DDoS Deflate and APF (Advanced Policy Firewall):A Report

Dr.S.Brilly Sangeetha

Head of the Department ,Department of CSE,IES College of Engineering
Chittilappilly,Thrissur,Kerala,India.

Abstract *The article helps to find solutions to totally slow network, websites loading was 10-20sec, slow loading, server load is very high and there are many clients who is doing problems. After connection made to the server and checking statistics - server CPU will remain all the time on 20-30%, memory was fine, all services were up-and-running so where it went wrong? There was so many connections from some IPs that was like wow...after blocking them, server statistics is back to normal again (probably some kind of DDOS attack) At this point, since Plesk donot have something like CSF on cPanel, being able to understand that the system need something to block this "Fake" IPs or at least the ones with a lot of connections automatically, without my concern doing it manually. Hence this paper helps inproviding the knowledge installing successfully (DDOS Deflate and APF (Advanced Policy Firewall).*

Keywords *APF (Advanced Policy Firewall), statistics, DDoS-Distributed Denial of service.*

I. Introduction

DOS/DDOS stands for Denial of Service/Distributed Denial of Service. DOS or DDOS is considered as a type of attack which is unavailable to its intended programmers. This is one of the most commonly known and very frequently occurring attacks in these days due to the ambience supply of various tools. Through the Google search, anyone can be accessed to thousands of DOS tools which are free of cost available on the Internet. It is very easy to use those available tools, even for beginners. These tools perform a DDOS attack by sending the UDP, TCP or HTTP requests from the master server to the victim server and the only thing is the system need to know the “URL or IP” of the server, and those tools will do rest of the job by faking it. Due to all this, the usage of DOS attack has increased exponentially in the past few years. Therefore it is highly required to create a safeguard measure which can at least help to protect the servers from these types of attacks.

The DDOS attack is mainly classified into three types:

- Application Layer DDOS attack
- Protocol DDOS attack
- Volume based DDOS attack

So, in this paper, there is a necessary to introduce a small script based tool “DOS Deflate” which helps to fight against these type of attacks.

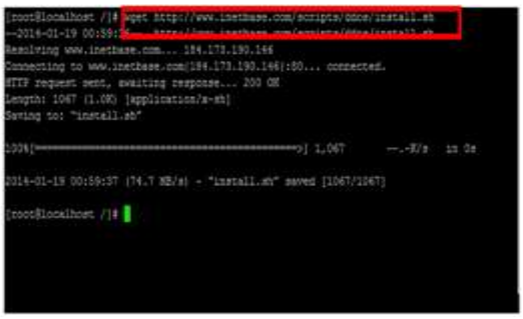
Application Layer DDOS:

Though it do not safeguard the system fully against large DDOS attacks, it is very helpful. DDOS deflate is considered as a lightweight bash shell script designed to help in the process of blocking a denial of service attack. It commonly tracks and monitors all the IP addresses making connections to the server by the netstat command. Whenever it detects the attack ,ie) number of connections from a single node that exceeding certain limits which are defined in the prescribed configuration file, the script will automatically go and block that IP address by the IP tables or APF based on the the configuration.

II. CONFIGURATION OF DDOS DEFLATE

Step 1:

First thing to remember is to download the installer script file, which is already available on the DDOS Deflate website through the wget utility. Open the terminal and then go with typing the following command

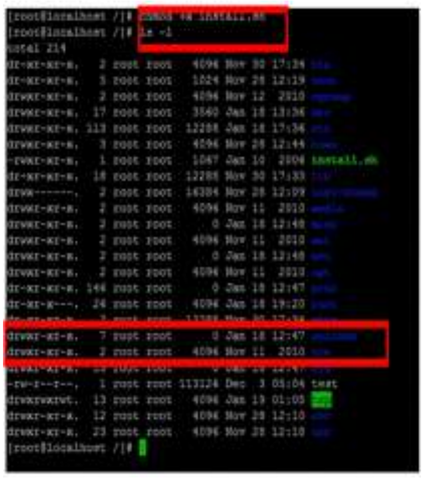


```
[root@localhost /]# wget http://www.inetbase.com/scripts/ddos/install.sh
--2014-01-19 00:59:37--  http://www.inetbase.com/scripts/ddos/install.sh
Resolving www.inetbase.com... 184.173.190.146
Connecting to www.inetbase.com|184.173.190.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1067 (1.0K) [application/x-sh]
Saving to: "install.sh"

100%[======================================>] 1,067       --.-K/s   in 0s

2014-01-19 00:59:37 (74.7 MB/s) - "install.sh" saved [1067/1067]

[root@localhost /]# 
```

