# Instructor Vita

## Contact Information

Kevin T Barnes – kevin.barnes@inl.gov - Idaho National Laboratory – (208) 526-9171

## EDUCATION AND TRAINING

| Degree | Year | Area/Major | Institution |
|---|---|---|---|
| BS | 1986 | Computer Science | Brigham Young University |

## RESEARCH AND PROFESSIONAL EXPERIENCE

**Cyber Security Researcher** **Oct. 2001 – Present**

- Researched and developed innovative ways to detect network intrusions and to protect the Idaho National Lab networks
- Perform and lead Industrial Control System (ICS) assessments from a determined aggressor's point of view at nuclear reactor facilities and DHS identified critical infrastructure facilities
- Coordinate support to the INL Cyber Security Operations Office providing high-level cyber security technical expertise in vulnerability scanning and analysis, intrusion detection, incident response/forensics, NIST 800-53 implantation, and other cyber security areas such as network traffic characterization.
- Instructor at the ICS-CERT training facility located in Idaho Falls, ID
- Instructor/facilitator on the DHS Cyber Security Evaluation Tool (CSET)

## PUBLICATIONS

No formal publications

## SYNERGISTIC ACTIVITIES

**Kevin Barnes** is currently a cyber security researcher with more than 25 years of experience writing software, defending networks, creating cyber security tools, and performing Industrial Control System (ICS) assessments. He recently performed ICS cyber assessments of the Advanced Test Reactor (ATR) located at the Idaho National Laboratory and a Category 1 Special Nuclear Material (SNM) storage facility. He has also performed ICS assessments at other Department of Energy labs and military installations. As a computer scientist he understands all aspects of computer systems from the bits and bytes to network packets and machine human interfaces. He has worked on all sides of cyber security in defending computer/network systems, implementing/interpreting NIST 800 guidelines, and attacking computer systems.

Kevin is also an Instructor for the ICS-CERT where he teaches the use of Metasploit, a network penetration testing tool, for both the 202 Intermediate Cybersecurity for Industrial Control Systems and the 301 ICS Cybersecurity courses. He also helps advise the red team members during course 301's 10 hour red/blue hands-on exercise where participants are either attacking (Red Team) or defending (Blue Team) an actual control system environment. These courses are attended by ICS professionals from around the world from both the public and private sectors.