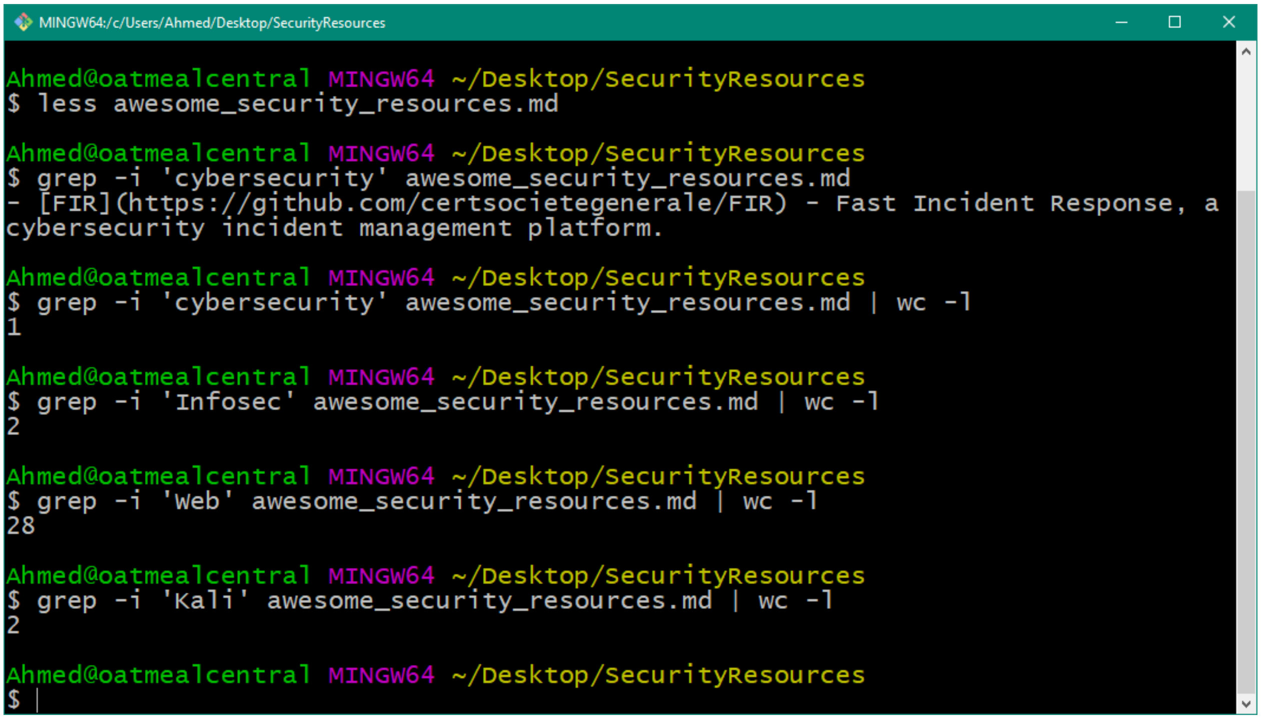
Sample Report – Find and Grep

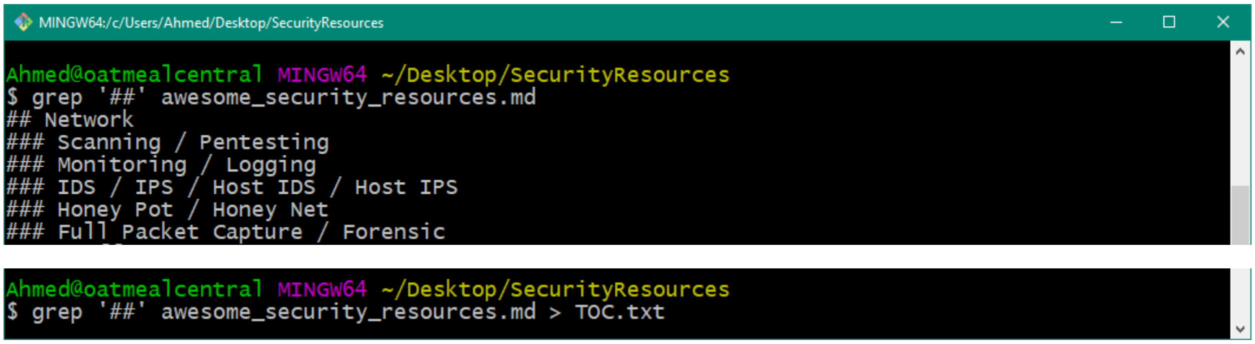
Sherlock. B Holmes | May 29, 2018

In this activity, we were tasked with investigating a markdown file filled with cybersecurity resources. My first task was to count the occurrences of specific phrases within the file. To accomplish this, I used the **`grep | wc -l`** command as follows:



```
Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ less awesome_security_resources.md

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -i 'cybersecurity' awesome_security_resources.md
- [FIR](https://github.com/certsocietegenerale/FIR) - Fast Incident Response, a
cybersecurity incident management platform.

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -i 'cybersecurity' awesome_security_resources.md | wc -l
1

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -i 'Infosec' awesome_security_resources.md | wc -l
2

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -i 'Web' awesome_security_resources.md | wc -l
28

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -i 'Kali' awesome_security_resources.md | wc -l
2

Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ |
```

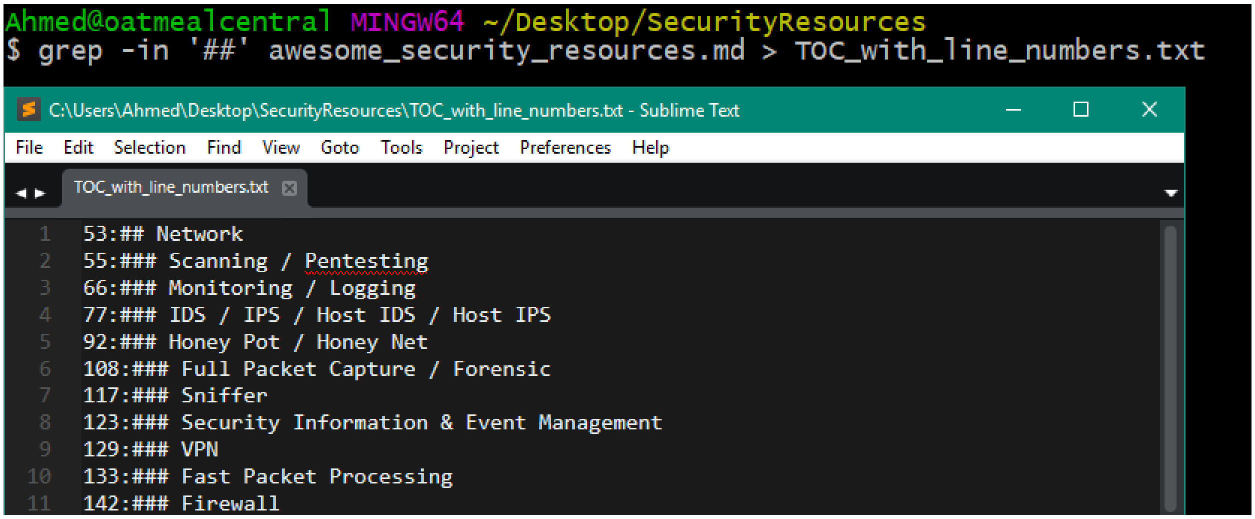
