SAULT COLLEGE OF APPLIED ARTS AND TECHNOLOGY

SAULT STE. MARIE, ONTARIO

COURSE OUTLINE

COURSE TITLE: Network Security

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

PROGRAM: Computer Network Technician /Technology

AUTHOR: Mark Allemang

DATE: Jan, 2012   **PREVIOUS OUTLINE DATED:**   Jan, 2011

APPROVED: "Brian Punch"   Jan/11

_____   _____
                                    CHAIR   **DATE**

TOTAL CREDITS: 5

PREREQUISITE(S):   CSN120

HOURS/WEEK: 4

Network Security   CSN208
COURSE NAME   *CODE NO.*

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.

2.   Deploy firewalls and other network defenses 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.
- Given the security policy requirement, produce the firewall rules in order to satisfy that requirement
- Compare and contrast other network defenses

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

Elements of the Performance:
- Compare various remote access services RAS, VPNs with respect to their operation and security issues.
- Compare and contrast the various wireless security mechanisms.
- Implement authentication and password policies that are appropriate for particular situations.

4. Analyze network requirements, perform risk assessment and plan security based on those requirements

Elements of the Performance:
- Define risk and risk management
- 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 and Unix servers.
- Implement security for workstations and common desktops.

5. Perform Vunerability Assessment, Develop Intrusion Detection and Response best practices in order to mitigate risk.

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.

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.
- Define the techniques and safeguards to ensure business continuity in the event of a disaster.
- 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.

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, 3rd edition, by Mark Ciampa   Published by Course Technology. ISBN:-13   978-1-4283-4066-4

V.   EVALUATION PROCESS/GRADING SYSTEM:

Tests and Quizes   60%
Labs and Assignments   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 quizzes and tests but is passing the lab portion (or vice versa).*

The professor reserves the right to adjust the mark up or down 5% based on

> attendance, participation, leadership, creativity and whether there is an
> improving trend.
>
> A minimum of **80% attendance** required in the labs and lectures.

- Late hand in penalties will be 10% per day. Assignments will not be accepted
  past one week late unless there are extenuating and legitimate circumstances.
- Makeup Tests are at the discretion of the instructor and will be assigned a
  maximum grade of 50%.
- The professor reserves the right to adjust the number of tests, practical tests and
  quizzes based on unforeseen circumstances. The students will be given sufficient
  notice to any changes and the reasons thereof.

NOTE: If action is to be taken, it will range from marks being deducted to a maximum
of removal from the course.

> 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.

Network Security   CSN208
COURSE NAME   *CODE NO.*

VI.   SPECIAL NOTES:

Attendance:
Sault College is committed to student success. There is a direct correlation between academic performance and class attendance; therefore, for the benefit of all its constituents, all students are encouraged to attend all of their scheduled learning and evaluation sessions. This implies arriving on time and remaining for the duration of the scheduled session.

VII.   COURSE OUTLINE ADDENDUM:

The provisions contained in the addendum located on the portal form part of this course outline.