Then after this the Installer script file “Install.sh” has been successfully downloaded. Check the downloaded files by using the ls-l command.

Step 2:

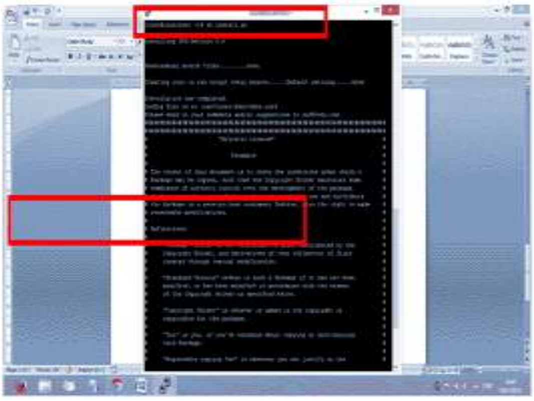
As it can be seen, the downloaded files does not have executable(process) permission. So there is a need to make it processable . This can be done by using the following command. chmod +x install.sh



```
[root@localhost /]# chmod +x install.sh
[root@localhost /]# ls -l
total 214
dr-xr-xr-x.   2 root root   4096 Nov 30 17:34 [illegible]
dr-xr-xr-x.   5 root root   1024 Nov 28 12:19 [illegible]
drwxr-xr-x.   2 root root   4096 Nov 12  2010 [illegible]
drwxr-xr-x.  17 root root   3560 Jan 18 13:36 [illegible]
drwxr-xr-x. 113 root root  12288 Jan 18 17:36 [illegible]
drwxr-xr-x.   3 root root   4096 Nov 28 12:44 [illegible]
-rwxr-xr-x.   1 root root   1067 Jan 10  2006 install.sh
dr-xr-xr-x.  18 root root  12288 Nov 30 17:33 [illegible]
drwx------.   2 root root  16384 Nov 28 12:09 [illegible]
drwxr-xr-x.   2 root root   4096 Nov 11  2010 [illegible]
drwxr-xr-x.   2 root root      0 Jan 18 12:48 [illegible]
drwxr-xr-x.   2 root root   4096 Nov 11  2010 [illegible]
drwxr-xr-x.   2 root root      0 Jan 18 12:48 [illegible]
drwxr-xr-x.   2 root root   4096 Nov 11  2010 [illegible]
dr-xr-xr-x. 144 root root      0 Jan 18 12:47 [illegible]
dr-xr-x---.  24 root root   4096 Jan 18 19:20 [illegible]
drwxr-xr-x.   7 root root      0 Jan 18 12:47 [illegible]
drwxr-xr-x.   2 root root   4096 Nov 11  2010 [illegible]
-rw-r--r--.   1 root root 113124 Dec  3 05:04 test
drwxrwxrwt.  13 root root   4096 Jan 19 01:05 [illegible]
drwxr-xr-x.  12 root root   4096 Nov 28 12:10 [illegible]
drwxr-xr-x.  23 root root   4096 Nov 28 12:10 [illegible]
[root@localhost /]#
```

STEP 3:

Then after opting the executable permission, the system has to run the install.sh file. This makes the system defaultly install DOS Deflate in the appropriate system

