Easy Linux

Knowledge is to be shared

Tuesday, March 19, 2013

Finding DDOS attacks

Finding DDOS attacks

Below are some of the useful netstat commands to check during DDOS attack.

To list the connections to the target IPs (server's IP's) use the below command :

netstat -alpn | grep :80 | awk '{print \$4}' |awk -F: '{print \$(NF-1)}' |sort |uniq -c | sort -n

To list the connections from source IP's use the below command:

netstat -alpn | grep :80 | awk '{print \$5}' |awk -F: '{print \$(NF-1)}' |sort |uniq -c | sort -n

To see the state of each connection and the value use the below command:

Search This Blog

Search

Popular Posts

the requested url /phpmyadmin was not found on this server webmin in debian

Hello. If you found the error as the requested url /phpmyadmin was not found on this server, then please try to do the following step...

Installing Mp4box in centos 6

Login to the server cd /usr/local/src/ Now we need to download the

netstat -an|grep ":80"|awk '/tcp/ {print \$6}'|sort| uniq -c

You can use topdump to identify the attacker too:

tcpdump -c -n -i eth"x" -p host IP Address

where x can be 0 or 1,n=number(100 or 1000). If it is a VPS, it can be venet0 too. Check the Output of ifconfig.

To check if a server is under a DoS attack with netstat, it's common to use:

netstat -ntu | awk '{print \$5}' | cut -d: -f1 | sort | uniq -c | sort -n|wc -l

If the output of below command returns a result like 2000 or 3000 connections!, then obviously it's very likely the server is under a DoS attack.

To detect a SYN flood with netstat:

netstat -nap | grep SYN | wc -l

If the output returns a value of 1032,1032 SYNs per second is quite a high number and except if the server is not serving let's say 5000 user requests per second, therefore as the above output reveals it's very likely the server is under attack, if however I get results like 100/200 SYNs, then obviously there is no SYN flood targetting

Checking if UDP Denial of Service is targetting the server :

netstat -nap | grep 'udp' | awk '{print \$5}' | cut -d: -f1 | sort |uniq -c |sort -n

The above command will list information concerning possible UDP DoS.

The command can easily be accustomed also to check for both possible TCP and UDP denial of

packages and libraries of MP4Box wget http://downloads. sourcefo...

Finding DDOS attacks

Finding DDOS attacks Below are some of the useful netstat commands to check during DDOS attack. To list the connections to the target IP...



mail accounts in webmin

Creating Email accounts in webmin First you have to look if Postfix and Dovecot are propely configured. Step 1 >> Add a Webmin use...

How to fix incorrect disk usage showing for a user in Cpanel

A customer complains that their reported disk usage is too service, like so:

netstat -anp |grep 'tcp\|udp' | awk '{print \$5}' | cut -d: -f1 | sort | uniq -c | sort -n

You can see the output as:

104 109.161.198.86

115 112.197.147.216

129 212.10.160.148

227 201.13.27.137

3148 91.121.85.220

If after getting an IP that has too many connections to the server and is almost certainly a DoS host you would like to filter this IP.

Here is how I remove hosts to not be able to route packets to my server:

route add 110.92.0.55 reject

The above command would null route the access of IP 110.92.0.55 to my server.

Later on to look up for a null routed IP to my host, I use:

route -n |grep -i 110.92.0.55

Block the IPs with high connection above using CSF or APF firewall:

csf -d IP {reason}

apf -d IP

Posted by Unknown at 5:51 PM



No comments:

high, that they are not using so much space. What do you do? 1. Get their...

Installing Flvtool2 in Centos 6

Installing Flvtool2 in Centos 6 You can install the module via ruby setup cPanel offers a script to install ruby /scripts/installrub y...

(no title)

Installing Ioncube loader, EAccelerator, Zendopt, SourceGuardian, PHPSuHosin To install Ioncubeloader: #/scripts/phpexte nsionmgr install

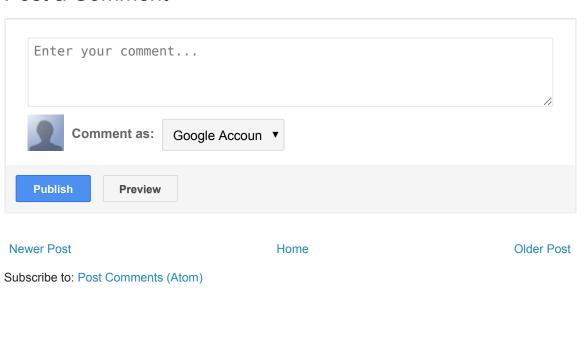
GPG key retrieval failed

GPG key retrieval failed: [Errno 14] Could not open/read file:///etc/pki/rpmgpg/RPM-GPG-KEY-rpmforgedag rpm --import http://apt.sw.be/R

..

Tuning Mysql Performance with Mysql tuner

Post a Comment



Tuning Mysql
Performance with
Mysql tuner
MYSQL Tuner:It is a perl script
that analyzes the
MYSQL
performance and
based on the
statis...

Server Error in '/' Application.

Compiler Error Message: The compiler failed with error code 1. The issue occurs due to a change that updates all the application pool 3...

Translate

Select Language

Powered by Google Translate

Simple theme. Powered by Blogger.