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

MASTER SYLLABUS

CYBR/CITA 352 - Ethical Hacking and Penetration Testing

Created by: Minhua Wang
Updated by: Minhua Wang

SCHOOL OF SCIENCE, HEALTH AND CRIMINAL JUSTICE
CENTER FOR CRIMINAL JUSTICE, INTELLIGENCE AND CYBERSECURITY
FALL 2021

A. **TITLE**: Ethical Hacking and Penetration Testing

B. **COURSE NUMBER:** CYBR/CITA 352

C. **CREDIT HOURS:** 3

- 3 hours of lecture per week

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

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

G. **COURSE DESCRIPTION:** This course introduces students to a wide range of topics related to ethical hacking and penetration testing. The course provides an in-depth understanding of how to effectively protect computer networks. The topics cover the tools and penetration testing methodologies used by ethical hackers and provide a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber-attacks.

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

a. Pre-requisite(s): CYBR 165 Survey of Cybersecurity or CITA 220 Data Communications and Network Technology
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. Illustrate the importance of ethical hacking	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Categorize the various techniques for performing reconnaissance	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
c. Demonstrate various types of system scanners and their functions	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
d. Demonstrate the function of sniffers on a network	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
e. Analyze systems for TCP/IP weaknesses	3. Use a variety of computer hardware and software and other technological	5

	tools appropriate and necessary for the performance of tasks	
f. Practice the fundamentals of encryption and decryption	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
g. Compare various types of attacks and practice the proper defensive recourse for each	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	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. The Ethics of Hacking and Cracking
- A. The impact of unethical hacking
- B. Hat categories
- C. Ethics and issues of information technology

II. Reconnaissance
- A. Defining legalities
- B. Social Engineering
- C. Internet foot printing

III. Scanners and Sniffers
- A. Scanners
- B. Sniffers

IV. TCP/IP Vulnerabilities
- A. IP Spoofing
- B. Connection hijacking
- C. ICMP attacks
- D. TCP SYN attacks
- E. RIP attacks
- F. IP Security Architecture (IPSec)

V. Encryption and Password Cracking
- A. Cryptography
- B. Cryptanalysis
- C. Description of popular ciphers
- D. Attacks on passwords
- E. Password crackers

VI. Types of Attacks
- A. Spoofing
- B. Session hijacking
- C. Hacking network devices
- D. Trojan Horses
- E. Denial of Service attacks
- F. Buffer overflows
- G. Programming exploits

VII. Types of Vulnerabilities
- A. Mail vulnerabilities
- B. Web application vulnerabilities
- C. Operating system vulnerabilities
- D. Incident Handling

Q. <u>LABORATORY OUTLINE</u>: N/A