**Lab - Encrypting and Decrypting Data using a Hacker Tool**

## Create and Encrypt Files

### Create text files.

* + - 1. Start the CyberOps Workstation VM.
      2. Open a terminal window. Verify that you are in the analyst home directory. Otherwise, enter **cd ~** at the terminal prompt.
      3. Create a new folder called Zip-Files using the **mkdir Zip-Files** command.
      4. Move into that directory using the **cd Zip-Files** command.
      5. Enter the following to create three text files.

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-1.txt**

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-2.txt**

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-3.txt**

A screenshot of a computer

Description automatically generated

* + - 1. Verify that the files have been created, using the **ls** command.

[analyst@secOps Zip-Files]$ **ls -l**

total 12

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-1.txt

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-2.txt

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-3.txt

A screenshot of a computer

Description automatically generated

### Zip and encrypt the text files.

* + - 1. Create an encrypted zip file called **file-1.zip** containing the three text files using the following command:

[analyst@secOps Zip-Files]$ **zip –e file-1.zip sample\***

* + - 1. When prompted for a password, enter a one-character password of your choice. In the example, the letter **B** was entered. Enter the same letter when prompted to verify.

[analyst@secOps Zip-Files]$ **zip -e file-1.zip sample-\***

Enter password:

Verify password:

adding: sample-1.txt (stored 0%)

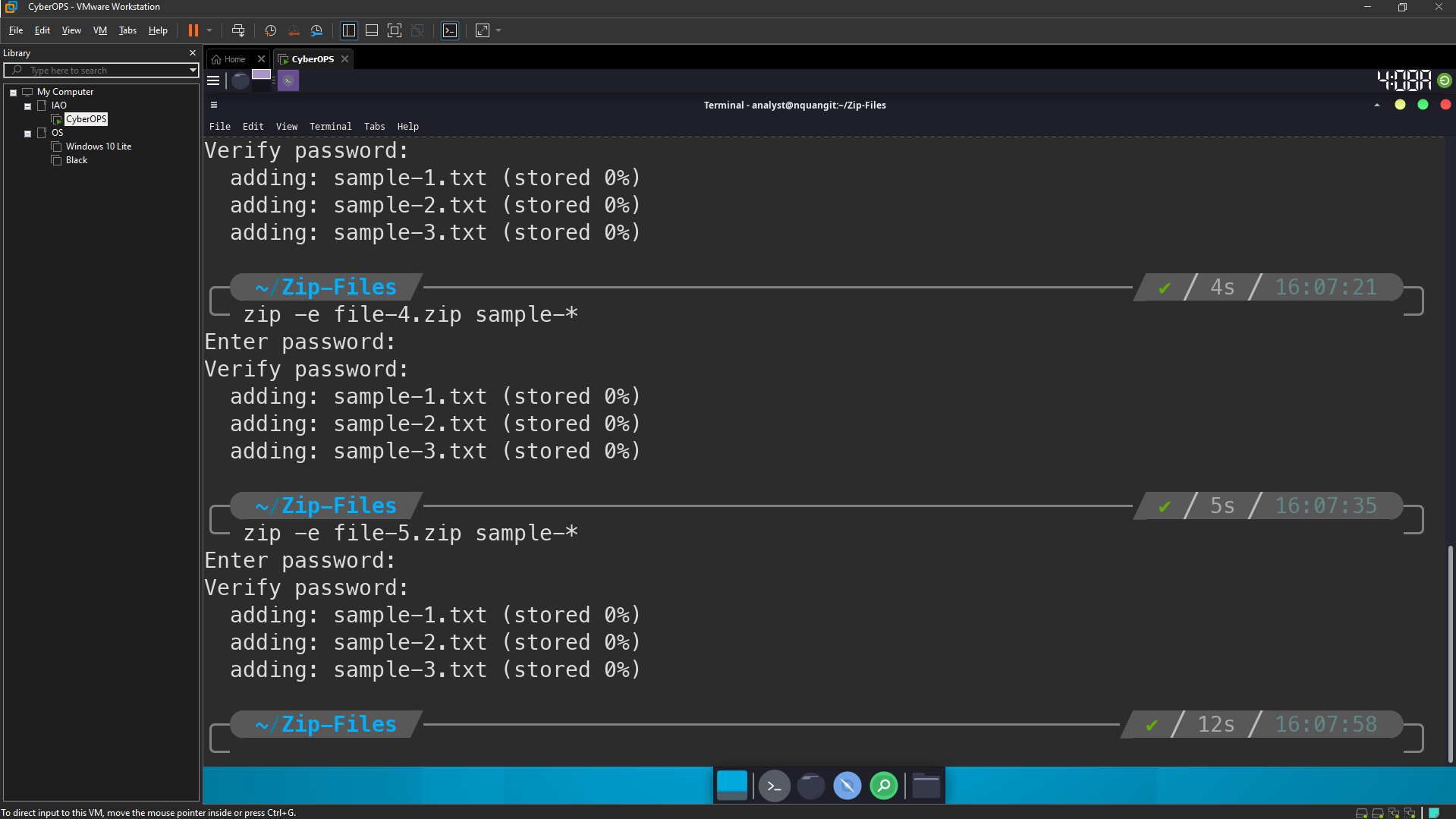
adding: sample-2.txt (stored 0%)

