Logging Service

Chun-Jen (James) Chung

Arizona State University

What is a log?

- For security professionals, a log is used to record data on who, what, when, where, and why (5W) an event occurred for a particular *device* or *application*.
- Linux logs everything starting from the system boot. You can see everything that happened on your system and read the whole process line by line.
- System logs are the starting point for *maintenance* and *troubleshooting*, and Linux keeps track of everything for you.

Local Logging

- Logging locally
- Default setting for most of Linux machine
- Efficient to log *local intrusion*
- Limited for multiple host analysis
- A root user can change anything within these logs and there are many *root kits* that will remove the whole log or just an entry.
  - This poses a serious problem if this is your sole source of log information.
  - Once the device is compromised you don't have full control of the machine and the integrity of your logs is questionable.

What is RootKit?

- A rootkit is a set of software tools that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.
- When a rootkit is installed, it overwrite many commands used on a daily basis such as *ls*, *ps*, or *netstat*.
- Rootkits exist for a variety of operating systems, such as Microsoft Windows, Linux and Solaris.
- Rootkits often modify parts of the operating system or install themselves as *drivers* or *kernel modules*.

For more information about rootkit, go to http://en.wikipedia.org/wiki/Rootkit

Log files

- **/var/log/messages**
  - Global system messages, including messages logged during system startup
- **/var/log/dmesg**
  - Kernel ring buffer information, contains information on hardware devices that the kernel detects during boot process. You can use the 'dmesg' command to list these events from the command line.
- **/var/log/auth.log**:
  - Authorization information, including user logins and authentication mechanism used.
- **/var/log/boot.log**:
  - Messages generated during the boot sequence.
- **/var/log/daemon.log**
  - The log file for any processes running in the background.

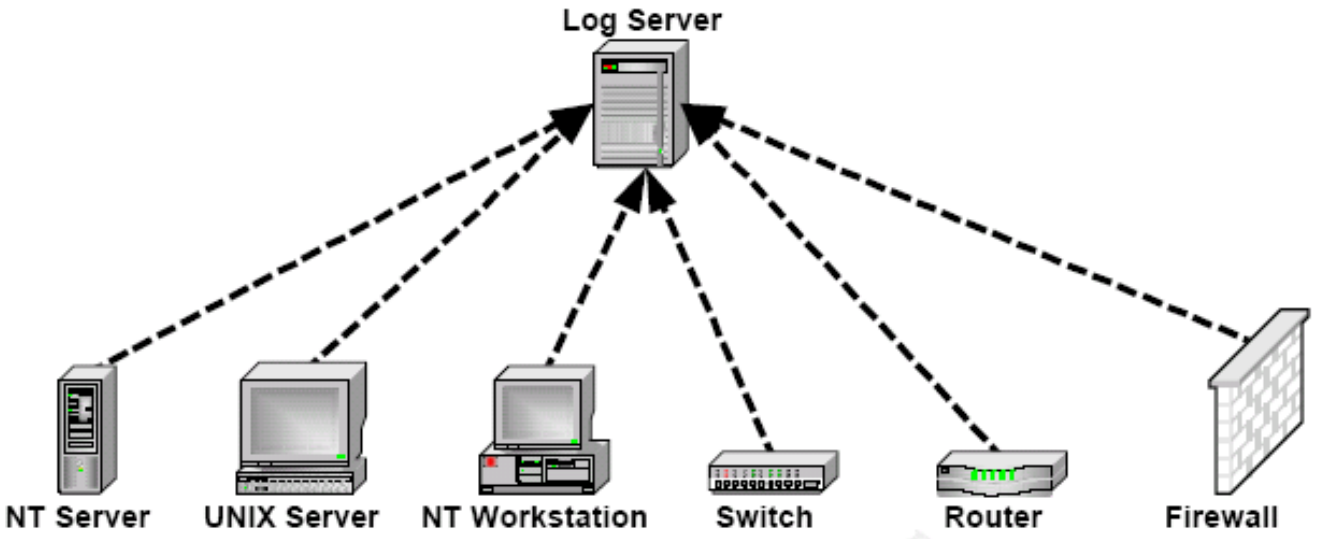
Log files (cont.)

