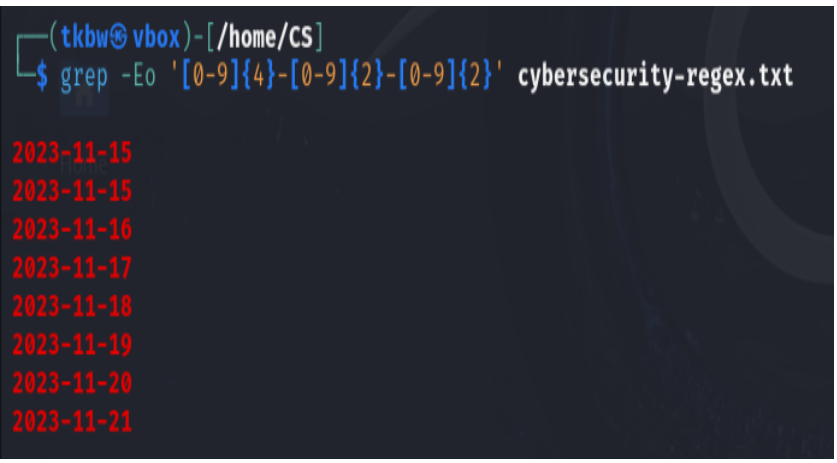
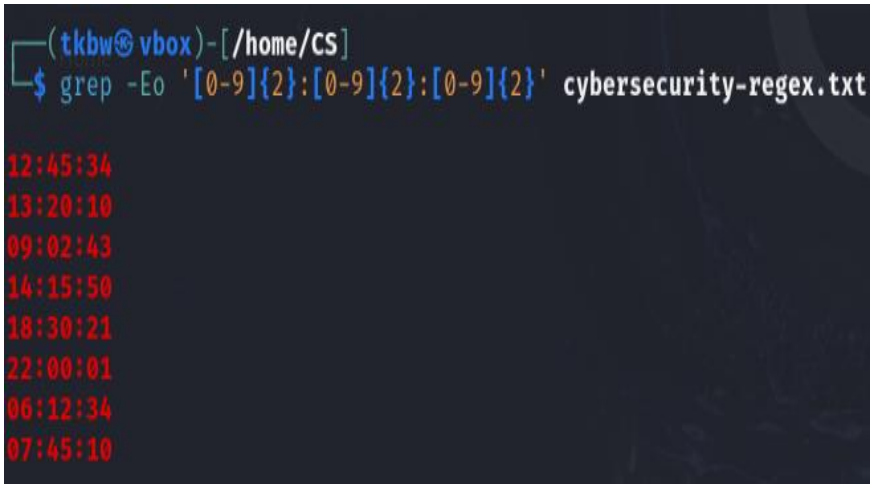
Assignment 5

Grep and Regex Analysis in Kali Linux

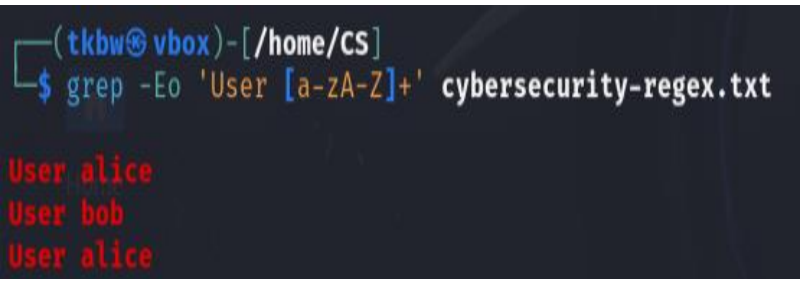
=> It is looking for IP addresses in the Cyblesecurity-Regex.txt file using the aforementioned formal expression. It will only display the addresses that are identical to the style, which is the IP address consists of four part.



=> This is looking for YYYY-MM-DD dates in the Cyblesecurity-Regex.TXT file and only displays the dates that match this format.