adding: sample-3.txt (stored 0%)

A screenshot of a computer

Description automatically generated

* + - 1. Repeat the procedure to create the following 4 other files
* **file-2.zip** using a 2-character password of your choice. In our example, we used **R2**.
* **file-3.zip** using a 3-character password of your choice. In our example, we used **0B1**.
* **file-4.zip** using a 4-character password of your choice. In our example, we used **Y0Da**.
* **file-5.zip** using a 5-character password of your choice. In our example, we used **C-3P0**.



* + - 1. Verify that all zipped files have been created using the **ls -l f\*** command.

[analyst@secOps Zip-Files]$ **ls -l f\***

-rw-r--r-- 1 analyst analyst 643 May 13 11:01 file-1.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:02 file-2.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-3.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-4.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-5.zip

A screenshot of a computer

Description automatically generated

* + - 1. Attempt to open a zip using an incorrect password as shown.

[analyst@secOps Zip-Files]$ **unzip file-1.zip**

Archive: file-1.zip

[file-1.zip] sample-1.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-1.txt incorrect password

[file-1.zip] sample-2.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-2.txt incorrect password

[file-1.zip] sample-3.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-3.txt incorrect password

### A computer screen shot of a program Description automatically generated

## Recover Encrypted Zip File Passwords

### Introduction to fcrackzip

A screenshot of a computer

Description automatically generated

### Recovering Passwords using fcrackzip

* + - 1. Now attempt to recover the password of the **file-1.zip** file. Recall, that a one-character password was used to encrypt the file.Therefore, use the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip -vul 1-4 file-1.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == B

**Note**: The password length could have been set to less than 1 – 4 characters.

A computer screen with white text

Description automatically generated

#### Question:

How long does it take to discover the password?

Very fast, < 1 second

* + - 1. Now attempt to recover the password of the **file-2.zip** file. Recall, that a two-character password was used to encrypt the file.Therefore, use the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-2.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == R2

A screenshot of a computer

Description automatically generated

#### Question:

How long does it take to discover the password?

Also very fast, less than 1 sec

* + - 1. Repeat the procedure and recover the password of the **file-3.zip** file. Recall, that a three-character password was used to encrypt the file.Time to see how long it takes to discover a 3-letter password.Use the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-3.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == 0B1

A screenshot of a computer

Description automatically generated

#### Question:

How long does it take to discover the password?

Fast, less than 1 sec

* + - 1. How long does it take to crack a password of four characters? Repeat the procedure and recover the password of the **file-4.zip** file. Time to see how long it takes to discover the password using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-4.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

checking pw X9M~

PASSWORD FOUND!!!!: pw == Y0Da

A screenshot of a computer

Description automatically generated

#### Question:

How long does it take to discover the password?

It take about 2 seconds.

* + - 1. How long does it take to crack a password of five characters? Repeat the procedure and recover the password of the **file-5.zip** file. The password length is five characters, so we need to set the **-l** command option to **1-5**. Again, time to see how long it takes to discover the password using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-5 file-5.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

checking pw C-H\*~

PASSWORD FOUND!!!!: pw == C-3P0

A screenshot of a computer

Description automatically generated

#### Question:

How long does it take to discover the password?

About 1m29s

* + - 1. Recover a 6 Character Password using fcrackzip

It appears that longer passwords take more time to discover and therefore, they are more secure. However, a 6 character password would not deter a cybercriminal.

#### Question:

How long do you think it would take fcrackzip to discover a 6-character password?

I think the time depend on the complexity of the password. If 6-character password like “aaaaaa”, it will be very fast to be discovered. But if we use the uppercase character and symbols, it will take more time to crack.

