

Brought to you by:



COURSE DATE AND TIME:

2-days

February 9-10, 2010

8AM-5PM (lunch included)

LOCATION

Norfolk Southern

Corporation

110 Franklin Road SE

Roanoke, VA 24042

FEES

Earlybird Fee (Until midnight 12/31/09):

Members: \$300

Non-members: \$325

Regular Fee (starting 1/1/09):

Members: \$350

Non-members: \$375

CPE HOURS

16

WHERE TO REGISTER

Enter the following link in your Web Browser to fill out the registration form:

<http://guest.cvent.com/i.aspx?4W,M3,73786569-785b-4e34-9cb5-21810b676303>

2-Day Seminar:

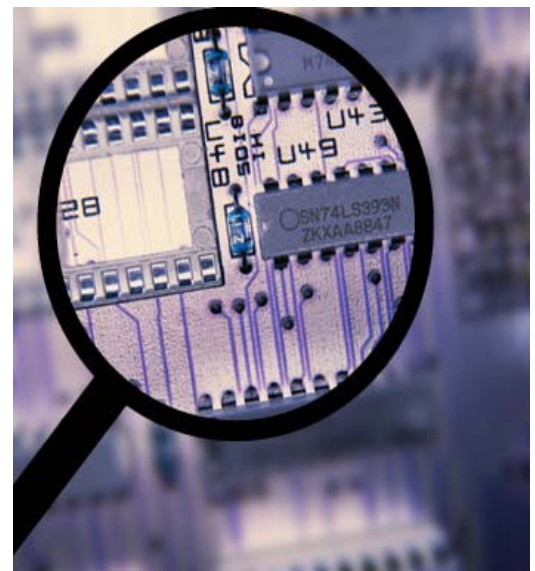
Computer Forensics for Security and Audit Professionals

DESCRIPTION

This course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be demonstrated during this course, including software, hardware and specialized techniques.

The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "cyber-criminal." It is no longer a matter of "will your organization be compromised (hacked)?" but, rather, "when?"

Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If either you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.



WHO SHOULD ATTEND

This course is targeted towards auditors, system administrators, Information Technology personnel, and all other security professionals requiring the knowledge and skills to track down and prosecute the perpetrator. This class is designed to increase the knowledge of participants of all levels.

Brought to you by:



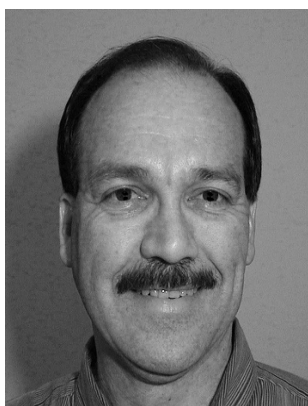
Instructor: Jeff Conner

SEMINAR LEVEL

Advanced Group-Live

PREPARATION FOR THE SEMINAR?

None required



Jeff Conner is a Senior Consultant at Canaudit and has been with the company for the past nine years. He specializes in performing computer forensics, Intranet, Internet, and Extranet penetration audits, along with providing network and system security consulting. As a nationally and internationally experienced instructor and conference speaker, Jeff uses his vast experience with system and network security in the corporate world along with the many penetration audits he has conducted to help students understand the sometimes complicated and technical security issues.

Jeff spent 22 years with Southwestern Bell (SBC Communications), one of the Nation's largest Regional Bell Operating Companies. He has over 17 years of diverse experience within the Audit and Security realm. Specifically, he has involved himself with Data Center User Administration, UNIX technical support, Network and Computer Security, Security Awareness Development and Training, TCP/IP Training, and Intranet/Internet Security Counseling and Implementation. He was a key figure in the installation of the company's Internet Firewall, FTP server, and World Wide Web Server.

Jeff has also performed multiple hacker investigations and interrogations and has an extensive background in computer forensics. He has taught *Internet Security* and *Penetration Testing* classes at Washington University in St. Louis, MO.

Brought to you by:



Seminar Outline

SEMINAR OUTLINE

I Introduction

Computer Crime in the news

II Understanding Computer Forensics

What is computer forensics?

Terminology

How it applies to you

Information Warfare

Hackers, Crackers & Cyber-Terrorists

Networking basics

- Communications
- Devices

Identifying your vulnerabilities

III Tracking the Culprit

Need for thorough documentation

What do you have to work with?

- Written Policies
- Technical Policies
- Permissions
- Billing statements

System, application, & device logs

Monitoring suspects

- Employer rights
- Employee rights
- Internet tracking
- Email tracking

Identifying a culprits tracks and signature

Creating a profile

IV Tools of the Trade

Software monitoring tools

- O/S first
- Key loggers
- System trackers

Software recovery tools

- Data Integrity
- Recovery/search
- Data wiping

Software imaging tools

Identifying a culprits tracks and signature

Creating a profile

Hardware monitoring tools

- Cameras
- Key loggers
- Recording devices

Password crackers

Sniffers

Encryption

Intrusion detection tools

V Preserving Evidence

Securing the crime scene

Backing up original data

- Disk imaging

Securing your data

- Public/Private Key
- Tokens
- Permissions
- Seals

Validation / Authentication

- Kerberos
- Digital Certificates
- Biometrics

VI Evidence Analysis

The many forms of digital evidence

General guidelines for analyzing evidence

What to look for

Data classification

Data reconstruction

Need for cooperation of agencies & departments

VII Computer Forensics and the Law

Investigative procedures

- Required search & seizure procedures
- Your company's ethics

Reconstructing the crime

Computer fraud & abuse act

Electronic communications & privacy act

Case studies & cyber-crimes

Presentation of evidence

VIII Checklists and Resources

Computer forensic checklists & resources

Computer forensic resources