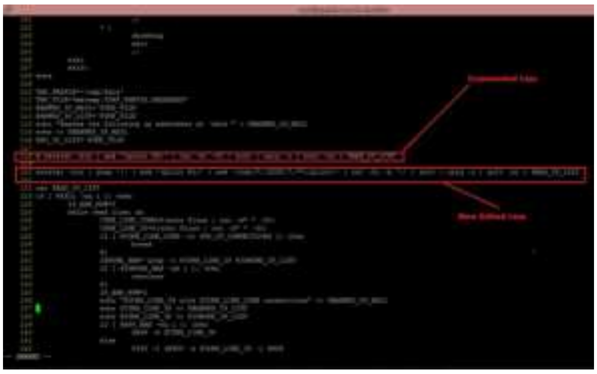


Now it is found that DDOS Deflate has been successfully installed in the master system. Check and make sure that the DOS Deflate files are in /var/local/ddos/ . There are three important files in the DDOS. First is the ddos. conf file where all tool configurations can be set as part of the prescribed requirement. The second file is ddos.sh, the main script file for the tool analysis, and third is the ignore.ip.list file, that is the IP white listed file where the system can define the IP addresses which is needed to be excluded through this tool analysis. Along with the installation of these , a Cron file is automatically formed in the /etc/cron.daily folder that may run every minute, as the default configuration is set as 1 min. But the configuration may be changed from time to time on the ddos.conf file. This file is used to check all IP connections on the server also.

STEP 4:

Firstand foremost the system will change some commands in the main ddos.sh file making the tool more effective. To do this, the system need to open the ddos file with the intervention of the editor and comment it on the line 118 by adding the '#' symbol before the line and scribble the following command:

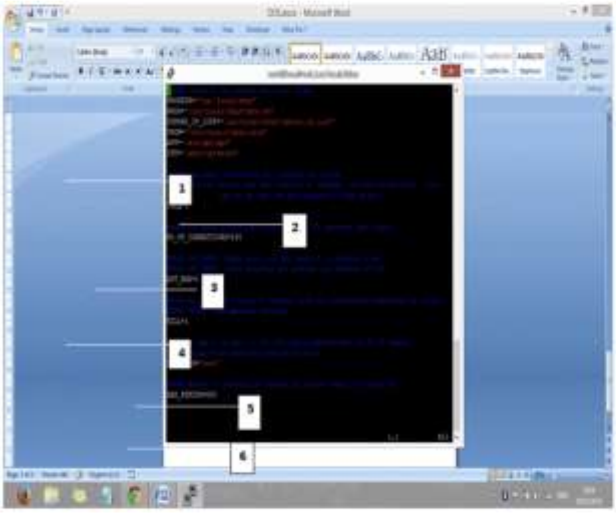
```
netstat -ntu | grep ':' | awk '{print $5}' | awk
'{sub("::ffff:","");print}' | cut -f1 -d ':' | sort | uniq -c |
sort -nr > $BAD_IP_LIST
```



The system may be able to act as this command is the heart of the DOS Deflate tool. This command is eligible of counting the total number of connections for every IP address connected to the master server.

STEP 5

After installing of the DDOS Deflate tool, the system has to configure this in the opt manner. In order to do this task efficiently, the system has to open the ddos.conf file in the VI editor as shown below.



In the above shown figure, It is described by numbers to indicate each configuration for more better understanding of the users or programmers. Each point is defined here as follows.

1. The system will start by configuring the frequency or bandwidth of the script. By default settings, the frequency is set to 1and reset to 0 , which means that the DDOS deflate script will run every minute without finding fault. The system can make changes to this configuration according to predefined requirement.

2. After setting the target frequency, the system has to set a limit based criteria for the total number of connections, in which the system has to define the maximum number of connections for an IP address. The default number of nodes is set to 200. If an IP address attains the maximum count of node limit, then DDOS Deflate treats the IP address as a bad IP address and blocks it accordingly.

3. In the area of above mentioned , the system has to define the firewall concept which we will be used to ban the bad IP addresses. DDOS Deflate supports two kinds of firewalls – APF firewall and IP tables. As it is discussed already, IP tables is by default installation process on the Linux machine. So the system will use IP tables to stop the bad IPs. By default it is set to 1and reset to 0. There can be a transition from 1 to 0.

