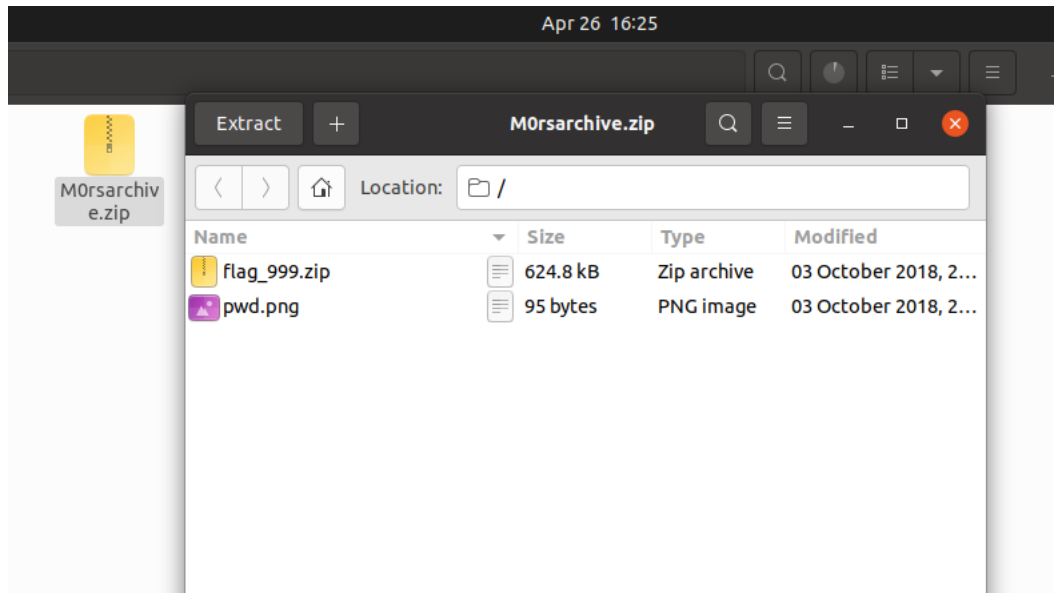


HackTheBox - M0rsarchive

באתגר זה היינו צריכים לפתוח zip בתוך zip (שרשרת של 1000 zip שנמצאים אחד בתוך השני) כאשר כל zip דורש סיסמא אחרת. הסיסמא כתובה בתמונה שבה יש קוד מורס .

התיקיה שיורדת מהאתר של האתגר :



קוד המורס שרשום בתמונה הראשונה מייצג את הספרה 9. (בדקנו באתר שבו יש מילון מורס)

International Morse Code		
A ·-·	N -·-	1 ·-·-·-
B -···	O -·-·	2 ··-·-·
C -·-··	P ·-·-·	3 ·-·-·-
D -···	Q -·-·-	4 ·-·-·-
E ·	R ·-··	5 ·-·-·-
F ·-·-·	S ···	6 -·-·-·
G -·-·	T -	7 -·-·-·
H ····	U ···	8 -·-·-·
I ··	V ···-	9 -·-·-·
J ·-·-·-	W ·-·-	0 -·-·-·
K -·-·	X -·-·-	· ·-·-·-·
L ·-·-·	Y -·-·-	, -·-·-·-
M -·-	Z -·-·-	? ·-·-·-

www.boxentriq.com

HackTheBox - M0rsarchive

בגלל שישנם כנראה 1000 תיקיות כאלה של flags (הבנו את זה כי כאשר פתחנו את הZIP הבא ע"י הסיסמא 9, קיבלנו תיקייה בשם flag ששם היה הקובץ flag_998.zip ותמונה חדשה עם סיסמא חדשה) כתבנו קוד קצר בפייטון שיחלץ את כולם באופן אוטומטי.

השתמשנו בספרייה שמישהו כתב בגיטהאב המקבלת תמונה וע"י שינויי הצבעים של הרקע, קוד המורס והשוואה למילון של מורס - מתרגמת את התמונה לקוד המתאים!

קישור לגיטהאב: <https://github.com/eauxfolles/morse-ocr>

ההפעלה ממש פשוטה – מריצים את הקובץ mocr.py שמקבל כארגומנט את שם התמונה עם קוד המורס והתוכנית מדפיסה את התרגום למסך. (דוגמת הרצה של זה בהמשך)

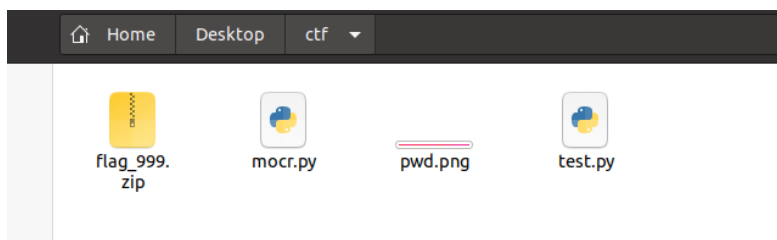
```
1 import zipfile
2 import os, shutil, pathlib, fnmatch
3
4
5 for i in range(999, 0, -1):
6
7     result = os.popen("python3 /home/noa/Desktop/ctf/mocr.py pwd.png").read()
8     result = result.replace("\n", "")
9
10    file_name = 'flag_{}.zip'.format(i)
11    pswd = result
12
13    print(i)
14
15    with zipfile.ZipFile(file_name) as file:
16        # password you pass must be in the bytes you converted 'str' into 'bytes'
17        file.extractall(pwd = bytes(pswd, 'utf-8'))
18
19    os.remove("pwd.png")
20    os.remove(file_name)
21    next_file_name = 'flag_{}.zip'.format(i-1)
22    shutil.move("/home/noa/Desktop/ctf/flag/{}".format(next_file_name), "/home/noa/Desktop/ctf/") #moving the new files back to the origin folder
23    shutil.move("/home/noa/Desktop/ctf/flag/pwd.png", "/home/noa/Desktop/ctf/")
24
25
26
```