- **/var/log/dpkg.log** (for Ubuntu or Debian)
  - The log file for the installed or removed packages using 'dpkg' command.
- **/var/log/kern.log**
  - Kernel logs. Helpful for you to troubleshoot a custom-built kernel.
- **/var/log/lastlog**
  - Login information for all the users. This is not an ascii file.
- **/var/log/cron.log**
  - Scheduled cron job logs.
- **/var/log/maillog**
  - Mail server logs.
- **/var/log/secure**
  - Authentication log

Application log:
- /var/log/httpd
- /var/log/apache2
- /var/log/mysql.log
- /var/log/snort

Centralized logging

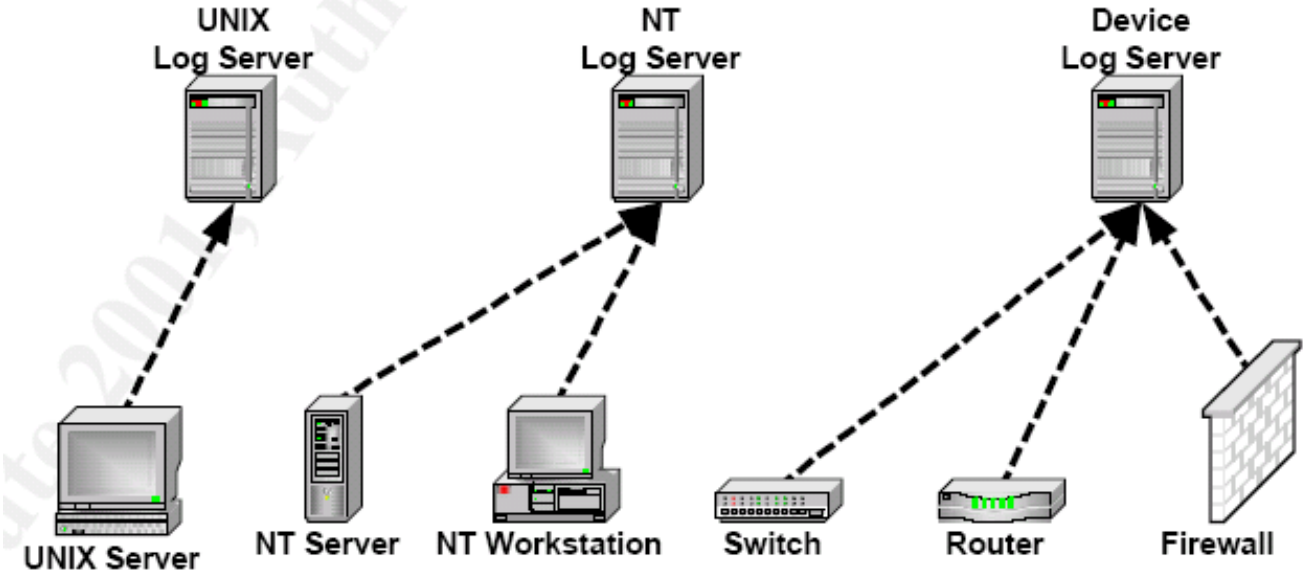
- Use a single centralized server to view and manage all your logs.



Logging Scenario A
All devices report back to a common central logging server.

Multiple logging server

- Uses a more robust method of breaking out the logs to specified servers. One server is used for one type of log source.



Logging Scenario B
All similar devices report back to a designated logging server.

