SAULT COLLEGE OF APPLIED ARTS AND TECHNOLOGY

SAULT STE. MARIE, ONTARIO

Sault College

COURSE OUTLINE

COURSE TITLE: NETWORK SECURITY

CODE NO. : CSN208 **SEMESTER:** 4

PROGRAM: COMPUTER NETWORK TECHNICIAN /TECHNOLOGY

AUTHOR: MARK ALLEMANG

DATE: JAN, 2005 **PREVIOUS OUTLINE DATED:** JAN, 2004

APPROVED:

_____ _____

DEAN **DATE**

TOTAL CREDITS: 5

PREREQUISITE(S): CSN120

HOURS/WEEK: 4

I. COURSE DESCRIPTION:

This course provides an in-depth study of network security issues, standards, best practices and current threats. Supported by extensive lab work, system vulnerabilities will be investigated and solutions implemented using a variety of operating systems and security tools.

II. LEARNING OUTCOMES AND ELEMENTS OF THE PERFORMANCE:

Upon successful completion of this course the student will demonstrate the ability to:

1. Understand network security principles and develop strategies for dealing with common network vulnerabilities and security issues.

Potential Elements of the Performance:

- Understand the need for network security and the tradeoffs associated with implementing security.
- Practice ethical behaviour as a network administrator.
- Identify legal issues associated with network administration and implement a security policy for network users to follow.
- Identify general security issues associated with LANs, WANs, Web Servers, VPNs and Remote Access.
- Identify and defend systems against the major types and categories of security threats.
- Implement virus protection and recovery practices on a network.
- Implement security policies and practices that lead to secure networks.

This learning outcome will constitute approximately 20% of the course.
Reference: (Chap 1 and 3) and other notes supplied.

2. Deploy firewalls to secure a network

Elements of the Performance:

- Compare different types of firewalls with respect to their principles of operation, their strengths and weaknesses.
- Specify and configure various firewall products to meet particular network requirements.
- Evaluate and compare various commercial firewalls.

This learning outcome will constitute approximately 15% of the course.
Reference: (Chap. 5)

3. Establish security practices to enable local and remote users to connect securely to internal networks.

Elements of the Performance:

- Compare dial-in networking services (RAS), VPNs and other Internet services with respect to their operation and security issues.
- Implement RAS or VPNs enabling secure remote access.
- Implement authentication and password policies that are appropriate for particular situations.

This learning outcome will constitute approximately 15% of the course.
Reference: (Chap. 7)

4. Analyze network requirements and plan security based on those requirements

Elements of the Performance:

- Analyze security requirements and be able to specify services, operating systems, and protocols appropriately.
- Identify the steps required to secure your network servers.
- Identify typical methods of securing network services including web and email
- Identify security issues and then implement appropriate security on Windows NT and Windows 2000 servers.
- Identify security issues and then implement appropriate security on Unix systems
- Implement security for workstations and common desktops.

This learning outcome will constitute approximately 25% of the course.
Reference: (Chap 4-6)

5. Develop Intrusion Detection and Response best practices.

Elements of the Performance:

- Describe the various types of intrusion detection systems.
- Compare commercial intrusion detection systems and implement one.
- Develop a security plan and an intrusion response procedure for situations where a site has been attacked.
- Investigate real case studies of network attacks, intrusion detection and recovery.

This learning outcome will constitute approximately 10% of the course.

Reference: (Chap 12)

6. Specify and implement appropriate tools, utilities and practices to prevent/recover from security attacks/intrusions.

Elements of the Performance:

- Use Internet resources to research current security threats and acquire needed software and security patches.
- Use various utilities such as network monitors, packet sniffers, security scanners, intrusion detection systems, password detectors, auditing and integrity checking to protect servers and network resources.

This learning outcome will constitute approximately 15% of the course.
Reference: Chapt 10,11.

III. TOPICS TO BE COVERED:

1. Security Fundamentals and Common Vulnerabilities
2. Firewalls
3. Server and Workstation Security
4. Security Planning and Policies
5. Intrusion Detection and Response
6. Security Tools and Best Practices

IV. REQUIRED STUDENT RESOURCES/TEXTS:

TEXT BOOK: "Security + Guide to Network Security Fundamentals Second Edition" by Ciampa. Thomson Course Technology (2005) ISBN 0-619-21566-6

V. EVALUATION PROCESS/GRADING SYSTEM:

3 WRITTEN TESTS	60%
LAB ASSIGNMENTS and QUIZZES	40%

(The percentages shown above may vary slightly if circumstances warrant.)

NOTE: ***It is necessary to pass both the theory and the lab parts of this course.*** *It is not possible to pass the course if a student has a failing average in the three written tests but is passing the lab portion (or vice versa).*

The following semester grades will be assigned to students in postsecondary courses:

Grade	*Definition*	*Grade Point Equivalent*
A+	90 – 100%	4.00
A	80 – 89%	
B	70 - 79%	3.00
C	60 - 69%	2.00
D	50 – 59%	1.00
F (Fail)	49% and below	0.00

CR (Credit)	Credit for diploma requirements has been awarded.
S	Satisfactory achievement in field /clinical placement or non-graded subject area.
U	Unsatisfactory achievement in field/clinical placement or non-graded subject area.
X	A temporary grade limited to situations with extenuating circumstances giving a student additional time to complete the requirements for a course.
NR	Grade not reported to Registrar's office.
W	Student has withdrawn from the course without academic penalty.

VI. SPECIAL NOTES:

Special Needs:
If you are a student with special needs (e.g. physical limitations, visual impairments, hearing impairments, or learning disabilities), you are encouraged to discuss required accommodations with your professor and/or the Special Needs office. Visit Room E1101 or call Extension 493 so that support services can be arranged for you.

Retention of Course Outlines:
It is the responsibility of the student to retain all course outlines for possible future use in acquiring advanced standing at other postsecondary institutions.

Plagiarism:
Students should refer to the definition of "academic dishonesty" in *Student Rights and Responsibilities*. Students who engage in "academic dishonesty" will receive an automatic failure for that submission and/or such other penalty, up to and including expulsion from the course/program, as may be decided by the professor/dean. In order to protect students from inadvertent plagiarism, to protect the copyright of the material referenced, and to credit the author of the material, it is the policy of the department to employ a documentation format for referencing source material.

Course Outline Amendments:
The professor reserves the right to change the information contained in this course outline depending on the needs of the learner and the availability of resources.

Substitute course information is available in the Registrar's office.

VII. PRIOR LEARNING ASSESSMENT:

Students who wish to apply for advanced credit in the course should consult the professor. Credit for prior learning will be given upon successful completion of a challenge exam or portfolio.

VIII. DIRECT CREDIT TRANSFERS:

Students who wish to apply for direct credit transfer (advanced standing) should obtain a direct credit transfer form from the Dean's secretary. Students will be required to provide a transcript and course outline related to the course in question.