CENTRAL LOGS - SYSLOG

Any administrator responsible for any type of system will tell you that logs are *very* important. They are not glamorous, they are not fun but they are tremendously useful and are your only record for what happened on your system. It is for this reason that one of an attackers first targets once they have compromised your system is your logs. If they can manipulate your logs then they are better able to hide their tracks and thus finding them or cleaning up is that much more difficult. So how do you stop someone who compromises your system from changing the logs, you cannot really. But you can create the logs somewhere else, on a secure system they do not have access to. *Syslog* is very useful for this.

What is needed?

Well you need a linux box running *syslog*. Any normal linux distribution install will include *syslog* and it can be easily changed to receive logs via the network. It is even possible to setup windows servers, cisco routers, and many other devices to log their events to a centralized *syslog* server. Changing *syslog* to listen for logs is as simple as adding a *"-r"* to your *syslog* startup options. Wherever these are set, just add a *"-r"* switch and restart your *syslog* instance. Now if you do a *netstat* for *udp* ports for should see..

```
# netstat -nulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
PID/Program name
udp        0      0 0.0.0.0:514                 0.0.0.0:*
6011/syslogd
```

Now each type of client has their own syntax or way of getting the messages to the central server, but we will focus on how to do it in linux. Edit your *syslog.conf* file, you should see something like the following in it..

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none              /var/log/messages
```

All you do is add the network address of the central *syslog* server for the logs you want centralized, so using the above setting..

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none              /var/log/messages
*.info;mail.none;news.none;authpriv.none;cron.none     @192.168.56.23
```

Now restart your *syslog* instance, and it will start sending those messages out. Thats about it.

Final Words

Centralized logs is a good thing, but any logs are useless if you do not actually use them, and it also helps a heck of a lot if you ensure that all your systems have the same time setups, this makes referencing the different events a lot easier. Another thing to watch for is that you do not flood your network with the *udp* traffic generated by this system. As always, have fun and learn.