תיאור הקוד:

מריץ את mocr.py על התמונה המתאימה עם קוד המורס, ופותחת את הקובץ flag המתאים לאותה סיסמא. לאחר מכן מוחקת את הקובץ flag והתמונה ומביאה מהתיקייה שנוצרה מהחילוץ את הקבצים הבאים. (עוד קובץ flag וקובץ תמונה חדשה מתאימה עם קוד מורס חדש)

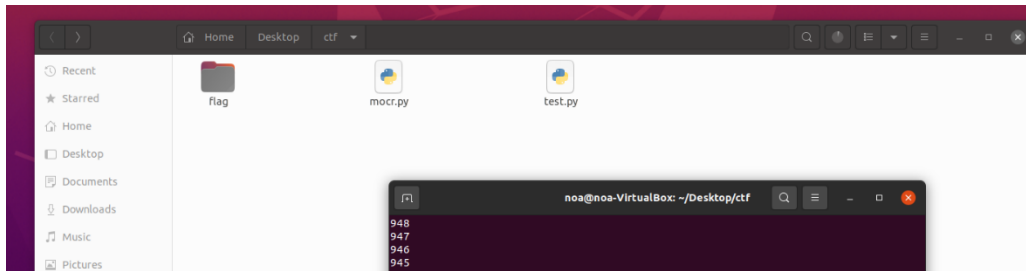
כדי להתחיל להריץ את הקוד, יש לשים באותה תיקייה את הקובץ הראשון שמקבלים – flag_999.zip והתמונה המתאימה. יש לשנות את הpath בקוד לפי הpath במחשב שלכם

תחילת ריצה:

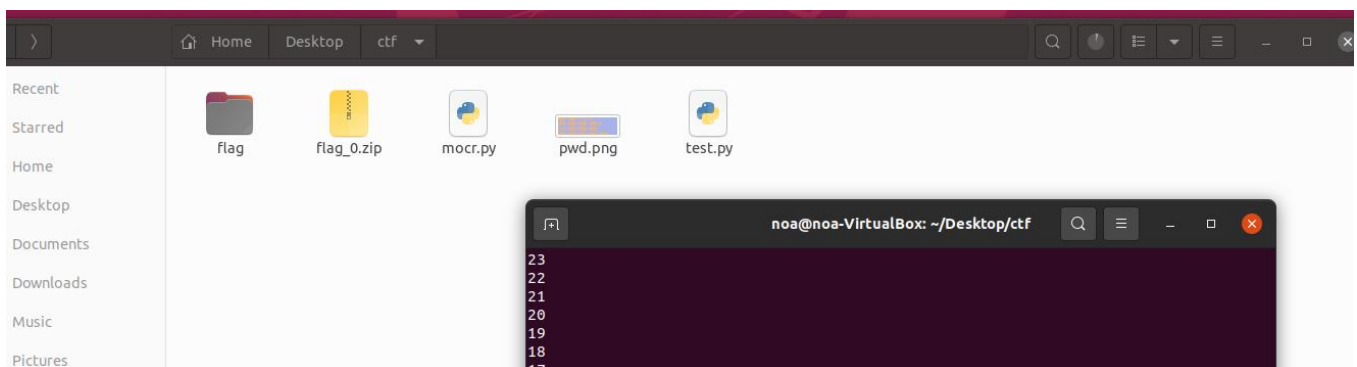


HackTheBox - M0rsarchive

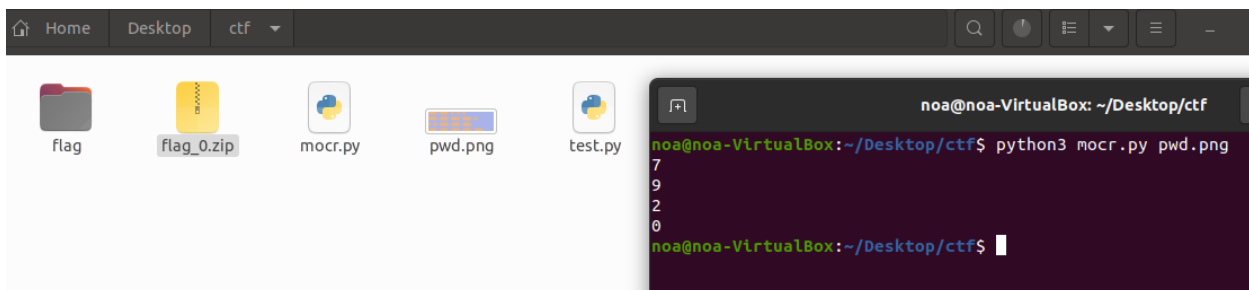
תמונה מריצת התוכנית :



סוף ריצת התוכנית קיבלנו את הקובץ flag האחרון עם התמונה המתאימה .



כדי לפתוח אותו, הרצנו את mocr.py ידנית וקיבלנו שהסיסמא לחילוץ הקובץ האחרון היא : 7920



ולבסוף קיבלנו את הקובץ ובו הדגל !

