Learn about DoS and DDoS denial of service attacks

Denial of service attacks can be difficult to distinguish from network activities, but there are many signs to detect these attacks and TipsMake.com will introduce some of them.

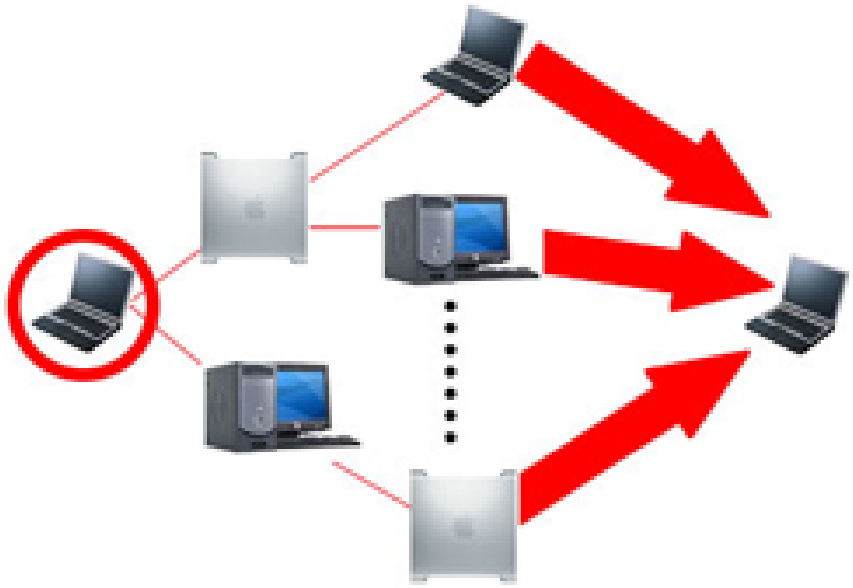
You may have heard of a denial of service attack and may have been a victim of this attack. Denial of service attacks can be difficult to distinguish from network activities, but there are many signs to detect these attacks and TipsMake.com will introduce some of them.

What is DoS denial of service attack?

DoS stands for English phrase Denial of Service, Vietnamese meaning is denial of service. DoS denial of service is a security event that occurs when an attacker acts to prevent legitimate users from accessing computer systems, devices or other network resources.

In denial-of-service attacks, an attacker targets computers and uses the computer network you are using to prevent access to email, websites, online accounts (such as banks) and services. other.

The most obvious and common type of Dos is that an attacker "massively" attacks traffic on the server, system or network, depleting the victim's resources, making it difficult for legal users or even unable to use them. More specifically, when you enter the URL of a website into the browser, you are sending a request to the site's server to view it. The server can only handle certain requests over a period of time, so if an attacker sends a lot of requests to the server it will overload it and your request is not processed. . This is a 'denial of service' type because it makes it impossible for you to access that page.



An attacker can use spam to perform similar attacks on your email account. Whether you have an email account provided by your employees or available through a free service such as Yahoo or Hotmail, there is still a limit to the amount of data in your account. By sending multiple emails to your account, an attacker can consume all the mail and prevent you from receiving other mail.

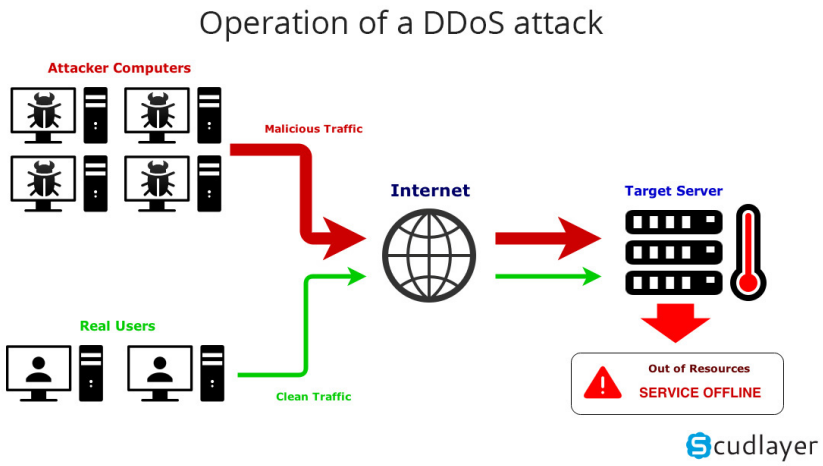
What is DDoS distributed denial of service attack?

