Secure Enterprise Computing

Incident Response and Corporate Forensics

Overview

Incident Response (IR) and Corporate Forensics (CF) deal with detective aspects of computer security within an enterprise context. IR goals include answering the questions: What happened? How did it happen? And who is responsible? CF goals include learning appropriate methodologies for the collection, preservation, analysis and presentation of evidence. Professional incident response frameworks and related constructs are also presented.

The course emphasizes planning and monitoring necessary for the successful detection, isolation and response to security incidents. It examines these issues from administrative, operational and technical perspectives. Significant issues include the creation and implementation of incident response teams. It also examines monitoring and reporting aspects of enterprise security policy.

Lectures are augmented with active learning activities. Included are 'hands-on' activities focusing on: drive forensics, file integrity, network monitoring, security tool kits and related issues.

Outcomes

Upon successful completion of this course, you will be able to

1. Describe policy and planning necessary for effective enterprise incident response.
2. Define and explain incident response and corporate forensics.
3. Explain basic incident response and forensic tools and processes.
4. Make an appropriate bit-stream copy of a disk drive and prepare it for forensics analysis.
5. Explain the relationship between the monitoring of enterprise digital assets and enterprise policy.
6. Demonstrate and explain network security monitoring.
7. Explain how system integrity monitoring programs, such as Tripwire, function.
8. Explain the role of system, network and Internet logs.
9. List, explain and demonstrate password auditing methodologies.
10. For forensic evidence, explain appropriate gathering, protecting and presenting methodologies.
11. List, define and utilize relevant cryptographic services and terms.

12. Define and demonstrate steganography as well as related terms and processes.
13. Articulate and demonstrate basic intrusion detection theory.

Texts

Required

Mandia, Prosise, and Pepe; Incident Response & Computer Forensics: Second Edition; McGraw Hill/Osborne; 2003
ISBN 0-07-222696-X

Matthews, Jeanna; Computer Networking, Internet Protocols in Action; John Wiley & Sons; 2005. ISBN 0-471-66186-4.

Online

Grance, T., Kent, K., & Kim, B. Computer Security Incident Handling Guide (Draft). NIST Publication SP800-61, 2007.

Chevalier, Grance, Dang, Kent, Guide to Integrating Forensic Techniques into Incident Response, NIST Publication SP800-86, 2006.

Projects/Activities

Each student will:

- Create an online portfolio.
- Participate in the class online discussion forum
- Plan, prepare and demonstrate an incident response (corporate forensics) toolkit (activity).
- Create and present a poster that demonstrates an appropriate application of technology to enterprise security.

Evaluation

Exams/Quizzes	40%
Class Portfolio	40%
Poster	10%
Class Activities	10%

Instructor	Office
Ed Crowley	T2, Room 337
Phone: 713-743-4096	Hours: By appointment and as posted.
E-mail: Crowleye@yahoo.com	Web: cybersd.com unokitty.freehostia.com

Recommended (*Not Required)* Reading

Kruse and Heiser; Computer Forensics: Incident Response Essentials; Addison-Wesley; 2001 ISBN 0201707195

Shema and Johnson; Third Edition, Anti-Hacker Tool Kit; McGraw Hill/Osborne; 2006 ISBN 0072262877

Policy

By design, this class conforms to all relevant College and University Policy. For more specific information concerning University Policy, please visit:

http://www.uh.edu/provost/stu/stu_syllabsuppl.html