Python Scripting for CS – Lab 3

Dictionary Attack

# Purpose

In this lab, you will have the opportunity to practice modifying an existing script and brute force a password.

## Skills

The purpose of this assignment is to help you practice the following skills that are essential to your success:

* Modify an existing script
* Use Visual Studio Code
* Use Kali Linux
* Use logic
* Utilize Python libraries and modules

## Knowledge

This assignment will also help you become familiar with the following important content knowledge in this discipline:

* Utilize the basic syntax, data types, and control structures of Python
* Apply Python scripting skills to cybersecurity tasks
* Write Python scripts in a virtual environment

# Instructions

Follow the instructions laid out in this lab. Your lab activities will begin with Task 1. Tasks will build on each other and should not be done out of order.

Answer the critical thinking questions as best you can.

# Formatting

|  |  |  |
| --- | --- | --- |
| Formatting | Explanation | Example |
| Definitions | Definitions are defined in bold | **Word:** This is the definition |
| Employability Skills | Employability skills are defined in green and associated with critical thinking questions | **Think Critically and Creatively** |
| Commands | Commands are written in Consolas and highlighted in yellow. Commands that are case sensitive will have an underline underneath the capitalized letter. | get-service |
| File names/paths, programs, & buttons | File names, programs, and buttons are written in Consolas and highlighted in gray. | C:\Tools\processes.txt |
| <dynamic content> | Content in <> should be replaced with what is required, removing the <> as well | \\<servername>\Home |
| Examples | Examples will be in Consolas and highlighted in blue | **skywalker.local** |
| Recall & Apply | Tasks that connect to previous course work will ask you to recall and apply learning from previous Learning Modules or classes | **Recall & Apply Learning from Network Essentials** |

# Criteria for Success

This assignment is worth 20 points. You will be graded on the script you created as part of this lab.

# Lab Environment

In this class, you will be using VMs set up in Cloud.

# Log into Cloud

1. Access NWTC cloud at <https://lab.nwtc.edu>
2. Login using your username and password assigned in Lab 1
3. Start your Kali Linux VM

# Task 1: Choose your path

In this lab, you have the option to do what is outlined below for one of our typical labs OR you can do the following:

1. Go to <https://www.w3resource.com/python-exercises/cybersecurity/index.php>
2. Select an exercise that was not presented in class already
3. Look at the code and try running it as is
4. Change it! Do you have an idea to make that code better? Is there another thing about passwords that you find interesting? How could you make it more nefarious?
5. Turn in your code and tell me what you changed in the comments.

# Task 2: Download and Run dictattack.py

Remember: You only have to complete the following tasks if you do not want to select your own exercise from above.

1. On your Kali VM, navigate to <https://github.com/RachelGehrke/PythonCS>
2. Go to LM03
3. Download dictattack.py and save it in your pythoncs/vepython3 folder
4. Open dictattack.py in VS Code
5. Open a terminal window
6. **Recall & Apply Learning from Lab 0** & **Think Critically and Creatively:** Activate your virtual environment
   1. This *must* be done prior to installing any packages or running our script
7. From your terminal and in your activated environment, run the following command:
   1. python dictattack.py
   2. HINT: Make sure your terminal window is pointing to your pythoncs/vepython3 folder. You may have to modify the above command depending on the current working directory of your terminal
8. **Think Critically and Creatively:** What were the results of running your script? Was your script able to find the hashed version of the super secret password?

# Task 2: Modifying dictattack.py

1. Save a copy of the dictattack.py as dictattackv2.py
2. Open dictattackv2.py in VS Code if you are not already in VS Code.
3. Our goal is to modify our dictionary attack script to do the following:
   1. Read a file of common\_passwords
   2. Read a file of password\_variations
   3. Ask the user for a password
4. **Think Critically and Creatively:** What modules would you need to import?
5. Turn in your .py file and your keylog.txt file to the dropbox on Canvas for up to 20 points.