Hands on Hacking

Duration: 4 days CPE: Up to 44 Type: In-Person Training

Prerequisites: Participants will need a fundamental understanding of cybersecurity concepts. Completion of ISACA's Cybersecurity Fundamentals Certificate is recommended but not required.

Equipment required: A laptop with the latest version of an internet-accessible browser.

Instructor: Frank Downs, Director of Cybersecurity Practice, ISACA
or Dustin Brewer, Manager, Product Platform Developer, Cybersecurity, ISACA

Course Overview

ISACA's Hands on Hacking Training Week class enables participants to see and experience organizational vulnerabilities as a hacker would—and embrace real-world tools and strategies professionals use to defend against their attacks. Participants will take part in red team and blue team activities:

- **Red Team**—take on the role of an ethical hacker. Work hands on with real-world systems and networks and leverage real vulnerability analysis and exploitation tools in a live environment.
- **Blue Team**—learn to defend against evolving cybersecurity threats. Build, hone, and evaluate technical cybersecurity skills through hands-on, skills-based labs conducted in the same live, real-world environment.

Red Team: CSX Penetration Testing Overview

The **CSX Penetration Testing Overview (CPTO)** session allows participants to see potential targets through the eyes of a cyber attacker (red team). It will help participants gain a comprehensive understanding of the overall concepts guiding penetration testing from a practical, hands-on vantage point and allow them to better protect enterprises, advance their career, and earn the CPTO certificate.

Learning objectives include:

- Understand TCP/IP Networks
- Learn methodology & tools for performing ethical hacking assessments
- Understand Network Discovery and foot-printing techniques
- Learn how to identify and enumerate TCP/IP services
- Learn how to identify and exploit network vulnerabilities
- Understand key reporting and follow-up areas
- Understand key network security controls

Blue Team: CSX Cybersecurity Practitioner

The **Accelerated CSX Cybersecurity Practitioner Certification (CSX-P)** session presents participants with real-world scenarios where they learn to respond to attacks as they occur (blue team) and provides an opportunity to earn the CSX-P certification. In-depth, hands-on lab experiences prep students for the attacks that cybersecurity professionals experience on a daily basis.

The performance-based CSX Practitioner Certification affirms participants have the ability to perform as a cybersecurity professional who is:

- Capable of following established procedures
- Proficient in using defined processes
- Able to work with known problems on a single system
- Proficient with antivirus, and has firewall and patching experience
- Qualified to implement common security controls, and perform vulnerability scans and some analysis

The course is comprised of five domains:

1. The Identify domain teaches students to recognize, assess and remediate specific internal and external network threats.
2. The Protect domain offers instruction in the basic concepts, methods, and tools associated with implementing cyber security controls to protect a system from the identified threats.
3. The Detect domain provides perspectives on analyzing and monitoring network output, detecting malware and incidents, notifying proper channels, analyzing attacks and escalating incidents. It also covers the performance of change monitoring.
4. The Respond domain focuses on the basic concepts, methods and tools required to draft and execute incident response plans, the provision of proper isolation response documentation and the practices related to documenting and maintaining information related to incident response.
5. The Recover domain enables participants to master the basic concepts, methods and tools needed to recuperate a system or network and learn how to implement continuity and contingency plans.

Learning objectives include:

- Provide students with an environment to discuss and practice methods implemented by cybersecurity professionals in the Identify, Protect, Detect, Respond, and Recover domains
- Prepare students to serve as workforce-ready complementary team members for real-world enterprises

Schedule

Day 1 **CPTO | Red Team**	Introduction to Penetration Testing	Lesson
	• Linux Shell and Commands Lab	Instructional Lab
	TCP/IP Basics	Lesson
	• TCP/IP Basics Lab	Instructional Lab
	Reconnaissance	Lesson
	• Packet Inquiry Lab	Instructional Lab
	• Network Discovery Lab	Instructional Lab
	Enumeration	Lesson
	• Service Enumeration Lab	Instructional Lab
Day 2 **CPTO | Red Team**	Vulnerability Identification	Lesson
	• Network Vulnerability Identification Lab	Instructional Lab
	• Network Vulnerability Exploitation Lab	Instructional Lab
	Reporting	Lesson
	Security Controls	Lesson
	• Evidence Removal Lab	Instructional Lab
	CPTO Challenge 1 Lab	Challenge Lab
	CPTO Challenge 2 Lab	Challenge Lab
	Review for Exam **CPTO Certificate Exam**	**Online Exam**
Day 3 **CSXP | Blue Team**	**Identify**	
	Network Infrastructure and Digital Assets	Lesson
	• Asset Identification Lab	Instructional Lab
	Identify Challenge Lab	Challenge Lab
	Protect	
	Security Tools and Systems	Lesson
	• Firewall Setup Lab	Instructional Lab
	Protect Challenge Lab	Challenge Lab
Day 4 **CSXP | Blue Team**	**Detect**	
	Malicious Activity Analysis	Lesson
	• Vulnerability Analysis Lab	Instructional Lab
	Detect Challenge Lab	Challenge Lab

Respond & Recover	
Incident Notification and Containment	Lesson
• Incident Correlation Lab	Instructional Lab
System Validation	Lesson
• Re-Imaging Lab	Instructional Lab
Post Incident Security Plan and Procedure	Lesson
• Restore Points Lab	Instructional Lab
Response Challenge Lab	Challenge Lab
Review for Exam	
CSX-P Certification Exam	**1-hour Online Exam**