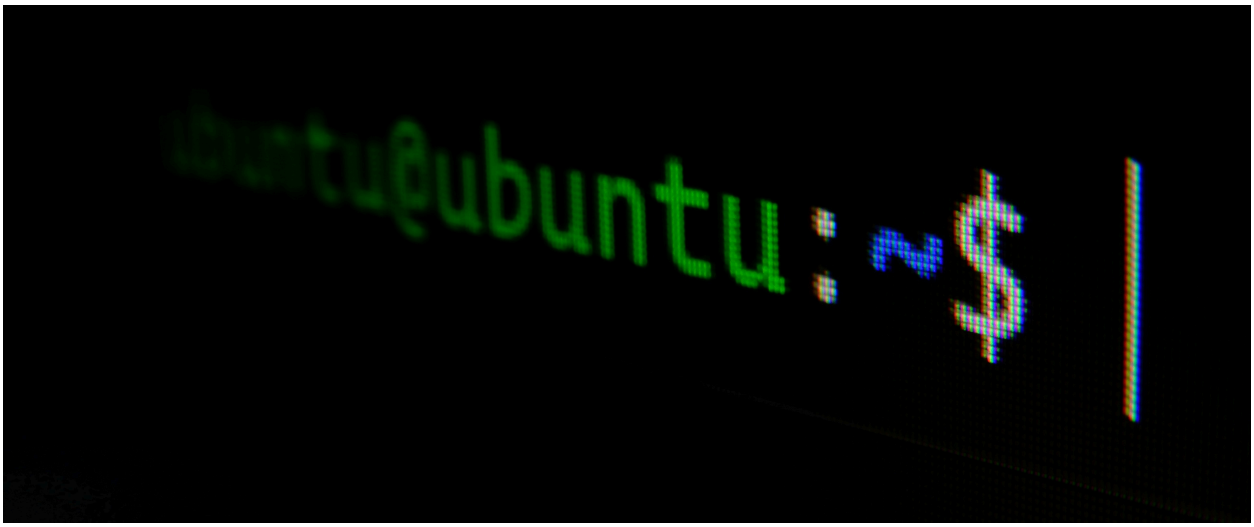

CHAPTER 2 - TEXT MANIPULATION

💡 In Linux, nearly everything is a file, and almost always a text file. For instance, all configuration files in Linux are text files. to reconfigure an application, open the configuration file, change the text, save it and restart application - application reconfigured.

▼ [2.1] Viewing Files

▼ [2.1.1] *head* command

If you want to view the beginning of a file which is huge and spans over multiple pages, use ***head*** command. By default, it shows only the first 10 lines of a file.

If you want to view more or less number of exact lines, enter quantity with a dash after call of head and before filename.

→ eg. ***head -20 /etc/snort/snort.conf***

▼ [2.1.2] *tail* command

tail command is similar to head file, only that it is used to view the last lines of a file instead of beginning as in head. By default, it shows only the last 10

lines of a file.

Similar to head, if you want to view more or less number of exact lines, enter quantity with a dash after call of tail and before filename.

→ eg. ***tail -20 /etc/snort/snort.conf***

▼ [2.1.3] *Numbering Lines* command

With files having huge number of lines and spanning over multiple tens of pages you often need numbered lines, easier for reference, trace-back and just overall NOT making you feel overwhelmed (just a personal take). Use ***nl*** command to number lines.

→ eg. ***nl /etc/snort/snort.conf***

▼ [2.2] Filtering Text

▼ [2.2.1] *grep* command

One of the most widely and prominently used text manipulation command is ***grep***.

Allows to filter out the contents of a file or command, for instance if you wan to see ***only*** lines with the word ***"output"*** in it, the command would look like:

→ eg. ***cat /etc/snort/snort.conf | grep output***

> 💡 '|' - is a pipeline character, it translates to forward the output as input from left of the pipeline to the right hand side- it could be another command or a file or multi-layered command for specific output. Extensively used in DFIR and Cybersecurity in image dump analysis to examine autopsy reports or screening/general disc scanning etc. Extremely crucial for anybody trying to sharpen their swords in the realm of CySec or DFIR.

▼ [2.1.2] *sed* command

sed [stream editor] command allows user to search for occurrences of a said word or text pattern, and essentially letting the user perform some sort of action over it, another very relevant and useful command for DFIR

analysts and Cyber enthusiasts or just general Linux proficiency as well. Some even call in “find and replace”.

Let’s say you wish to change the word game → to GAMES [every occurrence of it] in a file namely - studioGames. Here’s how you can achieve this with ***sed*** command:

→ ***sed s/game/GAMES/g ./games/studioGames > formatted.doc***

→ I’ll explain the command and give you a breakdown:

sed - stream editor command.

s - sed’s substitute command-option [find and replace].

[**/**] - delimiter (basically like a comma [,] for Linux to understand).

game - word to replace.

GAMES - what to replace with.

g - global, means not just the first occurrence change all the occurrence of [”game”] pattern, if you want to change only the foremost occurrence drop the ‘ ***s*** ’.

> You can also choose to change a specific number of occurrence as well, lets say 4 for eg., for the same your command would look like this:

> ***sed s/game/GAMES/4 ./games/studioGames > formatted.doc***

→ The command would only reflect upon the ***Fourth*** occurrence and not each.

./game/studioGames - path of file to to do operations upon.

‘***>***’ - overwrite the resulting text as a whole towards some file (generally, but not necessarily).

formatted.doc - name of the file to store it in, you can also choose the same file as well I'm just illustrating a point.

▼ [2.1.3] Viewing files MORE and LESS

▼ more Command

Displays a page at one time, and allows page down using the ENTER key. It is also the utility that man (manual) pages use, or press q (Quit) to exit.

eg. more /etc/snort/snort.conf

▼ less Command

Similar to more command but with additional functionalities, hence the Linux ***aficionado quip*** - “less is more”. ***less*** allows scrolling and filtering for terms. You can search for words by pressing forward slash [/], press ‘n’ [***next***] for traversing through each occurrence one after another.

eg. less /etc/snort/snort.conf