Security takes commitment

- Securing a server is not a one-time event
- Must have comprehensive, accurate, and closely watched logs
- Purpose:
  - Troubleshooting
  - Early warning signals
  - Forensics

Syslog

- Accepts log data from:
  - from the kernel (via klogd)
  - from local processes
  - from remote processes
- Is included pre-installed and preconfigured on most distributions
- Most administrators do not take the time to customize logs

Syslog can be easily customized

- Syslogd receives messages from many sources
- Acts on those messages based on facility and priority (selectors)
- Actions are specified in the /etc/syslog.conf file

Syslog - Facilities

- Facilities are categories
  - Auth: security events
  - Auth-priv: access control related messages
  - Daemon: used by system processes and other daemons
  - Kern: used for kernel messages
  - Mark: generated by syslog, a time stamp
  - User: a default facility when none is specified
  - Local7: boot messages
  - *: wildcard meaning any facility
  - None: wildcard meaning no facility

Syslog Priorities

- Priorities are hierarchical, meaning there is an increasing order of urgency
- Possible priorities are:
  - debug, info, notice, warning, err, crit, alert, emerg
- The urgency (priority) of a message is determined by the programmer who coded the program
- The wildcards ‘*’ and ‘none’ may be used in selector
- Modifiers ‘!’ (not) and ‘=’ (a single priority) may be used in selector
Syslog Selector Coding

- When a priority is specified, you are actually saying that priority and any higher priorities
- When a selector is modified by the equals, you are saying that priority only
- When you negate with the ! operator you will say except that priority or any higher priorities

Syslog selector examples

- mail.notice means:
  - All mail related messages of priority notice or higher
- mail.inotice means:
  - All mail related messages of except those of priority notice or higher
- mail.=notice means:
  - All mail related messages of priority notice (exclusively)

Syslog actions

- Most log messages are written to files
- If you list /var/log/filename as the action, syslog will write messages to that file
  - If the file does not exist, syslog will create it
  - *.emerg /var/log/emergency.log

Syslog actions

- Log messages can be written to other places as well:
  - *.emerg /dev/lp0
  - *.emerg /dev/ttyS3
  - *.emerg @logserver.ist.unomaha.edu
  - *.emerg @137.48.130.5
- In the last two examples above, the syslogd on the receiving computer must have been started with the --r option and allow incoming udp traffic on port 514
- There are NO access controls in syslog remote logging, use tcpwrappers or iptables to control where you accept traffic from

Stealth logging

- Can set up a machine with no IP address that will still listen on a network, but reserve an IP address for that machine (137.48.130.x)
- In RedHat, configure the ifcfg-ethx on the log server to start on boot, but include no IP information
- On the machine sending the log messages, include in the init process (rc.local) the line
  - \( \text{arp --s 137.48.130.x xx:xx:xx:xx:xx:xx} \)
- In the actions part of the syslog.conf entry use @137.48.130.x as your target

Syslog-ng (new generation)

- Better message filtering
- Better forwarding mechanisms
- Remote logging over either TCP or UDP
  - TCP allows use of ssh or stunnel, e.g. encryption
Monitoring logs - Swatch

- Tools exist to help separate critical log messages from relatively routine
- Swatch – Simple Watchdog
  - ftp.stanford.edu/general/security-tools/swatch
  - Perl script
  - Watches log file for events you define
  - Configuration file $HOME/.swatchrc

Logwatch

- Logwatch – another watchdog
  - http://www.logwatch.org/
  - Comes with RedHat
  - /etc/log.d directory holds scripts and configuration information
- LogWatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Easy to use - works right out of the package on almost all systems.

Security takes monitoring

- What to look for
  - Users logged in at strange times
  - Unexplained reboots
  - Unexplained changes to the system clock
  - Unusual messages in the logs
  - Unexpected or unauthorized use of the su command
  - Users logged in from unfamiliar sites
  - Unauthorized changes in system programs or user files
  - High network or mailer use
  - Unexplained user accounts
  - New SUID and SGID files

Assignment

- Assignment: Research default logging and log monitoring in your distro of choice
  - Examine log files created from a typical installation
    - Include log files messages, secure, maillog
    - Find the associated entries in /etc/syslog.conf
    - Describe the results in detail of each line in the configuration file
  - Recommend changes which would improve the usability of the logs assuming the computer was being used as a server allowing shell logins for program development