

PRINCE GEORGE'S COMMUNITY COLLEGE  
OFFICE OF INSTRUCTION

**MASTER COURSE SYLLABUS**

<u>CIS 162 Computer Security, Security+</u>	<u>Michael Burt</u>	<u>12/19/2006</u>
Course Designator and Title	Prepared by	Date
<u>Barry Bugg</u>	<u>Dr. Aaron Stucker</u>	
Department Chairman	Instructional Dean	Date

**COURSE DESCRIPTION:**

3 credits. This introduction to security systems will give students a solid foundation of understanding in different computer security concepts, functions and applications. The course maps to Comptia Security+ exam objectives which cover general security concepts, communication security, infrastructure security, basics of cryptography and operations/organizational security. Upon completion of this course, students will be prepared to take Comptia's vendor neutral Security+ exam. Security+ certification is globally recognized as equivalent to an entry-level security specialist. Security+ exam is accepted as one of the security certification exams by Microsoft toward its MCSA and MSCE certification. Prerequisite: CIS 140. 2 class/2 lab hrs.

**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. General computer and information security concepts	Multiple choice questions
2. OSI Model	Multiple choice questions
3. TCP three-way handshake, package capture and analysis	Lab
4. Malware	Lab and Multiple choice
5. Attackers method	Lab and Multiple choice

6. Security in remote access, email, web, wireless and instant messaging transmissions	Lab and Multiple choice
7. Security firewall, intrusion detection, security baselines for the Infrastructure	Lab and Multiple choice
8. Basic cryptography, Public Key Infrastructure, standards/protocols and applications	Lab and Multiple choice
9. Operational Security: Disaster Recovery Plan, Business Continuity Plan, and Organizational Policies	Multiple choice questions
10. Administrative Control: Security and Law, Privilege Management, Computer Forensics, risk management, and change management	Multiple choice questions

**RANGE OF SUBJECT MATTER -- MODEL COURSE OUTLINE:**

1. TCP/IP Concepts and OSI Model
  - a. Analyze TCP Three-way handshake
  - b. IP private address space
  - c. Domain Name Space security
  - d. Analyze IP, TCP, UDP and ICMP package format
  - e. Capture and analyze network traffic
  - f. Review and compare OSI model to DoD IP model
  - g. Analyze Kevin Mitnick versus T. Shimomura
2. General Security Concepts
  - a. Study security principles
  - b. Defense-in-depth (layered defense or onion defense)
  - c. Study diversity of defense
  - d. Study host counter-measures – lock-down and securing open ports
  - e. Confidentiality, Integrity and Availability (CIA) security model
  - f. Operation security model
  - g. Risk security model
  - h. Privilege security model and Access control model
    - Users, groups and roles
    - Discretionary access control (DAC)
    - Mandatory access control (MAC)
    - Role-based access control (RBAC)
    - Rule-based or List-based access control
    - Study least privilege, need to know and separation of duties principles
  - i. Identification, Authentication and Authorization (IAA) security
  - j. Authentication, Authorization and Accounting (AAA) security
  - k. Logging and Auditing
3. Malware and Attacks
  - a. Study attacker's method and types
  - b. Study types of attacks

- DoS, DDos, backdoor, trap door, MitM, replay, session hijack,
  - Inference, salami, fragmentation, chargen, sniffing
  - Spoofing: email, IP@, Web, Phishing, DNS, ARP
  - Mathematical, encryption, birthday, password attack, buffer overflow,
  - Social engineering, dumpster diving, war driving, war dialing, war chalking
- c. Study defense against DoS, DDoS, securing network, eMail and Web applications
  - d. Virus, worm, Trojan, logic bomb, spyware, adware
4. Study tools such as ping, trace route, port scanners, traffic sniffers, MAC spoofing, TCP injection, steganography, password crackers, baseline analyzer, intrusion detection, firewalls...
  5. Authentication
    - a. Identification and password
    - b. Multi-factor authentication
    - c. OTP, biometrics and tokens
    - d. PAP, CHAP, MS-PAP, LANMAN, Radius, Diameter, and Kerberos
  6. Communications Security
    - a. Telnet and SSH
    - b. VPN: L2TP, PPTP, and split VPN tunnel
    - c. IPSEC: AH and ESP protocols, transport and tunnel mode
    - d. Key exchange protocol: ISAKMP, Oakley, SKEMI
    - e. Wireless
      - WEP, WTLS, WAP gap, EAP, LEAP WTLS
      - 802.11: (a, b, and g), DSSS, FHSS and OFDM
    - f. Discuss instant messaging
    - g. Discuss securing transmission media
  7. Email Security
    - a. SMTP, POP3, IMAP4 and Secured mail protocols
    - b. S/MIME and PGP
  8. Web Security
    - a. HTTP, S-HTTP, HTTPS and FTP
    - b. SSL and TLS
    - c. CGI, Active-X, Java, JavaScript, VBScript, and HTA
    - d. Applets, cookies, plug-ins
  9. Infrastructure security
    - a. Study physical network topologies
    - b. Study logical network topologies and VLAN
    - c. Study network hubs, bridges, switches, routers and firewalls
    - d. Study desktops, servers and laptops defense
    - e. Study types of firewalls
    - f. Examine wireless, PBX, Windows telephony, microware and radio frequency

10. Study intrusion detection, intrusion prevention systems and security baselines
11. Cryptography
  - a. Exploits and attacks on cryptography
  - b. Symmetric cryptography such as DES, 3DES, AES, and Blowfish
  - c. Asymmetric cryptography such as Diffie-Hellman, Elliptic curve, and RSA
  - d. SSL six-way hand-shake
  - e. Cryptology and Encryption-based solutions
12. Public Key Infrastructure (PKI)
  - a. Study PKI Standards and Protocols, X.509 digital certificate
  - b. Certificate management and certificate enrollment protocols
  - c. Study cryptographic message syntax (CMS) and discuss XML key management
13. Look at standards
  - a. Federal Information Processing Standards (FIPS)
  - b. Common Criteria
  - c. ISO 17799
  - d. Legal, Ethical, and Professional Issues in Information Systems
14. Study physical security
  - a. Physical Controls
  - b. Technical Controls
  - c. Interception of Data
  - d. Special Considerations for Physical Security Threats
15. Forensics
  - a. Study computer forensic methodology
  - b. Study rules of evidence
16. Management
  - a. Study disaster recovery, business continuity and organizational policies
  - b. Study policies, procedures, standard and guidelines
  - c. Centralized and decentralized
  - d. Incident response process
  - e. Risk management and tools
  - f. Software change management
  - g. Data backup and recover
  - h. Security and Personnel

**EVALUATION OF STUDENT PERFORMANCE:**

Test 1	30%
Test 2	30%
Final Exam	30%
Lab Assignments	10%
Total	100%

**INSTRUCTIONAL MATERIALS:**

All-in-One Security+ Certification – Gregory White – McGraw Hill/Osborne