FITZHUGH

CSIA 450 – 8372 CYBER SECURITY CAPSTONE

SPRING 2020

Project 2

Objectives

Learn Python and Git fundamentals through application to network security fundamentals.

Problems

A. PYTHON FUNDAMENTALS

It is essential for security professionals to learn Python 3.

There are many great online resources for learning computing and Python. Use the search engine of choice to find relevant materials. I think this course from code academy is succinct and well done: https://www.codecademy.com/learn/learn-python-3. However, there are thousands (if not millions! :-)) of other Python resources available for learning, both free and paid.

Use test python.py as an example if needed to ensure your Python distribution is installed correctly.

```
***IMPORTANT***(!)
```

NOTE: For this project, you will submit two files: a normal PDF for ALL of the answers below and a supporting .py source code file.

Use the template re_robinson_project2.py for your Python code submission.

• Please use Python to complete the following.

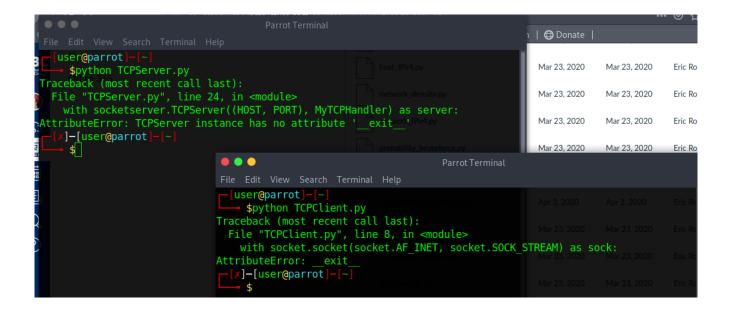
For Problems 1-15 please refer to FITZHUGH PROJECT2.py.

Use https://docs.python.org/3/library/socketserver.html If you need some background on Python sockets.

Use TCPServer.py and TCPClient.py as needed to complete the following. --- try running in linux

12. Change the port number to 8500 and run TCPServer.py and TCPClient.py, sending a network message that contains your name.

Encounter Attribute error in parrot.



Use email_start.py as an example if needed.

16. Use the 'urllib' and 're' modules, ATTEMPT to extract the email address from my CBC staff directory page (http://www.columbiabasin.edu/index.aspx?recordid=2956&page=45). You MUST submit code showing your email regular expression and an example of it working.

I was not successful with attempting to extract Mr. Robinsons email address for his staff directory page.

I found code online, that uses the 're' module, along with 'requests' module to extract email addresses from a URL.

I first tested it with the given URL to see if the code works, and it does. It only pulls the email addresses from the URL, as seen in the screenshots below.



Hello
This is Geeksforgeeks
review-team@geeksforgeeks.org
contribute@geeksforgeeks.org
GfG is a portal for geeks
feedback@geeksforgeeks.org
careers@geeksforgeeks.org

When I used this code with Mr. Robinsons staff directory page URL, I had no emails extracted.

```
#code from https://ide.geeksforgeeks.org/
# library that handles the URL stuff
import requests

# Importing module required for
import re
import re
# Assign urlopen to a file object variable
fhand = requests.get("http://www.columbiabasin.edu/index.aspx?recordid=29558page=45")

# email_pat = re.compile(r"[A-Za-z0-9._X+-]+"r"@[A-Za-z0-9.-]+"r"\.[A-Za-z]{2,4}")

for line in fhand:
# Getting the text file
# content line by line.

s = line.decode().strip()

# regex for extracting all email-ids
# from the text file
reg = re.findall(email_pat, s)

# printing the list output

print(reg)

| Console 1/A × Console 3/A ×

| Console 1/A × Console 3/A ×
| Console 1/A × Console 3/A ×
| Console 1/A × Console 3/A ×
| Console 1/A × Console 3/A ×
| Console 1/A × Console 3/A ×
| Console 1/A × Console 3/A × | Cons
```

17. Describe the problem with the HTML code that makes a simple extraction problematic.

The problem with the HTML code that makes this problematic is the email address we are trying to obtain, erobinson@columbiabasin.edu, is not listed as such in the HTML code.

Use PyNmap.py as a start and modify the script as needed.

- 18. Modify the header for your information. When the script is run, it should check for a "Logon ID" directory in its path and create one if needed.
- 19. The script should call Nmap and write the output to both a JSON or a pickle file with the format mmddyy.type. For example, if the scan was run on 09/01/2020 and saved as a pickle file, then the output file would be named 090120.pickle. If it were a JSON file, then it would be 090120.json.
- 20. Use the /24 network for your home and run the PyNmap.py script.
- 21. Wait a day or rename the first file. Using TCPServer.py, start a listener on port 80. Now re-run the PyNmap.py script. You should have two files: one before the listener and one after.
- 22.Use the application ndiff to compare the Nmap scans. Why doesn't it work?

23. Modify PyNmap.py so that ndiff will work and report TCP port "diffs" in the network.

B.GIT FUNDAMENTALS

It is essential for security professionals to have a basic understanding of Git as it is widely used

- Please use Git to complete the following.
- 24. Follow the instructions to create a GitHub account at https://github.com/and create a public GitHub repository.

I've created the public repository CBC-Code to post my python code to. The url is: https://github.com/redeyesyami/CBC-Code.

25. Upload your PyNmap.py file to the GitHub repository to make your code public and accessible.