Syslog

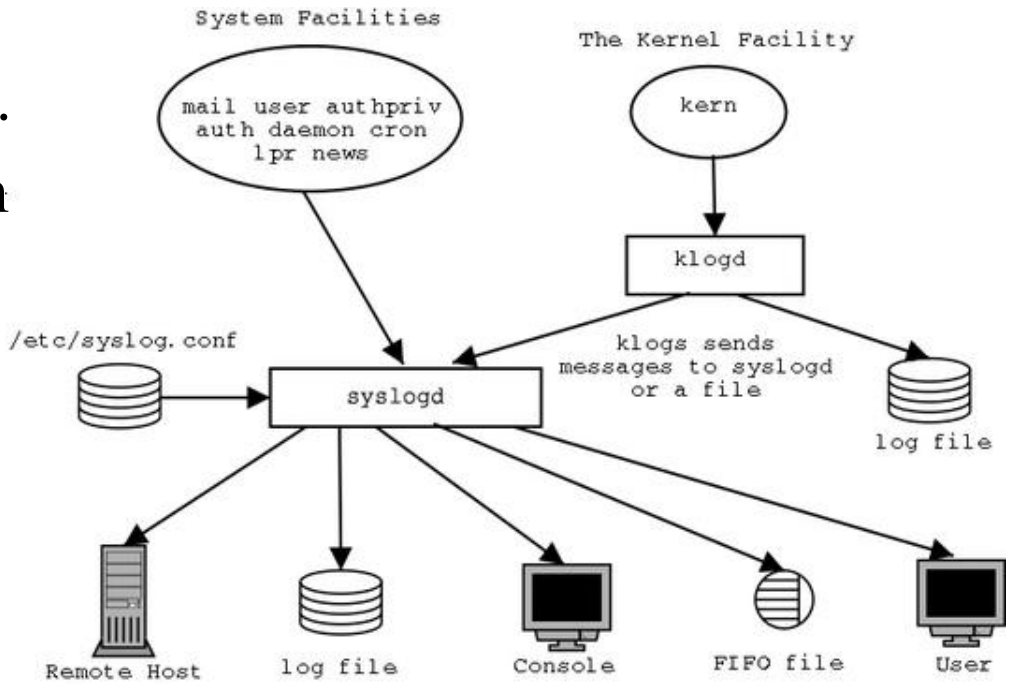
- Syslog is a utility for tracking and logging all manner of system messages from the merely *informational* to the *extremely critical*.
- Each system message sent to the syslog server has **TWO descriptive labels** associated with it that makes the message easier to handle.
  - **Function (facility)** of the application that generated it.
    - auth (security events), authpriv (user access message), cron, daemon, kern, lpr (print system), mail, mark (produce timestamp), news, syslog, user (for user program), uucp, local0~local7.
  - **Severity level** of the message. There are eight in all.

Severity Levels

Severity Level	Keyword for	Keyword for Cisco Router	Description
0	**emerg**	**emergencies**	System unusable
1	**alert**	**alerts**	Immediate action required
2	**crit**	**critical**	Critical condition
3	**err**	**errors**	Error conditions
4	**warning**	**warnings**	Warning conditions
5	**notice**	**notifications**	Normal but significant
6	**info**	**informational**	Informational messages
7	**debug**	**debugging**	Debugging messages

Logs and Auditing

- Syslog daemon - **syslogd**
  - The syslogd daemon for collecting the log message at a central place from various facilities.
  - The logging is configured in **/etc/syslog.conf** file, which contains the names and locations for your system log files.
- Klogd - a daemon for taking care of kernel log messages.



Syslog Configuration File – syslog.conf

```
1:  #kern.*                                          /dev/console
2:  # Log anything (except mail) of level info or higher.
3:  # Don't log private authentication messages!
4:  *.info;mail.none;authpriv.none;cron.none        /var/log/messages
5:  # The authpriv file has restricted access.
6:  authpriv.*                                       /var/log/secure
7:  # Log all the mail messages in one place.
8:  mail.*                                           /var/log/maillog
9:  # Log cron stuff
10: cron.*                                           /var/log/cron
11: # Everybody gets emergency messages
12: *.emerg                                          *
13: # Save news errors of level crit and higher in a special file.
14: uucp,news.crit                                   /var/log/spooler
15: # Save boot messages also to boot.log
16: local7.*                                         /var/log/boot.log
17: # To specifiy a single priority rather than all priorities above.
18: *.=debug                                         /var/log/debug.log
```

Other Log Files – Non-ASCII Format

- **utmp**
  - stores information about who is currently logged into a system (/var/run or /var/adm) – using command "who" to read it.
- **wtmp**
  - this file records all logins and logouts to and from the system (/var/log, var/adm) – using command "last"to read it.
- **lastlog**
  - contains information about the time and location of each user's last login to the system (/var/log/lastlog) – using command "lastlog"to read it.

