DoS Protection via APF, BFD, DDOS and RootKit

Being a web host, your servers are constantly being attacked by hackers by denial-of-service (DoS) and other brute force attacks. There is no foolproof method to stop 100% of all attacks, but there are ways to protect your servers by applying firewall rules, and detecting and banning attacking IPs.

This article makes use of the APF , BFD , DDoS Deflate and RootKit to detect and protect your server from denial-of-service type attacks. To apply those utilities, please follow the instructions below:

To begin installation, login to your server as a root user.

```
% ssh -l root [hostname]  root@[hostname]'s password: [password]  Last login: [Date] from [hostname]
```

APF -- Advanced Policy-based Firewall

Get the latest source from the rfxnetworks, and install the software.

```
# cd /usr/src  # mkdir utils  # cd utils  # wget http://rfxnetworks.com/downloads/apf-current.tar.gz  # tar xfz apf-current.tar.gz  # cd apf-*  # ./install.sh
```

Read the README.apf and README.antidos for configuration options. Edit the /etc/apf/conf.apf and modify the following lines to your need.

```
DEVEL_MODE="0"  IG_TCP_CPORTS="21,22,25,53,80,110,143,443,3306"  IG_UDP_CPORTS="53,111"  USE_AD="1"
```

By default, APF is setup to run in development mode which flushes firewall rules every 5 minutes. Running in development mode defeats the purpose of running APF, as it will automatically flush every 5 minutes. Configure the Ingress (inbound) TCP and UDP ports that need to be opened. Finally, enable AntiDos by setting USE_AD="1".

Edit the /etc/apf/ad/conf.antidos as you fit necessary, and start the APF firewall.

```
# apf --start
```

BFD -- Brute Force Detection

BFD is a shell script which parses security logs and detects authentication failures. It is a brute force implementation without much complexity, and it works in conjunction with a APF (Advanced Policy-based Firewall).

```
 ## Get the latest source and untar.  # cd /usr/src/utils  # wget  http://rfxnetworks.com/downloads/bfd-current.tar.gz  # tar xfz
bfd-current.tar.gz  # cd bfd-*  # ./install.sh
```

Read the README file, and edit the configuration file located in /usr/local/bfd/conf.bfd.
Find ALERT="0" and replace it with ALERT="1"
Find EMAIL_USR="root" and replace it with EMAIL_USR=" username@yourdomain.com "

Edit /usr/local/bfd/ignore.hosts file, and add your own trusted IPs. BFD uses APF and hence it orverrides allow_hosts.rules, so it is important that you add trusted IP addresses to prevent yourself from being locked out.

```
 ## Start the program.  #  /usr/local/sbin/bfd -s
```

DDoS Deflate

```
 ## Get the latest source   # cd /usr/src/utils  # mkdir ddos  # cd ddos  # wget  http://www.inetbase.com/scripts/ddos/install.sh
 # sh install.sh
```

Edit the configuration file, /usr/local/ddos/ddos.conf, and start the ddos.

```
 # /usr/local/ddos/ddos.sh -c
```

RootKit -- Spyware and Junkware detection and removal tool

Go to Rootkit Hunter homepage, and download the latest release.

```
 ## Get the latest source and untar  # cd /usr/src/utils  # wget  http://downloads.rootkit.nl/rkhunter-1.3.8.tar.gz  # tar xfz
rkhunter-1.3.8.tar.gz  # cd rkhunter  # ./installer.sh  ## run rkhunter  # rkhunter -c
```

Setup automatic protection on System Reboot

```
 ## Edit /etc/rc.d/rc.local   ##      (or similar file depending on Linux version)  ## Add the
following lines at the bottom of the file    /usr/local/sbin/apf --start  /usr/local/ddos/ddos.sh -c
```

Note:

The SYN Floods and ICMP DDoS may also be prevented by utilizing the Linux traffic control utility (tc). To view setup instructions, please see relevant sections of Linux Advanced Routing

&amp; Traffic Control HOWTO
.

Notes from the users:

Some of the users experienced following errors while starting APF.

```
bash# apf --start
Unable to load iptables module (ip_tables), aborting.
```

According to Burst and Ryan of r-fx.org, changing the SET_MONOKERN variable in /etc/apf/conf.apf to "1" will correct the problem.