CyberSec First Responder® – Advanced (CFR-A): Applying Your Security Expertise (Exam CFA-110)

Course Number: CNX0021

Course Length: 5 days

Overview:

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.

The "A" in CFR-A can also refer to the cybersecurity modes this course is built around:

- Attack: Simulating attacks on computing assets to test security measures and learn more about threat vectors.
- Analyze: Identifying, detecting, and assessing threats to learn more about how they operate and how they affect security.
- Address: Implementing countermeasures and other protections to mitigate the impact of threats to security.

Course Objectives:

In this course, you will simulate, analyze, and address attacks on computing and network environments.

You will:

- 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.

Target Student:

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.

This course is also designed to assist students in preparing for the CFR-A credential, available through the CHOICE platform.

The skills covered in this course also complement the security theory that is covered in more conceptually oriented programs, such as Certified Information Systems Security Professional (CISSP®). For CFR-A candidates who are also considering the CISSP certification, we have provided a bonus study guide on the CHOICE platform. Log in to your CHOICE course screen for more information.

Prerequisites:

To ensure your success in this course, you should have taken the CyberSec First Responder® (Exam CFR-410) 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.

Logical Operations offers a couple Python courses that can help you obtain this experience:

- Introduction to Programming with Python®
- Advanced Programming Techniques with Python®

CFR
Advanced

Course Content

Lesson 1: Getting Oriented to Your Tools and Environment

Topic A: Explore the CFR-A Activity Environment

Topic B: Perform Reconnaissance

Topic C: Simulate an Attack Using Metasploit

Lesson 2: Exploiting Software Vulnerabilities

Topic A: Exploit Code-Execution and Injection Vulnerabilities

Topic B: Exploit Web-Application Vulnerabilities

Lesson 3: Exploiting System Vulnerabilities

Topic A: Exploit Access Vulnerabilities

Topic B: Exploit Network Vulnerabilities

Topic C: Exploit Data Vulnerabilities

Topic D: Exploit File-Configuration Vulnerabilities

Lesson 4: Analyzing Attacks

Topic A: Analyze Logs for Signs of Attack

Topic B: Detect Attacks Using Active Monitoring Systems

Topic C: Perform Digital Forensics

Lesson 5: Protecting Assets

Topic A: Protect Data

Topic B: Protect Access

Topic C: Protect Software

Topic D: Protect Networks and Systems