DDoS stands for Distributed Denial of Service, the Vietnamese meaning is to deny distributed services. DDoS attack is an attempt to crash an online service by flooding it with traffic from multiple sources.

In distributed denial of service (DDoS) attacks, an attacker can use your computer to attack other computers. By taking advantage of security vulnerabilities and ignorance, this person can gain control of your computer. They then use your computer to send large amounts of data to a website or send spam to a certain mailbox address. This attack is called 'distributed' because an attacker uses multiple computers including your computer to perform Dos attacks.

Although DDoS provides a less complex attack mode than other types of network attacks, they are becoming more powerful and sophisticated. There are three basic types of attacks:

1. Volume-based: Use high traffic to flood network bandwidth
2. Protocol: Focus on exploiting server resources
3. Application: Focus on web applications and is considered the most sophisticated and serious attack



Current popular denial of service attacks

SYN Flood:

SYN Flood exploits weaknesses in TCP connection strings, called three-way handshakes. The server will receive a sync message (SYN) to start "shaking hands". The server receives the message by sending an acknowledgment flag (ACK) to the original host, then closing the connection. However, in a SYN Flood, the fake message is sent and the connection is not closed => the service collapses.

UDP Flood:

User Datagram Protocol (UDP) is a network protocol that does not session. A UDP Flood targets random ports on the computer or network with UDP packets. The server checks the application at those ports but no applications are found.

HTTP Flood:

HTTP Flood is almost like legitimate GET or POST requests exploited by a hacker. It uses less bandwidth than other types of attacks, but it can force the server to use the maximum resources.

Ping of Death:

Ping of Death controls IP protocols by sending malicious code to a system. This type of DDoS was popular two decades ago but was no longer effective at the present time.

Smurf Attack:

Smurf Attack Internet Protocol (IP) and ICMP (Internet Control Message Protocol) uses a malware program called smurf. It spoofs an IP address and uses ICMP, then pings IP addresses on a given network.

Fraggle Attack:

Fraggle Attack uses a large amount of UDP traffic to the router's broadcast network. It's like a smurf attack, using UDP more than ICMP.

Slowloris:

Slowloris allows an attacker to use minimal resources in an attack and targets on the web server. Once connected to the desired goal, Slowloris keeps the link open for as long as possible with HTTP overflow. This attack was used in some high-end hacktivist DDoSing (political attack), including the 2009 Iranian presidential election. Minimizing the impact on this type of attack is very hard.

Application Level Attacks:

Application Level Attacks exploit vulnerabilities in applications. The goal of this type of attack is not the entire server, but applications with known weaknesses.

NTP Amplification:

NTPAmplification exploits NTP (Network Time Protocol) servers, a protocol used to synchronize network time, flooding UDP traffic. This is the reflection attack is amplified. In any reflection attack, there will be a server response to the fake IP, when amplified, the response from the server will no longer match the initial request. Because of the large bandwidth used when DDoS is used, this type of attack is destructive and high volumne.

Advanced Persistent DoS (APDoS):

Advanced Persistent DoS (APDoS) is a type of attack used by hackers with the desire to cause serious damage. It uses many types of attacks mentioned earlier, HTTP Flood, SYN Flood, etc.) and often targets attacks by sending millions of requests per second. APDoS attacks can last for weeks, depending on the hacker's ability to switch tactics at any time and create diversity to avoid security protections.

Zero-day DDoS Attacks:

Zero-day DDoS Attacks are names assigned to new DDoS attack methods, exploiting unpatched vulnerabilities.

