Step by step on how to setup and monitor important log information (i.e. logins, connections, running systems)

**Set up central logging server rsyslog/ElasticSearch**

1. Ensure rsyslog is downloaded on machine
   1. If not (sudo apt OR apt-get install rsyslog OR sudo yum install rsyslog)
2. **IF SELinux enabled-** Enable SElinux (semanage -a -t syslogd\_port\_t -p udp 514)
3. Open the config file ( sudo vi /etc/rsyslog.conf)
4. Uncomment 4 lines in modules section
   1. #module(load="imudp")
   2. ​#input(type="imudp" port="514")
   3. #module(load="imtcp")
   4. ​#input(type="imtcp" port="514")
5. Restart server (sudo systemctl rsyslog restart)
6. Unlock firewall for this port (iptables -A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT)
7. Check rsyslog file (sudo rsyslogd -N1)

**Set up clients on all machines that want to be monitored rsyslog/ElasticSearch**

1. Ensure rsyslog is downloaded on machin(s)
   1. If not (sudo apt install rsyslog OR sudo yum install rsyslog)
2. Open config file (sudo vi /etc/rsyslog.d/50-default.conf)
3. Add to bottom of the file (\*.\* @@SERVERIPADDRESS:514)
4. Create new file (sudo vim /etc/rsyslog.d/10-rsyslog.conf)
5. Add to top of file replacing private\_ip\_of\_ryslog\_server with (@@ SERVERIPADDRESS:514)
6. Restart rsyslog (sudo systemctl rsyslog restart)
7. Check rsyslog file (sudo rsyslogd -N1)

**Testing the server**

Client

[root@server2 ~]# logger Test from system   
 [root@server2 ~]# tail /var/log/messages   
 Dec 25 00:00:01 server2 root: Test from system

Server

[root@server1 ~]# tail /var/log/messages   
 Dec 25 00:00:01 server2 root: Test from system

**Common log files within linux and where to find them**

* /var/log/message – Where whole system logs or current activity logs are available.
* /var/log/auth.log – Authentication logs.
* /var/log/kern.log – Kernel logs.
* /var/log/cron.log – Crond logs (cron job).
* /var/log/maillog – Mail server logs.
* /var/log/boot.log – System boot log.
* /var/log/mysqld.log – MySQL database server log file.
* /var/log/secure – Authentication log.
* /var/log/utmp or /var/log/wtmp : Login records file.
* /var/log/yum.log: Yum log files
* /var/log/syslog - logs critical information, beside auth logs

**\*How to parse log files\***

* Use head/tail to focus on smaller portion of log files
* Grep WORD TO LOOK FOR logpath
  + Use grep to search for keywords within files
    - Grep “authentication failure” /var/log/auth.log
* Awk REGEXPRESSION logpath
  + Uses REGEX to parse for very specific files
    - awk ‘/sshd.\*invalid user/’ /var/log/auth.log

**Helpful tools for monitoring outside of log’s**

Monitor running processes

* 1. Linux
     1. System processes (top / htop)
     2. Apache Monitoring (apachetop)
     3. FTP monitoring (ftptop)
     4. SQL monitoring (mytop)

Monitor Desktop processes

* 1. Linux
     1. **If Internet is Available** (ntopng)
        1. Provides windowed server to analyze ip address connections, usage by each one, and where they originated from.
     2. Built in service similar to wireshark (iftop/jnettop)
        1. Watches packets being sent and received from the computer
     3. Monitor Connections (netstat)
        1. For focusing on one specific tcp packet (justsniffer/tcpdump)
     4. Ultimately if possible download and use wireshark because we have all previously used it and provides the most information for packet and transport layer communications

Monitor entire system

* 1. Linux
     1. Monitorix
        1. Provides default http page with information about the current system it is downloaded on, reports on all mechanisms within the machine
     2. Uptime
        1. Shows the information on run time and how many users are currently logged on. (can be helpful to ensure only the users you know are on the system)
     3. acct / psacct
        1. Acct (for when the system uses apt-get)
           1. Monitors the commands that are entered on the machine (can be used to ensure commands that are malicious are not entered and if they are quickly seen)
        2. Psacct (for when the system uses yum)
           1. Monitors the commands that are entered on the machine (can be used to ensure commands that are malicious are not entered and if they are quickly seen)