Resources

Episode 2.1

1. Penetration Testing Methodologies - OWASP: https://www.owasp.org/index.php/Penetration_testing_methodologies
2. PTES Technical Guidelines: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
3. Penetration Testing Methodologies and Standards: https://resources.infosecinstitute.com/penetration-testing-methodologies-and-standards/

Reference:

Duffy, C., Mohit, Buchanan, C., Ip, T., & Mabbitt, A. (2016) - *Python: Penetration Testing for Developers.* Packt Publishing. Available at: https://www.amazon.com/dp/B01M5FAV4Q/

Episode 2.2

1. Install Python 3, for your OS, by following this extensive guide: https://realpython.com/installing-python/
2. Installing the python-nmap module:
    a. **2.1.** In the terminal or command prompt type: pip install python-nmap
3. Download Visual Studio Code for your OS from this link: https://code.visualstudio.com/Download
4. Install Visual Studio Code, for your OS, following the instructions here: https://code.visualstudio.com/docs/setup/setup-overview

Reference: Duffy, C., Mohit, Buchanan, C., Ip, T., & Mabbitt, A. (2016) - *Python: Penetration Testing for Developers.* Packt Publishing. Available at: https://www.amazon.com/dp/B01M5FAV4Q/

Episode 3.1

Required modules:

1. Installing pynput Python module. Open a terminal or command prompt window and type:

    pip install pynput

   a. More about this module: https://pypi.org/project/pynput/
2. More about ftplib: https://docs.python.org/3/library/ftplib.html

References and Inspiration for the code:
James George 007 Github:
https://gist.github.com/jamesgeorge007/cb68fedd8419721f6f4c7a7643181974

Episode 3.2
References and Inspiration for the code:

James George 007 Github:
https://gist.github.com/jamesgeorge007/cb68fedd8419721f6f4c7a7643181974

Episode 3.3
Setting Up VirtualBox and Metasploitable 2:

1. Download VirtualBox from here: https://www.virtualbox.org/wiki/Downloads
2. Install VirtualBox, follow the instructions relevant to your OS: https://www.virtualbox.org/manual/ch02.html
3. Download Metasploitable 2 vulnerable machine: https://www.vulnhub.com/entry/metasploitable-2,29/
4. Install Metasploitable 2 in VirtualBox. Follow the instructions, starting from "Step 2": https://pdrcybersecurity.com/six-steps-install-metasploitable-2-virtualbox/

References and Inspiration for the code:
James George 007 Github:
https://gist.github.com/jamesgeorge007/cb68fedd8419721f6f4c7a7643181974

Episode 4.1
Further readings:

1. More about zipfile Python library: https://docs.python.org/3/library/zipfile.html
2. More about argparse Python library: https://docs.python.org/3/library/argparse.html

Episode 4.3
Instructions:

1. Download and put the following files into a new folder on your system:

   - archive.zip
   - passlist.txt
   - zipbrute.py

2. Open up a command prompt or terminal window (depending on your OS) and navigate to the folder where these files are. Type:

> python zipbrute.py -z archive.zip -p passlist.txt

1. If successful, you should have a new file in the directory: important.txt
2. Congratulations, you have successfully completed this module!

Episode 5.1
More resources:
Video courses at https://cybrary.it:

1. Penetration Testing and Ethical Hacking - Ken Underhill - https://www.cybrary.it/course/ethical-hacking/
2. Python for Security Professionals - Joe Perry - https://www.cybrary.it/course/python/
3. Advanced Penetration Testing - Georgia Weidman - https://www.cybrary.it/course/advanced-penetration-testing/

Books: Python Penetration Testing for Developers - C. Duffy et al. (2016)
- https://www.amazon.com/dp/B01M5FAV4Q/

Practice:

1. Hands-on Labs at: https://www.cybrary.it/catalog/?type=practice_labs

2. Build your coding skills at: https://codewars.com