Lab - Encrypting and Decrypting Data using a Hacker Tool

Objectives

Part 1: Create and Encrypt Files

Part 2: Recover Encrypted Zip File Passwords

Background / Scenario

What if you work for a large corporation that had a corporate policy regarding removable media? Specifically, it states that only encrypted zipped documents can be copied to portable USB flash drives.

In this scenario, the Chief Financial Officer (CFO) is out-of-town on business and has contacted you in a panic with an emergency request for help. While out-of-town on business, he attempted to unzip important documents from an encrypted zip file on a USB drive. However, the password provided to open the zip file is invalid. The CFO contacted you to see if there was anything you could to do.

Note: The provided scenario is simple and only serves as an example.

There may some tools available to recover lost passwords. This is especially true in situations such as this where the cybersecurity analyst could acquire pertinent information from the CFO. The pertinent information could be the length of the password and an idea of what it could be. Knowing pertinent information dramatically helps when attempting to recover passwords.

Examples of password recovery utilities and programs include hashcat, John the Ripper, Lophtcrack, and others. In our scenario, we will use **fcrackzip** which is a simple Linux utility to recover the passwords of encrypted zip files.

Consider that these same tools can be used by cybercriminals to discover unknown passwords. Although they would not have access to some pertinent information, with time, it is possible to discover passwords to open encrypted zip files. The amount of time required depends on the password strength and the password length. Longer and more complex passwords (mix of different types of characters) are more secure.

In this lab, you will:

- Create and encrypt sample text files.
- Decrypt the encrypted zip file.

Note: This lab should be used for instructional purposes only. The methods presented here should NOT be used to secure truly sensitive data.

Required Resources

- CyberOps Workstation virtual machine

Instructions

Part 1: Create and Encrypt Files

In this part, you will create a few text files that will be used to created encrypted zip files in the next step.

Step 1: Create text files.

a. Start the CyberOps Workstation VM.

b. Open a terminal window. Verify that you are in the analyst home directory. Otherwise, enter **cd ~** at the terminal prompt.

c. Create a new folder called Zip-Files using the **mkdir Zip-Files** command.

d. Move into that directory using the **cd Zip-Files** command.

e. 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
```

f. 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
```

Step 2: Zip and encrypt the text files.

Next, we will create several encrypted zipped files using varying password lengths. To do so, all three text files will be encrypted using the **zip** utility.

a. 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*
```

b. 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%)
```

c. 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**.

d. 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
```

e. 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
```

Part 2: Recover Encrypted Zip File Passwords

In this part, you will use the **fcrackzip** utility to recover lost passwords from encrypted zipped files. Fcrackzip searches each zip file given for encrypted files and tries to guess the password using brute-force methods.

The reason we created zip files with varying password lengths was to see if password length influences the time it takes to discover a password.

Step 1: Introduction to fcrackzip

From the terminal window, enter the **fcrackzip –h** command to see the associated command options.

In our examples, we will be using the **–v**, **-u**, and **-l** command options. The -l option will be listed last because it specifies the possible password length. Feel free to experiment with other options.

Step 2: Recovering Passwords using fcrackzip

a. 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.

How long does it take to discover the password?

b. 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
```

How long does it take to discover the password?

c. 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
```

How long does it take to discover the password?

d. 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
```

How long does it take to discover the password?

e. 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
```

How long does it take to discover the password?

f. 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.

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

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*
```

g. 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
```

How long does it take fcrackzip to discover the password?

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

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