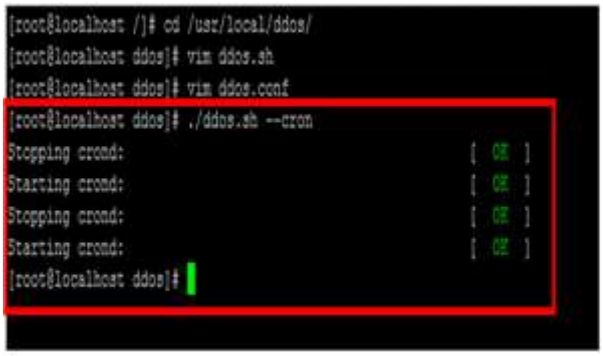
4. DDOS Deflate runs in two types of modes. First and foremost is the interactive mode where DDOS Deflate will not stop the bad IPs, It will only send an electronic mail when the maximum number of nodes are reached. In the second mode it will stop the IP address according to the above mentioned settings and also send the electronic mail. So, if the system want to test the tool, just run the above tool in interactive mode. To set the interactive mode, the system has to set the value to 0, and reset the value to 1. By default it is set to 1.

5. As mentioned above, the system has to define the electronic mail address. When an IP address is stopped by DDOS deflate, an email will be sent to the mentioned email address. By default it is set to root or parent. The system can give any email address in place of root or parent.

6. When the IP Address is stopped, to define the stop time also. The stop time should be defined in seconds as per the basic need and the criteria used. By default it has been set to 300 seconds. It means that the bad IPs will be stopped only for 5 minutes.

STEP 5

After configuring the script in the language known the system has to restart the DDOS Deflate script language.

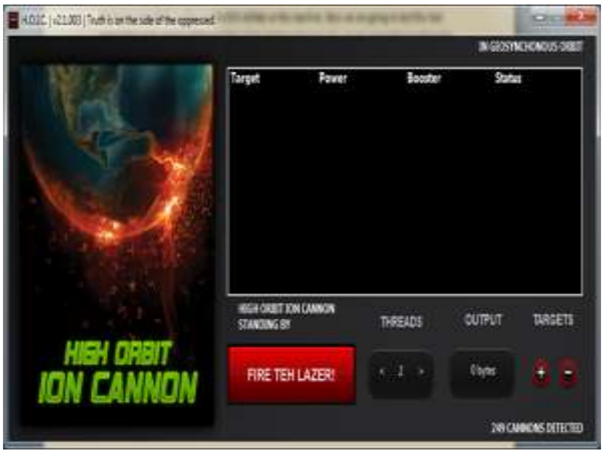


```
[root@localhost /]# cd /usr/local/ddos/
[root@localhost ddos]# vim ddos.sh
[root@localhost ddos]# vim ddos.conf
[root@localhost ddos]# ./ddos.sh --cron
Stopping crond:                                            [  OK  ]
Starting crond:                                            [  OK  ]
Stopping crond:                                            [  OK  ]
Starting crond:                                            [  OK  ]
[root@localhost ddos]#
```

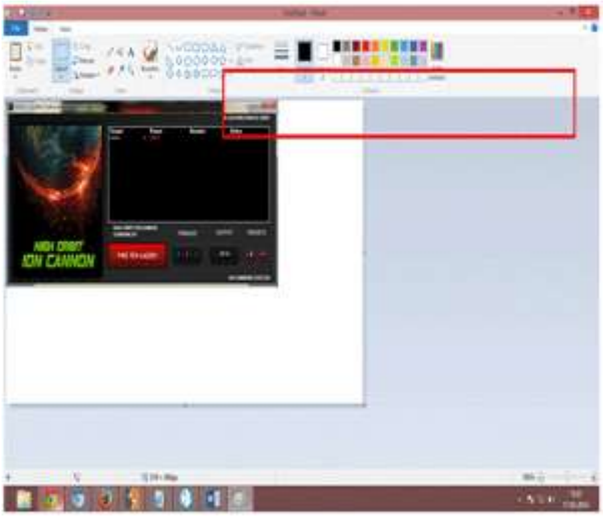
The system has successfully configured the DDOS Deflate on the server or remote machine. Now, the system is going to test the tool against the most important common DDOS attacking tools. Some of the frequently used DDOS attacking tools are being used to launch the DDOS attack and are very easily available on the Internet services or under various search engines. The list is mentioned below.

