STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR 356 - CYBERSECURITY DEFENSE AND COUNTERMEASURES

Created by: Minhua Wang
Updated by: Minhua Wang

CANINO SCHOOL OF ENGINEERING TECHNOLOGY
DECISION SYSTEMS
FALL 2018

A. **TITLE**: CYBERSECURITY DEFENSE AND COUNTERMEASURES

B. **COURSE NUMBER:** CYBR 356

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

 # Credit Hours: 3
 # Lecture Hours: 3 **per week**
 # Lab Hours: **per week**
Other: **per week**

Course Length: 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Fall

G. **COURSE DESCRIPTION:** This course provides a thorough guide to perimeter defense fundamentals, including intrusion detection and firewalls. It covers advanced topics such as security policies, network address translation (NAT), packet filtering and analysis, proxy servers, virtual private networks (VPN), and network traffic signatures. This course examines the latest technology, trends, and techniques including virtualization, IPv6, and ICMPv6 structure, making it easier to stay on the cutting edge and one step ahead of potential security threats.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CITA 250 Information Security
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	***PSLO***	***ISLO***
a. Specify fundamental concepts and components of network defense and countermeasures	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Summarize and compare various methodologies in network defense and countermeasures	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA] 5
c. Recommend network defense and countermeasures solutions to specific electronic system implementations	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA, PS] 5

d. Identify examples of most current developments in network defense and countermeasures	6. Adapt to new situations and demands by applying and/or updating his/her knowledge and skills	5

J. APPLIED LEARNING COMPONENT: **Yes__X___ No_____**

- Classroom/Lab

K. TEXTS: None

L. REFERENCES: Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database

M. EQUIPMENT: Computer lab classroom with virtual machine software installed

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Exams
- Quizzes
- Participation

P. DETAILED COURSE OUTLINE:

I. Introduction to Cybersecurity Defense and Countermeasures
- A. Cybersecurity Offense vs. Defense.
- B. Cybersecurity Countermeasures.

II. Cybersecurity Defense Fundamentals
- A. Network Security Fundamentals.
- B. TCP/IP.
- C. Network Traffic Signatures.
- D. Routing Fundamentals.
- E. Cryptography.
- F. Wireless Networking Fundamentals.
- G. Understanding Wireless Network Security.

III. Cybersecurity Countermeasures Implementations
- A. Intrusion Detection and Prevention System Concepts.
- B. Firewall Concepts.
- C. Firewall Design and Management.
- D. VPN Concepts.
- E. Internet and Web Security.
- F. Security Policy Design and Implementation.
- G. Ongoing Security Management.

IV. Other Topics: As Defined by the Instructor (The topics on most recent Cybersecurity Defense and Countermeasures developments are strongly recommended.)

Q. LABORATORY OUTLINE: N/A