1. Create the following hierarchy of directories and numbered files (1. 2. 3.)
    a. Cyber_Dept
        i. GRC
            1. Governance
            2. Risk_Management
            3. Compliance.txt
        ii. VAPT
            1. Vulnerability Assessment
            2. Penetration Testing
        iii. SOC
            1. SIEM.txt ; and write down its index number
            2. Incident_Response
            3. Threat_Intelligence
        iv. Monitoring

2. Use a text editor to add the following text to “SIEM” file

    Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. The term and the initialism SIEM were coined by in 2005

3. Use a text editor to add the following text to “Compliance” file

    Remote access policy:85.54: admin: compliant
    Physical security policy:73.91: management
    Auditing policy:94.66: Finance: compliant

4. Copy the SIEM file to the Monitoring directory

5. Rename the copied file to “Logging”

6. Delete the Monitoring directory and all its contents

7. Create a hard link to SIEM file in the path /var/log and write down its index number

8. Create a soft link to SIEM file in the path ~/Desktop and write down its index number

9. Display “Compliance” file contents in the terminal
10. Display the Auditing policy line from “Compliance” file in the terminal
11. Display the first two line from “Compliance” file to the terminal
12. Display the last two line from “Compliance” file to the terminal
13. Find how many links SIEM file has
14. Find all text files in the Cyber_Dept hierarchy
15. Find how many lines and words SIEM file has
16. Find the compliant policies lines and write them to the Governance file
17. Compare between the files Compliance and Governance, then find the non-compliant policies
18. Write the non-compliant policies to the Incident_Response file
19. Sort the policies alphabetically based on their names
20. In the Compliance file, replace all “policy” word with “Rules”
21. Display in the terminal the second field of “Compliance” file with one digit after the decimal point
22. Find all file which have zero size in the Cyber_Dept hierarchy