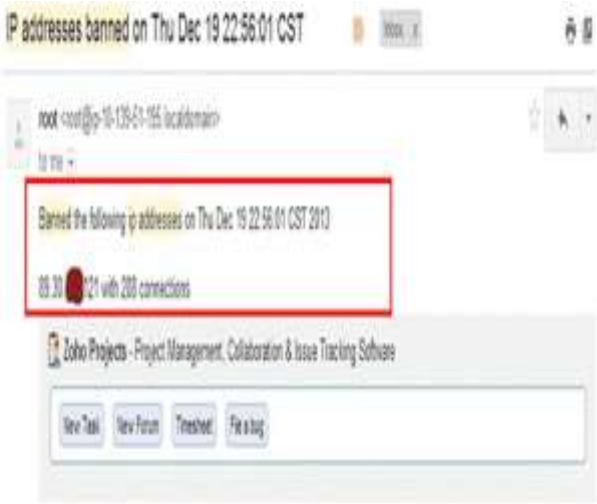
1. HOIC (High Orbit Ion Canon)
2. LOIC (Low Orbit Ion Canon)
3. XOIC
4. R-U-DEAD-Yet
5. Pyloris
6. OWASP DOS HTTP Post
7. GoldenEye HTTP Denial of Service Tool
8. Slowloris HTTP Dos

Here, the system are testing DDOS Deflate against HOIC. It is one of the most popular and challenging task ever seen before .DDOS attacking tools are freely available on the Internet or under various search engines. The tool is really easy to use even for a beginner to start up their process. The system can download the tool from the URL noted below.
https://mega.co.nz/#!IMw0iCJY!Hg5oQHdQu9FLZcbCJ_HTi1X0F98djiXDLLjWs2N6SIk
After downloading the tool by using search machine , the system need to extract it into the folder or a copy in drive and open it by clicking the hoic.exe file. Then the following HOIC interface will be obtained.



Now, the system need to connect the IP Address or the URL of the server or host machine in which the system has configured the DDOS Deflate. After adding the target or remote URL, the system needs to see this URL in the target or remote section. Then, click ok on the "FIRE THE LAZER" icon and it will start the DDOS attack on the server. After 5 minutes the system will receive an email at the email address which was provided earlier in the server configuration, stating that the IP address has been stopped in the server or host machine.





IP addresses banned on Thu Dec 19 22:56:01 CST

root <root@ip-10-139-51-195.localdomain>

to me

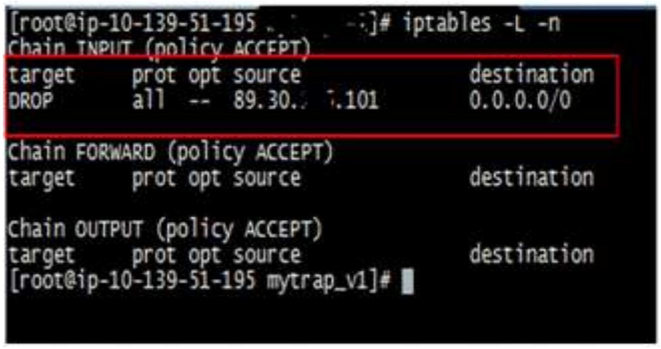
Banned the following ip addresses on Thu Dec 19 22:56:01 CST 2013

89.30.[redacted]21 with 200 connections

Zoho Projects - Project Management, Collaboration & Issue Tracking Software

The system can also have the right to check the stopped IP address by logging in to the server or host machine and checking the IP tables. The system can check the IP tables status by the following command.

