CS 7349
Data and Network Security
Homework #3

Name: Bingying Liang
ID: 48999397

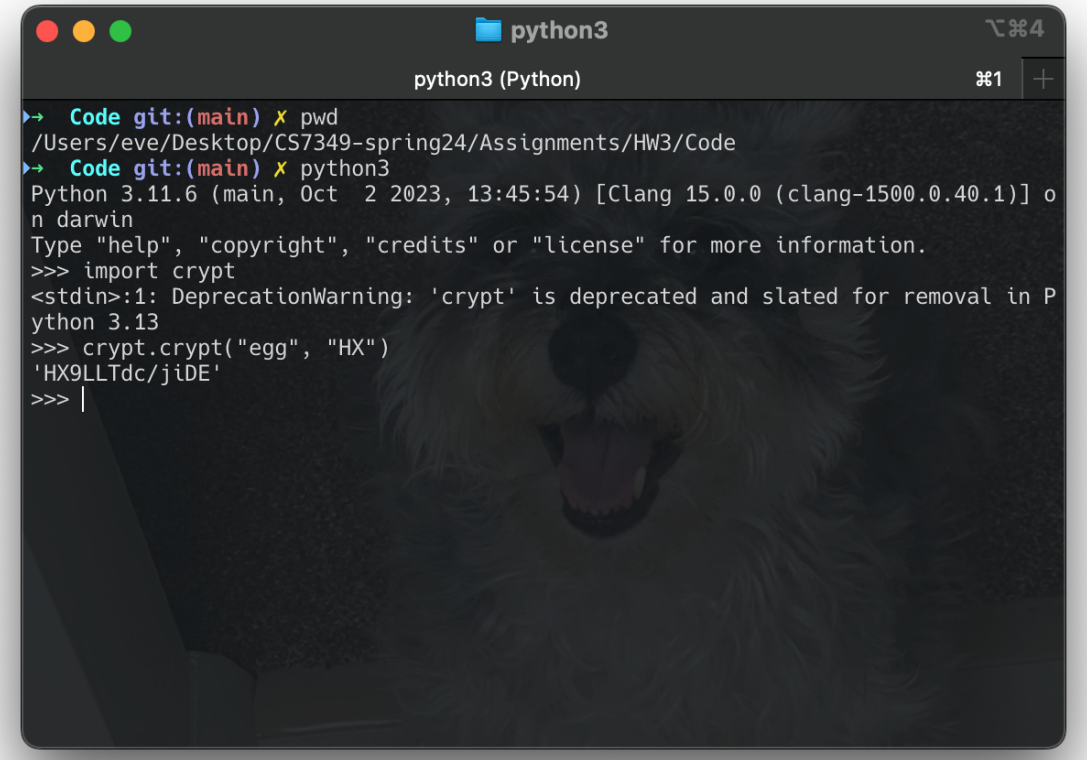
Due: Mar 20 2024

Name: Bingying Liang 
What to Submit

Your final submission shall be a single pdf document that includes this document, screen captures of your exercises plus your answers to each of the written questions (if any). Note that you are expected to clearly label each section so as to make it clear to the instructor what files and data belong to which exercise/question.
Collaboration is expected and encouraged; however, each student must hand in their own homework assignment. To the greatest extent possible, answers should not be copied but, instead, should be written in your own words. Copying answers from anywhere is plagiarism, this includes copying text directly from the textbook. Do not copy answers. Always use your own words. For each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, and Google search results. Note that 'Google' is not a resource. Don't forget to place your name on the document.

Exercise 1: UNIX Password Cracker

The goal of this exercise is to write a password cracker for the UNIX file system. UNIX stores all passwords in the file `/etc/passwd`. Well, it doesn't store the password itself. Instead, it stores a *signature* of the password by using the password to encrypt a block of zero bits prepended by a *salt* value with a one-way function called `crypt( )`. The result of the `crypt( )` function is stored in the `/etc/passwd` file. For example, for a password of "*egg*" and salt equal to "*HX*", the function `crypt('egg','HX')` returns `HX9LLTdc/jiDE`.



When you try to log in, the program `/bin/login` takes the password that you typed, uses `crypt( )` to encrypt a block of zero bits, and compares the result of this function with the value stored in the `/etc/passwd` file.

The security of this approach rests on both the strength of the `crypt( )` function and the difficulty i n g uessing a user's password. The `crypt( )` algorithm has proven to be highly resistant to attacks. Conversely, the user's choices for passwords have been found to be relatively easy to guess, with many passwords being words contained in the dictionary.

To write our UNIX password cracker, we will need to use the `crypt( )` algorithm that hashes UNIX passwords. Fortunately, the crypt library already exists in the Python 2.79 standard library (on UNIX-based operating systems). (Note: for Windows-based operating systems, you will need to find t he c orrect w ay t o i mport t he U NIX `c rypt()` a lgorithm.) To c alculate the encrypted UNIX password signature, we simply call the function `crypt.cypt( )` and pass it the password and salt as parameters. This function returns the signature as a string.