=> It comes to search for times in the HH: MM: SS in the Cybersecurity-Regex.txt File, and only shows the times that match these formulas



=> This search for texts containing the word "USer", followed by a name of only English letters in the Cybersecurity-Regex.txt file. "User" will be presented with the name related to it only.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E 'logged in|logged out' cybersecurity-regex.txt

- 2023-11-15 12:45:34 INFO User alice logged in from 192.168.1.100
- 2023-11-16 09:02:43 INFO User bob logged in from 172.16.0.3
- 2023-11-21 07:45:10 INFO User alice logged out from 192.168.1.100
3. List all users who logged in or out.
```

=> This is searching for any line that contains either "Logged" in the Cyblesecurity-Regex.txt file.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -Ei 'CRITICAL|ERROR' cybersecurity-regex.txt

- 2023-11-15 13:20:10 ERROR Unauthorized access attempt from 10.0.0.45
- 2023-11-19 22:00:01 CRITICAL Kernel panic on host server02
2. Identify errors and warnings.
```

=> It is searching for any line that contains either "Critical" or "Error" in the Cyblesecurity-Regex.txt file, regardless of the case of letters.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -Eo 'server[0-9]+' cybersecurity-regex.txt

server01
server02

┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -v 'INFO' cybersecurity-regex.txt
```

=> This is looking for texts that start with "Server" and followed by one or more in the Cyblesecurity-Regex.txt file and only display these texts

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -v 'INFO' cybersecurity-regex.txt
Alice had always been curious about cybersecurity. One day, she stumbled upon the mysterious world of Linux. Intrigued, she decided t
o explore it further. Her journey began with Kali Linux, a popular distribution tailored for penetration testing. With every command
she learned, her confidence grew.

Alice found the `grep` command particularly fascinating. It allowed her to search for patterns in text files quickly. She used it to
sift through log files, configuration files, and even code.

Here are a few examples of the logs Alice worked on:

- 2023-11-15 13:20:10 ERROR Unauthorized access attempt from 10.0.0.45
- 2023-11-17 14:15:50 WARNING Disk space running low on server01
- 2023-11-19 22:00:01 CRITICAL Kernel panic on host server02

She also experimented with different regex patterns to extract insights:

1. Extract all dates.
2. Identify errors and warnings.
3. List all users who logged in or out.
4. Find IP addresses.

Alice knew regex was a powerful skill for any Linux user. She practiced diligently, noting her progress as she mastered the `grep` co
mmand.
```

=> It comes to search for lines that do not contain the word "Info" in the Cyblesecurity-Regex.TXT file, then displays those lines

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -c 'WARNING' cybersecurity-regex.txt
1
```

=> It calculates the number of lines that contain the word "Warning" in the CyberseCury-Regex.TXT file.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep 'Unauthorized access' cybersecurity-regex.txt
- 2023-11-15 13:20:10 ERROR Unauthorized access attempt from 10.0.0.45
```

=> Take a search for lines that contain the "Unauthorized Access" text within the Cyblesecurity-Regex.TXT file and display these lines.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E 'INFO|WARNING|ERROR|CRITICAL' cybersecurity-regex.txt

- 2023-11-15 12:45:34 INFO User alice logged in from 192.168.1.100
- 2023-11-15 13:20:10 ERROR Unauthorized access attempt from 10.0.0.45
- 2023-11-16 09:02:43 INFO User bob logged in from 172.16.0.3
- 2023-11-17 14:15:50 WARNING Disk space running low on server01
- 2023-11-18 18:30:21 INFO File /etc/passwd accessed by user alice
- 2023-11-19 22:00:01 CRITICAL Kernel panic on host server02
- 2023-11-20 06:12:34 INFO SSH session closed for user bob
- 2023-11-21 07:45:10 INFO User alice logged out from 192.168.1.100
```

=> It is searching for any of the words "Info", "Warning" or "Error" in the Cyblesecurity-Regex.txt file and only displays those identical words

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E  'User alice|User bob' cybersecurity-regex.txt

- 2023-11-15 12:45:34 INFO User alice logged in from 192.168.1.100
- 2023-11-16 09:02:43 INFO User bob logged in from 172.16.0.3
- 2023-11-21 07:45:10 INFO User alice logged out from 192.168.1.100
```

=> This is searching for lines that contain the text "User Alice" or "User Bob" in the Cyblesecurity-Regex.txt file, and displays that medium

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E  'File' cybersecurity-regex.txt

- 2023-11-18 18:30:21 INFO File /etc/passwd accessed by user alice
```

=> This is searching for all lines that contain the word "File" in the Cybersecurity-Regex.TXT file.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E '2023-11-18' cybersecurity-regex.txt
```

