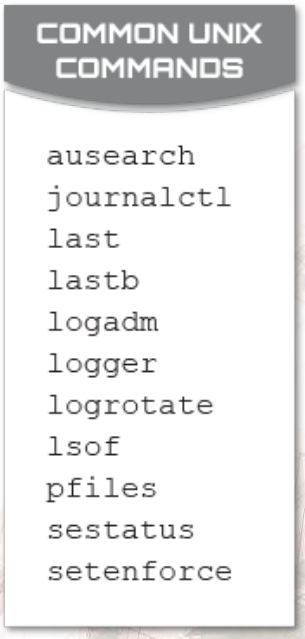
UNIX Commands

Some common UNIX commands to research and become proficient with are:



SYSLOG Facility Levels

The facility level is used to specify what type of program is logging the message. The configuration file can then handle messages from different facilities in different ways.

Code Facility Number	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security or authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem

Code Facility Number	Keyword	Description
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security or authorization messages that can only be read by selected users
11	ftp	FTP daemon
12		NTP subsystem
13		log audit
14		log alert
15	cron	clock daemon
16	local0	local use 0
17	local1	local use 1
18	local2	local use 2
19	local3	local use 3
20	local4	local use 4
21	local5	local use 5
22	local6	local use 6
23	local7	local use 7

SYSLOG Severity Levels

There are eight severity levels.

Code	Severity	Keyword	Description
0	Emergency	emerg	The system is unusable. This is a panic condition affecting multiple apps, servers, or sites. All tech staff on call are usually notified.
1	Alert	alert	Take action immediately. Make any corrections immediately. Tech staff who can fix the problem are notified.
2	Critical	crit	Take action immediately, but the failure is a secondary system such as the loss of a backup system.
3	Error	err	System or application failures are non-urgent. They are usually relayed to developers or admins for resolution within a timeframe.
4	Warning	warn	A warning that an error will occur, but no immediate action is required. Warnings are often summarized and emailed to developers and admins.
5	Notice	notice	An event has occurred that is normal, but significant or unusual. No immediate action is required. Notices are often summarized and emailed to developers and admins to spot potential problems.
6	Informational	info	Normal operational messages that require no action. These messages may be analyzed for reporting purposes.
7	Debug	debug	Information useful to developers for debugging an application. These messages are not useful during operations.

Recommended Internet Sites

- Man (manual) pages – Use any search engine using the format “[Topic] man page”
- RFCs – Use any search engine using the format “RFC [RFC NUMBER]”

- https://web.archive.org/web/20160801104028/http://www.rsyslog.com/
- https://web.archive.org/web/20160801104354/https://syslog-ng.org/
- https://web.archive.org/web/20160801104532/https://www.freedesktop.org/wiki/Software/systemd/
- https://web.archive.org/web/20170314180702/https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-system_auditing.html
- https://web.archive.org/web/20160801105003/http://security.blogoverflow.com/2013/01/a-brief-introduction-to-auditd/
- https://web.archive.org/web/20160801105412/https://wiki.gentoo.org/wiki/SELinux/Tutorials/Where_to_find_SELinux_permission_denial_details
- https://web.archive.org/web/20160801105506/https://www.nsa.gov/what-we-do/research/
- https://web.archive.org/web/20160809163739/http://freecomputerbooks.com/books/The_SELinux_Notebook-4th_Edition.pdf
- https://web.archive.org/web/20160801105700/http://alvinalexander.com/blog/post/linux-unix/linux-lsof-command

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.