Linux Commands

Getting around

Command	Description
`cd logs`	Move to the logs directory, which is located in the **current** directory.
`cd /logs`	Move to the logs directory, which is located in the **top-level** directory.
`cd ..`	Move up one directory.
`cd ~`	Move to your home directory (the "tilde" character is left of the 1 key).
`cd -`	Move to the directory you were previously in.

Tip – Tab Completion

Use tab completion to type filenames faster.
As you're typing a filename (or directory), hit the tab key. If there's only one file that matches what you've typed, the rest of the filename will be filled in. If nothing happens when you hit tab, simply hit tab again to see a list of matches.

Viewing and searching in files

Command	Description
`cat data.txt`	Display data.txt
`cat *.txt`	Display all files that end with .txt
`head data.txt`	Display the **first** 10 lines of data.txt.
`head -n 20 data.txt`	Display the **first** 20 lines of data.txt.
`tail data.txt`	Display the **last** 10 lines of data.txt.
`tail -n 30 data.txt`	Display the **last** 20 lines of data.txt.
`tail -F data.txt`	Display the last 10 lines of data.txt and continue running, displaying any new lines in the file. *Note: Press Ctrl+C to exit.*
`grep malware data.txt`	Display all lines in data.txt that contain 'malware'.
`grep -v malware data.txt`	Display all lines that **do not** contain 'malware'.
`grep 'mal ware' data.txt`	To search for phrases with spaces, use single quotes.
`grep -F 1.2.3.4 data.txt`	To search for phrases with periods, use –F
`grep -c exe data.txt`	Display how many lines in data.txt contain 'exe' (but don't display them).
`grep -F -c 1.2.3.4 *.txt`	Display the number of lines with IP 1.2.3.4 in each file that ends in .txt.
`less large.file`	Display large.file in less (see right).
`less -S large.file`	Display large.file in less (see right), **and allow for side-to-side scrolling**.

Navigating in less

Key or Command	Description
`q`	Quit
`Up/down arrow`	Move up/down one line.
`Left/right arrow`	Move left/right half of a page. *Note: requires less –S*
`Page up/down`	Move up/down one page.
`g`	Go to the **first** line
`G`	Go to the **last** line
`F`	Go to the last line, and display any new lines (similar to tail –F). *Note: Press Ctrl+C to exit.*
`/malware`	Search - go to the next line containing the word 'malware.'
`/!malware`	Search – go to the next line **NOT** containing the word 'malware.'
`?malware`	Search – go to the previous line containing the word 'malware.'
`n`	Repeat a previous search.
`N`	Repeat a previous search, but in the opposite direction.

Putting it all together

Command	Description
`| (AKA "pipe")`	Pass the output of one command to another command. *Note: For the "pipe" character, use the key above enter (same key as backslash).*
`grep malware data.txt | tail -n 30`	Display the last 30 lines in data.txt that contain the word 'malware.'
`grep malware data.txt | grep blaster`	Display lines in data.txt that contain 'malware' **and also contain 'blaster.'**
`cat data.txt | sort`	Display data.txt, sorted alphabetically.
`cat data.txt | sort | uniq`	Display data.txt, sorted alphabetically, with duplicates removed.
`cat data.txt | sort | uniq -c`	Sort, remove duplicates, and display the number of times each line occurred.
`cat data.txt | sort | uniq -c | sort -n`	Sort, remove duplicates, and display the most frequent lines.
➔ `cat data.txt | sort | uniq -c | sort -n | tail -n 20`	Sort, remove duplicates, and display the 20 most frequent lines.
`cat conn.log | bro-cut id.resp_h proto service`	Only display the id.resp_h, proto and service columns of the conn Bro log.
`cat http.log | bro-cut -d ts method host uri`	Only display the timestamp, method, host and uri columns, **and convert the timestamp to human-readable format.**

Tip – Compressed Files

Files that end in .gz are compressed, and might require some different commands:

Command	Modification for .gz
cat or grep	Use zcat or zgrep.
head or tail	Use zcat | head or zcat | tail

Tip – Documentation

Linux commands are all well documented. To view the documentation:

- Run the command with --help (e.g. tail --help) to see the options.
- Use the manual pages for more detail (e.g. man tail). *Note: these open in less.*

Tip – Working With Big Files

Commands take longer to run on larger files. Some things to keep in mind are:

- Use grep –F instead of plain grep.
- For viewing the file, use less instead of cat.
- Try to use grep as early as possible, so if you pipe to other tools, there's less data to crunch.