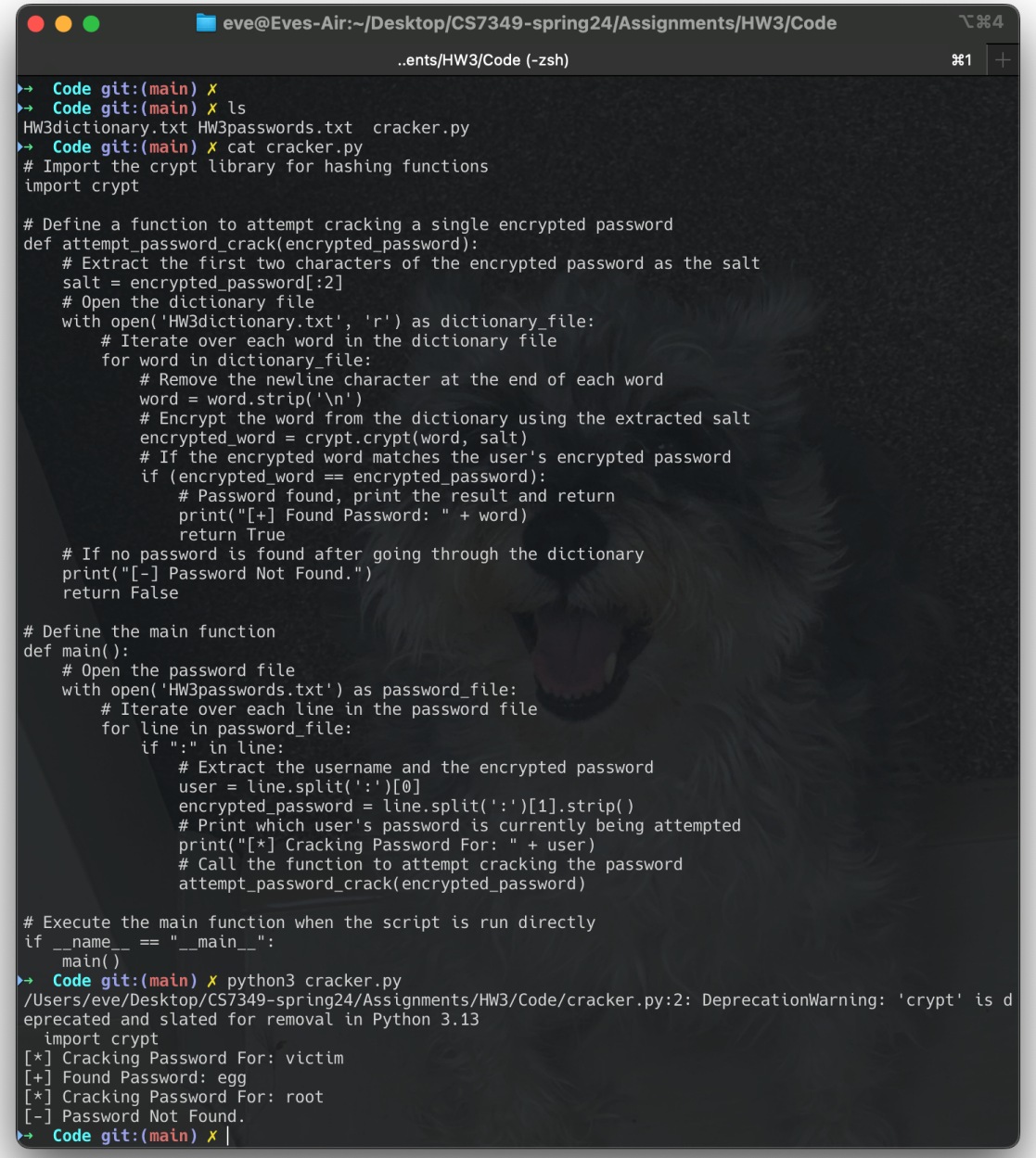
A simple dictionary attack involves computing the possible signatures generated for each word in the dictionary with a range of salt values.

Let's create our first password cracker using a dictionary attack.

1) Create a file called cracker.py. Start your program by reading in the HW2-passwords.txt file and, for each password found in the file, iterate through each dictionary word found in the HW2-dictionary.txt file and appropriate salt value. Report out the password found, if any, for each user. If no password is found, indicate that no password was found.
2) Using literature review, identify from where you can retrieve the salt value used in generating the signature.

Solution:

