Lesson Guide

Cybersecurity Professional Program

Introduction to Python for Security

Python for Security

Course Path

- PY-01: Introduction to Programming
- PY-02: Data Types & Conditions
- PY-03: Loops
- PY-04: File System & Error Handling
- PY-05: Functions
- PY-06: Network Communication
- **PY-07: Python for Security**

Lesson Objectives

This lesson is a summary of the Introduction to Python module. It focuses on the creation of a fully configured and working script.

Lesson Overview

The lesson provides an opportunity to test learner ability via a real-world programming solution. The project takes the learners through a step-by-step process to develop a tool that detects ARP Spoof attacks.

Learner Level

Learners are familiar with all the topics covered in the course and have the necessary knowledge to complete the project.

Lesson Notes

Be familiar with the project's flow and requirements. Provide an overview of the project using the presentation and make sure learners understand the tasks. Since they may be overwhelmed with the project's size and requirements, reassure them and point out that you are there to help.

Environment & Tools

A computer with a connection to the Internet, with:

- Windows, MacOS, and Linux
  - PyCharm
  - Python 3
- ***Kali Linux ISO***

Overview

In this section, explain the usage of Python for security programming. Explain how it can be leveraged to create tools for various security-related purposes. Don’t spend too much time on this part, since the main focus should be on completing the project.

Python for Security

Security purposes: Explain that different tools can be designed to detect attacks.
Dedicated libraries: Explain that more libraries are being built to make the job easier.
Flexible security measures: Explain that we can script tasks per our needs and requirement sets.

Information Gathering

Knowing the right information at the right time gives you an advantage in almost any endeavor.

Automation

SIEM Integration: Explain that SIEM platforms use code to automate processes and tasks.

ARP Spoof

Explain what an ARP Spoof attack is and its purpose.

ARP Spoof Detector

Explain that an ARP Spoof Detector is a Python script that checks if a machine is being ARP Spoofed.

Project Requirements

Review the requirements for the project and make sure learners are aware of them to avoid major issues later in the project. Offer some tips regarding smart project preparation and scripting.

Before You Start

Explain that learners should think carefully about the code flow before starting to write it.

Project Steps

Review the tasks and what learners will need to know to complete the project. Assure them that they have the knowledge required to accomplish all the tasks.

Project PY-07-L1: Final Project

The project should be completed in class with your assistance, if necessary.

TDX Arena

Learners will need to navigate to the TDX Arena practice area as described in the slide deck.

Asynchronous Learning: Shifting Left for Security

This assignment asks the learner to use the TDX Arena platform to practice secure Python coding. To complete the assignment, learners will need to visit the outlined TDX Arena lab. Learners can work on the TDX Arena practice area as a learning opportunity.

Asynchronous Learning: Log Analyzer

This assignment asks the learner to use the TDX Arena platform to practice everything they have learned to analyze an Apache log. To complete the assignment, learners will need to visit the outlined TDX Arena lab. Learners can work on the TDX Arena practice area as a learning opportunity.