**1st Oct ‘23**

**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

**Windows Event Logs**

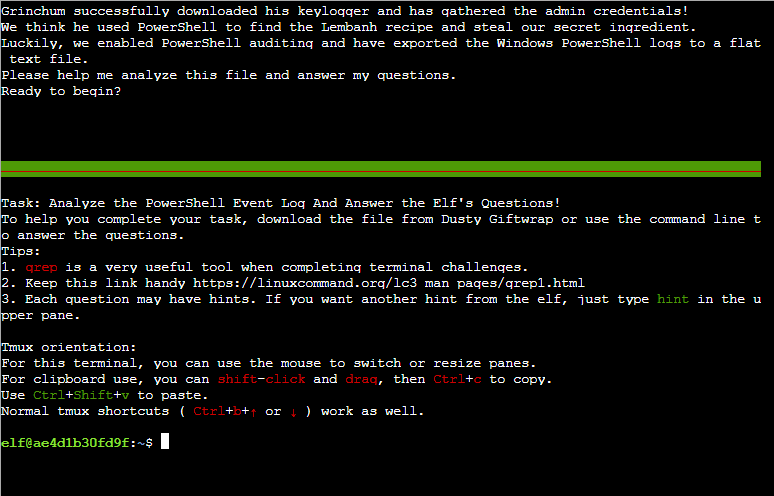
**Amogh Patel**

**Collaborator: Frances Brandofino**

**Source used: Hint tab**

**A screenshot of a video game

Description automatically generated**

****

**Prompt 1:** 

**Answer:** 12/24/2022

**A blue screen with white text

Description automatically generated**

**Explanation:** After going through each date section 12/24/2022 has the highest events count (3540).

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 2: **

**Answer: Recipe**

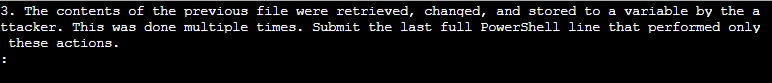
**Explanation:** From using the hints, we can use the **“Add-Content”** command on the provided log file. Using the command **grep “Add-Content” powershell.evtx.log**, we can see file names **‘recipe’** and ‘**recipe updated’**.From the available file names **‘recipe’** would be the original file name.

The search term, **‘add-content’**, is a command that changes or adds content to an already made file. By putting it as the search term, we find all the parts of the file that had been given changes and what the original versions looked like.

**A screen shot of a computer

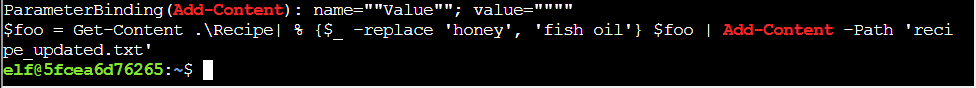
Description automatically generated**

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 3: **

**Answer: $foo = Get-Content .\Recipe| % {$\_ -replace 'honey', 'fish oil'}**

**Explanation:** In the previous answer,a variable **‘$foo’** can be seen towards the bottom of the search results (variables are labeled through the $ before the word). From the **‘$foo’** variable we can see the file being changed or replaced (-replace). We copy the command and use that for the answer.



--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 4: **

**Answer:** **$foo | Add-Content -Path 'recipe'**

**Explanation:** From prompt 2 output, look for the first Add-Content line with the variable **‘$foo’**. This command, like the name suggests, adds content to the file, meaning that it modifies the content. Therefore, any line with this command is modifying the file.

**A screenshot of a computer program

Description automatically generated**

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 5: **

**Answer: Recipe.txt**

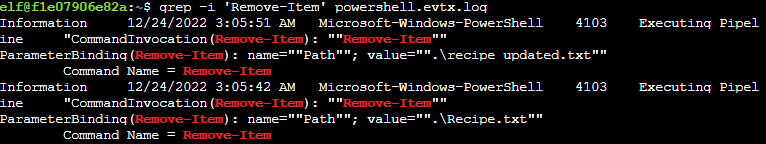
**Explanation:** From prompt 2 output, we find that the term **‘Recipe.txt’** appears more often than other file names, such as **‘Recipe’** and **‘recipe updated.txt’**

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 6: **

**Answer: Yes**

**Explanation:** Using the hints, the command to search for here is **‘Remove-Item’**, which as the name suggests, deletes files and items. As such, using the command **grep -i ‘Remove-Item’ powershell.evtx.log** will show any instances of a file being removed. And because there are clearly some examples of this, the answer is Yes.



--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 7: **

**Answer: No**

**Explanation:** The original file is **‘Recipe’** with no added text. From our knowledge gained in the previous question, **‘Recipe’** was never deleted.

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 8: **

**Answer: 4104**

**Explanation:** From the previous output the Event ID ‘4103’ might seem like the correct answer after using the hints it states, ‘there are more context in the output’. Using Event Viewer if we sort the Event IDs and observe the Taks category it states ‘Executing Pipeline’ for Event ID 4103 and ‘Execute a remote command’ for ID 4104. We pick 4104.

A screenshot of a computer

Description automatically generated

--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 9: **

**Answer: Yes**

**Explanation:** In the search results for **‘grep -i ‘$foo’ powershell.evtx.log’**, there is an ingredient that is changed. Therefore, this ingredient has been compromised.



--------------------------------------------------------------------------------------------------------------------------------------------------------

**Prompt 10: **

**Answer: Honey**

**Explanation:** Using the previous answer, the original secret ingredient is Honey.