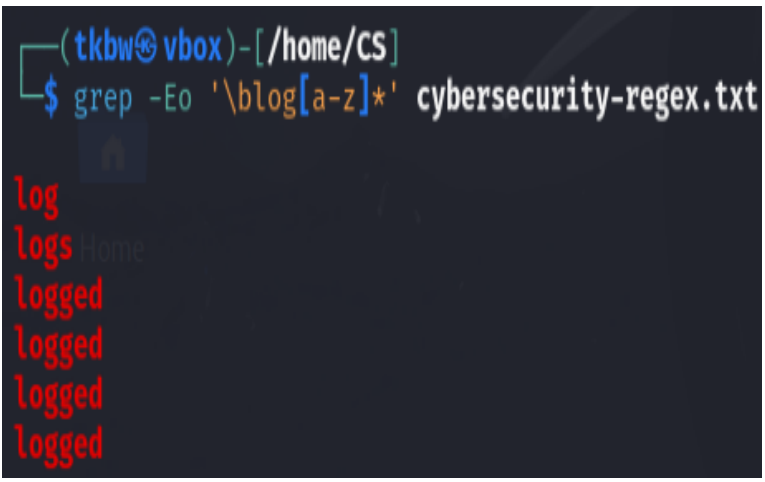
=> This is searching for lines that contain the date "2023-11-18" in the Cyblesecurity-Regex.txt file and displays these lines.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E 'SSH session closed' cybersecurity-regex.txt
- 2023-11-20 06:12:34 INFO SSH session closed for user bob
```

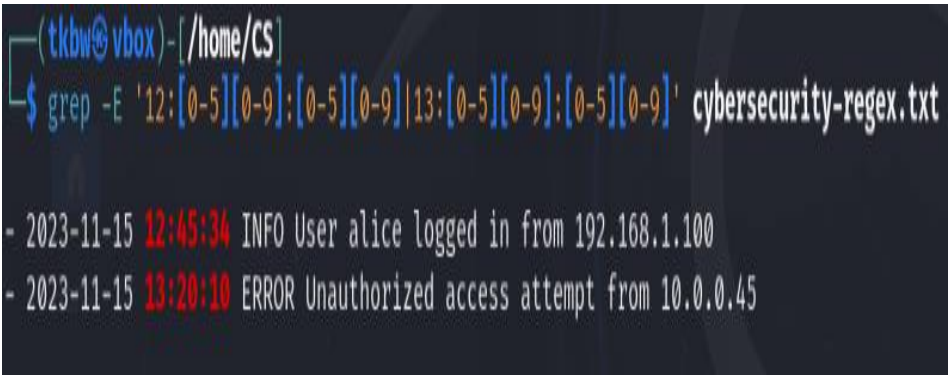
=> The "SSH Session Closed" text is searching in the Cyblesecurity-Regex.txt file and only displays this phrase in the lines it contains.

```
┌──(tkbw㉿vbox)-[/home/CS]
└─$ grep -E 'Disk space' cybersecurity-regex.txt
- 2023-11-17 14:15:50 WARNING Disk space running low on server01
```

=> It is searching for lines that contain the "Disk Space" text in the Cyblesecurity-Regex.txt file and displays these lines.

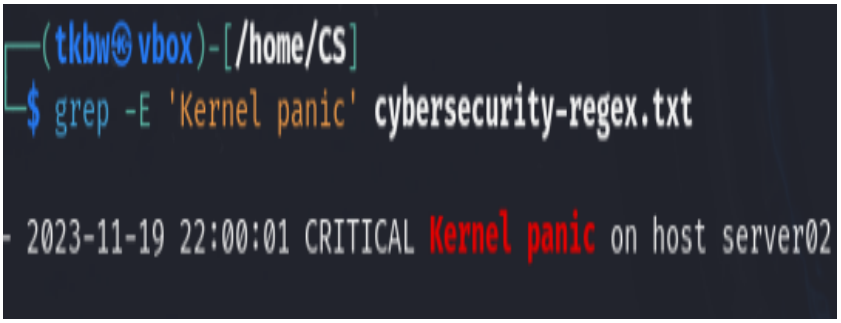


=> This search for words that start with "Log" followed by any number of small letters (such as "Logger", "Login", "LOGS", etc.) in the Cyblesecurity-Regex.TX file, and only displays those identical words.



=> It is searching for any congruence of time in Figure 12: MM: SS or 13: MM: SS where minutes and seconds range between 00 and 59 in the Cybersecurity-Ragex.txt file and displays lines that contain a match.

=> This matter searches for titles that start with 192.168.1.1, and is followed by a number of 1 to 3 numbers (such as 192.168.1.1 or 192.168.1.255) in the Cyberssecurity-Regex.txt file, and displays lines that contain a match.



=> This is searching for lines that contain "Kernel Panic" text in the Cyber view-progex.txt file and display these lines

---

2305573 / عبدالرحمن حسام