Information Warfare Center

DUNS: 965387785
CAGE: 66D04

Our mission is to provide premier technical solutions that empower our clients with the latest technical knowledge.

We specialize in computer security and have extensive knowledge of securing not only operating systems, but also applications and networks.

Our experts have expertise in commercial, health care, financial, governmental and military applications and environments and we also offer support with Certification and Accreditation in the DoD, DOE, and other federal agencies using DIACAP, NIST, NIACAP and other C&A processes.

TECHNICAL TRAINING

We offer comprehensive training courses to build the knowledge required for certification. Our training is offered at our site, on your site or online.

Certification not only meets mandated requirements but demonstrates commitment to the profession. Receiving a professional certification shows peers, supervisors and, in turn, the general public - sincere commitment to a chosen career and the ability to perform to established standards. Obtaining certification demonstrates leadership in the computer security field.

Training courses we offer include:

- CISSP
- CISSP-ISSAP
- CISSP-ISSEP
- CISSP-ISSMP
- CISM
- CISA
- C|EH
- ECSA
- LPT
- C|HFI
- DIACAP
- Cisco - CCNA/CCNP/INCD
- Microsoft
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- SCADA Security
- Application Security
- Data Recovery
- Reverse Engineering

OUR PASS GUARANTEE

If after attending our training you do not pass the certification exam on your first attempt, you can retake the class again for free.

CONSULTING SERVICES

Information Warfare Center offers consulting services in the following functional areas:

- Networking
- Unix / Linux
- Windows
- Cisco
- Computer Forensics
- Incident Response
- Ethical Hacking Center of Excellence
- Open Source Intelligence

We offer complete system and network integration from the architecture and design through implementation and support.

We always keep security in mind throughout the entire system development life cycle (SDLC). We also provide solutions covering all steps from small business networks to international extranet WANs and support all of the common technologies.

Computer forensics is becoming an increasingly important part of doing business. We offer expertise in incident response, e-discovery, digital forensic investigation, and litigation support. Our certified personnel have experience working with events ranging from corporate espionage to international cyber extortion.

Complete Red Team penetration testing capability is available with a wide range of focus. Our services range from PCI compliance testing to complete physical, cyber, and procedural security validation. We use internationally recognized information security assessment methodologies. Our testing includes but is not limited to social engineering, access control exploitation, war-dialing, reverse engineering, vulnerability assessments, and system compromise testing. The goal of this service is to emulate potential adversaries, test the current state of security in your organization, and report weaknesses along with providing solutions to mitigate those risks.

Additional security, forensics and hacking services include but are not limited to:

- Intellectual Property theft
- Employee/employer misconduct
- Malware, Trojans, & Rootkits
- Establish forensic timelines
- Recovery of deleted information/failed drives
- Network usage monitoring
- Discovery of hidden data
- Password cracking
- Reverse Engineering
- LM Hash cracking 99.997% success rate
- Rogue WiFi Access point cracking
- Litigation support
- Security Policy verification
- System and physical penetration testing
- Information exfiltration simulations
- Network monitoring/traffic recreation
- Discovery of deliberately hidden documents
- Wireless cracking/interception
- Security in a virtual computing environment

What Students Say About Our Instructors & Courses

"The instructor provided real world scenarios that added value to course material. His explanations were well thought and his knowledge of the subject matter is unquestioned. Ethical Hacking is a very complicated set of material that was expressed very well in this course. I look forward to using these skills on the job."
– Booz Allen Hamilton

"The instructor ROCKS. very helpful. I will be taking another course with this instructor."
– Northrop Grumman Information Technology

"I found the instructor to be very motivating. The course was difficult, but very detailed and thorough in its coverage. I liked how I was forced to learn a lot of information in a short time frame. I feel up to speed on pen testing subjects after the class." –Director, Technical Assessment Directorate (TAD), Department of Defense, Office of the Inspector General

"You have a real competent teacher: not a teacher but somebody who works with it. The instructor is simply great! He knows the topic and he is a Team Builder, making the atmosphere nice and relaxed. I would rate him 10/10!!!! –

NATO Communications and Information Systems School "Excellent Instructor. Nice to have someone who is in the field doing this everyday to teach the class. Great class. Had a lot of fun in it. I liked the hands on labs and knowledge transfer from instructor. I plan on taking Advanced Ethical
Hacking, Reversing Malware, or Incident Response in the future." – Information Security, Scottrade Inc.

"This was a very informative and technically in-depth training course. All aspects of the advertised course were fully covered and ample opportunity was given for questions and interaction with the instructor."
– National Aeronautics and Space Administration (NASA)

"I enjoyed the way the instructor taught the class, he is a good instructor. He is able to communicate well with all different levels of technical abilities and personalities. I loved how there was lot of knowledge crammed into a short period of time."
– US State Department

Contact us: 719.359.8248
Sales@informationwarfarecenter.com
www.informationwarfarecenter.com