تقديم الطالبة: رؤى محمد عارف عوده

1. Create the following hierarchy of directories and numbered files (1. 2. 3.)

a. Cyber_Dept

```
mkdir Cyber_Dept
 cd Cyber_Dept
```

i. GRC

1. Governance
2. Risk_Management
3. Compliance.txt

```
mkdir GRC
cd GRC
touch Governance
touch Risk_Management
touch Compliance.txt
cd ..
```

ii. VAPT

1. Vulnerability Assessment
2. Penetration Testing

```
mkdir VAPT
cd VAPT
touch Vulnerability_Assessment
touch Penetration_Testing
cd ..
```

iii. SOC

1. SIEM.txt ; and write down its index number
2. Incident_Response
3. Threat_Intelligence

```
mkdir SOC
cd SOC
touch SIEM.txt
ls -i SIEM.txt
touch Incident_Response
touch Threat_Intelligence
cd ..
```

iv. Monitoring

```
mkdir Monitoring
```

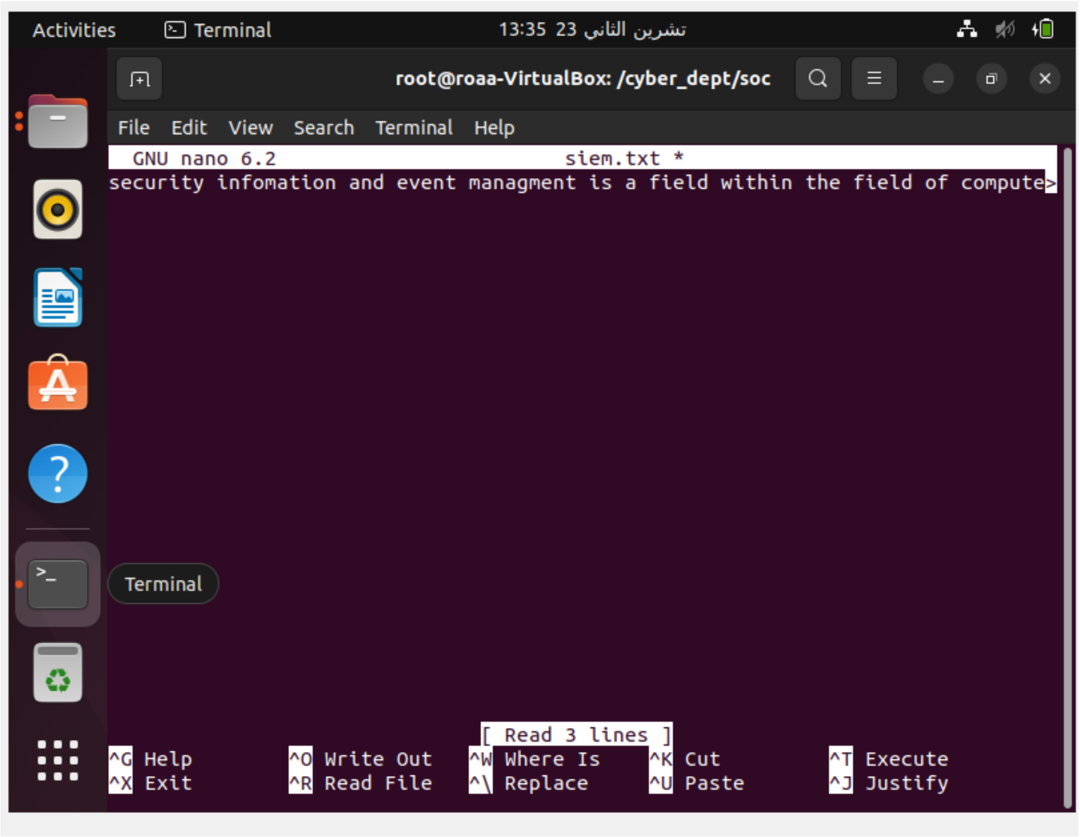
Additional commands

```
sudo apt  install tree
tree
```

