

1.a. Encrypting and Decrypting Data Using a Hacker Tool

```
mkdir first
cd first
echo "this is my first practice1" > sample1.txt
echo "this is my first practice2" > sample1.txt
echo "this is my first practice3" > sample1.txt
zip -e file1.zip sample* pass:g
zip -e file2.zip sample* pass:w1
unzip file1.zip
fcrackzip --help
fcrackzip -vul 1-2 file1.zip
fcrackzip -vul 1-2 file2.zip
```

<https://itexamanswers.net/9-1-1-7-lab-encrypting-and-decrypting-data-using-a-hacker-tool-instructor-version.html>

b. Encrypting and Decrypting Data Using OpenSSL

```
echo "hello world" > text1.txt
Encryption:
openssl aes-256-cbc -a -in text1.txt -out text2.txt
cat text2.txt
Decryption:
openssl aes-256-cbc -a -d -in text2.txt -out text3.txt
cat text3.txt
or
openssl aes-256-cbc -a -d -in text2.txt
cat text2.txt
```

```
openssl aes-256-cbc -a -in letter_to_grandma.txt -out msg.enc
openssl aes-256-cbc -a -d -in msg.enc -out text4.txt
```

<https://www.studocu.com/en-au/document/holmesglen-institute-of-tafe/cyber-security/9116-lab-encrypting-and-decrypting-data-using-open-ssl/55246450>

```
+++++
to create the below letter_to_grandma.txt file use below command
+++++
nano letter_to_grandma.txt
```

Hi Grandma,
I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,
Your cookie-eater grandchild.

c. Hashing a Text File with OpenSSL and Verifying Hashes

```
openssl sha256 letter_to_grandma.txt
openssl sha512 letter_to_grandma.txt
nano letter_to_grandma.txt //change the letter to check the hash
```

cat letter_to_grandma.txt

openssl sha256 letter_to_grandma.txt

openssl sha256 letter_to_grandma.txt

Reference

<https://itexamanswers.net/21-1-6-lab-hashing-things-out-answers.html>

Hi Grandma,

I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,

Your cookie-eater grandchild.

2a. Examining Telnet and SSH in Wireshark

<https://itexamanswers.net/9-1-1-8-lab-examining-telnet-and-ssh-in-wireshark-instructor-version.html>

b. Investigating an Attack on a Windows Host

<https://itexamanswers.net/27-2-16-lab-investigating-an-attack-on-a-windows-host-answers.html>

c. Investigating a Malware Exploit

<https://itexamanswers.net/27-2-15-lab-investigating-a-malware-exploit-answers.html>

3. a. Demonstrate the use of Snort and Firewall Rules

<https://itexamanswers.net/26-1-7-lab-snort-and-firewall-rules-answers.html>

b. Demonstrate Extract an Executable from a PCAP

<https://itexamanswers.net/27-2-10-lab-extract-an-executable-from-a-pcap-answers.html>

c. Demonstrate a practical for Exploring DNS Traffic

<https://itexamanswers.net/3-8-8-lab-explore-dns-traffic-answers.html>

4. a. Using Wireshark to Examine HTTP and HTTPS Traffic

<https://itexamanswers.net/10-6-7-lab-using-wireshark-to-examine-http-and-https-traffic-answers.html>

vulnerable site:

<http://www.altoromutual.com:8080/login.jsp>

non vulnerable site:

<https://demo.testfire.net/login.jsp>

b. Exploring Processes, Threads, Handles, and Windows Registry

<https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html>

5. Perform a practical to Attack on a MySQL Database by using PCAP file.

<https://itexamanswers.net/7-3-2-4-lab-attacking-a-mysql-database-instructor-version.html>

6. Create your own syslog Server/7. Configure your Linux system to send syslog messages to a syslog server and read them

<https://computingpost.medium.com/configure-rsyslog-centralized-log-server-on-ubuntu-22-04-20-04-18-04-b5222129b3f3>

8. Install and Run Splunk on Linux

Splunk:

<https://medium.com/@dannypara/installing-splunk-enterprise-on-ubuntu-step-by-step-guide-b545982038c3>

Installer:

+++++

wget -O splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb

"<https://download.splunk.com/products/splunk/releases/9.4.0/linux/splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb>"

9 Install and Configure ELK on Linux

<https://medium.com/@redswitches/how-to-install-elk-stack-on-ubuntu-20-04-22-04-2c4f13a08c63>

10 Install and Configure GrayLog on Linux

<https://www.chirags.in/tutorial/index.php/97/how-to-install-graylog-on-ubuntu-24-04-lts-step-by-step>