iptables -L –n

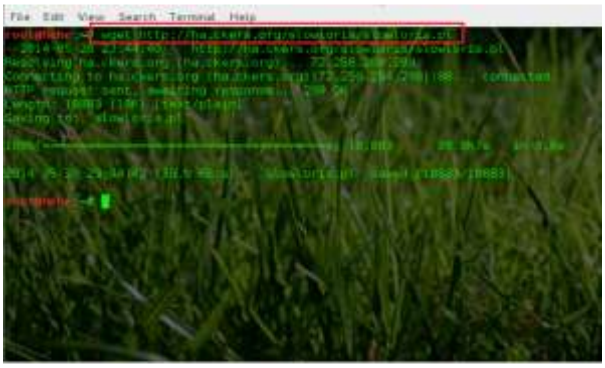


```
[root@ip-10-139-51-195 .  .    ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  89.30.[redacted].101         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@ip-10-139-51-195 mytrap_v1]#
```

As shown in above screen there are various screen shot that DDOS Deflate has stopped the current IP address through the IP tables in which the system had started the HOIC DOS tool.

Another widely used DDOS attacking tool is Slowloris HTTP DOS. It was developed in Python programming. It has some of the very good and best features in it. The tool is available in two platforms,Windows and Linux platforms, but the system will use the Linux platform only of the tool as it is suitable to handle all types of risk management. The system can download the available Python programs based tool by running the command below.

wget http://ha.ckers.org/slowloris/slowloris.pl



```
root@bt:~# wget http://ha.ckers.org/slowloris/slowloris.pl
--2014-05-28 23:44:40--  http://ha.ckers.org/slowloris/slowloris.pl
Resolving ha.ckers.org (ha.ckers.org)... [illegible]
Connecting to ha.ckers.org (ha.ckers.org)|[illegible]|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18883 (18K) [text/plain]
Saving to: `slowloris.pl'

100%[=====================================>] 18,883      [illegible]   in [illegible]

2014-05-28 23:44:40 ([illegible]) - `slowloris.pl' saved [18883/18883]

root@bt:~# 
```

After downloading the tool, the system will make it sure whether it can be executable, then give the following command which will launch it on the URL.

1. ./slowloris.py –dns <URL of the Server>
2. ./slowloris.py –dns <URL of the Server>

III.DDoS Deflate A Protection Against DDoS Attacks

Distributed Denial of service (DDoS) attacks are attacks that are vulnerable attacks on the network properties to provide denial of services to legitimate users. When these attacks seems to shoot from different distributed sources, they become distributed denial of service (DDoS) attacks.

Long back, it was very common to use spoofing techniques where a hacker could actually use very few machines (or just one machine) as a spoof machine and spoof mutliple IP addresses. To find the proper attacked destination it is better to take that the attack is coming from multiple IP addresses. However now a days , with the findings of virus affected PCs and there is a enomourous increase in number of smart mobile phones, many botnets are found around the world, which can be used to sign up a real DDoS attack.

How to Stop DDoS attacks.

Unfortunately till now there is no complete protection against this type of attack as some large tools and security platforms are used to squeeze its effect. Large organizations are paying millions of dollars to protect their remote servers against DDoS but small scale business owners failed tomake an attempt to do so. To overcome the effect of DDoS attack DDoS deflate was released as a free and open source DDoS protection software.

What Is DDoS Deflate:-

DDoS Deflate is a lightweight bash shell script designed to help in the process of blocking a distributed denial of service attacks. It makes use of the command below to create a list of IP addresses which are connected to the server, along with their total number of nodes.

IV.APF FIREWALL

APF is a policyor a protocol based ip tables firewall system designed for easy usage to the programmers andto configure the system properly. It employs a subset of features to maintain the host or remote Linux user and the novice alike. They are packaged in tar.gz format and RPM formats, make APF feel free for deployment in many server either remote or host environments based on the Linux platform. APF is developed and is followed up by R-fx Networks Themanual or guide will show how to install and configure APF firewallin the system to use by the programmer and to safe guard the one which is better known as Linux firewalls.

