RARITAN VALLEY COMMUNITY COLLEGE
COURSE OUTLINE

CISY-274 – Privacy, Ethics & Computer Forensics

I. Basic Course Information

A. Course Number & Title: **CISY-274 - Privacy, Ethics, & Computer Forensics**

B. New or Modified Course: **Modified**

C. Date of Proposal: Semester: **Spring** Year: **2012**

D. Sponsoring Department: **Computer Science (CS) Department**

E. Semester Credit Hours: **3**

F. Weekly Contact Hours: **4** Lecture: **2**
Laboratory: **2**

G. Prerequisites: **MATH 020 Elementary Algebra or satisfactory score on placement test**

H. Laboratory Fees: **Yes, at prevailing rate**

I. Name and Telephone Number or E-mail Address of Department Chair: **Tom Edmunds, x8304, tedmunds@raritanval.edu**

II. Catalog Description

Prerequisite: MATH 020 Elementary Algebra or satisfactory score on placement test. This course provides the student with an understanding of security issues pertaining to privacy and ethics, as well as instruction and practice of forensics skills. Students perform hands-on exercises using the UNIX, Linux, and Windows operating system, including evidence collection and forensics activities at various levels including technical and process-oriented exercises. Students learn how to collect, catalog, sort, analyze and organize evidence. In addition, students learn how to package and present their findings to legal and law enforcement agencies with special consideration given to privacy issues and ethics.

III. Statement of Course Need

A. Due to the widespread acceptance of both networking and Internet integration into most business models, and widespread personal use of high-speed internet access and home networks, many computers are now vulnerable to a wide range of malicious attacks. The widespread knowledge of this vulnerability, the low threshold of knowledge needed to exploit many of the vulnerabilities, and the funding and/or use of such attacks by many countries and special interest groups as “information warfare,” has caused a need for comprehensive security measures to be administrated on all networks. This need is being recognized by many small to medium sized businesses that until now have not had a security policy.

The increase in companies of all sizes which now are engaged in web based information transfers such as e-business, data mining, and product information distribution has created a large market for security professionals. In addition to the financial risks that security breaches cause, new federal and European Union laws requiring stringent privacy requirements have created legal risks for companies with poor data security. Ethics, laws and privacy issues have become part of the fabric of conducting business over the internet. Therefore understanding citizen rights for privacy, ethical consideration for investigators and the limitation and boundaries of the law have all become interconnected in the new world of doing business over the internet.

B. This course does have lab component. Students are expected to use computers in the lab to work with various operating systems. Currently this course requires the Networking Lab in Bridgewater, Room B105.

C. This course generally transfers as a Computer Science Elective**.**

IV. Place of Course in College Curriculum

A. Free Elective
B. This course meets a program requirement for:
   1. Computer Networking and Security Certificate, Traditional Emphasis
   2. Computer Networking A.A.S
   3. Computer Support Certificate
   4. Web Developer A.S.
   5. Web Developer Certificate
C. CIS Elective
D. Course Transferability: for New Jersey schools, go to the NJ Transfer website, www.njtransfer.org . For all other colleges and universities, go to their individual websites.

V. Outline of Course Content

A. Introduction.

1. Rationale for forensics, ethics and privacy
2. The role of security fits in the overall IT industry.
3. Potential areas of employment

B. Risk mitigation

1. Understanding damage control, crime in cyberspace, cyber terror, information warfare, hackers, crackers, and social engineering
2. Motives, threats and trends
3. Privacy issues and constitutional protections
4. Legal issues regarding computer seizure
5. Court references and dependencies

C. Incident response techniques, processes and architecture

1. The need for Incident Response and Forensics
2. Computer Intrusion Laws
3. Incident response preparation and toolkits
4. Incident verification and response actions
5. Trend analysis and tracking incidences
6. Raid and Seizure
7. Evidence recording, photographing, backup, labeling, classifying and storage

