Hacking Zipped Files with Python

# lesson

**Lesson 1 Details:**

**Background:** A Best Buy employee has been fired (was it Matt??) for posting confidential information to several web sites and online forums. Before the employee was escorted from their desk by security, they hid all their documents in a password-protected .ZIP file on their desktop named ***topsecret.zip***, and they refuse to provide the password. You have been hired to crack the password and extract the contents of the zipped file to see what the employee was hiding.

In the wastebasket next to the employee’s desk, the security team found the following text scrawled on a torn sticky note: University0… but the rest of the note is missing. Security thinks it could be part of the password to the zipped file.

To help you practice cracking the file, the security team produced a similar zipped file, ***test.zip***, encrypted with a password starting with University0, followed by an additional digit. See if you can manually brute-force that file by trying the passwords University00, University01, and so on.

You can find both zipped files on the Github page in the Thursday folder. To get these files onto your Pi, try the following:

1. Open the bash terminal
2. Run the command: git clone <https://github.com/LSCCyberHawks/GenCyber2022.git>

A screenshot of a computer

Description automatically generated

1. Use the change directory command to move into the Thursday directory: Graphical user interface, text

   Description automatically generated

**Lesson:** The security team believes the password for ***topsecret.zip*** is perhaps an additional **5 digits** after University0, so they know they’re going to have to use a computerized app or tool to crack the password. They have enough programming skill internally to crack a password with a single extra digit (like the one for *test.zip*) in Python, and they’ve created the Python 3.X file ***zipit.py*** below to help you get the basic idea:

import zipfile

myzip = zipfile.ZipFile("test.zip")

password = "University0" + str(7)

try:

myzip.extractall(pwd=bytes(password, encoding="utf-8"))

print("File extracted! The password was " + password)

except Exception as e:

print(e)

To use the Python program to crack the zip file, **both files must be located in the same directory** (e.g. put both *test.zip* and *zipit.py* on the Desktop before running *zipit.py* to crack the file). You’ll know the program was able to crack the zip file’s password when a new file, *test.txt*—the content from the zip file, appears next to the *test.zip* and *zipit.py* files.

Your challenge is to modify this code to brute-force the password for the **Topsecret.zip and topsecret.zip** files by adding as many as five digits (or more) after the partial password University0 that we found on the partial sticky note in the fired employee’s trashcan.

After you’ve cracked the file yourself, you can help your peers or teammates with their programs, but remember: no hands-on-keyboard help, all typing and coding must be their own.

**Helpful Hints:**

* can use a variable in the str()
* a for loop with a range might help
* can also try importing the ‘itertools’ library to iterate over every possible combination of numbers.