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

cd SOC
nano SIEM.txt
Type the text or Paste it
Ctrl + X
Y
Enter
cat SIEM.txt

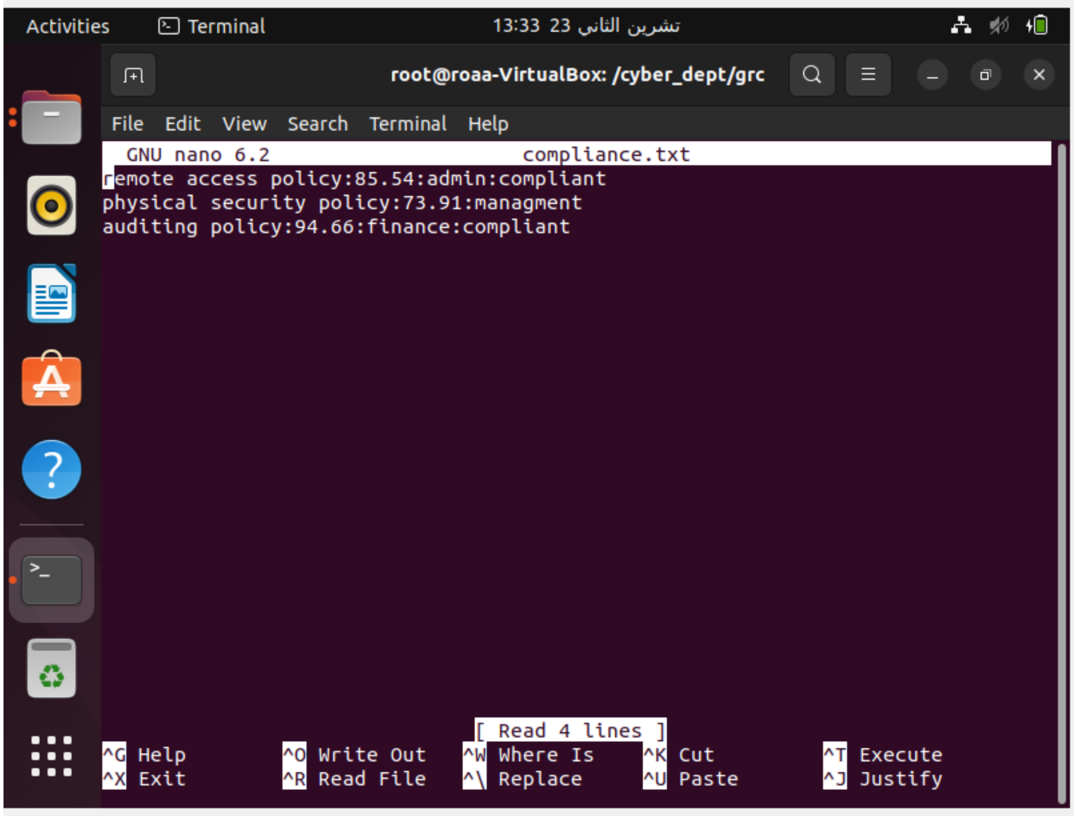

Activities
Terminal
13:35 23 تشرين الثاني
root@roaa-VirtualBox: /cyber_dept/soc
File Edit View Search Terminal Help
Terminal

```
  GNU nano 6.2                          siem.txt *
security infomation and event managment is a field within the field of compute>




                                   [ Read 3 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

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

cd ../GRC/
nano Compliance.txt
Type the text or Paste it
Ctrl + X
Y
Enter
cat Compliance.txt
cd ..



```
  GNU nano 6.2                          compliance.txt
remote access policy:85.54:admin:compliant
physical security policy:73.91:managment
auditing policy:94.66:finance:compliant
```

```
                                    [ Read 4 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

4. Copy the SIEM file to the Monitoring directory

```
cp SOC/SIEM.txt Monitoring
```

5. Rename the copied file to “Logging”

```
cd Monitoring
mv SIEM.txt logging.txt
```

6. Delete the Monitoring directory and all its contents

```
cd ..
rm –rv Monitoring
```

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

```
sudo ln SOC/SIEM.txt /var/log/hardl
cd /var/log/
ls -i hardl
```

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

```
cd ~/Cyber_Dept
ln -s ~/Cyber_Dept/SOC/SIEM.txt ~/Desktop/softl
cd ~/Desktop
ls -i softl
readlink -f ~/Desktop/softl
cat softl
```

9. Display “Compliance” file contents in the terminal

```
cd ~/Cyber_Dept/GRC
cat Compliance.txt
```

10. Display the Auditing policy line from “Compliance” file in the terminal

```
grep Auditing Compliance.txt
```

11. Display the first two line from “Compliance” file to the terminal

```
head -n 2 Compliance.txt
```

12. Display the last two line from “Compliance” file to the terminal

```
tail -n 2 Compliance.txt
```

13. Find how many links SIEM file has

```
cd ../SOC
stat SIEM.txt
cd ..
```

14. Find all text files in the Cyber_Dept hierarchy

```
find ~/Cyber_Dept -name "*.txt"
```

15. Find how many lines and words SIEM file has

```
cd SOC
wc -wl SIEM.txt
cd ..
```

16. Find the compliant policies lines and write them to the Governance file

```
cd GRC
grep compliant$ Compliance.txt >> Governance
cat Governance
```

17. Compare between the files Compliance and Governance, then find the non-compliant policies

```
diff Compliance.txt Governance
```

18. Write the non-compliant policies to the Incident_Response file

```
diff Compliance.txt Governance >> ../SOC/Incident_Response
cat ../SOC/Incident_Response
```

19. Sort the policies alphabetically based on their names

```
sort Compliance.txt
```

20. In the Compliance file, replace all “policy” word with “Rules”

```
sed 's/policy/rules/' Compliance.txt  > test.txt
mv test.txt Compliance.txt
cat Compliance.txt
```

21. Display in the terminal the second field of “Compliance” file with one digit after the decimal point

```
printf "%0.1f\n" $(cut -d ":" -f 2 Compliance.txt)
```

22. Find all file which have zero size in the Cyber_Dept hierarchy

```
cd ..
find ~/Cyber_Dept -size 0
```