1. cd /root/downloads or create any another temporary folder wherethe data can be stored .
2. wget http://www.rfxnetworks.com/downloads/apf-current.tar.gz
3. . tar -xvzf apf-current.tar.gz
4. cd apf-0.9.5-1/ or tie up with the latest version .
5. Now it is better to run the popular version of install file:./install.sh and receive a computer generated message saying that it has been installed successfully. For eg) Installing APF 0.9.5-1: Completed.
6. Do the configuration of the firewall as mentioned: pico/etc/apf/conf.apf so that the system will reside over the general configuration to make sure that the firewall is running.
7. Configuration of the Firewall Ports is done as follows: Cpanel Servers that is used for the following on the Cpanel Servers .Common ingress (inbound) ports # Common progress (outbound) TCP ports -3000_3400 = passive port range for Pure FTPD IG_TCP_CPORTS=”21,22,25,53,80,110,143 ,443,2082,208 3, 2086,2087, 2095, 2096,3000_3500″

   # Common progress (outbound) UDP ports IG_UDP_CPORTS=”53″ Common egress (outbound) ports# Egress filtering [0 = Disabled / 1 = Enabled]EGF=”1″# Common progress (in bound) TCPportsEG_TCP_CPORTS=”21,25,80,443, 43,20 9″# Common progress (in bound) UDP ports
   EG_UDP_CPORTS=”20,21,53″
8. Start up the firewall by using /usr/local/sbin/apf –s
9. After the startup process , update the DEV option
   Ban the firewall from automatically signing off itself every 3 minutes from cron.The recommendations for changing this back to “1” after the system had a chance tomake sure that everything is working fine and tested the server out. pico /etc/apf/conf.apf
10. Configuration of AntiDOS for APF
    No matter relatively shifting new to APF is the new AntiDOS feature that can be found in: /etc/apf/ad
    The log file will be located at /var/log/apfados_log so that it might want to make a note of the sequence and watch it! pico /etc/apf/ad/conf.antidos
11. Check the APF Log tail -f /var/log/apf_log
12. New – Make APF Start up automatically at boot time chkconfig –level 2345 apf on
    To remove it from autostart, run this:
    chkconfig –del apf
13. Deny the needed IPs with APF Firewall (Blocking)
    Pico /etc/apf/deny_hosts.rules
    The system can then just enter a new line and enter the IP that wish to block. Before this becomes active though the system need to reload the APF ruleset. /etc/apf/apf –r
14. Allow the IPs with APF Firewall (Unblocking) I know I know, the system has added an IP now and need it removed right away! The need to manually remove IPs that are blocked from deny_hosts.rules. pico /etc/apf/deny_hosts.rule.

References

[1] Patrikakis, C., Masikos, M., & Zouraraki, O. (2004). Distributed denial of service attacks. Internet Protocol Journal,7(4),Retrievedfromhttp://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_74/dos_ attacks.html
Rashid, F. (2011). Ddos attack knocks out hong kong stock exchange news website. eWeek, Retrieved from http://www.eweek.com/c/a/Security/DDoS-Attack Knocks-Out-Hong-Kong-Stock-Exchange-News-Web-Site-389466/

[2] Rashid, F. (2011). Sony data breach was camouflaged by anonymous ddos attack. eWeek, Retrieved from http://www.eweek.com/c/a/Security/Sony-Data-Breach-Was-Camouflaged-by-Anonymous-DDoS-Attack-807651/

[3] Subramani, R. (2011). Denial of service attacks and mitigation techniques: real time implementation withdetailed analysis. Retrieved from http://www.sans.org/reading_room/whitepapers/detection/denial-serviceattacks-mitigation-techniques-real-time-implementation-detailed-analysi_3376

[4] Verisign. (2012). Products and services - network intelligence and availability. Retrieved fromhttp://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/index.xhtml

[5] Walfish, M. (2006). DdoS defense by offense. Retrieved from http://nms.lcs.mit.edu/papers/ddos offensesigcomm06.pdf

[6] Zheng, Y. (2011). Distributed denial of service attack principles and defense mechanisms. Advances in Natural Science, 4(2)