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

Course Outline for NCIS 202

CYBERSECURITY COMPETITION PREP

Effective: Fall 2019

I. CATALOG DESCRIPTION:
NCIS 202 — Noncredit

This course prepares students to participate in cyber security competitions (CyberPatriot, National Cyber League, etc). Topics include an overview of cyber competitions, virtual machines, Linux operating systems and administration, Windows operating systems and administration, CISCO networking, and packet tracer. Through business scenarios, students will create checklists of potential vulnerabilities and work in teams to secure networks and sensitive data.

Grading Methods:
Pass/No Pass/Satisfactory Progress

Discipline:
- Vocational (short-term): Noncredit

Noncredit Category
J - Workforce Preparation

	MIN
Total Noncredit Hours:	30.00

II. PREREQUISITE AND/OR ADVISORY SKILLS:

III. MEASURABLE OBJECTIVES:

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

A. Document system changes and best practices learned during cybersecurity defense competitions as a member in cybersecurity competitions
B. Implement and correct Windows desktop and server operating system configurations
C. Implement and correct Linux operating system configurations
D. Productively participate as a member of a cybersecurity team
E. Explain basic IT security concepts and models

IV. CONTENT:
A. Windows
1. Installation
2. Navigation
3. File structure
4. System Configuration
5. File and Folder Permissions
6. Windows Powershell Command Line
7. Identify security vulnerabilities
B. Server Roles and Features
C. Linux
1. Installation
2. Navigation: GUI, command line
3. System Configuration
4. Linux Services
5. Identify security vulnerabilities
D. CISCO
1. Introduction to networks hardware, e.g, routers, switches
2. CISCO Routing and Switching
3. Packet Tracer software
E. VMWare
1. Overview of VMWare
2. Create multiple virtual machines
F. CyberSecuirty Competition
1. Develop checklists of potential security vulnerabilites for Windows and Linux operating system for use during competitions
2. Participate as a team member in cybersecurity competitions
3. Develop team leadership skills

V. METHODS OF INSTRUCTION:
A. **Lab** - Hands-on cybersecruity lab tasks
B. **Lecture** -
C. **Classroom Activity** - Hands-on labs, cyber competitions

D. **Discussion** - Sharing of competition results, lists, debrief, etc.
E. **Lecture** - Lecture on cyber security topics, Windows administration, Linux administration, networking

VI. TYPICAL ASSIGNMENTS:
A. Given a Windows desktop operating system image, find and fix the security vulnerabilites
B. As a team, create a check list of possible vulnerabilites to check in a Linux operating system
C. Download and install Virtual Machine

VII. EVALUATION:
Methods/Frequency

A. Exams/Tests
frequent practice quizzes
B. Lab Activities
1-2 hands-on class activities every session

VIII. TYPICAL TEXTS:
1. Ulsch, MacDonnell. *Cyber Threat!! How to Manage the Growing Risk of Cyber Attacks.* 2nd ed., Wiley, 2017.
2. US Airforce Associations CyberPatriot Academy. *Training Modules.* 11th ed., US Air Force Association CyberPatriot, 2018.

IX. OTHER MATERIALS REQUIRED OF STUDENTS:
A. storage: flash, portable hard drive, cloud