

THE COMPLETE INTRODUCTORY SCRIPTING FOR CYBERSECURITY COURSE

MC-2600

Coding is a key component of cybersecurity. It is important that cybersecurity personnel across various 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 common cybersecurity roles that rely heavily on 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:

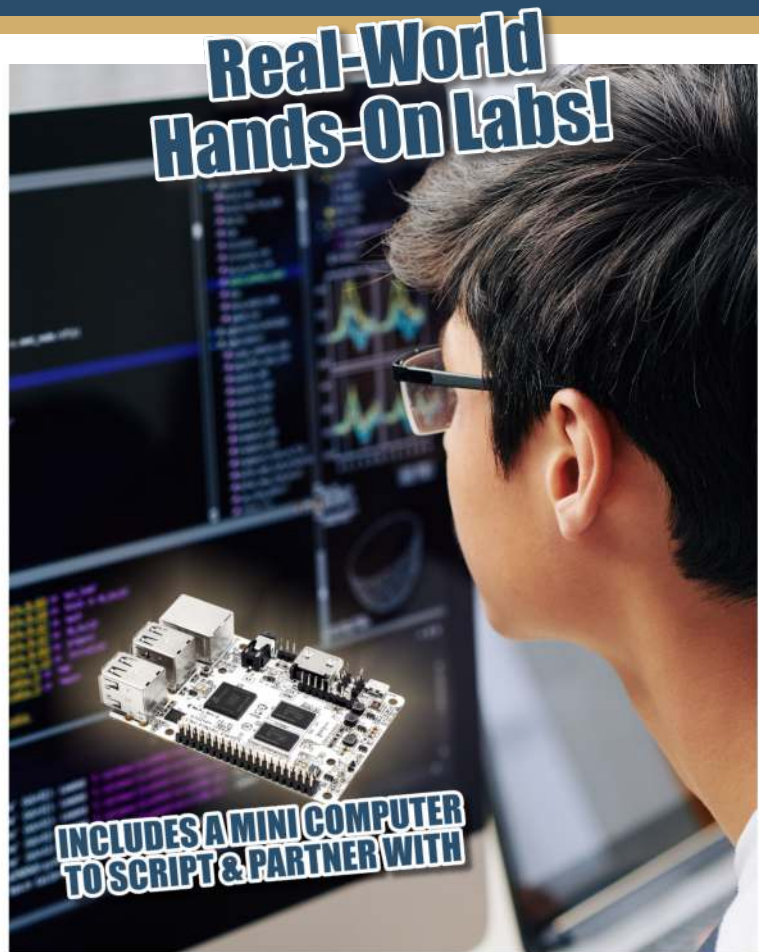
Python
Ruby
PowerShell
Bash

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.

Marcrafft's Complete Introductory 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!

**Designed for 24 Students Working in Pairs
(Requires 12 PC Workstation Computers)**



INCLUDES:

MC-2600	The Complete Introductory Scripting for Cybersecurity Package
MC-260	12 Complete Introductory Scripting for Cybersecurity Text/Lab Guides
MC-260IG	Instructor's Guide with Digital Media (1 Per Classroom)



ACCESSORIES:

MC-260	Additional Complete Introductory Scripting for Cybersecurity Text/Lab Guides
--------	--