Defensive Counter Cyber Operator -Hunt (DCCO-H)

This is a 2-week follow-on course to DCCO-I and is particularly focused on taking the hunting aspects to the next level. The course is intended to teach defensive cyber operators the over-arching capabilities associated with all phases of exploitation. Students will learn more sophisticated hacker exploitation techniques, primarily against emergent technologies and infrastructure. Students will be exposed to router and firewall exploitation techniques, embedded device exploitation, wireless exploitation, and advanced network forensic identification. These methods include tunneling traffic through normal security filters, devices, and defenders, anonymizing IP addresses, creating forged packets, deciphering encrypted and hidden data exfiltration techniques, and uncovering sophisticated backdoor techniques. Students will depart this course with an understanding of advanced techniques used by the most sophisticated attackers to maintain stealth and security while minimizing their footprint and identity.

Locating the Cyber Ninja

- Creating an anonymous environment
- Fingerprinting the attack
- Recovering tunneling and redirection techniques
- Locating network scans that fly under the radar
- Identifying forged packets
- Extracting covert, obfuscated data from network traffic
- Uncover sophisticated implants
- Performing anomaly detection
- Implanting multi-layered security
- Monitoring cleaning techniques

Emergent Technologies and Critical Infrastructure

- Firewall Exploitation and Defensive Security
- Router Exploitation and Secure Deployment
- Wireless Exploitation and Protection, Perseverance
- Embedded Devices; Developing Firmware-based Exploits

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

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

info@root9b.com
www.root9b.com

USA ONLY