COURSE OUTLINE
CITA 352 - Ethical Hacking and Penetration Testing

Revised By: Minhua Wang

CANINO SCHOOL OF ENGINEERING TECHNOLOGY
INFORMATION TECHNOLOGY
May 2015
A. **TITLE:** Ethical Hacking and Penetration Testing

B. **COURSE NUMBER:** CITA 352

C. **CREDIT HOURS:** 3

D. **WRITING INTENSIVE COURSE:** No

E. **COURSE LENGTH:** 15 weeks

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

G. **HOURS OF LECTURE, LABORATORY, RECITATION, TUTORIAL, ACTIVITY:**
   3 lecture hours per week

H. **CATALOG 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.

I. **PRE-REQUISITES/CO-REQUISITES:**
   a. Pre-requisite(s): CITA 250 Information Security
   b. Co-requisite(s): none

J. **GOALS (STUDENT LEARNING OUTCOMES):**
   By the end of this course, the student will be able to:

<table>
<thead>
<tr>
<th>Course Objective</th>
<th>Institutional SLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Illustrate the importance of ethical hacking</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
<tr>
<td>b. Categorize the various techniques for performing reconnaissance</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
<tr>
<td>c. Demonstrate various types of system scanners and their functions</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
<tr>
<td>d. Demonstrate the function of sniffers on a network</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
<tr>
<td>f. Practice the fundamentals of encryption and decryption</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
<tr>
<td>f. Compare various types of attacks and practice the proper defensive recourse for each</td>
<td>2. Crit. Thinking 3. Prof. Competence</td>
</tr>
</tbody>
</table>
K. **TEXTS:**

L. **REFERENCES:** N/A

M. **EQUIPMENT:** computer class room with virtual machine software installed

N. **GRADING METHOD:** A-F

O. **MEASUREMENT CRITERIA/METHODS:**
- Individual projects
- Quizzes
- Exams

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. LABORATORY OUTLINE: N/A