October 2007

ERIE COMMUNITY COLLEGE

COURSE OUTLINE

A. COURSE TITLE

AND NUMBER: DA206 Networking & Net. Forensics

B. CURRICULUM: Information Technology (1492)

C. COURSE

DESCRIPTION:

An overview of network technology, network components, network operating system software and network interconnection schemes. A detailed overview of network traffic capturing, packet analysis, intrusion detection, firewalls, proxy servers, image capturing and transportation, and memory forensics.

Prerequisite: CS 101, DA 107 or computer literacy (N.B. this means command prompt

familiarization), or permission of the instructor. (N)

D. DURATION OF

INSTRUCTIONAL

PERIOD:

Two hundred and fifty minutes per week for fifteen weeks

(150 minutes lecture, 100 minutes lab).

E. ACADEMIC

CREDIT HOURS: (3,2,4)

Four (4.0) credit hours.

F. SUGGESTED TEXT/COURSE MATERIALS: See Book Specific Outline

G. COURSE OUTCOMES: Upon completion of this of this course, the student will be able to:

1. To run and interpret results of:
   1. ping
   2. tracert
   3. arp
   4. netstat
   5. nbtstat
   6. ipconfig
   7. Ifconfig
   8. iwconfig
   9. winipcfg
   10. nslookup
2. Create network twisted pair cables
3. Setup a fire wall
4. Setup a proxy server
5. Setup Snort
6. Put a LAN together
7. Map network drives
8. Setup NSF
9. Setup samba shares
10. Setup and configure live usb sticks
11. Setup scripts for network auditing
12. Install and use network tool packages
13. Do memory foot printing and acquisition
14. Setup a network sniffer

15. Setup a honey pot.

16. TECHNOLOGY OBJECTIVES:

* 1. Use a computer to setup and install operating systems and network software packages.
  2. Use the Windows and UNIX/Linux operating environment effectively

H. **Program Competencies:**

Upon graduation with an Associate in Applied   
 Science degree in Information Technology, the   
 graduate will be able to:

1. Demonstrate knowledge of a broad business and real world perspective of information technology.
2. Demonstrate analytical and critical thinking skills.
3. Demonstrate the ability to apply analytical and logical thinking to gathering and analyzing information, designing and testing solutions to problems, and formulating plans.
4. Demonstrate the ability to visualize and articulate complex problems and concepts.
5. Demonstrate the ability to gather, analyze and organize data using a logical and systematic process.
6. Demonstrate the ability to select, implement and evaluate appropriate problem solving techniques and tools.
7. Demonstrate the ability to effectively adapt problem solving techniques to specific situations.
8. Use and apply current technical concepts and practices in the core information technologies.
9. Identify and evaluate current and emerging technologies and assess their applicability to address the users’ needs.
10. Analyze the impact of technology on individuals, organizations and society, including ethical, legal and policy issues.
11. Demonstrate an understanding of best practices, standards and their application.
12. Demonstrate independent critical thinking and problem solving skills.
13. Communicate effectively and efficiently with clients, users and peers both verbally and in writing, using appropriate terminology.
14. Demonstrate the ability to present and discuss how computer systems impact the operation and management of business and society.
15. Demonstrate the ability to discuss the impact of information technology on society and the workplace.

CERTIFICATE COMPETENCIES:

Upon completion of the course, students will:

1. Be able to acquire, validate, extract, analyze and report upon digital evidence.

2. Be conversant with multiple digital devices including, but not limited to; computers, personal digital assistants, cameras, cell phones, ipods, removable flash media

3. Be knowledgeable about the physical handling of digital devices

4. Be able to create understandable and accurate reports.

I. SUNY General Education

Knowledge and Skills: Not Applicable

J. ECC Graduate Learning

Outcomes (GLO): 1. Communicate effectively.

Related Course Outcomes:

1, 3, 4, 5, 8, 9, 11, 14, 15, 16

2. Read and think critically.

Related Course Outcomes:

1 to 16

3. Demonstrate adequate preparation for a career or

continuing education.

Related Course Outcomes: 1-16

4. Demonstrate competence with computers and technology.

Related Course Outcomes: 1 – 16

K. ASSESSMENT OF

STUDENT LEARNING: Achievement of the Course Outcomes will be measured by:

1. A minimum of 150 minutes of examination to be determined

by the instructor. Test questions will include programming

questions.

2. Several graded assignments that involve researching current trends in network forensics.

L. LEARNING RESOURCE

CENTER AND OTHER

SUPPORT: Computer Lab and Library Resources.

M. TOPICAL OUTLINE: INSTRUCTIONAL

PERIODS

I. INTRODUCTION 1 weeks

A. Network Security Policies

B. Network Technologies

C. Network Components

D. Wireless Network Technologies

E. Wireless service Factors

F. Wireless security an oxymoron

II. Network Technology in Detail 2 weeks

A. TCP/IP Model

B. Open Systems Interconnect Model (OSI)

C.. Ethernet Technology

D. MAC addresses

E. IP Addresses

F. IP Addressing Methods

G. Ports

H. Services

I. Protocols

III. Network Implementation 2 weeks

A. Server Operating Systems

1. Unix/Linux

2. Windows

3. Mac OS X Server

B. Client Connectivity

IV. Tools for Networking 3 weeks

A. Firewalls

B. Proxy Service

C. Natting

D. Virtual Area Networks

E. Internal Networks vs External Networks

F. Fault Tolerance

G. Disaster Recovery

V. Intrusion Detection 3 weeks

A. Ping Sweeps

B. ISS scans

C. php and webservers

D. False Positive/Negatives

E. IDS notification

F. Protection of Notification Channel

G. Network Audit Techniques

H. Attack Detection

I. Anomaly Detection

J. Misuse Detection

K. Honey Pots

L. Snort in detail

VI. Transmission Security 1 week

1. Data and signals
2. Securing remote access

C. Securing digital cellular telephony

D. Hardening wireless local area networks

E. Error detection and error control

VII. Forensics Analysis 2 weeks

A. Traffic Capture Techniques

B. Imaging Network Drives

C. Encrypted files

D. Deep analysis

E. Network Forensics Tools

VII. Evaluation 1 week

LAB TOPICS (at the discretion of the instructor) INSTRUCTIONAL

PERIODS

15 weeks

N. PREPARED BY: Anthony Kuroski