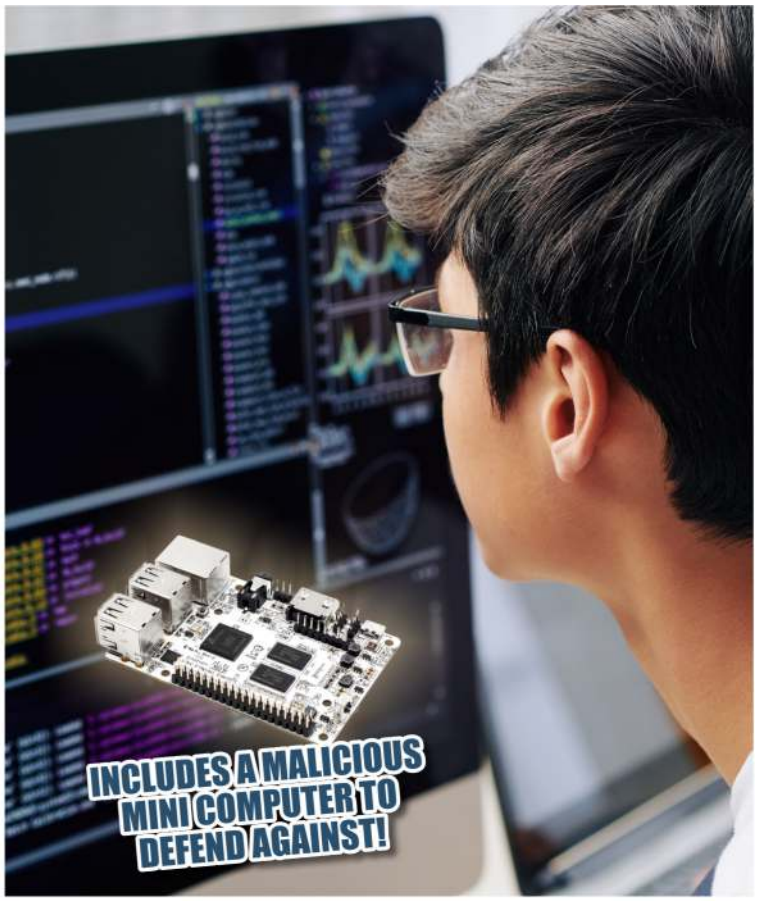
INTRODUCTION TO SCRIPTING FOR CYBERSECURITY

MC-2600

Coding is the heart of cybersecurity. It is important that cybersecurity personnel in various job roles understand programming tools so that they can decipher the overall strategies, tactics and goals of attackers. In addition, they often use scripting languages to create programs that will carry out specific or repetitive cyber operations. Four of the most widely used scripting languages include – Python, Powershell, Bash and Ruby.

Some of the most common cybersecurity-related job roles and their relationships with coding include: Penetration testers, Incident responders, and Cyber System Analysts.

This course introduces the student to these scripting languages and leads them to develop applications to perform cybersecurity-related activities.



Not Just a Simulation! Hands-on Labs Use the Following Scripting Languages:

- Python
- Ruby
- PowerShell
- Bash

Students will use the provided Single Board Computer (SBC) as an endpoint to test and use networking scripts. The board will be directly networked to the student laptop, so students can write scripts that craft and send packets to the board while monitoring the network traffic to confirm that the scripts work as intended.

The Marcraft Introduction to Scripting for Cybersecurity Course covers these topics:

- Differences Between Structured Programming and Coding (using Scripting Languages)
- Basic Commands of Ruby, Python, Bash, and PowerShell
- Command Line Structures for Each Language
- Applications to Automating Cybersecurity-Related Operations

AND MUCH MORE!

Real World Hands-on Labs!

INCLUDES:

MC-2600	The Complete Introductory Scripting for Cybersecurity Package for 24 Students Working in Pairs (Requires PC Workstation Computers)
MC-260IG	Instructor's Guide with PowerPoint Presentation USB Drive (1 Per Classroom)

ACCESSORIES:

MC-260	The Complete Introductory Scripting for Cybersecurity Text/Lab Guide