Next, I was tasked with identifying all of the headers and sub-headers of the document. To accomplish this, I used the **`grep '##' awesome_security_resources.md`**. In this case, the command effectively searched for each instance of the `##` symbol in the document. To store the contents in a file, I modified the script to include **`> TOC.txt`**. This has the effect of saving my search result inside a file called TOC.txt.



```
Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep '##' awesome_security_resources.md
## Network
### Scanning / Pentesting
### Monitoring / Logging
### IDS / IPS / Host IDS / Host IPS
### Honey Pot / Honey Net
### Full Packet Capture / Forensic
```

```
Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep '##' awesome_security_resources.md > TOC.txt
```

In the case, I wanted to include line numbers in my file, I could further modify the script to use the `**-in**` modifier as in the below:



```
Ahmed@oatmealcentral MINGW64 ~/Desktop/SecurityResources
$ grep -in '##' awesome_security_resources.md > TOC_with_line_numbers.txt
```

C:\Users\Ahmed\Desktop\SecurityResources\TOC_with_line_numbers.txt - Sublime Text
File
Edit
Selection
Find
View
Goto
Tools
Project
Preferences
Help
TOC_with_line_numbers.txt

```
53:## Network
55:### Scanning / Pentesting
66:### Monitoring / Logging
77:### IDS / IPS / Host IDS / Host IPS
92:### Honey Pot / Honey Net
108:### Full Packet Capture / Forensic
117:### Sniffer
123:### Security Information & Event Management
129:### VPN
133:### Fast Packet Processing
142:### Firewall
```