

**COURSE OUTLINE  
ANNE ARUNDEL COMMUNITY COLLEGE  
ARNOLD, MARYLAND**

COURSE NAME: Network Security Fundamentals  
 COURSE NUMBER: CSI 165  
 CREDIT HOURS: 3 Credit hours  
 INITIATOR: Paul Derdul  
 SCHOOL: School of Business, Computing and Technical Studies  
 DEPARTMENT: Computer Information Systems  
 DATE: March 18, 2004 (revised September 2009)

**CATALOG DESCRIPTION**

CSI 165  
 Network Security Fundamentals  
 3 credit hours – Three hours weekly; one semester  
 Offers in-depth coverage of the current risks and threats to an organization’s data together with a structured way of addressing the safeguarding of these critical electronic assets. The course provides a foundation for those responsible for protecting network services, devices, traffic and data. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. It is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association’s (CompTIA) Security + Certification exam. Lab fee \$100.  
 Prerequisite: CSI 157 or CSI 260.  
 Note: CSI 157 and CSI 260 may be taken concurrently with CSI 165 with permission of the computer technologies director. This course is equivalent to CyberWatch course CW 160.

**LEARNING OBJECTIVES**

- At the conclusion of this course the student will be able to:
- Identify security threats to network services, devices, traffic and data
  - Harden internal systems and services
  - Harden inter-network devices and services
  - Secure network communications
  - Manage a PKI
  - Manage certificates
  - Enforce an organizational security policy
  - Monitor the security infrastructure
  - Identify the characteristics of various media

**DIVISION OF SUBJECT MATTER**

<u>Main Topic</u>	<u>Lecture Hours</u>
1. Overview of Security Law	3.0
2. Security Overview	2.0
3. Authentication	3.0
4. Attacks and Malicious Code	3.0
5. Remote Access	3.0
6. E-mail	3.0
7. Web Security	3.0
8. Directory and File Transfer Services	3.0
9. Wireless and Instant Messaging	3.0
10. Devices	3.0
11. Media and Medium	2.0
12. Network Security Topologies	3.0
13. Intrusion Detection	3.0
14. Cryptography	3.0
15. Physical Security	2.0
16. Testing	3.0
<b>Total</b>	<b>45.0</b>

## DETAILED COURSE OUTLINE

<u>Main Topic</u>	<u>Lecture Hours</u>
1. Overview of Security Law	3.0
1.1 Business Law Considerations	
1.2 Criminal Law Considerations	
2. Security Overview	2.0
2.1. Security Threats	
2.2. Security Ramifications: Costs of Intrusion	
2.3. Goals of network Security	
2.4. Creating a Secure Network Strategy	
3. Authentication	3.0
3.1. Kerberos	
3.2. Challenge Handshake Authentication Protocol	
3.3. Mutual Authentication	
3.4. Digital Certificates	
3.5. Security Tokens	
3.6. Biometrics	
3.7. Multi-Factor Authentication	
4. Attacks and Malicious Code	3.0
4.1. Denial-of-Service Attacks	
4.2. IP Fragmentation Attack: Ping of Death	
4.3. Distributed Denial-of-Service Attacks	
4.4. Spoofing	
4.5. Man in the middle	
4.6. Replays	
4.7. TCP Session Hijacking	
4.8. Social Engineering	
4.9. Attacks Against Encrypted Data	
4.10. Software Exploitation	
5. Remote Access	3.0
5.1. IEEE 802.1x	
5.2. Virtual Private Networks	
5.3. RADIUS	
5.4. TACACS	
5.5. PPTP	
5.6. L2TP	
5.7. IPSec	
5.8. Telecommuting Vulnerabilities	
6. E-mail	3.0
6.1. Secure E-mail Encryption	
6.2. How Secure E-mail Works	
6.3. E-mail Vulnerabilities	
6.4. Spam	
6.5. Hoaxes and Chain Letters	
7. Web Security	3.0
7.1. SSL and TLS	
7.2. HTTPS	
7.3. Instant Messaging	
7.4. Vulnerabilities of Web Tools	
8. Directory and File Transfer Services	3.0
8.1. Directory Services	
8.2. File Transfer Services	
8.3. Secure File Transfers	
8.4. File Sharing	
9. Wireless and Instant Messaging	3.0
9.1. The Alphabet Soup of 802.11	
9.2. WAP1.x and WAP 2.0	

9.3. Wired Equivalent Privacy	
9.4. Conducting a Wireless Site Survey	
9.5. Instant Messaging	
10. Devices	3.0
10.1. Firewalls	
10.2. Routers	
10.3. Switches	
10.4. Wireless	
10.5. Modems	
10.6. RAS	
10.7. Telecom/PBX	
10.8. VPN	
10.9. Workstations and Servers	
10.10. Mobile Devices	
11. Media and Medium	2.0
11.1. Transmission Media	
11.2. Securing Transmission Media	
11.3. Storage Media	
11.4. Catastrophic Loss	
11.5. Encryption	
11.6. Storing and Destruction of Media	
12. Network Security Topologies	3.0
12.1. Perimeter Security Topologies	
12.2. DMZ	
12.3. NAT	
12.4. Tunneling	
12.5. VLANs	
13. Intrusion Detection	3.0
13.1. The Value of Intrusion Detection	
13.2. Network-based and Host-based IDS	
13.3. Active Detection and Passive Detection	
13.4. Honeypots	
13.5. Incident Response	
14. Cryptography	3.0
14.1. Algorithms	
14.2. Symmetric versus Asymmetric Algorithms	
14.3. Concepts of using Cryptography	
14.4. Certificates	
14.5. Key and Certificate Life Cycle Management	
15. Physical Security	2.0
15.1. Physical Controls	
15.2. Technical Controls	
16. Testing	3.0
<b>Total</b>	<b>45.0</b>

### TEXTBOOK

Title: Security + Guide to Network Security Fundamentals  
 Author: Paul Campbell, Ben Calvert, Steven Boswell  
 Publisher: Thomson Course Technology  
 Date: 2003 Cisco Learning Institute