Log Rotation

- Log files can grow a lot and become useless. The ***logrotate*** service 'rotates' log files conserving only compressed logs under a specified age.
- Logrotate service is executed by crond in regular basis and it has the main configuration file on /etc/logrotate.conf.

```
$ cat /etc/logrotate.conf

# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# drop log rotation information into this directory
include /etc/logrotate.d
```

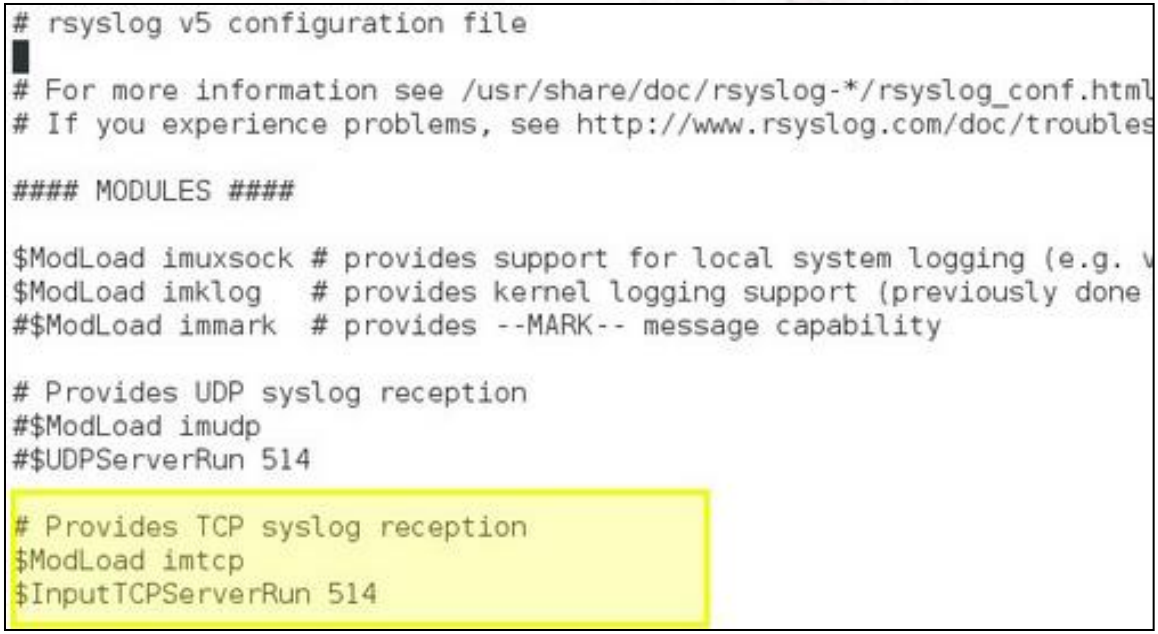
Configure a remote syslog server

1. Edit /etc/rsyslog.conf

2. Restart rsyslog service

   service rsyslog restart

3. Adding a rule to the iptables file if needed.



```
# rsyslog v5 configuration file
#
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubles

#### MODULES ####

$ModLoad imuxsock # provides support for local system logging (e.g. v
$ModLoad imklog   # provides kernel logging support (previously done
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

iptables –A INPUT –m state –state NEW –m tcp –p tcp --dport 514 –j ACCEPT

4. Restart iptables service

Configure a system to log to a remote system

1. Edit /etc/rsyslog.conf
2. Restart the logging service – **service rsyslog restart**

```
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###
```

```
## Custom forwarding rules

## Forward logs to server
*.* @@192.168.1.50:514
```