Course Content

Course Description:
This course takes cybersecurity practice to the next level. It is an advanced experience that builds upon the defensive skills and knowledge taught by the CyberSec First Responder® (Exam CFR-410) course. It is an applied experience in that it almost entirely consists of hands-on exercises featuring many different tools and environments.

Course Objectives:
- Get oriented to your tools and environment.
- Exploit vulnerabilities in software.
- Exploit vulnerabilities related to system access, networking, data, and file configurations.
- Analyze attacks using passive and active methods.
- Implement security protections to minimize the impact of attacks.

Prerequisites:
To ensure your success in this course, you should have taken the CyberSec First Responder® (Exam CFR410) course and passed the associated exam. This validates you have intermediate skills in working with the Linux® operating system; working at the command line; using fundamental cybersecurity tools like Nmap and Metasploit; and following an incident-response process—all of which are important to this course. And, it ensures you have foundational cybersecurity and networking knowledge.

In addition, you should have some familiarity with computer programming and scripting. Expertise in writing code is not necessary, but you should be able to comprehend code at a high level, and follow the logic behind a script as it is explained to you. Knowledge of one particular programming language is not required. Python is fairly universal, especially among technology professionals who are not software developers by trade.

Target Audience:
This course is designed for cybersecurity professionals who want to expand their practical skills in the three aforementioned modes. The target student is also someone who has taken the CyberSec First Responder® (Exam CFR-410) course and wants to dive deeper into the methods and tactics used to defend against a range of cyber threats.

CyberSec First Responder – Advanced (CFR-A)

Topics:

1- Getting Oriented to Your Tools and Environment
- Explore the CFR-A Activity Environment
- Perform Reconnaissance
- Simulate an Attack Using Metasploit

2 - Exploiting Software Vulnerabilities
- Exploit Code-Execution and Injection Vulnerabilities
- Exploit Web-Application Vulnerabilities

3 - Exploiting System Vulnerabilities
- Exploit Access Vulnerabilities
- Exploit Network Vulnerabilities
- Exploit Data Vulnerabilities
- Exploit File-Configuration Vulnerabilities

4 - Analyzing Attack
- Analyze Logs for Signs of Attack
- Detect Attack Using Active Monitoring Systems
- Perform Digital Forensics

5 - Protecting Assets
- Protect Data
- Protect Access
- Protect Software
- Protect Networks and Systems

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535

NASBA Information

Level: Intermediate
Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.
Fields: Computer Software & Applications
CPEs: 39

Policies: Course Registration, Cancellation, Refund and Complaint Resolution
For more information regarding administrative policies such as complaint and refund, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:
The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our web site or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.