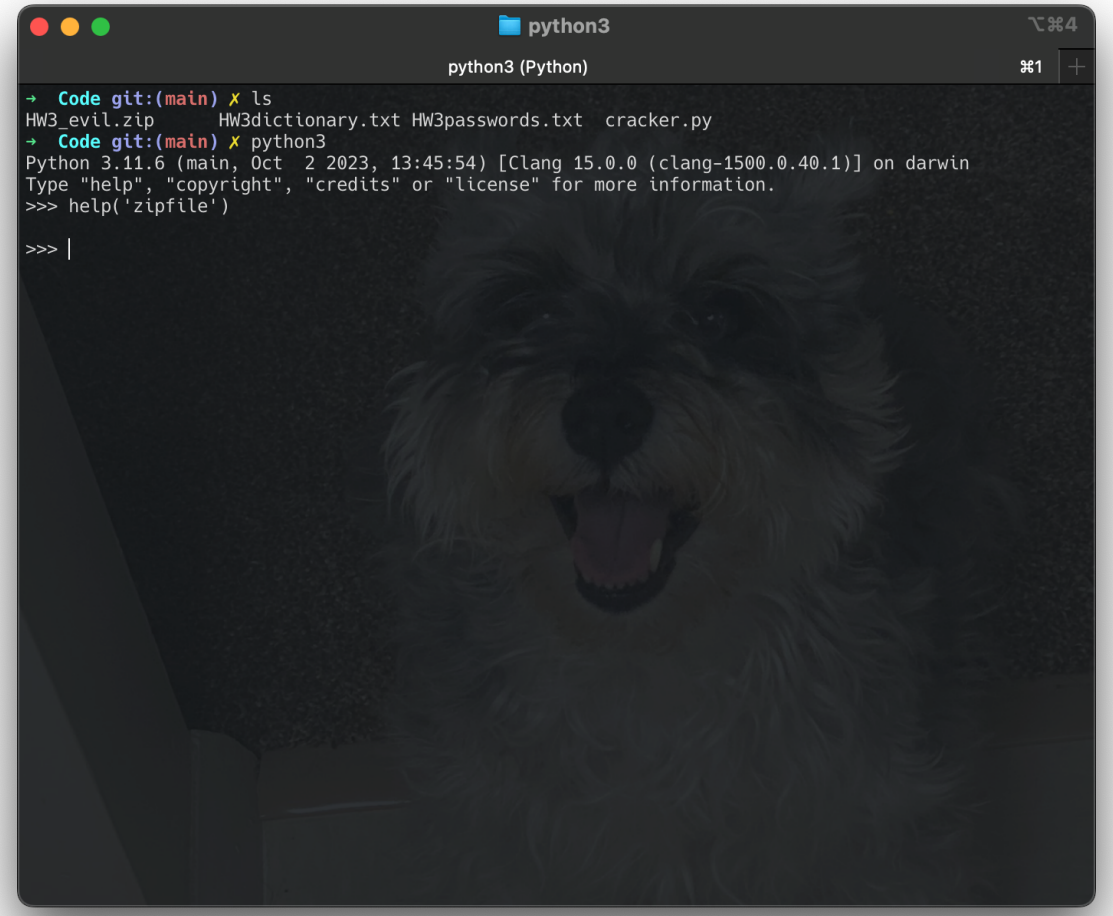
1) The code and result are in the following[1]:

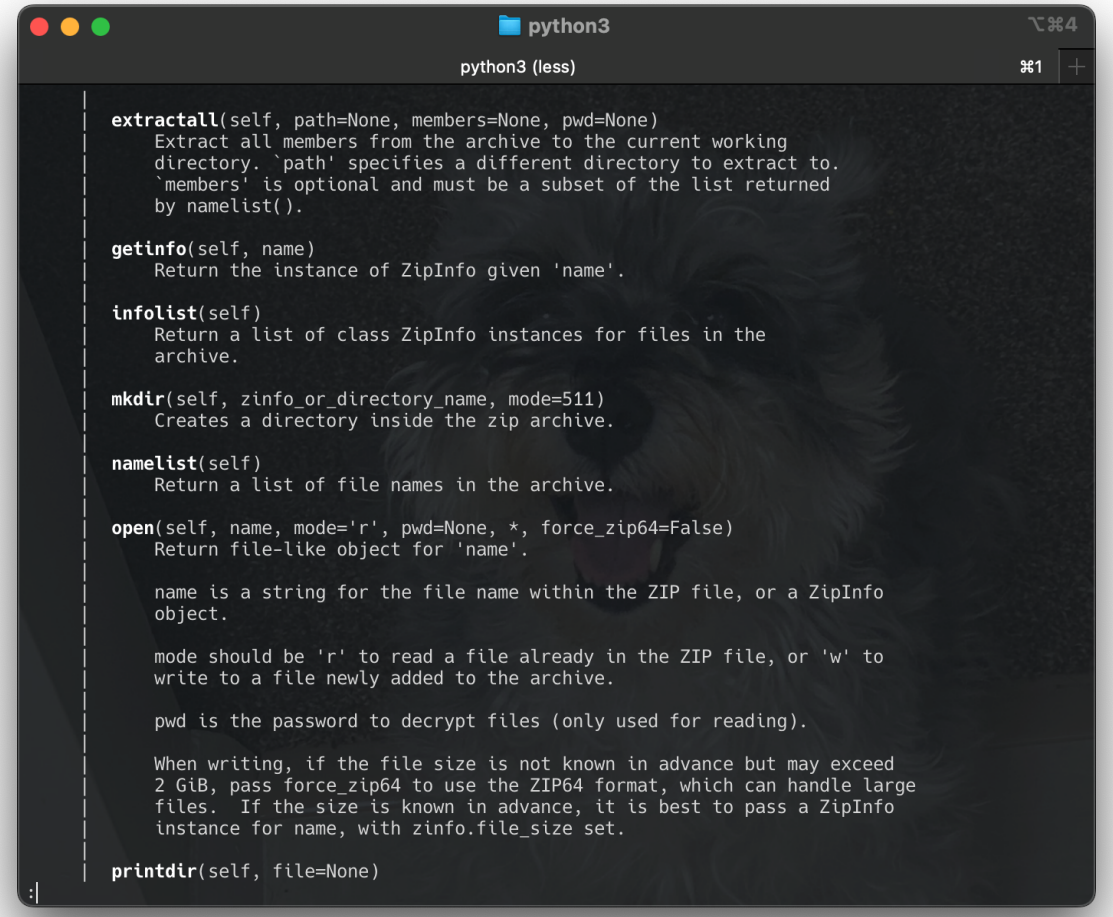


2) In the process of UNIX system password encryption, the salt is an essential component used alongside the user's plaintext password to generate an encrypted password hash. The purpose of the salt is to enhance the complexity and uniqueness of the encryption. In UNIX password storage, the salt typically comprises the first two characters of the encrypted password hash[2]. The way to retrieve the salt[3], extraction from the Encrypted Password: The salt is the first two characters of the stored encrypted password hash. For example, if the encrypted password is "HX9LLTdc/jiDE", the salt would be "HX".

