5755 Mark Dabling | Suite 250
Colorado Springs | CO | 80919

3463 Magic Drive | Suite 225
San Antonio | TX | 78229

info@root9b.com
www.root9b.com

Defensive Counter Cyber Operator (DCCO-I)

This is an intense 4-week hands-on course focused on protecting and securing critical network infrastructure as well as the discovery and methods of hunting the adversary on friendly networks. The objective of this course is to develop a new line of defensive cyber operators who are combat-ready and well trained in conducting adversarial hunting, forensic investigations, and defensive posturing. Students will be trained offensively in nature to "think like the attacker" and will practice defensive postures to elude some of the world's most sophisticated and tailored attacks. Our instructors promote innovative solutions and will help students to conduct secure techniques in a manner most conducive to the attack at hand. Rather than "reacting" to network attacks, Defenders will be trained to view Cyberspace defensive operations as plans of attack that need to be formulated, assessed, and continuously calculated in order to refresh tactics prior, during, and after offensive adversarial operations.

The course begins with network forensics as a basis to help students understand real-time detection and identification of network-based attacks. Next, students will be engaged with operating system fundamentals, with an emphasis on learning how attackers manipulate file systems, in order to identify, mitigate, and preserve critical information. Students will move into more advanced training concepts such as forensics, malware analysis, reverse engineering, and finally defensive computer deterrence and protection. Students will leave this course with a clear understanding that a true defensive posture promotes more than implementing an anti-virus solution. Students will learn to deter attacks, create mitigation techniques, provide attribution, detection, and an appropriate response.

Defensive Posturing: Thinking like the Attacker

- Understand Your Footprint
- Securing Data
- Mitigating Spoofing and Phishing techniques
- Mitigating, network beacons, malware, implants
- Performing Vulnerability Assessments
- Locating, Acknowledging, & Securing Vulnerabilities
- Preserving infrastructure
- Protecting servers
- Identifying Remote attack techniques
- Recovering from attacks

Network and Host Forensic Investigations

- File System Forensics
- Open Source Computer Forensics Investigations
- Malware Analysis and Reverse Engineering
- Advanced Forensics Timeline Analysis

Adversarial Hunting and Profiling

- Network Packet Analysis
- Statistical Flow Analysis
- Network Intrusion Detection and Analysis
- Scanning, Enumerating, Exploitation Techniques
- Signature, Protocol, Anomaly Detection
- Advanced Network Timeline Analysis
- Profiling the Attacker

USA ONLY