BUTTE COLLEGE
COURSE OUTLINE

I. **CATALOG DESCRIPTION**

CSCI 17 - Computer and Network Security/Security+ **3 Unit(s)**

Prerequisite(s): CSCI 49
Recommended Prep: Reading Level IV; English Level IV; Math Level III
Transfer Status: CSU
34 hours Lecture
51 hours Lab

This is an advanced course in computer and network security. This course will prepare students to evaluate, secure and manage network information assurance, and take the CompTIA Security+ certification exam. Course topics include threat management, security standards and protocols (including public key infrastructure and cryptography), intrusion detection and prevention, forensics, system recovery, and disaster planning. The principles of data integrity, user accountability, and policy management will be explored in detail. Students will develop and demonstrate intrusion detection skills utilizing a virtual network to configure and test security procedures.

II. **OBJECTIVES**

Upon successful completion of this course, the student will be able to:

A. Implement secure network practices while assuring that authorized users are able to do legitimate work in a cost efficient manner.
B. Define, develop and deploy acceptable use policies.
C. Configure appropriate backup and recovery strategies.
D. Identify the techniques of secure coding and defensive programming in the software development life-cycle.
E. Summarize the security implications and risks for distributed Information Technology (IT) systems.
F. Perform a risk assessment analysis and develop and implement appropriate proactive security policy and procedures.
G. Monitor a network and detect system intrusion, and secure a compromised system for a forensic investigation.
H. Perform a threat assessment analysis, identify threats and vulnerabilities associated with enterprise assets, determine impact and make appropriate mitigation recommendations.
I. Comply with the requirements of regulatory agencies to secure financial data or Personally Identifiable Information (PII).

III. **COURSE CONTENT**

A. **Unit Titles/Suggested Time Schedule**

Lecture

Topics	Hours
1. Security concepts, trends, legal issues, ethics, and privacy	4.00
2. Physical and network infrastructure security, intrusion detection/prevention, auditing/security baselines, protocol analysis	6.00
3. Risk assessment and management, privilege/change management, business continuity	3.50
4. Disaster recovery and computer forensics	3.50

5. Malicious code, e-mail, messaging and web vulnerabilities, social engineering	3.00
6. Avenues of attack, minimizing attack surface, network/application hardening	3.00
7. Organizational policies: procedures, standards, guidelines, bring your own device (BYOD) management, secure software development	5.00
8. Authentication and remote access control authorizations, tokens, protocols permissions and methods	3.00
9. Cryptography symmetric/asymmetric and Public Key Infrastructure, wireless vulnerabilities	3.00
Total Hours	34.00

Lab

Topics	Hours
1. Security concepts, trends, legal issues, ethics, and privacy	4.50
2. Physical and network infrastructure security, intrusion detection/prevention, auditing/security baselines, protocol analysis	8.50
3. Risk assessment and management, business continuity, privilege/change management	5.00
4. Disaster recovery and computer forensics	5.00
5. Malicious code, e-mail, messaging and web vulnerabilities, social engineering	5.00
6. Avenues of attack, minimizing attack surface, network/application hardening	4.50
7. Organizational policies: procedures, standards, guidelines, bring your own device (BYOD) management, secure software development	7.50
8. Authentication and remote access control authorizations, tokens, protocols permissions and methods	6.50
9. Cryptography symmetric/asymmetric and Public Key Infrastructure, wireless vulnerabilities	4.50
Total Hours	51.00

IV. METHODS OF INSTRUCTION

A. Lecture
B. Homework: Students are required to complete two hours of outside-of-class homework for each hour of lecture
C. Demonstrations
D. Multimedia Presentations
E. Practical Exercises

V. METHODS OF EVALUATION

A. Exams/Tests
B. Quizzes
C. Oral Presentation
D. Lab Projects
E. Essays and research papers

VI. EXAMPLES OF ASSIGNMENTS

A. Reading Assignments

1. Read the article provided by the instructor about how a NYC data center dealt with Hurricane Sandy. Write a few paragraphs about what you learned from their preparation and be prepared to discuss the article in class.
2. You have a single domain website and want to secure your online sales transactions, you also want it to be obvious to your buyers that it is a secure site. Read the documentation about the cost and services provided by two different trusted commercial CAs. Compare and contrast the reputation for an EV SSL Certificate. Submit an outline of your findings to your instructor.

B. Writing Assignments
1. Write a one page acceptable use policy for employees of an enterprise level company. Include an explanation of security and malware risks to the company network and what users can do to help avoid infection.
2. Compare a disaster recovery plan and a business continuity plan. Compare and contrast the value of each in a half-page description.

C. Out-of-Class Assignments
1. Research a vendor of F5 security appliances and evaluate the types of products and services they provide. Be prepared to explain to the class what appliances would be best to secure a midsized business.
2. On your home computer, download and install an encryption application like GPG. Experiment with it and be prepared to discuss your findings with the class.

VII. **RECOMMENDED MATERIALS OF INSTRUCTION**

Textbooks:

A. Conklin, W.A., White, G., Davis, R.L., Cothren, C. Principles of Computer Security: CompTIA Security+ and Beyond. 4th Edition. McGraw-Hill, 2015.

B. Nestler, V. Principles of Computer Security: CompTIA Security+ and Beyond Lab Manual. 4th Edition. McGraw-Hill, 2015.

Created/Revised by: Linda Fischer
Date: 03/07/2016