Exercise 2 : Zip File Password Cracker

The goal of this exercise is to write a zip file extractor and password cracker. For this exercise, we will use the zipfile library. You may view information about the zipfile library in Python 2.79 by issuing the command `help('zipfile')` to learn more about the library. Pay close attention to the `extractall( )` method. You may use this method to extract the contents from a zip file.



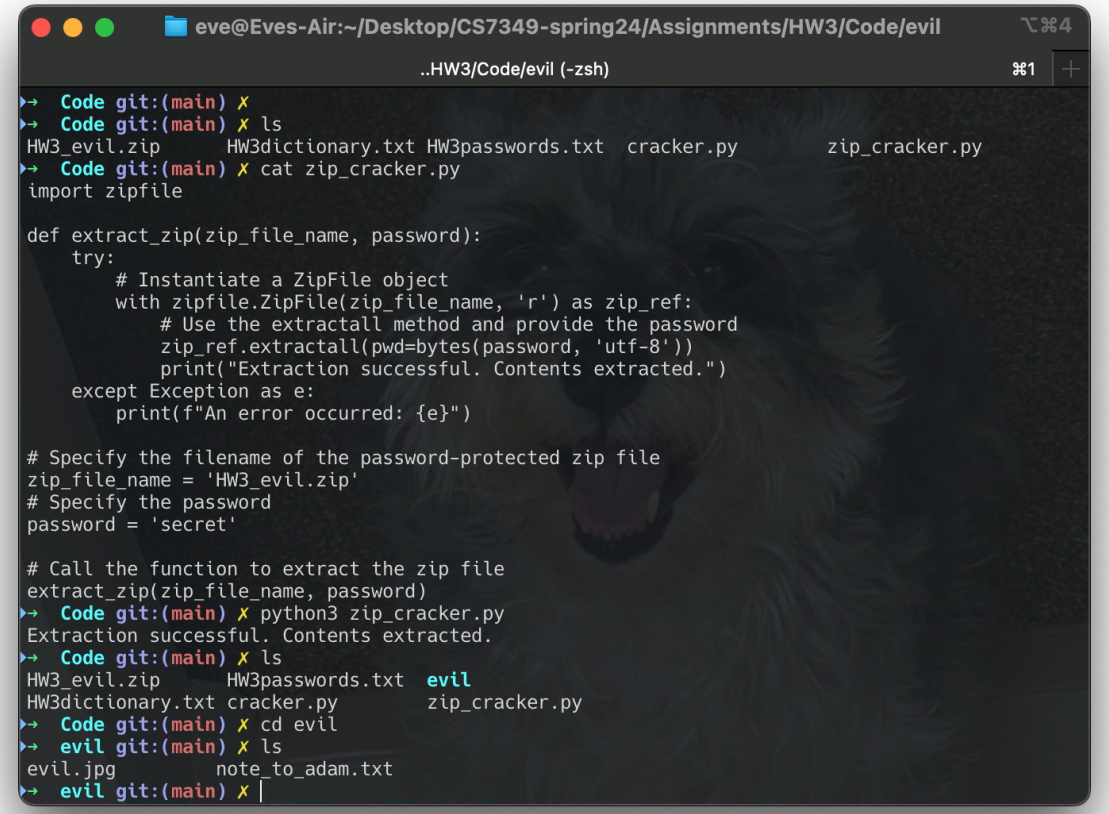


Let's begin the process of writing a zip file password cracker.