D. Preservation of evidence

1. Digital evidence
2. Verifying without damaging evidence
3. Escalation techniques
4. Preserving the chain of evidence
5. Contacting law enforcement agencies
6. Coordinating with legal and understanding the law
7. Detailing and logging the event
8. Identify digital and non-digital artifacts.
9. System and network logs
10. Cost of damage including hours expended in incident recovery, loss of revenue, and value of trade secrets

E. Analysis of computer files based on file creation, file modification and file access

F. Mal-ware - understanding viruses, Trojan horses, worms and bombs

1. Abnormal Processes
2. Reviewing Relevant Files
3. Unusual or Hidden Files
4. Unauthorized Access Points
5. Trust Relationships
6. Security Identifiers

G. Differences among DOS, Windows and Windows NT/2000/XP from a forensics standpoint. Windows methods that will ensure maximum evidence capture.

H. Computer forensics processing methods and procedures
    1. Trust Relationships Forensics
    2. Incident handling
    3. Intellectual property theft, computer abuse, and intrusions,
    4. Investigative methods for incident response
    5. Documentation of computer forensics findings for use in trial and management review
    6. Issues relevant to overcoming a legal junk science attack.

I. Cyberspace Ethics
    1. Ethics in the new internet age
    2. Homeland security
    3. Social responsibilities
    4. Role of government in ethics
    5. Business responsibilities
    6. Personal responsibilities

J. Privacy Environment
    1. HIPAA, EU Directives, GLB, CPNI, PI, CA 1386
    2. Privacy assessment and policy
    3. Privacy incident reporting and tracking
    4. Acceptable use and acceptable terms

VI. Educational Goals and Learning Outcomes

A. Educational Goals– Students will be able to:

1. Communicate information security solutions that reflect critical and creative thought (GE-NJ 1)
2. Use the Internet for research, information analysis, problem solving, and decision making regarding information security (GE-NJ 4).
3. Develop the ability to make informed judgments concerning ethical issues in Information Security (GE-NJ 9)

B. Student Learning Outcomes - Students will be able to:

1. Identify the types of security and privacy threats that are prevalent today. Categorize and identify the types of malicious software currently used to exploit these threats.

2. Perform a security evaluation and draft a security policy for an enterprise class or smaller entity.

3. Explain the legal constraints required by security and privacy related laws and regulations as they pertain to information security and intrusion investigations.

4. Prepare and implement a procedure for responding to computer intrusions, including documentation of methods used, tracking of evidence, and other methodologies needed for the forensic investigation to pass legal challenges in court.

5. Explain the ethical issues involved in security practices at the governmental, business, and personal levels.

VII. Modes of Teaching and Learning

A. lecture/discussion
B. small-group work
C. computer-assisted instruction
D. laboratory exercises
E. student oral presentations
F. simulation/role playing

VIII. Papers, Examinations, and other Assessment Instruments

A. laboratory products & reports
B. weekly assignments
C. research papers
D. oral presentations
E. exams and quizzes
F. mid-term and final exams
G. classroom participation

IX. Grade Determinants

A. Laboratory products & reports
B. Weekly assignments
C. Research paper
D. Oral presentations
E. Exams/quizzes

X. Texts and Materials

A. Suggested Textbooks

1. Hacking Exposed by Joel Scambray, Stuart McClure and George Kurtz, McGraw-Hill Professional Publishing; ISBN: 0072127481
2. The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

by Ronald L. Krutz, Russell Dean Vines, Edward M. Stroz (Foreword), John Wiley & Sons; ISBN: 0471413569

(Please Note: The course outline is intended only as a guide to course content and resources. Do not purchase textbooks based on this outline. The RVCC Bookstore is the sole resource for the most up-to-date information about

XI. Resources

1. library resources
2. technology support
3. Hands-on Networking Lab (currently at Bridgewater, B105)
4. http://www.cissp.com/default.html, the web portal for the certified information systems security professional
5. http://www.microsoft.com