OHLONE COLLEGE
Ohlone Community College District
OFFICIAL COURSE OUTLINE

I. **Description of Course:**

1. **Department/Course:** CNET - 170
2. **Title:** Network Security (Security+)
3. **Cross Reference:**
4. **Units:** 4
   Lec Hrs: 3
   Lab Hrs: 3
   Tot Hrs: 108.00
5. **Repeatability:** No
6. **Grade Options:** Letter Grade, May Petition for Pass/No Pass (GC)
7. **Degree/Applicability:** Credit, Degree Applicable, Transferable - CSU (T)
8. **General Education:**
9. **Field Trips:** Not Required
10. **Requisites:**
12. **Catalog Description:**
    This course provides an in-depth study of Network Security fundamentals and provides a comprehensive overview of network security. Students will gain the knowledge and skills required to identify risk and participate in risk mitigation activities; provide infrastructure, application, operational, and information security; apply security controls to maintain confidentiality, integrity, and availability; identify appropriate technologies and products; and operate with an awareness of applicable policies, laws, and regulations. This course provides the foundation for students preparing to take the CompTIA Security+ certification exam.
13. **Class Schedule Description:**
    Comprehensive overview of network security. Prep for Security+ certification.
14. **Counselor Information:**
    This course provides an in-depth study of Network Security fundamentals and provides a comprehensive overview of network security. Course content and objectives map to CompTIA's Security+ Certification Exam.

II. **Student Learning Outcomes**

The student will:

1. Identify the fundamental concepts of computer security, security threats and vulnerabilities and examine network security.
2. Manage application, data and host security and identify access control and account management security measures.
3. Identify compliance and operational security measures.
4. Manage certificates, risk, and security incidents.
5. Develop business continuity and disaster recovery plans.

III. **Course Content:**

A. Introduction to security
    1. Challenges of securing information
    2. What is information security?
    3. Who are the attackers?
    4. Attacks and defenses
    5. Defenses against attacks
B. Malware and social engineering attacks
    1. Attacks using malware
    2. Social engineering attacks
C. Application and network attacks
    1. Application attacks
    2. Network attacks
D. Vulnerability assessment and mitigating attacks
    1. Vulnerability assessment
    2. Vulnerability scanning and penetration testing
    3. Mitigating and detering attacks
E. Host, application, and data security
    1. Securing the host
    2. Application security
    3. Securing data
F. Network Security
    1. Security through network devices
    2. Security through network technologies
    3. Security through networkdesign elements
G. Administering a secure network
    1. Common network protocols
    2. Network administration principles
    3. Securing network applications
H. Wireless network security
    1. Wireless attacks
    2. Vulnerabilities of IEEE 802.11 security
    3. Wireless security solutions
I. Access control fundamentals
    1. What is access control?
    2. Implementing access control
    3. Authentication status
J. Authentication and account management
    1. Authentication credentials
    2. Single sign-on
    3. Account management
K. Basic cryptography
    1. Defining cryptography
    2. Crytographic algorithms
    3. Using cryptography
L. Advanced cryptography
    1. Digital certificates
    2. Pulic Key Infrastructure (PKI)

3. Key management
4. Transport encryption alogorithms

M. Business continuity
1. What is business continuity
2. Disaster recovery
3. Environmental controls
4. Incident response procedures

N. Risk mitigation
1. Controlling risk
2. Reducing risk through policies
3. Awareness and training

O. LABS - Network Security
1. Network Devices and Technologies - Capturing Network Traffic
    a. Using tcpdump to Capture Network Traffic
    b. Capturing and Analyzing Traffic with Wireshark
    c. Capturing and Analyzing Traffic with Network Miner
2. Secure Network Administration Principles - Log Analysis
    a. Log Analysis in Linux Using Grep
    b. Log Analysis in Linux Using Gawk
    c. Log Analysis in Windows Using Find
3. Protocols and Default Network Ports - Transferring Data Using TCP/IP
    a. Using Hyper Text Transfer Protocol (HTTP) to Transfer Files
    b. Using Fire Transfer Protocol (FTP) to Transfer Files
    c. Transferring Files Securely Using SCP
4. Protocols and Default Network Ports - Connecting to a Remote System
    a. Connecting to a Windows system Through the Command Line
    b. Connecting to a Linux System Through the Command Line
    c. Analyzing Remote Connections in Network Traffic
5. Secure Implementation of Wireless Networking
    a. Examining Plain Text Traffic
    b. Cracking and Examining WEP Traffic
    c. Cracking and Examining WPA Traffic

