Python Forensics

Course 71589 – 40 Hours

Overview

What makes an excellent digital forensics investigator is to have the knowledge and skill to automate forensics stages using the Python programming language's power. Many laboratories rely on Python to build basic models for predictions and to run experiments. It also helps to control critical operational systems. Python has built-in capabilities to support the digital investigation and protect the integrity of evidence during an investigation. This training will provide the student with steppingstones on how to take forensics skills to the next level, combining them with powerful Python scripting.

On completion, Delegates will be able to

- Lear to work with different modules to accomplish tasks
- Analyze artifacts left on a compromised system using Python
- Perform network traffic monitoring and analyzing logs

Who should attend

- Law enforcement officers & intelligence corps
- Incident responders
- Computer investigators
- IT/network administrators
- IT security personnel
- Junior-Cyber forensics analysts

Prerequisites

Advanced knowledge of:

- Linux
- Network Forensics (Course 71586) or Windows Forensics (Course 71585)

Course Contents:

Module Title	Description
Module 1: Introduction to Python During this module, students will be introduced to the world of Python. Students will learn to install Python and its additional modules, write basic scripts, create clients and servers' socket, and work with files.	▪ **Introduction to Python Scripting** ○ Installing of Python ○ Python Basics ▪ **OS and Networks** ○ Using PIP to Install Additional Modules ○ The OS Module ○ Sockets
Module 2: Basic Python Network Forensics This module will cover the subject of network forensics; students will learn to install and work with a variety of network frameworks and tools and network trace analyses and capturing, recovering, and visualizing the traffic.	▪ **Pandas and Scapy** ○ Introduction to Scapy ○ Crafting Raw Packets with Scapy ○ Communicating with SSL ○ Introduction to Numpy ○ Panda Basics ○ Panda Dataframe Basics ▪ **Analyzing Network Traces** ○ DSHELL Framework ○ Network Traces Statistics ○ Visualizing Network Traces ○ Converting Pcap to Pandas DataFrame ○ Basic Payload Investigation
Module 3: Python OS Forensics Python OS Forensics is a core essential of Python forensics; this module will cover forensics in both primary operating systems today, image manipulation, and metadata analysis.	▪ **Python Forensics in Windows** ○ Basic File Metadata ○ Data Representation ○ Carving Data and Metadata ○ Analyzing Windows Artifacts ○ Windows Event Logs Handling ▪ **Python Forensics in Linux** ○ The Linux Filesystem ○ Analyzing User's Command-Histories ○ Capturing Images ○ Extracting Object from Image ○ Memory Capture and Analyzes
Module 4: Advanced Forensics During this module, students will learn to deal with advanced networking.	▪ **Advanced Forensics** ○ Advanced Networking ○ Working with Data ○ TWISTED Python ○ Footprinting Applications