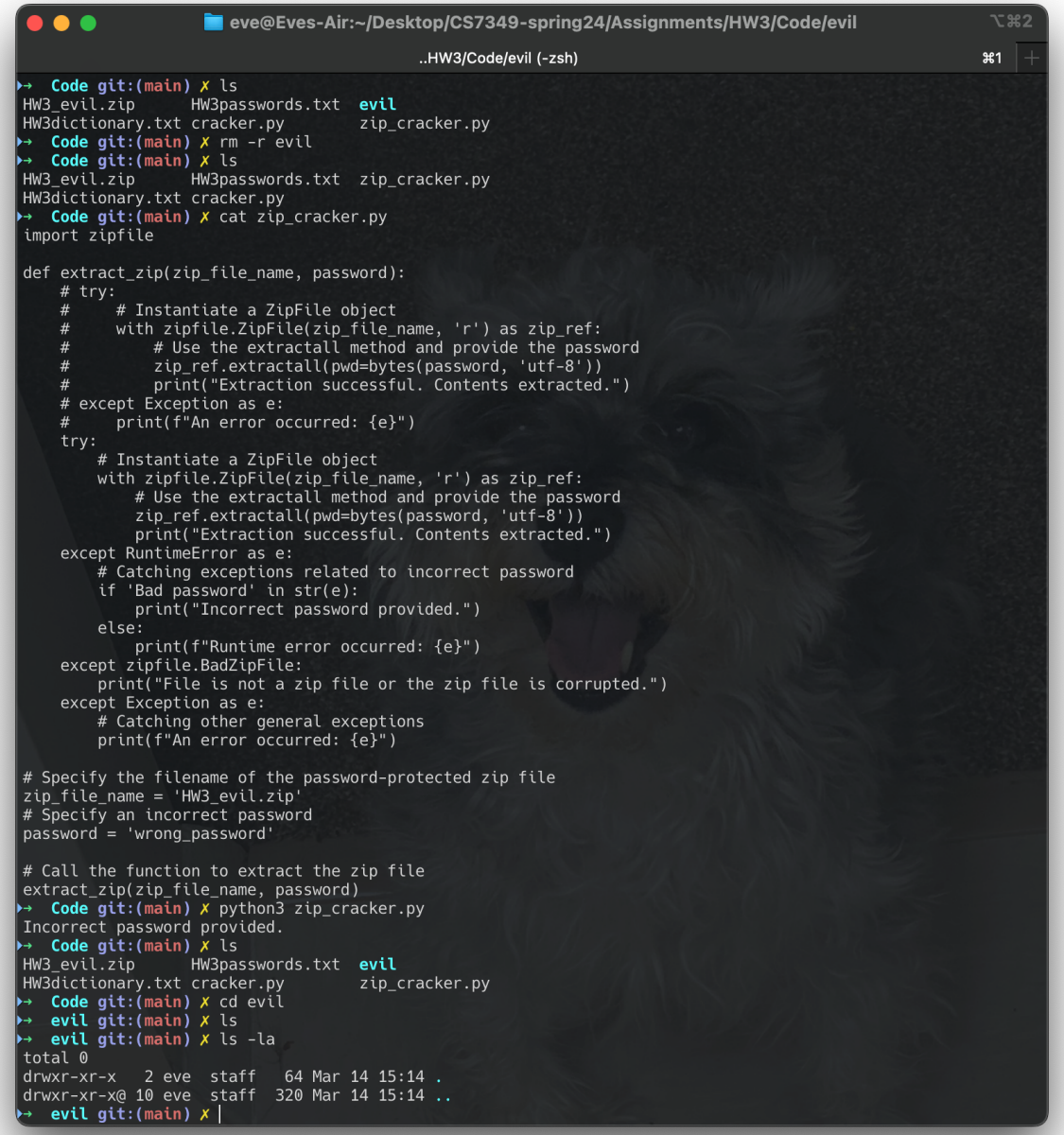
1) Write a quick script to test the use of the zipfile library. After importing the library, instantiate a new ZipFile class by specifying the filename of the password-protected zip file (*evil.zip*). utilize the `extractall( )` method and specify the optional parameter for the password (*secret*). Execute your script and turn in the code and output.
2) Use the `except Exception` exception handler to catch exceptions and print them out when an incorrect password is used. Execute your script with an incorrect password and exception handler and turn in the code and output.
3) Write a script that performs a dictionary attack on the password protected zip file. Execute your script and turn in the code and output. Be sure to provide user feedback on exceptions thrown.

Solution:

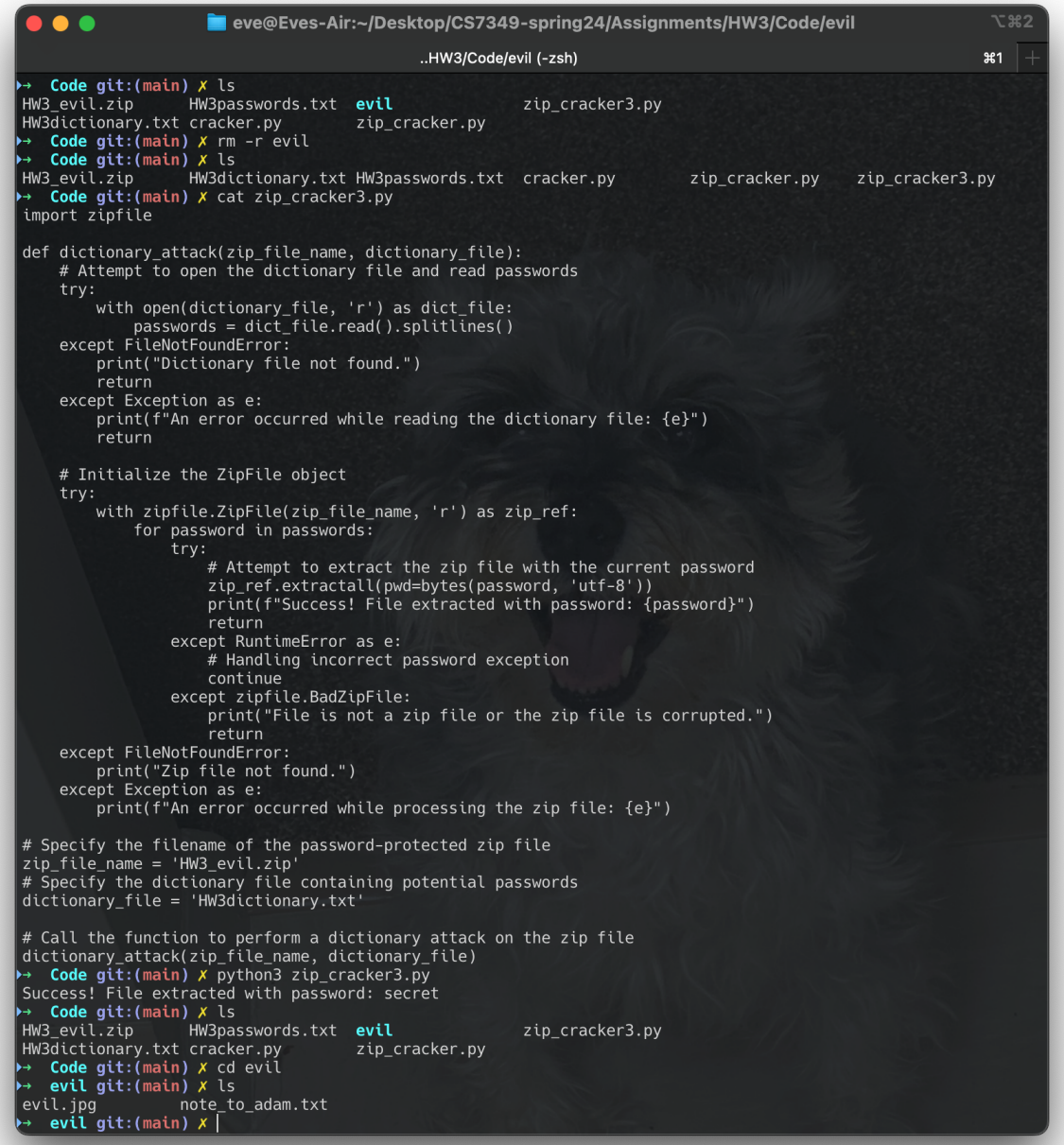
1) The code and result are in the following[4]:



