Course Prefix and Number: CIT 115

Course Title: Network Defense

Course Prerequisite: None.


Course Description: This course provides students with a foundation in network security fundamentals. The course focuses on how to develop effective security strategies, including basic principles of encryption. This course is required toward the CNSS 4011-4016 certifications.

Learning Outcomes:
At the end of this course, the student will:
   A. perform risk analysis and create security policies;
   B. demonstrate how to secure Internet and Websites; and
   C. demonstrate how to secure Windows Server 2003.

To achieve the learning outcomes, the student will or will be able to:
(The letter designations at the end of each statement refer to the learning outcome(s).)
1. recognize risk analysis factors and methods and outline the process of conducting a risk analysis (A);
2. use techniques for minimizing risks (A);
3. create a security policy for organizations and outline the seven main steps of policy development (A);
4. explain the overview of handling security incidents and the basics of security policy life cycle management (A);
5. recognize the main methods of network reconnaissance that attackers use (B);
6. identify the components of a packet capture and how to analyze normal and abnormal network traffic signatures (B);
7. discuss cryptography and the components of cryptographic protocols (B);
8. examine attacks against websites and internet users, and identify techniques and tools for hardening internet and web resources (B);
9. identify the security related components of a Windows Server network (C);
10. recognize Windows Server authentication, auditing, and logging (C);
11. secure a Windows Server network (C);
12. recognize the INFOSEC security basics overview including: critical information characteristics – availability, critical information characteristics – confidentiality, critical information characteristics – integrity, information states – processing, information states – storage, information states – transmission, security...
countermeasures - education, training and awareness, security countermeasures - policy, procedures, and practices, threats and vulnerabilities (A);

13. recognize the security basics of information security including: application dependent guidance, policy, and roles and responsibilities (A);

14. recognize the INFOSEC security basics including: computer security - access control, cryptography - encryption (e.g., point-to-point, network, link), cryptography - key management (to include electronic key), cryptography - strength (e.g., complexity, secrecy, characteristics of the key), emanations security, physical, personnel and administrative security and transmission security (B);

15. memorize the NSTISS basics national policy and guidance including: AIS Security, communications security, employee accountability for agency information and protection of information (B);

16. identify NSTISS basic threats to vulnerabilities of systems including: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring) and threat impact areas (A, B);

17. explain NSTISS basic concepts of risk management including consequences (e.g., corrective action, risk management and cost/benefit analysis of controls) (CNSS 4011);

18. recognize the NSTISS basic agency specific security policies including: guidance, points of contact and roles and responsibilities (A);

19. recognize NSTISS basic agency specific AIS and telecommunications policies including: points of contact and references (A);

20. recognize NSTISS Planning and Management systems life cycle management including systems certification and accreditation process (B);

21. identify NSTISS Planning and Management contingency planning/ disaster recovery including: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for off-site processing, emergency destruction procedures, guidelines for determining critical and essential workload and team member responsibilities in responding to an emergency situation (A,B);

22. explain NSTISS Policies and Procedures personnel security practices and procedures including: access authorization/verification (need to know), contractors, employee clearances, position sensitivity, security training and awareness and systems maintenance personnel (A);

23. recognize NSTISS Policies and Procedures auditing and monitoring including: conducting security reviews, effectiveness of security programs, investigation of security breaches, monitoring systems for accuracy and abnormalities, privacy review of accountability controls, review of audit trails and logs, review of software design standards and verification, validation, testing, and evaluation processes (C);

24. recognize NSTISS Policies and Procedures crypto security including: crypto variable or key, electronic key management system and encryption/decryption method, procedure, algorithm (C); and
25. recognize the purpose and contents of Approval to Operate (ATO) and the risk assessment to support granting an ATO (A).

**Course Requirements:**
1. A student must successfully complete the course with an average of 70% or above on the combined learning outcomes.
2. Each student is expected to attend classes regularly; excessive unexcused absences constitute grounds for suspension (refer to the student handbook for attendance policies).

**Course Grading Scale:**
- 90 – 100 = A
- 80 – 89 = B
- 70 – 79 = C
- 60 – 69 = D
- 0 – 59 = F

**Attendance Policy:** The college attendance policy is available at http://www.bpcc.edu/catalog/current/academicpolicies.html

**Course Fees:** This course is accompanied with an additional fee for supplemental materials.

**Nondiscrimination Statement:** Bossier Parish Community College does not discriminate on the basis of race, color, national origin, gender, age, religion, qualified disability, marital status, veteran's status, or sexual orientation in admission to its programs, services, or activities, in access to them, in treatment of individuals, or in any aspect of its operations. Bossier Parish Community College does not discriminate in its hiring or employment practices.

Title VI, Section 504, and ADA Coordinator  
Sarah Culpepper, Coordinator  
Disability Services, D-110  
6220 East Texas Street  
Bossier City, LA 71111  
Phone: 318-678-6539  
Email: sculpepper@bpcc.edu  
Hours: 8:00 a.m.-4:30 p.m. Monday - Friday, excluding holidays and weekends.

Equity/Compliance Coordinator  
Teri Bashara, Director of Human Resources  
Human Resources Office, A-105  
6220 East Texas Street  
Bossier City, LA 71111  
Phone: 318-678-6056  
Hours: 8:00 a.m.-4:30 p.m. Monday - Friday, excluding holidays and weekends.