HTTP GET

HTTP GET is an Application Layer attack, smaller in scale and targeted to more targets. Application Level Attacks exploit vulnerabilities in applications. The goal of this type of attack is not the entire server, but applications with known weaknesses. This type of attack will target the 7th Layer in the OSI model. This is the class with the highest network traffic, instead of looking into the third layer, it is often chosen as the target in Bulk Volumetric attacks. HTTP GET exploits the process of a certain web browser or HTTP application and requests an application or server for each HTTP request, either GET or POST. HTTP Flood is almost like legitimate GET or POST requests exploited by a hacker. It uses less bandwidth than other types of attacks, but it can force the server to use the maximum resources. It is difficult to resist this type of attack because they use standard URL requests, instead of broken or large volumes.

How to avoid denial of service attacks?

There is really no specific measure to avoid becoming a victim of DoS or DDoS. However, we will show you a few steps with the purpose of somewhat reducing the type of attack that will use your computer to attack another computer.

1. Install and maintain antivirus software.
2. Install a firewall and configure it to limit traffic to and from your computer.

3. Follow the safe practice guidelines for distributing your email address.
4. Use email filters to help you manage unwanted traffic.

Specifically, for example, for a data center, the following preventive measures should be implemented:

ISPs often have DDoS protection in Layer 3 and Layer 4 (network traffic), but ignore Class 7, which is targeted more, and in general, the uniformity of the protection layers is not possible either. guaranteed.

Companies that handle DDoS: they use their existing infrastructure to combat any threats to them. Usually, this is done through load balancer, content distribution network (CDN) or a combination of both. Smaller sites and services may hire outside of third parties if they do not have the capital to maintain a variety of servers.

DDoS providers are always available. Usually, they will reroute your incoming traffic through their own system and "scour" it to combat known attacks. They can scan suspicious traffic from sources or from uncommon geolocation. Or they can re-route your legitimate traffic from botnet sources.

Most modern firewalls and Intrusion Protection Systems (IPS) provide protection against DDoS attacks. These devices can be in the form of a single device that scans all traffic to the system or software distributed at the server level. Dedicated anti-DDoS applications are also available on the market and can better protect against Class 7 attacks.

Regular network scanning and traffic monitoring with alerts can also help you understand the risks of an early DDoS attack, as well as take actions to minimize the damage.

Get to know Dos attacks and DDos

Not a complete collapse of the service is also the result of a denial of service attack. There are many technical problems with a network or with administrators performing maintenance and management. However, with the following symptoms, you can recognize DoS or DDoS attacks:

1. Exceptionally slow network execution (opening files or accessing websites)
2. Do not access the website you still see
3. Cannot access any website
4. The number of messages increases dramatically in your account.

What to do if you think you are being denied a service attack?

Whether you have correctly identified a DoS or DDoS attack, you cannot determine the source or destination of the attack. Therefore, you should contact technical experts for assistance.

1. If you find that you cannot access your own files or go to any extended website from your computer, you should contact the network administrator of that network. This may indicate whether your computer or the organization's network is being hacked.
2. If you see problems on your own computer, contact your service provider (ISP). If there is a problem, the ISP may advise you to take appropriate actions.

Inspection and preparation work in DDoS response in data centers

When you own a DDoS protection system in place, the first step is to identify attack methods and critical applications. Which port is open? Which bandwidth is available for you to use? Where is the network congestion possible? What important systems need additional protection?

Pay more attention to vulnerable areas based on dependence on other systems in your infrastructure, such as a central database that can remove functionality for some applications. in case it is overloaded.

There are many open source software tools that you can use to test DDoS mitigation, as well as hardware options that can reach multi-gigabit traffic. However, hardware options will be an expensive solution. Instead, a professional white hat security company can provide you with testing as an optional service.

DDoS attacks are sure to cause a lot of trouble, but with careful preparations, you can be prepared to prevent or offer solutions quickly, thereby avoiding interruptions. service for users while significantly reducing the damage that DDoS causes.