2) The code and result are in the following:



3) The code and result are in the following:



Exercise 3: Port Scanner

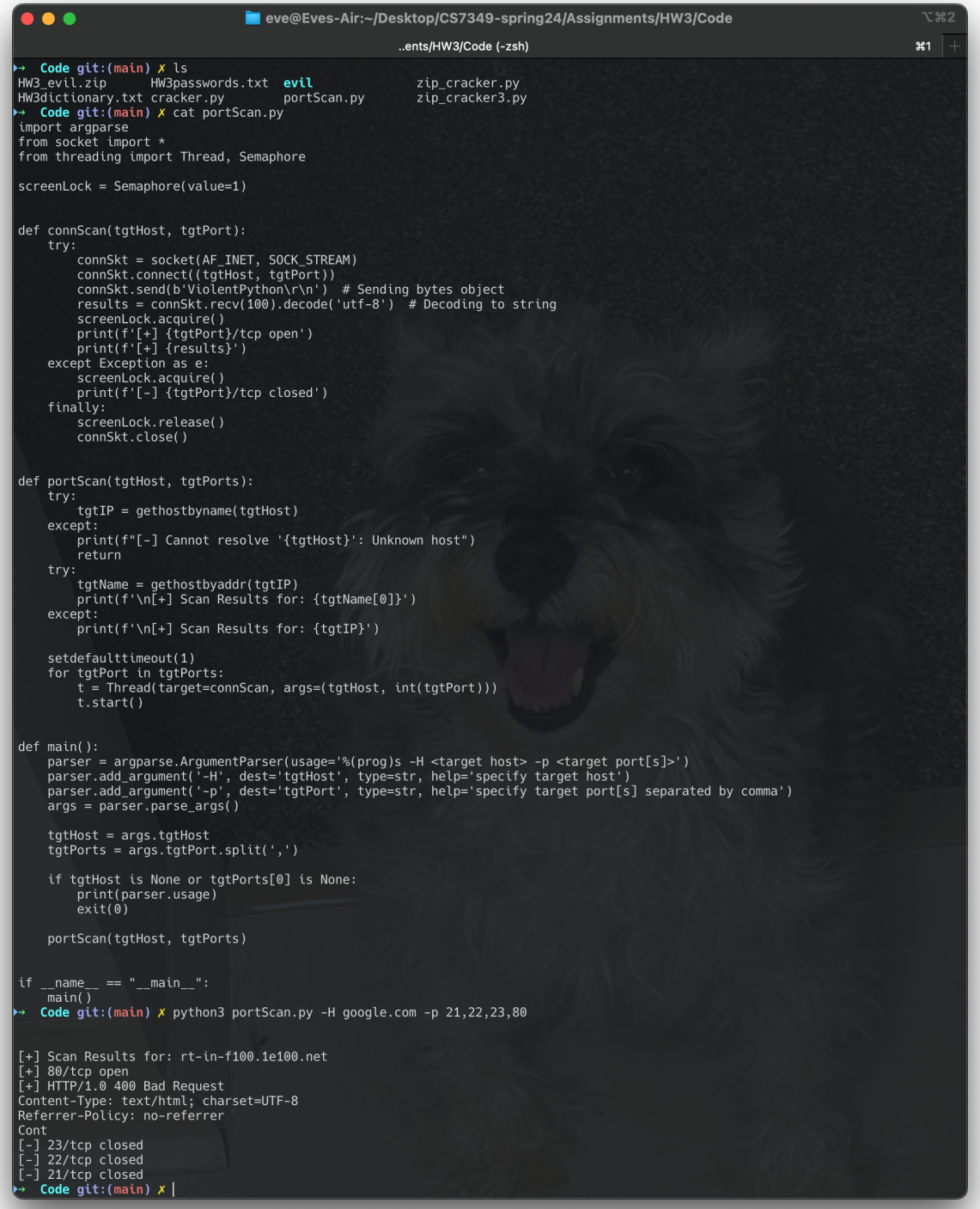
The goal of this exercise is to learn about port scanners for networked systems.

First, create a simple Python-based port scanner. Using the socket library, you will create a script that iterates through a range of IP addresses, and, for each IP address, will identify the active ports available for that IP address. At least ports corresponding to telnet, ftp SSH, smtp, http, imap, and https services should be scanned and identified.

