7 categories to prevent denial of service attacks

Denial of Service (DDoS) attacks will always be the top threat to systems around the world. Technically, we can only hope that attackers use tools and have a poor understanding of protocols to be able to

Denial of Service (DDoS) attacks will always be the top threat to systems around the world. Technically, we can only hope that attackers use tools and have a poor understanding of protocols to be able to identify and eliminate traffic that triggers an attack. One thing everyone acknowledges is that if DDoS is done by a qualified hacker, defending is impossible.

Four years ago, the world's official hackers died of this attack technique and put an end to all research-demonstration or dispersal tools because they themselves also saw the level of danger and injustice. equal to this type of attack.For a class hacker, 'Hacking is get root!'

With a very weak network infrastructure, along with e-commerce and early formation, DDOS will be a huge threat to Vietnam's internet.All members of the Vietnamese internet community should have a genuine look and action, DDOS is a very meaningless action in every way!

Denial of Service (DoS) attacks are attacks on the network that prevent access to a service.DoS attacks destroy network services by flooding the number of connections, server overloads or programs running on the server, consuming server resources, or preventing legitimate users from accessing network services.

There are many ways to perform denial-of-service attacks, so there are many ways to classify DoS.

Common classification is based on the protocol of DoS attack, such as flooding ICMP with Smurf, Ping of Death, exploiting the weakness of TCP in protocol operation and packet fragmentation with SYN flood, LanD attacks, TiaDrop or above service level as with Flash Crowds (in Vietnam often known as X-flash).

Sorting by attack method, DoS can be executed by several single packets sent directly to the disruptive server that operates (such as slammer worm), or activated to send from multiple sources (deny distributed services Canopy - DoDS).Attack can be done on the Internet (using web servers), or broadcast within the network (insider attacks - like with Blaster worm), on P2P (P2P index poinsioning) or Wireless (WLAN authentication rejection attack-) spoof sender).However, it can be seen that the above classification is based mainly on the view from the attack generation, and therefore, does not systematize the prevention method.

Most commonly, there are 7 categories of organizations to consider when dealing with DoS threats as follows:

1 / Prevent application weaknesses (Application Vulnerabilities)

Weak points in the application layer can be exploited causing a buffer overflow leading to a broken service.The error is mainly found on Windows intranet applications, on webserver, DNS, or SQL database programs.Patching is one of the important requirements for prevention.During the time when the entire network cannot be updated, the system must be protected by a virtual patch (virtual patch).In addition, the system needs to specifically consider the content exchange requirements between the client and server, to prevent the server from being attacked through indirect components (eg SQL injection).

2 / Prevent the recruitment of zombies

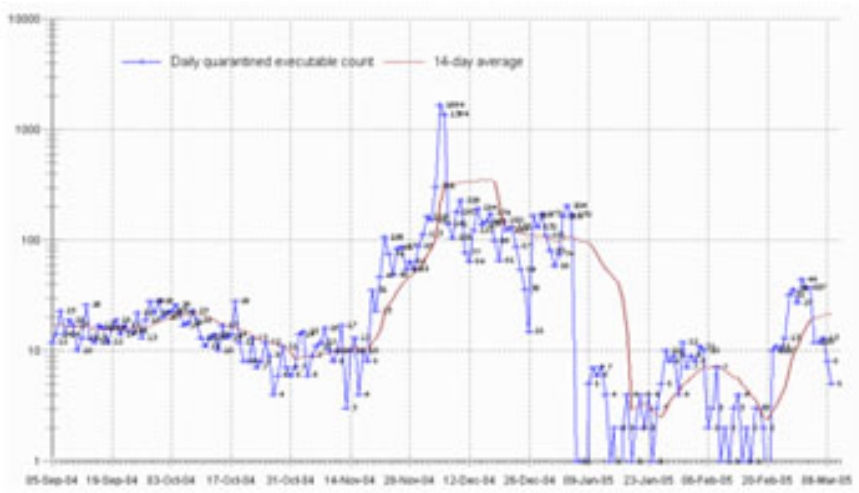
Zombies are objects that are used to become attackers.Some typical cases are via rootkits (Sony or Symantec), or active components included in mail, or web pages, such as using jpeg files to exploit errors of image processing software, The code is attached to a flash file, or a trojan installed under phishing, or through the spread of worms (Netsky, MyDoom, Sophos).As a defense, the network needs content filtering and monitoring tools to prevent hacker recruitment.

