DOS / DDOS Attacks

What is a denial-of-service attack?

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

What are common denial-of-service attacks?

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

In a Smurf Attack, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.

A SYN flood occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect

.

Individual networks may be affected by DoS attacks without being directly targeted. If the network's internet service provider (ISP) or cloud service provider has been targeted and attacked, the network will also experience a loss of service.

What is a distributed denial-of-service attack?

A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control

numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

Botnets—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to "attack-for-hire" services, which allow unskilled users to launch DDoS attacks.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things (IoT) (see Securing the Internet of Things). IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners' knowledge.

How do you avoid being part of the problem?

While there is no way to completely avoid becoming a target of a DoS or DDoS attack, there are proactive steps administrators can take to reduce the effects of an attack on their network.

1. Enroll in a DoS protection service that detects abnormal traffic flows and redirects traffic away from your network. The DoS traffic is filtered out, and clean traffic is passed on to your network.
2. Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.
3. It is also important to take steps to strengthen the security posture of all of your internet-connected devices in order to prevent them from being compromised.
4. Install and maintain antivirus software: Install a firewall and configure it to restrict traffic coming into and leaving your computer (see Understanding Firewalls for Home and Small Office Use).
5. Evaluate security settings and follow good security practices in order to minimalize the access other people have to your information, as well as manage unwanted traffic (see Good Security Habits).

How do you know if an attack is happening?

Symptoms of a DoS attack can resemble non-malicious availability issues, such as technical problems with a particular network or a system administrator performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack:

1. Unusually slow network performance (opening files or accessing websites),
2. Unavailability of a particular website, or
3. An inability to access any website.

The best way to detect and identify a DoS attack would be via network traffic monitoring and analysis. Network traffic can be monitored via a firewall or intrusion detection system. An administrator may even set up rules that create an alert upon the detection of an anomalous traffic load and identify the source of the traffic or drops network packets that meet a certain criteria.

What do you do if you think you are experiencing an attack?

If you think you or your business is experiencing a DoS or DDoS attack, it is important to contact the appropriate technical professionals for assistance.

Contact your network administrator to confirm whether the service outage is due to maintenance or an in-house network issue. Network administrators can also monitor network traffic to confirm the presence of an attack, identify the source, and mitigate the situation by applying firewall rules and possibly rerouting traffic through a DoS protection service.

Contact your ISP to ask if there is an outage on their end or even if their network is the target of the attack and you are an indirect victim. They may be able to advise you on an appropriate course of action.

In the case of an attack, do not lose sight of the other hosts, assets, or services residing on your network. Many attackers conduct DoS or DDoS attacks to deflect attention away from their intended target and use the opportunity to conduct secondary attacks on other services within your network.