

## Red/Blue Kung Fu Training

The CGI's Red/Blue Kung Fu course of instruction is a robust offering for skilled security professionals. Security threat and vulnerability awareness are not enough to meet mission requirements. Experienced security professionals require advanced training to meet these risks head-on. We will develop a comprehensive training platform that builds upon CGI's Red/Blue Team experience for the Department of Defense (DoD). CGI will provide Risk management mitigation through "White Box" penetration demonstration and testing. We will demonstrate "Hacker" methodologies and methods to improve Red and Blue Team members' skills using material related to Ethical Hacking, Penetration Testing, Computer Network Operations, Vulnerability mitigation and Red and Blue team testing.

A blended learning solution of classroom lecture, hands-on exercises, demonstrations, tests and evaluations will ensure comprehension of these important topics. The instructor will use CGI's Centurion system (discussed below) to simulate ITS systems to provide hands-on laboratory opportunities, hone skills and understand these advanced concepts.

## Red/Blue Kung Fu Overview

Topics for the Red/Blue Kung Fu course offered through CGI's security practice include:

- Ethical Hacking: What is ethical hacking, legal responsibilities, methods and methodologies, how intruders escalate privileges, intrusion detection and steps to secure a system
- Advanced Persistent Threat (APT): Social Engineering, Social Networks, Denial of Service, Buffer Overflows, SQL injection, Virus, Trojans, best practices to mitigate these threats and tools to educate their users
- Methodologies: Reconnaissance (passive/active), Open source Collection, Spear Phishing, Port Scanning, Service enumeration, vulnerability exploitation, privileges escalation, owning the box, evading detection, erasing tracks, and maintaining and expanding access
- Penetration Testing: Red/Blue teaming (attack and defend), OS security flaws, vulnerability exploits and resultant control a Hacker could achieve if unfixed
- Vulnerability Assessment: OS vulnerabilities, application vulnerabilities, database vulnerabilities, Web Server vulnerabilities, TCP Stack vulnerabilities and the importance of physical security safeguards
- Tools and Techniques: Introduction to the standard tools and software used in vulnerability assessment, ethical hacking and penetration testing to include: Nmap, Whois, SuperScan, Nessus, Wireshark, Ethereal, Backtrack.

## Training approach

To meet the training requirements of the DIR and to reduce costs, CGI will use two innovative technological solutions currently in use. The first is a mobile information security training lab, known as the Cyber and Enterprise Network Training Unit for Roaming Instruction, On-site as Needed (CENTURION). CENTURION is essential to delivering our training in a secure environment. Many of the key components taught during our instructor-led training require a secure environment in which to run the hacking tools and malware that are crucial to these courses. CENTURION provides that environment, ensuring ITS systems remain separated from these tools.

CGI's approach to innovative cyber-security technology and solutions is evident in our second corporate resource, the Global Cyber Innovation Center. CGI's Cyber Center is located at two geographic locations, in Annapolis Junction, Maryland, and in Manassas, VA. Within this Center of Excellence sits the Cyber Lab Operations Network (CYLON). CYLON is a simulated enterprise environment that leverages customer use remotely via secured connections. CENTURION can also connect to CYLON through a virtual private network (VPN) link, established with the Cisco ASA 5510 via a broadband connection at the customer's location. This connection back to CYLON can greatly expand the virtual environment when it is necessary to simulate a large enterprise. This presents a significant costs savings to the customer by conducting training at the customer site and reducing travel costs for the customer.