

PRINCE GEORGE'S COMMUNITY COLLEGE
OFFICE OF INSTRUCTION

MASTER COURSE SYLLABUS

<u>CIS 166 Network Defense and Countermeasures</u>	<u>Michael E. Burt</u>	<u>06/23/09</u>
Course Designator and Title	Prepared by	Date
<u>Sally Sullivan</u>	<u>06/24/09</u>	<u>Louis Renaud</u>
Department Chairman	Date	Instructional Dean
		Date

COURSE DESCRIPTION:

3 credits. This course focuses on the understanding of the network security architecture. The course covers network attacks and defenses, firewall systems, network design and configuration, Virtual Personal Networks (VPN) configuration, Intrusion Detection System (IDS) design and configuration, intrusion signatures, and network security policies and configurations.
Prerequisite: CIS 163. 2 class/2 lab hours.

EXPECTED COURSE OUTCOMES:

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

<i>No.</i>	<i>Course Learning Outcomes</i>	<i>Planned Assessment Tools</i>
1	Examine network defenses.	Multiple Choice/True or False Questions
2	Identify the objectives of Access Control.	Multiple Choice & True or False Questions
3	Define the concepts of network auditing.	Multiple Choice & True or False Questions
4	Design and create a firewall policy.	Multiple Choice & True or False Questions
5	Create rule sets and packet filters.	Multiple Choice & True or False Questions
6	Install, configure and monitor a firewall.	Lab / Multiple Choice & True or False Questions
7	Summarize VPN fundamentals.	Multiple Choice & True or False Questions
8	Analyze IP Security Protocol - IPsec.	Lab / Multiple Choice & True or False Questions
9	Configure a VPN connection.	Lab / Multiple Choice & True or False Questions
10	Explain Host based IDS.	Multiple Choice & True or False Questions
11	Explain Network based IDS.	Essay, Multiple Choice, & True or False Questions
12	Configure an IDS.	Lab / Multiple Choice & True or False Questions
13	Interpret the concepts of Signature Analysis.	Lab / Multiple Choice & True or False Questions
14	Explain Traffic Signatures.	Multiple Choice & True or False Questions
15	Explain Abnormal Traffic Signatures.	Multiple Choice & True or False Questions
16	Describe the concepts of risk analysis.	Multiple Choice & True or False Questions
17	Identify the methods of risk analysis.	Multiple Choice & True or False Questions
18	Demonstrate the techniques to minimize risk.	Lab / Multiple Choice & True or False Questions
19	Describe the concepts of security policies.	Essay, Multiple Choice, & True or False Questions
20	Enumerate sample security policies.	Multiple Choice & True or False Questions
21	Explain incident handling & escalation procedures.	Essay, Multiple Choice, & True or False Questions

RANGE OF SUBJECT MATTER -- MODEL COURSE OUTLINE:

1. Network Defense Fundamentals
 - a) Describe network defense
 - b) Identify defensive technologies
 - c) Describe the objectives of Access Control
 - d) Identify the impact of defense
 - e) Define the concepts of network auditing
2. Designing Firewall Systems
 - a) Examine firewall components
 - b) Create a firewall policy
 - c) Rule sets and packet filters
 - d) Proxy servers
 - e) The bastion host
 - f) The honeypot
3. Configuring Firewall
 - a) Firewall implementation practices
 - b) Installing, configuring, and monitoring Firewall-1
 - c) Installing, configuring, and monitoring ISA Server
 - d) IP Chains concepts
 - e) Implementing firewall technologies
4. Configuring VPNs
 - a) VPN fundamentals
 - b) IP Security Protocol (IPSec)
 - c) VPN design and architecture
 - d) VPN security
 - e) Configuring a VPN
5. Designing an IDS
 - a) Goals of an IDS
 - b) Technologies and techniques of intrusion detection
 - c) Host-based IDS
 - d) How to use an IDS
 - e) What an IDS cannot do
6. Configuring an IDS
 - a) Snort foundations
 - b) IDS center
 - c) Configuring ISS Scanners
7. Analyzing Intrusion Signatures
 - a) Describe the concepts of signature analysis
 - b) Common vulnerabilities and exposures (CVE)
 - c) Signatures
 - d) Normal traffic signatures
 - e) Abnormal traffic signatures

8. Performing a Risk Analysis
 - a) Concepts of risk analysis
 - b) Methods of risk analysis
 - c) The process of risk analysis
 - d) Technique to minimize risk
 - e) Continual risk analysis
9. Creating A Security Policy
 - a) Concepts of security policies
 - b) The policy design
 - c) The policies
 - d) A sample policy
 - e) Incident handling and escalation procedures
 - f) Partner policies

EVALUATION OF STUDENT PERFORMANCE:

Test 1	= 15%
Test 2	= 15%
Test 3	= 15%
Lab Assignments/Quizzes/Writing Assignments	= 30%
Attendance/Class Participation	= 10%
Final Exam	= 15%
Total	= 100%

INSTRUCTIONAL MATERIALS:

Check with CIS department