**Linux for hackers 2 – Text manipulation**

[**https://www.snort.org/**](https://www.snort.org/)

to install snort: apt-get install snort

1. **cat** etc/snort/snort.conf

To view key content of the file we use **head** or **tail**

1. **head** etc/snort/snort.conf – head will give the default first 10 lines of the file and incase if you want to see 20 lines use : **head -20** /etc/snot/snort.conf
2. **tail** etc/snort/snort.conf – to view last 10 lines and incase if you want to see last 20 line use tail -20
3. **nl** etc/snort/snort.conf – here nl will display line numbers in terminal output.
4. **grep** to filer: ex – cat etc/snort/snort.conf | grep output
5. Using **sed** to find and replace : cat etc/snort/snort.conf | grep mysql which will give 2 results and we can replace it with MYSQL or anyother word of your choice. Using **sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf**

If you want to replace only the first occurrence use this command (remove g from the above command)

**sed s/mysql/MySQL/ snort.conf > snort2.conf**

sed s/mysql/MySQL/**2** snort.conf > snort2.conf (to change only the second occurrence)

1. View files using more and less. More displays the first page and then stops. For every enter it will move forward and ends when you press **q** (quit)

**more /etc/snort/snort.conf**

**less /etc/snort/snort.conf**

**to know more about the differences view here:** [**https://www.baeldung.com/linux/more-less-most-commands**](https://www.baeldung.com/linux/more-less-most-commands)

**Exercise**

1. Navigate to /usr/share/wordlists/metasploit. This is a directory of multiple wordlists that can be used to brute force passwords in various password-protected devices using Metasploit, the most popular pentesting and hacking framework.

2. Use the cat command to view the contents of the file passwords.lst.

3. Use the more command to display the file passwords.lst.

4. Use the less command to view the file passwords.lst.

5. Now use the nl command to place line numbers on the passwords in passwords.lst. There should be 88,396 passwords.

6. Use the tail command to see the last 20 passwords in passwords.lst. 7. Use the cat command to display passwords.lst and pipe it to find all the passwords that contain 123.