

PRINCE GEORGE'S COMMUNITY COLLEGE
OFFICE OF INSTRUCTION

MASTER COURSE SYLLABUS

CIS 269 Information Security Capstone	Michael Burt	12/19/2006
Course Designator and Title	Prepared by	Date
Barry W. Bugg	Dr. Aaron Stucker	
Department Chairman	Instructional Dean	Date

COURSE DESCRIPTION:

This capstone course in the Information Security A.A.S. Program should be taken near the end of the student's program of study. Students will be required to analyze, research, design, and develop a fully-document network attack strategy. Functioning in teams, students will design a strategy for attacking a fictitious network. The teams will defend their network attack strategy during class presentations.

EXPECTED COURSE OUTCOMES:

- *For proposed general education courses, indicate correlation with core learning outcomes by placing letter(s) of outcomes in parentheses next to course learning outcome. See document "General Education Core Learning Outcomes" for a lettered list. For example if course outcome 1 correlates with core learning outcome C, place (C) at the end of the outcome statement.*
- *For each course learning outcome, indicate briefly the planned assessment tools, such as cases, essay, multiple choice questions, etc.*
- *Course learning outcomes should be numbered for referral purposes.*

Upon successful completion of this course, the student will be able to:

Course Learning Outcomes (General Education correlation as applicable, see above note)	Planned Assessment Tools
1. Demonstrate the ability to conduct independent research.	documentation submission
2. Demonstrate the ability to work effectively as a team member.	oral presentation
3. Perform Risk Analysis	lab completion
4. Perform Information Systems Audit	lab completion
5. Perform Computer Security Checklist	documentation submission
6. Understand and use selected hacker tools	lab completion

7. Research hacker sites to find, explore and successfully use new hacker tools	documentation submission
8. Interpret the results of the various responses resulting from the attack.	documentation submission
9. Document and interpret network security findings.	documentation submission presentation
10. Demonstrate the ability to formulate and recommend countermeasures to the identified network weaknesses.	documentation submission
11. Organize, create, and present a presentation.	documentation submission presentation
12. Defend network attack strategy, tools and techniques	presentation

RANGE OF SUBJECT MATTER -- MODEL COURSE OUTLINE:

1. Introduction of independent research requirements.
2. Risk Analysis
3. Information Systems Audit
4. Computer Security Checklist
 - a. General information
 - b. Fire risk and water damage analysis
 - c. Air conditioning systems
 - d. Electrical systems
 - e. Natural disasters
 - f. Backup systems
 - g. Physical access control
 - h. System utilization and operation
 - i. Software and Hardware
 - j. File security
 - k. Data file standards
 - l. Shared Resource Systems Security
 - m. Information Systems Development
 - n. Systems Lifecycle Management
5. Hacker sites
6. Hacker tools
7. Attack results
8. Countermeasures
9. Team presentations and strategy defense
10. Additional Topics Discussed from Supplemental Text
 - a. OPSEC Process
 - b. OPSEC surveys/OPSEC planning
 - c. Unclassified Indicators
 - d. Application Guidance
 - e. Emanations Security
 - f. HUMINT
 - g. Telecommunications Systems, Telecommunications Policies and Security, Contacts and References, Vulnerabilities, Threats, and Counter Measures
 - h. Security Policies, Guidance, Contracts, and Roles
 - i. Security Policies - Budgeting, Valuation, and Training
 - j. System Life Cycle Processes, Certification and Accreditation
 - k. Software Security
 - l. Media Processes - Attribution, Destruction, Classification, Sanitization, Transportation, and Inventory
 - m. Incident Reporting
 - n. National Threats, Vulnerabilities, Countermeasures, Risk Management, and other facets of NSTISS

EVALUATION OF STUDENT PERFORMANCE:

Team Project - 50%

 Project Score - 25%

 Team Member Score - 25%

Quizzes - 20%

Final - 15%

Team Project Documentation - 15%

INSTRUCTIONAL MATERIALS:

Required: Textbook TBD