Python Scripting for CS – Lab 5

Firewall Management

# Purpose

In this lab, you will have the opportunity to practice modifying an existing script and using Python to manage and test your firewalls.

## 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 critical thinking questions at the end 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

# Setup:

As a system security engineer, you are tasked with tracking everything that hits your firewall. You’ve found that searching through event logs and using the built-in monitoring log to be lacking.

You want to do the following:

1. Create a test server that has a constantly running IP of 0.0.0.0 on port 9999
2. Use PowerShell on a Windows machine to send a packet
3. The test server will log each packet sent and include the following information:
   1. IP address of the client
   2. Port of the client
4. To make it easier to access, you also want to set up a website which takes the logged information and displays it in an easier format.

# Task 0: Preflight checklist

1. Start your new Win10 machine
2. Add your VM to the powershell-b network.

# Task 1: Download and Run tcpserver\_logging.py

1. On your Kali VM, navigate to <https://github.com/RachelGehrke/PythonCS>
2. Go to LM06
3. Download tcpserver\_logging.py and save it in your pythoncs/vepython3 folder
4. Open tcpserver\_logging.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 tcpserver\_logging.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:** In your own words, describe what this script is doing.
   1. **HINT:** I used this in LM5 lecture!
9. Keep this running for the rest of the tasks!

# Task 2: Send a Packet

1. On your new Win10 VM, download the senddata.ps1 file
2. **Recall & Apply Learning from Intro to PowerShell** : How do you change your Win10 machine to allow you to run unsigned scripts?
   1. Execute the command you need to set your execution policy to “unrestricted”
3. Run the downloaded script with the IP address of your Kali linux server.
4. On your Kali VM, go to your vepython3 folder and open your firewall.log.
5. Hopefully, you see some information logged!
6. Optional Fun: Use last week’s port scanner to send a packet to your TCP server on its 9999 port. Check your log again. Does it look any different?

# Task 3: Create a Website

To make your monitoring website, you decide to use Flask.

1. Using the Flask documentation, install the Flask module to your virtual environment on your Kali VM.
   1. <https://flask.palletsprojects.com/en/3.0.x/>
2. Take a look around the website after you’ve installed Flask. Look at things like creating a simple application, the tutorial, etc.
3. In your vepython3 folder, create a folder named templates.
4. From the class Github LM06, download app.py and save it to your vepython3 folder (NOT the templates folder).
5. Open app.py in VSCode and try to decipher what it’s doing based on what you saw in the Flask documentation.
6. From the LM06 folder, download index.html and save it to your new templates folder.
7. In a different terminal than you are running your TCP logging server, run app.py.
   1. HINT: Remember to activate your virtual environment first.
8. You should see Flask start and warn you that this is not for a production server.
9. In a web browser on your Kali VM, access your website by going to <http://KALIVMIP:5000>
   1. Remember to change KALIVMIP to the IP of your Kali VM.
10. Try to access this from your Win10 VM. Can you access it? Is that good or bad…?

# Task 4: Assessment

1. Using what you’ve learned in this lab, go to LM6 in Canvas and answer the critical thinking questions.