To answer that question, create a file called **file-6.zip** using a 6-character password of your choice. In our example, we used **JarJar**.

[analyst@secOps Zip-Files]$ **zip –e file-6.zip sample\***

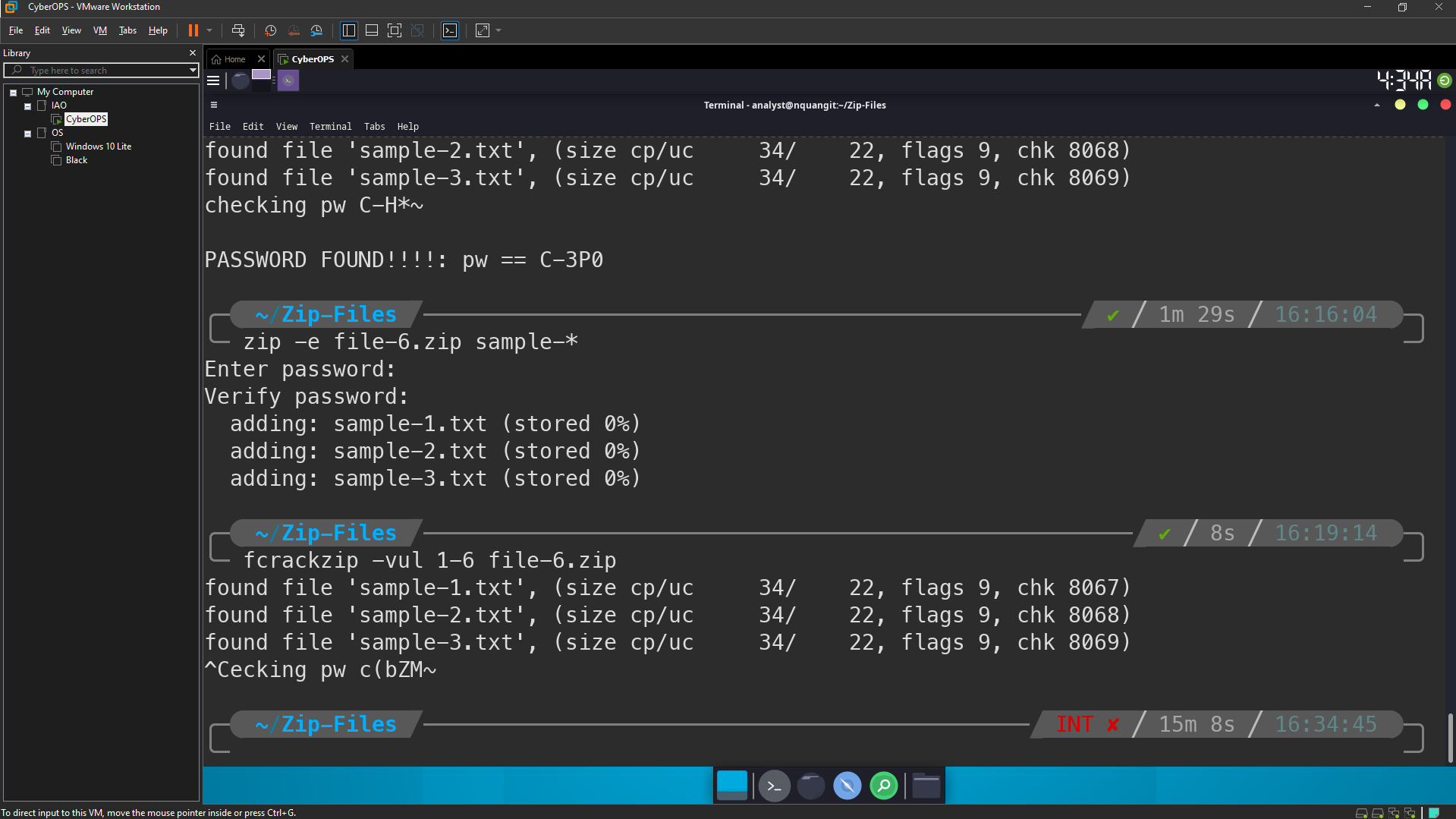
* + - 1. Repeat the procedure to recover the password of the **file-6.zip** file using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-6 file-6.zip**

#### Question:

How long does it take fcrackzip to discover the password?

Very long time. (hours)



The simple truth is that longer passwords are more secure because they take longer to discover.

#### Question:

How long would you recommend a password needs to be for it to be secure?

Use long password with min length 15 characters.

Use lowercase, uppercase, numbers and symbols.