Instructor Info:
Chris Prosise
Cell: 650.218.0885
Work: 949.450.5964
chris.prosise@foundstone.com

Teaching Assistant:
Earl Crane
Cell: 949.637.8330
Work: 949.297.5600 X2620
earl.crane@foundstone.com

Abstract:
Computer intrusions and security incidents are a part of life. Responding to these incidents is complex due to the technologies and disciplines involved. Effective response requires an understanding of technology, investigative sciences, legal requirements, and political considerations.

System and security administrators as well as managers are often asked to respond to and resolve incidents, but rarely have the requisite knowledge to do so. This course teaches the theory and principles of incident response through a hands-on and practical approach.

Students will see common network attacks first hand, then learn the specific steps and methodology necessary to resolve the incident. The entire lifecycle of incident response is covered, from pre-incident preparation through notification, initial response, and recovery. Real world case studies will provide insight into the computer crime cases that corporations and government are currently facing.

Goals:
- Learn a methodology for identifying and resolving computer security incidents
- Gain hands-on experience using the tools and techniques currently used by government and private industry to respond to incidents
- Introduce the forensic process and legal requirements of response
- Learn unique critical thinking skills

Requirements:
- A fundamental understanding of TCP/IP
- Some programming experience in C, Java, Perl, Shell, or similar
- A basic understanding of Windows NT/2000 and Unix
- Hacking Exposed (95-586) is highly recommended
- Intellectual curiosity
• Laptop with Windows 2000 or NT (9X not permitted)
• Wireless or Ethernet PCMCIA card
• Attendance at every class is required for a grade

Evaluation:
Grades will be based on assignments (50%) and a final project (50%).

Due to the compressed nature of this course, attendance is mandatory at all sessions. The assignments cover material presented in class.

The final project may be done in groups. Results will be presented to the class during the final session.

Grades:
A = 90-100%
B = 80-90%
C = 70-80%
F = below 70%

Course Schedule: (Hamburgh Hall, 1000)

Session 1, Saturday, March 15th: 10:00 AM – 3:00 PM (Five Hours)
Overview of Course
Real World Case Study
Review of Basic Security Principles
Introduction to Intrusions
The Response Life Cycle
  - Detection
  - Notification

Session 2, Sunday, March 16th: 10:00 AM – 3:00 PM (Five Hours)
Real World Case Study
The Response Life Cycle
  - Initial Response
    ▪ Windows
    ▪ Unix
  - Strategy Decisions
  - Response

Assignment
Students will be asked to apply the tools and techniques learned in the first two sessions and document the results. They will prepare a report to be submitted prior to the third session.
Session 3, Saturday, April 5th: 10:00 AM – 3:00 PM (Five Hours)
The Response Life Cycle
- Response
  - Monitoring
  - Investigation
- Recovery
- Reporting

Session 4, Sunday, April 6th: 10:00 AM – 3:00 PM (Five Hours)
Forensic Analysis
- Evidence Collection
- Duplication
- Evidence Handling
- Analysis
- Documentation

Session 5, Saturday, April 26th: (Five Hours)
Case Studies
Response Examples (Practical, hands-on laboratory exercises)

Session 6, Sunday, April 27th: (Five Hours)
Students will present the results of their final project to the class.

Textbook:
Students should order the textbook before class begins, and bring it to the first day of class. It is available on Amazon.com.
Incident Response: Investigating Computer Crime, Prosise, Mandia
ISBN: 0072131829