

**OAKTON COMMUNITY COLLEGE
GENERIC COURSE SYLLABUS**

I.	<u>COURSE PREFIX</u>	<u>COURSE NUMBER</u>	<u>COURSE NAME</u>	<u>CREDIT</u>	<u>LECTURE</u>	<u>LAB</u>
	CNS	172	Network Defense and Countermeasures	3	3	1
	(Formerly LAN 184)					

II. PREREQUISITE:

CNS 111 (Formerly LAN 111); or LAN 171 or consent of instructor, coordinator or program chair.

III. COURSE (CATALOG) DESCRIPTION:

This course provides students with the knowledge and concepts needed for protecting computers and networks. The course covers intrusion detection, develop a security policy, implement Network Address Translation (NAT) and packet filtering by installing proxy servers, firewalls, and virtual private network (VPNs). The course also assists students in preparation for the appropriate Network or Information Security Certification examinations.

IV. LEARNING OBJECTIVES:

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

1. The individuals who might attempt to break into your network
2. Set goals for developing a network security system
3. Aspects of Internet-based Communications that present Security Risks
4. Covert Channeling and other common Attack Threats you need to defend against
5. Integrate an Intrusion Detection System (IDS) into a Network Security configuration
6. The Basics Concepts of Risk Analysis
7. What makes an Effective Security Policy
8. List the requirements for steps involved in setting up a Bastion Host
9. Design common Firewall Configurations
10. How to Choose the right Product for your Organization's need
11. How to Create different Packet Filter Rules for Real-world situations
12. How to Set up Network Address Translation (NAT)
13. How to work with a Proxy Server to supplement a Firewall with a Proxy Server
14. How to Install and Configure Microsoft ISA Server 2000
15. The Tunneling Protocols that Enable Secure VPN Connections
16. The encryption Schemes used by VPNs
17. Options for configuring intrusion detection systems
18. The issues involved in choosing an intrusion detection system
19. The benefits of the Common Vulnerabilities and Exposures (CVE) Standard
20. Why Logging Network Traffic is an Integral Part of Intrusion Detection
21. How to Respond for False Alarms to Reduce Reoccurrences
22. Options for Dealing with Legitimate Security Alerts

V. **ACADEMIC INTEGRITY:**

Students and employees at Oakton Community College are required to demonstrate academic integrity and follow Oakton's Code of Academic Conduct. This code prohibits:

- cheating
- plagiarism (turning in work not written by you, or lacking proper citation)
- falsification and fabrication (lying or distorting the truth)
- helping others to cheat
- unauthorized changes on official documents
- pretending to be someone else or having someone else pretend to be you
- making or accepting bribes, special favors, or threats, and
- any other behavior that violates academic integrity.

There are serious consequences to violations of the academic integrity policy. Oakton's policies and procedures provide students a fair hearing if a complaint is made against you. If you are found to have violated the policy, the minimum penalty is failure on the assignment and, a disciplinary record will be established and kept on file in the office of the Vice President for Student Affairs for a period of 3 years.

Details of the Code of Academic Conduct can be found in the Student Handbook.

VI. **OUTLINE OF TOPICS:**

1. Foundations of Network Security
2. Designing a Network Defense
3. Risk Analysis and Security Policy Design
4. Choosing and Designing Firewalls
5. Configuring Firewalls
6. Strengthening and Managing Firewalls
7. Setting up a Virtual Private Network
8. Intrusion Detection: An Overview
9. Intrusion Detection: Preventive Measures
10. Intrusion Detection: Incident Response
11. Strengthening Defense through Ongoing Management

VII. **METHODS OF INSTRUCTION:**

Methods include lectures, class exercises and class discussion, perform lab exercise and projects.

VIII. **COURSE PRACTICES REQUIRED:**

- Read course materials - textbook and current journals
- Attend and participate in class lecture and lab
- Complete required assignments, exercises, quizzes, and exams

IX. INSTRUCTIONAL MATERIALS:

- Textbook and Lab book: Guide to Network Defense And Countermeasures, Thomson Course Technology
- Current Self-Test Software
- Software manuals

X. METHODS OF EVALUATING STUDENT PROGRESS:

Quizzes, examinations, completion of lab assignments, exercises, and LAN project

XI. OTHER COURSE INFORMATION:

If you have a documented learning, psychological, or physical disability you may be entitled to reasonable academic accommodations or services. To request accommodations or services, contact the ASSIST office in the Learning Center. All students are expected to fulfill essential course requirements. The College will not waive any essential skill or requirement of a course or degree program.