keep patches updated on all of your systems.

This type of attack is becoming less common as newer versions of operating systems are able to handle the overly large packets better that Ping of Death depends on. If the operating system is properly designed, it will drop any oversized packets, thus negating any possible negative effects a PoD attack might have.

2.1.4 UDP Flood

UDP (User Datagram Protocol) is a connectionless protocol that does not require any connection setup procedure to transfer data. TCP packets connect and wait for the recipient to acknowledge a receipt before sending the next packet. Each packet is confirmed. UDP packets simply send the packets without confirmation. This allows packets to be sent much faster, making it easier to perform a DoS attack.

A UDP flood attack occurs when an attacker sends a UDP packet to a random port on the victim’s system. When the victim’s system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that no application is waiting on the port, it will generate an ICMP packet of destination, unreachable to the forged source address. If enough UDP packets are delivered to ports on the victim, the system will go down.

2.1.5 DoS Tools

One reason that DoS attacks have become so common is because a number of tools are available for executing DoS attacks. These tools are widely available on the Internet, and are in most cases free to download. This means that any cautious administrator should be aware of them. In addition to their common use as an attack tool, they can also be very useful for testing your anti-DoS security measures.

Low Orbit Ion Cannon (LOIC) is probably the most well-known and one of the simplest DoS tools. You first put the URL or IP address into the target box. Then click the Lock On button. You can change the settings regarding what method you choose, the speed, how many threads, and whether or not to wait for a reply. Then simply click the IMMA CHARGIN MAH LAZER button and the attack is underway.

High Orbit Ion Cannon (HOIC) is a bit more advanced than LOIC, but if anything simpler to run. Click the + button to add targets. A popup window will appear where you put in the URL as well as a few settings.

2.1 Denial of Service Attacks

The first type of attack we should examine is the denial of service (DoS). A denial of service attack is any attack that aims to deny legitimate users the use of the target system. This class of attack does not actually aim to infiltrate a system or to obtain sensitive information. It simply aims to prevent legitimate users from accessing a given system.

This type of attack is one of the most common categories of attack. Many experts feel that it is so common due to the fact that most forms of denying a service attack can be fairly easy to execute. These attacks can be executed with ease, meaning that even attackers with minimal technical skills can often successfully perform a denial of service.

The concept underlying the denial of service attack is based on the fact that any device has operational limits. This fact applies to all devices, not just computer systems. For example, bridges are designed to hold weight up to a certain limit, aircraft have limits on how far they can travel without refuelling, and automobiles can accelerate until a certain point. All of these various devices share a common trait: They have set limitations to their capacity in order to perform work. Computers are no different from these, or any other machine; they too also have limits. Any computer system, web server, or network can only handle a finite load.

How a workload (and its limits) can be defined depends on the machine. A workload for a computer system might be defined in a number of different ways, including the number of simultaneous users, the size of files, the speed of data transmission, or the amount of data stored. Exceeding any of these limits will stop the system from responding. For example, if you can flood a web server with more requests than it can process, it will overload and will no longer be able to respond to further requests. This reality underlies the DoS attack. Simply overload the system with requests, and it will no longer be able to respond to legitimate users attempting to access the web server.

2.1.1 SYN Flood

Sending a flood of pings is the most primitive method of performing a DoS. More sophisticated methods use specific types of packets. One very popular version of the DoS attack is the SYN flood. This particular attack depends on the hacker’s knowledge of how connections are made to a server. When a session is initiated between the client and server in a network using the TCP protocol, a small buffer space in memory is set aside on the server to handle the “hand-shaking” exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange.

A SYN flood attempts to disrupt this process. In this attack, the attacker sends a number of connection requests very rapidly and then fails to respond to the reply that is sent back by the server. In other words, the attacker requests connections, and then never follows through with the rest of the connection sequence. This effect leaves connections on the server half open, and reserves the buffer memory allocated, making it not available to other applications. Although the packet in the buffer is dropped after a certain period of time (usually about three minutes) without a reply, the effect of these false connection requests makes it difficult for legitimate requests to be established within a session.

2.1.2 Smurf Attack

The Smurf attack is a popular type of DoS attack. It was named after the application first used to execute this type of attack. In the Smurf attack, an ICMP packet is sent out to the broadcast address of a network, but its return address has been altered to match one of the computers on that network, most likely a key server. All the computers on the network will then respond by pinging the target computer.

ICMP packets use the Internet Control Message Protocol to send error messages on the Internet. As the address of packets are sent to a broadcast address, that address responds by echoing the packet out to all hosts on the network, that then sends it to the spoofed source address.

Continually sending such packets will cause the network to perform a DoS attack on one or more of its member servers. This attack is both clever and simple. The greatest difficulty here is to get the packets to start on the target network. This can be accomplished via certain software such as a virus or Trojan horse that will begin sending the packets.

2.1.3 Ping of Death

The Ping of Death (PoD), is perhaps the simplest and most primitive form of DoS attack. It is based on overloading the target system. TCP packets have limited size. In some cases, by simply sending a packet that is too large, it can shut down a target machine.

The aim of this attack is to overload the target system and to cause it to quit responding. The PoD works to compromise systems that cannot deal with extremely large packet sizes. If successful, the server will actually shut down. It can, of course, be rebooted.

The only real safeguard against this type of attack is to ensure that all operating systems and software are routinely patched. This attack relies on vulnerabilities in the way a particular operating system or application handles abnormally large TCP packets. When such vulnerabilities are discovered, the vendor customarily releases a patch. The possibility of PoD is amongst one of many reasons why you must keep patches updated on all of your systems.

This type of attack is becoming less common as newer versions of operating systems are able to handle the overly large packets better that Ping of Death depends on. If the operating system is properly designed, it will drop any oversized packets, thus negating any possible negative effects a PoD attack might have.

2.1.4 UDP Flood

UDP (User Datagram Protocol) is a connectionless protocol that does not require any connection setup procedure to transfer data. TCP packets connect and wait for the recipient to acknowledge a receipt before sending the next packet. Each packet is confirmed. UDP packets simply send the packets without confirmation. This allows packets to be sent much faster, making it easier to perform a DoS attack.

A UDP flood attack occurs when an attacker sends a UDP packet to a random port on the victim’s system. When the victim’s system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that no application is waiting on the port, it will generate an ICMP packet of destination, unreachable to the forged source address. If enough UDP packets are delivered to ports on the victim, the system will go down.

2.1.5 DoS Tools

One reason that DoS attacks have become so common is because a number of tools are available for executing DoS attacks. These tools are widely available on the Internet, and are in most cases free to download. This means that any cautious administrator should be aware of them. In addition to their common use as an attack tool, they can also be very useful for testing your anti-DoS security measures.

Low Orbit Ion Cannon (LOIC) is probably the most well-known and one of the simplest DoS tools. You first put the URL or IP address into the target box. Then click the Lock On button. You can change the settings regarding what method you choose, the speed, how many threads, and whether or not to wait for a reply. Then simply click the IMMA CHARGIN MAH LAZER button and the attack is underway.

High Orbit Ion Cannon (HOIC) is a bit more advanced than LOIC, but if anything simpler to run. Click the + button to add targets. A popup window will appear where you put in the URL as well as a few settings.