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

Course Outline for CIS 42

CYBERSECURITY COMPETITION PREP

Effective: Fall 2018

I. CATALOG DESCRIPTION:
CIS 42 — CYBERSECURITY COMPETITION PREP — 0.50 units

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.

0.50 Units Lab

Strongly Recommended
CIS 41 - CyberSecurity Camp
with a minimum grade of C

Grading Methods:
Letter or P/NP

Discipline:
- Computer Information Systems

	MIN
Lab Hours:	27.00
Total Hours:	27.00

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 1

III. PREREQUISITE AND/OR ADVISORY SKILLS:

Before entering this course, it is strongly recommended that the student should be able to:

A. CIS41
1. 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
2. Productively participate as team member in a cyber security defense competition

IV. 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

V. 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

VI. METHODS OF INSTRUCTION:

A. **Lab** -
B. **Lecture** -

VII. 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

VIII. EVALUATION:

A. **Methods**

1. Exams/Tests
2. Quizzes
3. Lab Activities

B. **Frequency**

1. chapter quizzes (theory) per chapter
2. final exam (hands-on) practice competion -- required final
3. lab activities -- each class

IX. TYPICAL TEXTS:

1. Ulsch, MacDonnell. *Cyber Threat!! How to Manage the Growing Risk of Cyber Attacks.* 1st ed., Wiley, 2015.
2. US Airforce Associations CyberPatriot Academy. *Training Modules.* 10th ed., US Air Force Association CyberPatriot, 2017.

X. OTHER MATERIALS REQUIRED OF STUDENTS:

A. storage: flash, portable hard drive, cloud