P. LABS - Compliance and Operational Security
1. Incident Response Procedures
    a. Using db_autopwn to Attack a Remote System
    b. Collecting Volatile Data
    c. Viewing Network Logs

Q. LABS - Threats and Vulnerabilities
1. Analyze and Differentiate Types of Malware
    a. Using Netcat to Send a Reverse Shell
    b. Using Ncat to Send a Reverse Shell
    c. Sending a Bash Shell to a Windows Machine using NetCat
2. Analyze and Differentiate Types of Attacks Using Window Commands
    a. Viewing Network Resources
    b. Using PSEXEC to Connect to a Remote System
    c. Stopping, Starting, and Removing Services
3. Analyze and Differentiate Types of Application Attacks
    a. Scanning the Network for Vulnerable Systems

b. Introduction to Metasploit, a Framework for Exploitation
c. Attacking a Remote System Utilizing Armitage
d. Post Exploitation of the Remote System

4. Mitigation and Deterrent Techniques - Anti Forensic
   a. The Windows Event Viewer
   b. Enabling Auditing
   c. Clearing the Event Logs
5. Mitigation and Deterrent Techniques - Password Cracking
   a. Cracking Linux Passwords
   b. Cracking Windows Passwords
   c. Cracking Windows Passwords with Cain
6. Discovering Security Threats and Vulnerabilities
   a. Scanning the Network for Vulnerable Systems
   b. Using Nessus
   c. Introduction to Metasploit, a Framework for Exploration

R. LABS - Application, Data and Host Security
1. Importance of Data Security - Data Theft
   a. Using Metasploit to Attack a Remote System
   b. Stealing Data using FTP and HTTP
   c. Stealing Data using Meterpreter
2. Importance of Data Security - Securing Data Using Encryption Software
   a. Installing TrueCrypt
   b. Creating a TrueCrypt Container
   c. Opening and Viewing Data within a TrueCrypt Container

S. LABS - Access Control and Identity Management
1. Authentication, Authorization and Access Control
   a. Adding Users, Groups, and Passwords
   b. Absolute Permissions

T. LABS - Cryptography
1. General Cryptography Concepts
   a. Hiding a Picture within a Picture Using S-Tools
   b. Hiding a Media File within a Picture Using S-Tools
   c. Revealing Hidden Data Using S-Tools

IV. **Course Assignments:**

A. Reading Assignments
1. Textbook readings and online supporting webpages to inform the student on the fundamental concepts of computer security, security threats and vulnerabilities, and on how to examine network security.

B. Projects, Activities, and other Assignments
1. Hands-on lab assignments using the Ohlone NetLAB to develop skills on how to manage application, data and host security and identify access control and account management security measures. Troubleshooting non-expected outcomes.

C. Writing Assignments
1. Assignment worksheets and lab reports to support the lab assignments and document the results of those lab assignments.

V. **Methods of Evaluation:**

A. Objective quizzes on fundamental concepts of computer security, security threats and vulnerabilities and examine network security.
B. Lab Projects to build skills to manage application, data and host security and identify access control and account management security measures; and to develop skills to dentify compliance and operational security measures.
C. Comprehensive Final Exam on network security and the fundamental concepts of computer security, security threats and vulnerabilities and examine network security.
D. Skills-based assessment (hands-on final exam) on network security steps, practices, and techniques.

VI. **Methods of Instruction:**

A. Lecture
B. Laboratory
C. Discussion
D. Demonstration
E. Distance Learning

VII. **Textbooks:**

Recommended

1. Mark Ciampa *Security+ Guide to Network Security Fundamentals* 4th Edition, Cengage Learning, 2011 ISBN: 978-1111640125

Supplemental

VIII. **Supplies:**

Approval Date: 05/09/2013
CCC Number: CCC000445326
TOP Codes:
0708.10
C-ID Number: