MSDS 7349-HW3

Name:

**Exercise 1: UNIX Password Cracker (30)**

1. Write the cracker.py program. Turn in the code and output. (20)



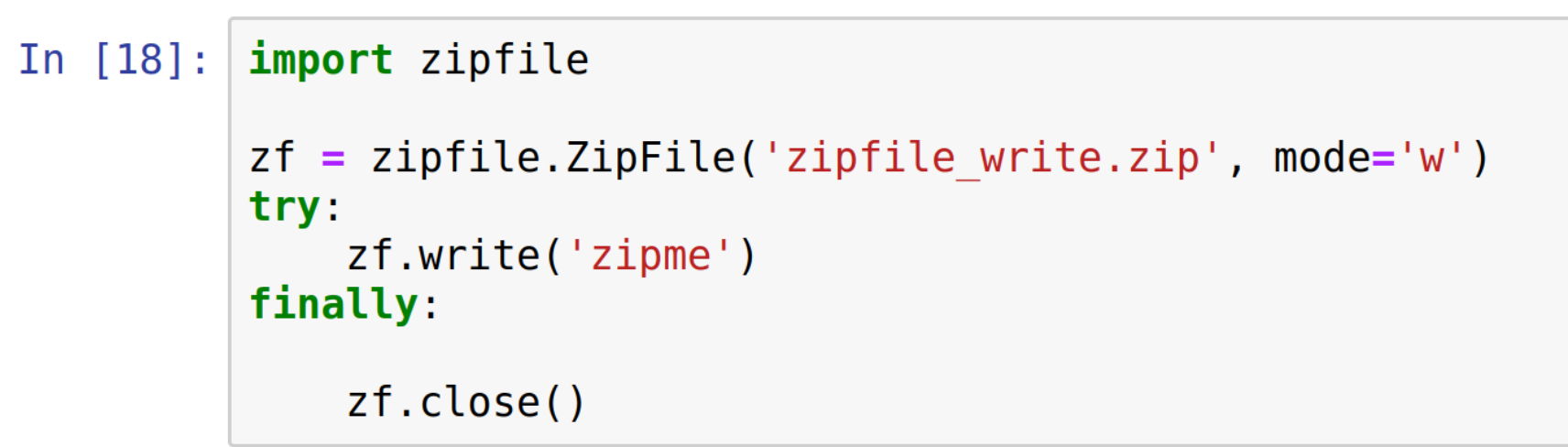
**Though my function doesn’t seem to be working in cell 2 the concept is proven in cell 1. I may come back to this if there is time. Code is attached in ipynb**

2) Identify from where you can retrieve the salt value used in generating the signature (10)

**In older Unix systems the salt value is usually the first 2 characters in the encrypted password string.**

**Exercise 2: Zip File Password Cracker (30)**

1. Write a script to test the use of the zipfile library (10)



1. Use the except Exception handler to catch exceptions and print them out when an incorrect password is used. (10)

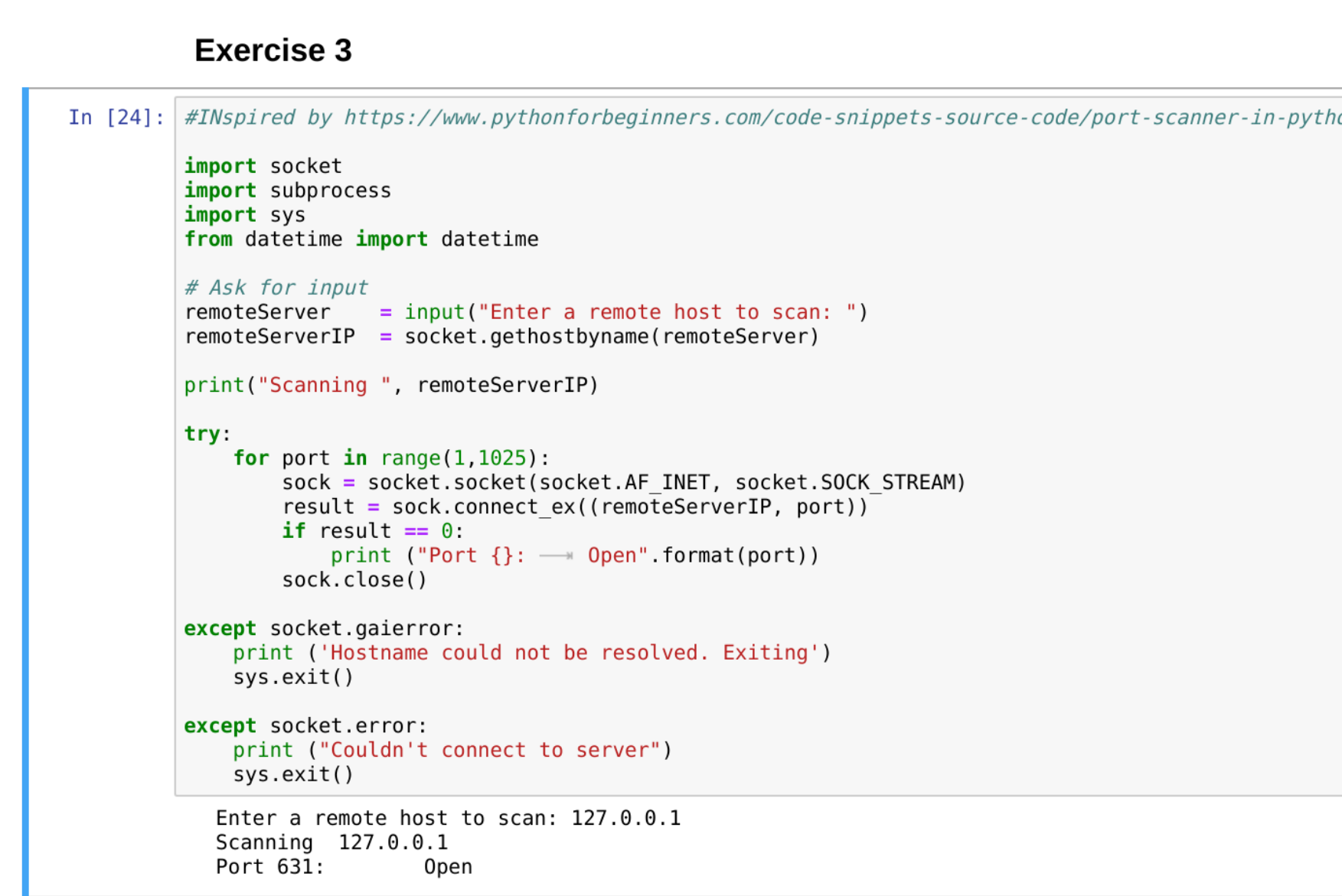


1. Write a script that performs a dictionary attack on the password protected zip file. Execute your script and turn in the code and output. (10)

**It is included in the screenshot above. I googled and copied passwords fomr many dictionaries. Even added the word “evil” but had no luck.**

**Exercise 3: Port Scanner (40)**

1-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 (20)



2- 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 (20)