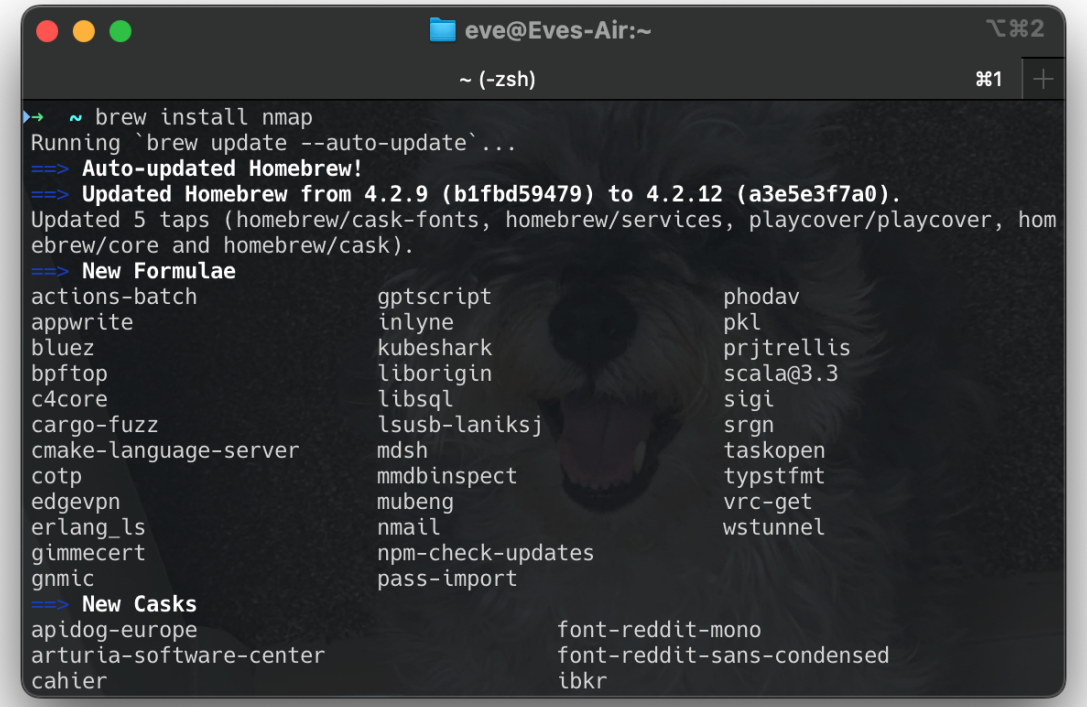
Second, download and install the `nmap` port scanning software from nmap.org. Utilize `nmap` to identify the operating system and the open ports of devices on a range of IP addresses.

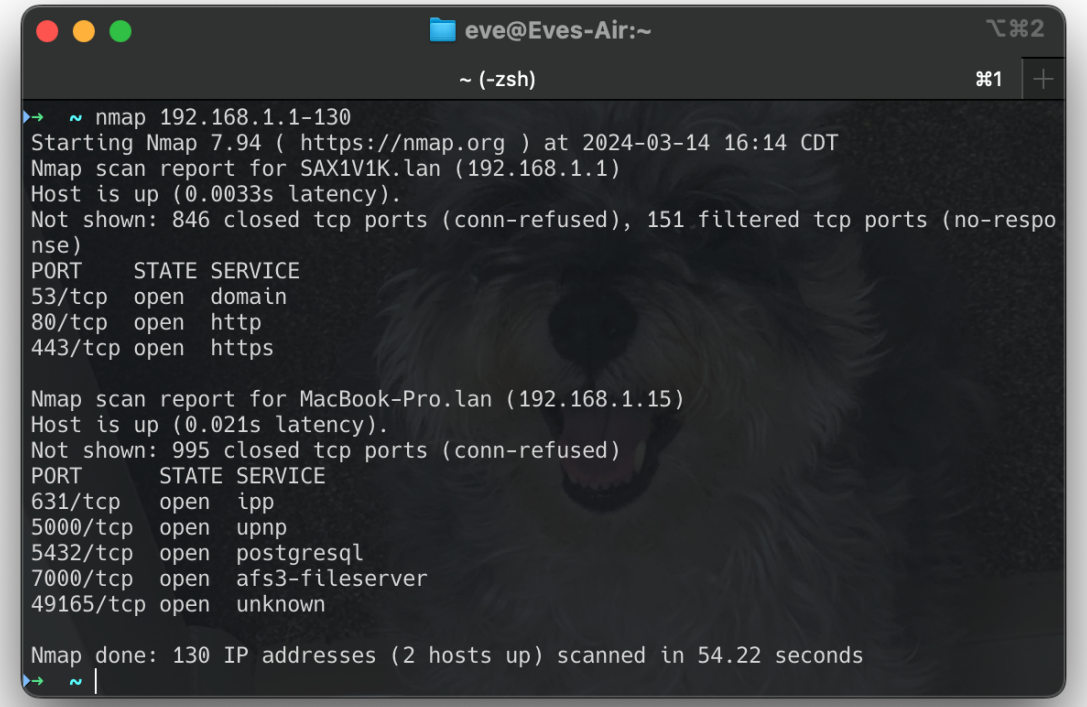
Solution:

First[5],


eve@Eves-Air:~/Desktop/CS7349-spring24/Assignments/HW3/Code
..ents/HW3/Code (-zsh)
→ Code git:(main) ✗ ls
HW3_evil.zip HW3passwords.txt evil zip_cracker.py
HW3dictionary.txt cracker.py portScan.py zip_cracker3.py
→ Code git:(main) ✗ cat portScan.py
import argparse
from socket import *
from threading import Thread, Semaphore
screenLock = Semaphore(value=1)
def connScan(tgtHost, tgtPort):
try:
connSkt = socket(AF_INET, SOCK_STREAM)
connSkt.connect((tgtHost, tgtPort))
connSkt.send(b'ViolentPython\r\n') # Sending bytes object
results = connSkt.recv(100).decode('utf-8') # Decoding to string
screenLock.acquire()
print(f'[+] {tgtPort}/tcp open')
print(f'[+] {results}')
except Exception as e:
screenLock.acquire()
print(f'[-] {tgtPort}/tcp closed')
finally:
screenLock.release()
connSkt.close()
def portScan(tgtHost, tgtPorts):
try:
tgtIP = gethostbyname(tgtHost)
except:
print(f"[-] Cannot resolve '{tgtHost}': Unknown host")
return
try:
tgtName = gethostbyaddr(tgtIP)
print(f'\n[+] Scan Results for: {tgtName[0]}')
except:
print(f'\n[+] Scan Results for: {tgtIP}')
setdefaulttimeout(1)
for tgtPort in tgtPorts:
t = Thread(target=connScan, args=(tgtHost, int(tgtPort)))
t.start()
def main():
parser = argparse.ArgumentParser(usage='%(prog)s -H <target host> -p <target port[s]>')
parser.add_argument('-H', dest='tgtHost', type=str, help='specify target host')
parser.add_argument('-p', dest='tgtPort', type=str, help='specify target port[s] separated by comma')
args = parser.parse_args()
tgtHost = args.tgtHost
tgtPorts = args.tgtPort.split(',')
if tgtHost is None or tgtPorts[0] is None:
print(parser.usage)
exit(0)
portScan(tgtHost, tgtPorts)
if __name__ == "__main__":
main()
→ Code git:(main) ✗ python3 portScan.py -H google.com -p 21,22,23,80
[+] Scan Results for: rt-in-f100.1e100.net
[+] 80/tcp open
[+] HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Cont
[-] 23/tcp closed
[-] 22/tcp closed
[-] 21/tcp closed
→ Code git:(main) ✗

Second[6],


eve@Eves-Air:~
⌥⌘2
~ (-zsh)
⌘1
→ ~ brew install nmap
Running `brew update --auto-update`...
==> Auto-updated Homebrew!
==> Updated Homebrew from 4.2.9 (b1fbd59479) to 4.2.12 (a3e5e3f7a0).
Updated 5 taps (homebrew/cask-fonts, homebrew/services, playcover/playcover, homebrew/core and homebrew/cask).
==> New Formulae
actions-batch
appwrite
bluez
bpftop
c4core
cargo-fuzz
cmake-language-server
cotp
edgevpn
erlang_ls
gimmecert
gnmic
gptscript
inlyne
kubeshark
liborigin
libsql
lsusb-laniksj
mdsh
mmdbinspect
mubeng
nmail
npm-check-updates
pass-import
phodav
pkl
prjtrellis
scala@3.3
sigi
srgn
taskopen
typstfmt
vrc-get
wstunnel
==> New Casks
apidog-europe
arturia-software-center
cahier
font-reddit-mono
font-reddit-sans-condensed
ibkr


eve@Eves-Air:~
⌥⌘2
~ (-zsh)
⌘1
➜ ~ nmap 192.168.1.1-130
Starting Nmap 7.94 (https://nmap.org) at 2024-03-14 16:14 CDT
Nmap scan report for SAX1V1K.lan (192.168.1.1)
Host is up (0.0033s latency).
Not shown: 846 closed tcp ports (conn-refused), 151 filtered tcp ports (no-respo
nse)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
443/tcp open https
Nmap scan report for MacBook-Pro.lan (192.168.1.15)
Host is up (0.021s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT STATE SERVICE
631/tcp open ipp
5000/tcp open upnp
5432/tcp open postgresql
7000/tcp open afs3-fileserver
49165/tcp open unknown
Nmap done: 130 IP addresses (2 hosts up) scanned in 54.22 seconds
➜ ~

References

[1] ‘crypt — Function to check Unix passwords’, Python documentation. Accessed: Mar. 14, 2024. [Online]. Available: https://docs.python.org/3/library/crypt.html

[2] W. Stallings, Cryptography and network security: principles and practice, Seventh edition. Boston: Pearson, 2014.

[3] ‘How Unix Implements Passwords - Practical UNIX and Internet Security, 3rd Edition [Book]’. Accessed: Mar. 14, 2024. [Online]. Available: https://www.oreilly.com/library/view/practical-unix-and/0596003234/ch04s03.html

[4] ‘zipfile — Work with ZIP archives’, Python documentation. Accessed: Mar. 14, 2024. [Online]. Available: https://docs.python.org/3/library/zipfile.html

[5] ‘Python Programming Tutorials’. Accessed: Mar. 14, 2024. [Online]. Available: https://pythonprogramming.net/python-port-scanner-sockets/

[6] ‘Download the Free Nmap Security Scanner for Linux/Mac/Windows’. Accessed: Mar. 14, 2024. [Online]. Available: https://nmap.org/download#macosx