3 / Preventing the channel to launch attacks using tools

There are a lot of automated DoS attack tools, mainly DDoS distributed attacks such as TFN, TFN2000 (Tribe Flood Network) attacks based on the principle of Smurf, UDP, SYN, or ICMP;Trinoo for UDP flood;Stacheldraht for TCP ACK, TCP NULL, HAVOC, DNS flood, or flooded with TCP random packet headers.These tools have the characteristics of needing channel launches for zombies to attack to a specific destination.The system needs to be monitored and prevented by those channels.

4 / Prevent attack on bandwidth

When a DDoS attack is launched, it is often detected based on a significant change in the composition of network traffic.For example, a typical network may have 80% TCP and 20% UDP and ICMP.This statistic if there is a significant change may be a sign of an attack.The Slammer worm will increase UDP traffic, while Welchi worm will generate ICMP flooding.The dispersion of traffic is caused by those worms that damage the router, firewall, or network infrastructure.The system needs tools to monitor and coordinate bandwidth to minimize the impact of this attack.



5 / Prevent attacks via SYN

SYN flood is one of the oldest surviving attacks to the present, although its harm is not reduced.The key to preventing this attack is the ability to control the number of SYN-ACK requests to the network.

6 / Detect and prevent critical attacks from connecting

The servers themselves have a critical amount that responds to connections to it.Even the firewall itself (especially for firewalls with stateful inspection capabilities), connections are always attached to the state table with capacity limits.Most attacks generate virtual connections through spoofing.To prevent this type of attack, the system needs to analyze and resist spoofing.Limit the number of connections from a specific source to the server (quota).

7 / Detect and prevent critical attacks on connection setup speed

One of the points that servers often take advantage of is the ability of limited buffers to establish a connection speed, resulting in overload when subjected to a sudden change in the number of connections.Here the

application of filters to limit the number of medium connections is very important.A filter determines the connection speed threshold for each network object.Usually, this is equal to the number of connections in a given time to allow for fluctuations in traffic.

The above analysis is based on the following basic implications for system protection.

First , it is the protective devices that need to be placed on the information flow and directly implement the prevention.This comes from the reason for the speed of an attack (for example, about 10,000 member registrations over 1s towards a server, or spreading worms at 200ms on a 100M Ethernet network).With such a speed, the way to prevent form detection - blocking message (Shun Host and TCP Reset) is no longer appropriate.

Second,denial-of-service attacks are primarily aimed at the processing capabilities of network systems, first of all information security devices.IPS processing capabilities or content filtering components are one of the points of interest, especially in the stability of concurrent processing of mixed traffic types with variable packet sizes.

Third , attacks are always blended with a combination of different methods.Therefore, the importance of preventing simple signs of infection is the first step to preventing denial-of-service attacks.

In the overall security system, to deal with denial-of-service attacks, the IPS component is considered to be the most important for users to be transparent, so analyzing the flow of information exchanged between The server and the user are not affected by the attacks directed towards it.

Below is a summary of NSS reports, the organization examines the ability of network devices in an emulated attack environment for leading firms' IPS devices.

- TopLayer Attack Mitigator IPS

As the name implies, this device performs offensive attacks, not necessarily preventing attacks.That's why the latency is high in the attacked environment.Toplayer is recommended when used for the right purpose as an attack transfer device.

- ISS Proventia G

ISS Proventia G shows the ability to respond to most types of attacks with low latency, except for DoS with small packets.ISS Proventia can be used in internal network with non-Gigabit infrastructure.

- McAffee IntruShield

MacAffee IntruShield is a rated device that meets the requirement for full coverage of attack signals as well as low latency levels.

- TippingPoint UnityOne

This is the only device that NSS provides NSS Gold certification (compared to the other NSS Approve certificates).In addition to meeting the latency criteria and the ability to detect attacks, UnityOne is better than McAffee IntruShield for predictive response (predictable response) with every attack.

You finished reading the article "**7 categories to prevent denial of service attacks**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com