



COURSE DETAILS

INTENDED AUDIENCE

Technical staff members with at least two years' experience, basic security knowledge, and a strong background either in Windows or Unix environments.

LENGTH

Five Days; Days 1-4 (0900-1700)
Day 5 (0900-1500)

COST

\$2749 including course notebook and course CD. Lab Fee of \$250 includes student use of all PC and software required for the class. Refreshments and catered lunch provided.

PREREQUISITES

Completion of "Information Security for Technical Staff" course or hold equivalent experience and knowledge.

This course may also be offered by arrangement at customer sites. Contact Outbreak Security for further information.

Outbreak Security

7 West Queens Way
Hampton, VA 23669 USA
1.757.265.0891

www.outbreaksecurity.com

ADVANCED INFORMATION SECURITY FOR TECHNICAL STAFF

Overview:

This five-day course, developed by the Software Engineering Institute at Carnegie Mellon University, is designed to increase the depth of knowledge and skills of technical staff charged with administering and securing information systems and networks. Developed around a scenario in which a production network has failed an information security audit, students will implement numerous technical security solutions to bring the network into compliance. Participants will work in teams to integrate these solutions throughout the enterprise. Each student will have the use of a dual-boot laptop for the duration of the course, as well as direct administrative access to a wide variety of networked systems.

The first two days of the course utilize lecture/presentations, demonstrations and hands-on exercises to teach topic areas. During the final 3 days, instructors will facilitate participants through the implementation of the network's get-well plan and compliance task list. Students will use various freeware/open-source software and operating system specific technologies to accomplish these tasks. [This course is part of the curriculum for the CERT-Certified Incident Handler Program.](#)

Topics Include:

- System hardening
- System availability monitoring
- Network access control techniques
- Applied encryption
- Secure network architectures
- Intrusion detection systems
- Secure logs & network monitoring
- Forensics and incident response

Technical Activities:

Hands-on labs and demonstrations include subjects such as: implement a new segmented network topology and IP addressing scheme; install, configure and test 2 enterprise class, Unix-based firewalls and create a DMZ to isolate public services; implement an isolated administrative/management network; install, configure a centralized syslog server and configure hosts to send encrypted log information to this system; install, configure an HTTP application proxy server and implement content filtering; install, configure several intrusion detection sensors to include Snort/ACID; techniques to harden Windows and Linux systems; install, configure system availability monitoring tools and configure alerts; configure numerous network monitoring tools. and analyze data for suspicious events.

About Outbreak:

Outbreak Security was established in 2007 by four distinguished information security professionals whose operational and executive information security and incident handling experience in the government, military, and private sector dates back to 1988 and the birth of the incident response community. Outbreak's instructors are also Visiting Scientists at the Software Engineering Institute at Carnegie Mellon University and have taught numerous incident handling courses there for the CERT/CC.

Instructor biographies and corporate information may be found at www.outbreaksecurity.com.