Las Positas College
3000 Campus Hill Drive
Livermore, CA 94551-7650
(925) 424-1000
(925) 443-0742 (Fax)

Course Outline for NCIS 201

CYBERSECURITY CAMP

Effective: Fall 2019

I. CATALOG DESCRIPTION:
NCIS 201 — Noncredit

This course will introduce the novice to cybersecurity career opportunities, cyber ethics, online safety, and cyber threats. Students will be introduced to cybersecurity principles, virtual machines, basic Windows and Linux administration security policies, fundamental CISCO network routing and CISCO packet tracer. As a culminating activity students will compete by analyzing and fixing vulnerabilities on the provided Windows and Linux images.

Grading Methods:
Pass/No Pass/Satisfactory Progress

Discipline:
- Vocational (short-term): Noncredit

Noncredit Category
J - Workforce Preparation

	MIN
Total Noncredit Hours:	40.00

II. PREREQUISITE AND/OR ADVISORY SKILLS:

III. MEASURABLE OBJECTIVES:

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

A. Describe cybersecurity career opportunities, cyber ethics, online safety, and cyber threats
B. Participate in hands-on introduction to the fundamentals of cybersecurity, from system hardening to access control to system protection for both Windows and Linux operating systems
C. Gain an appreciation of the importance to our nation of cyber, cyber security, and good computer practices
D. Productively participate as team member in a cyber security defense competition
E. Explain basic IT security concepts and models

IV. CONTENT:
A. Cyber Ethics - This module outlines the fundamentals of ethical behavior in the real world and online.
    1. Important definitions
    2. Ethical behavior
    3. Ethics and cybersecurity
    4. Ethics applications
B. Introduction to CyberPatriot and Cybersecurity– This module contains information about the CyberPatriot program and cybersecurity concepts in general.
    1. Cyber Competition basics: CyberPatriots, NCL, etc
    2. The importance of cybersecurity
    3. Cyber careers
C. Online Safety – This module outlines ways to stay safe on the Internet. Topics include:
    1. Cyberbullying
    2. Personally identifiable information
    3. Social media tips
D. Computer Basics and Virtual Machines – This module provides information about computer hardware and the software used to play competition virtual machine images. Topics include:
    1. Computer hardware basics
    2. Networking basics
    3. An overview of virtualization
    4. How to start a virtual machine
E. Principles of Cybersecurity – This module describes cybersecurity concepts in more detail. Topics include:
    1. CIA Triad
    2. How to build strong passwords
    3. Social engineering
    4. Malware
F. Microsoft Windows Security: This module is the most important for understanding how to find and fix common vulnerabilities on Windows images. Topics include:
    1. An introduction to Windows operating systems
    2. Firewalls
    3. Security tools and policies
G. Windows File Protections and Monitoring – This module contains more advanced Windows security topics, including:

1. File protections
2. Encryption
3. Backups
4. Auditing
5. System monitoring

H. Introduction to Linux and Ubuntu – This module is helpful for gaining an introduction to non-Windows systems that may be used during the competition. Topics include:
   1. An introduction to Unix
   2. Linux Flavors
   3. Introduction to command line

I. Ubuntu Security- This module includes tips for securing an Ubuntu operating system. Topics include:
   1. GUI security
   2. Updates
   3. Command line security
   4. Security tools and policies

J. Additional Training Topics and Tips- This module contains other tips for competing in the CyberPatriot competition. Topics include:
   1. Topics for further study
   2. Tips from CyberPatriot veterans

K. CISCO Networking, routing, Packet Tracer
   1. Intro to Networks
   2. Intro to CISCO routing
   3. Intro to Packet Tracer

V. METHODS OF INSTRUCTION:

A. **Classroom Activity** - Hands-on labs, cyber competitions
B. **Lecture** - Lecture on cyber security topics, Windows administration, Linux administration, networking
C. **Lab** - Hands-on computer lab tasks
D. **Discussion** - Sharing of competition results, lists, etc

VI. TYPICAL ASSIGNMENTS:

A. Hands-on operating system (Windows and/or Linux) adminstration
   1. Apply security policies in a a Windows and/or Linux environment
B. Develop a security check list for use during the competition activities
C. Web search

VII. EVALUATION:

Methods/Frequency

A. Group Projects
   min 1-2
B. Class Participation
   daily
C. Lab Activities
   50% hands-on labs

VIII. TYPICAL TEXTS:

1. Lehto, Marti. *Cyber Security Analytics, Technology, and Automation.* 1st ed., Springer, 2016.
2. US CyberPatriot. *AFA CyberCamp Kit.* 11th ed., US Air Force Association CyberPatriot, 2018.

IX. OTHER MATERIALS REQUIRED OF STUDENTS:

A. storage: flash, portable hard drive, cloud