GROSSMONT COLLEGE

Official Course Outline

# COMPUTER SCIENCE INFORMATION SYSTEMS 264 – ETHICAL CYBERSECURITY HACKING

1. Course Number Course Title Semester Units Semester Hours

CSIS 264 Ethical Cybersecurity 3 2 hours lecture: 32-36 hours

Hacking 3 hours lab: 48-54 hours

64-72 outside-of-class hours for lecture

144-162 total hours

2. Course Prerequisites

A “C” grade or higher or “Pass” in CSIS 263 or equivalent.

Corequisite

None

Recommended Preparation

None

3. Catalog Description

This course immerses IT professionals in hands-on intensive environments, providing in-depth knowledge and experience with current essential security systems. Provides understanding of perimeter defenses and leads to scanning and attacking networks; no real networks are harmed. Students learn how intruders escalate privileges and the steps to be taken to secure a system. Also covers Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virtual Creation. Focus includes legal and regulatory requirements, ethical issues, basic methodology and technical tools used for ethical hacking and penetration tests. Students establish a pre-test agreement with the enterprise, discover and exploit vulnerabilities, participate as a member of a pen test team and prepare a penetration test report.

4. Course Objectives

The student will:

a. Evaluate the legal and regulatory requirements of ethical hacking and penetration tests.

b. Produce a penetration test authorization and rules of engagement document.

c. Contrast penetration testing methodologies.

d. Derive system reconnaissance and network scan to detect open ports and vulnerable systems.

e. Elaborate social engineering techniques for a penetration test.

f. Compile penetration test scanning results to exploit vulnerabilities.

5. Instructional Facilities

Standard computer lab with one internet-connected workstation per student with appropriate software installed.

6. Special Materials Required of Student

Flash/USB drive or cloud storage for backup of in-class work.

# COMPUTER SCIENCE INFORMATION SYSTEMS 264 – ETHICAL CYBERSECURITY HACKING Page 2

7. Course Content

a. Footprinting and Reconnaissance

b. Scanning Networks

c. Enumeration

d. System hacking

e. Trojans and Backdoors

f. Viruses and Worms

g. Sniffing

h. Social engineering

i. Denial of Service

j. Session Hijacking

k. Hacking Webservers

l. Hacking Web Applications

m. SQL Injection

n. Hacking Wireless Networks

o. Hacking Mobile Platforms

p. Evading IDS, Firewall, and Honeypots

q. Buffer Overflow

r. Cryptography

s. Penetration Testing

8. Method of Instruction

a. Lecture and demonstration in a traditional classroom or via electronic means

b. Hands-on practice in either a dedicated or a virtual lab environment

c. Topical discussion of current operating system trends and issues

9. Methods of Evaluating Student Performance

a. Examinations including a final.

b. Skill demonstrations: securing a provided network

c. Classroom Discussion

d. Reports: students will be provided with specific scenarios relating to "real life" events that have taken place that relate to cyber security breaches and will be instructed to provide a limited written report relative to implementation of procedures and processes designed to combat future potential breaches. Instructor will evaluate the report based upon a rubric provided to students.

10. Outside of Class Assignments

a. Utilizing virtual machines configured with windows and windows server operating systems:

b. Configure specific computer security functions and/or subsystems.

c. Troubleshoot/analyze imposed security problems, investigate potential alternatives, and implement corrective action to achieve a determined result.

e. Read and analyze instructor assigned case studies; post analysis and comments to the class discussion board.

f. Respond to other students’ analysis and comments on the class discussion board.

11. Texts and References

a. Required (representative example)

Orivano, Sean-Philip. *Hacker Techniques, Tools, and Incident Handling.* 2nd Edition.Burlington, MA: Jones and Bartlett Learning, 2014.

b. Supplemental: None

# COMPUTER SCIENCE INFORMATION SYSTEMS 264 – ETHICAL CYBERSECURITY HACKING Page 3

Addendum: Student Learning Outcomes

Upon completion of this course, our students will be able to do the following:

a. Describe the legal and regulatory requirements for ethical hacking and prepare documentation to reflect this skill and prepare the necessary documentation for authorization, performance, results and recommendations based on penetration testing.

b. Compare and contrast different penetration testing methodologies and describe the correct circumstance to apply those methodologies.

c. Perform system scan and reconnaissance to determine vulnerabilities, then create a report showing vulnerabilities and recommendations for rectifying the cited weaknesses.

d. Demonstrate social engineering techniques to discover system vulnerabilities.

Date approved by the Governing Board: May 15, 2018