

I. COURSE DESCRIPTION:

This course provides an in-depth study of network security policy, design, analysis, and implementation of security systems and critically evaluates their performance. This is an advanced security course and a continuation of CSN208. Areas of study include 802.1x access control, advanced wireless security, secured Web servers, and secured email servers. It includes the study of effective strategies for data collection, data preservation, data analysis and reporting of forensic computing investigations. The theory is supported by extensive lab work 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. **Advanced Network Security**

Potential Elements of the Performance:

- Identify the role of and describe the types of Network Security Policies
- Plan and implement Network Policies for Client logins including Virtual Private Networks (VPN's)
- Install and configure advanced Wireless Security including WPA and WPA2 configurations
- Authenticate Wireless users with protocols such as 802.1x, Radius, EAP and PEAP and EAE SIM
- Encrypt Wireless traffic using IPsec

2. **Secure Web and Email Servers**

Potential Elements of the Performance:

- Configure user authentication using Integrated Windows Authentication, Digest Authentication and .NET Passport authentication
- Install and configure a Certificate Server for your Web Server and implement SSL on your Web Server
- Configure URL authentication

3. **Computer Forensics Environment and Tools**

Potential Elements of the Performance:

- Define the role of Computer Forensics including its history
- Define the role of a Computer Forensics Investigator
- Review Computer Forensics Certifications and Training
- Demonstrate knowledge of Computer Crime scenes and situations
- Define the requirements of a Computer Forensics lab
- Review Computer Forensics lab certifications
- Budget plan for a Computer Forensics lab
- Identify duties of laboratory manager and staff
- Demonstrate the use of various Forensics software tools

4. **Data Acquisition, Analysis and Validation**

Potential Elements of the Performance:

- Demonstrate knowledge of correct procedures to follow in Data Acquisition
- Take a systematic approach to Acquisition, Analysis and Validation
- Contrast the difference between Data Recovery and Computer Forensics
- Determine proprietary formats
- Implement contingency plans for Image Acquisition
- Manage a Data Acquisition situation
- Use Data Acquisition tools
- Compare digital camera formats
- Contrast Bitmap, Raster and Vector images
- Contrast Lossless and Lossy compression
- Recover graphic files
- Repair damaged headers
- Reconstruct file fragments

5. **Investigating Crime and Incident Scenes**

Potential Elements of the Performance:

- Demonstrate professional conduct as a computer investigator
- Learn the rules of evidence
- Demonstrate knowledge of the various types of computer investigations including employee termination, Attorney-Client, Media leak and Industrial espionage
- Secure the scene
- Gather the evidence
- Plan an investigation
- Determine who is in charge
- Determine the tools you will require for the job
- Prepare the Investigating team

- Research background information to the crime scene
- Document findings
- Define the processing of Law Enforcement Crime Scenes
- Investigate E-Mail criminal Incidents
- Explore the roles of Client and Server in E-Mail Investigations
- Example E-Mail messages
- View E-Mail headers
- Review and examine E-mail logs
- Use specialized E-mail forensics tools

6. **Prepare Forensics Reports**

Potential Elements of the Performance:

- Understand the importance of reports
- Determine the types of reports in Computer Forensics
- Define the legal processes of Computer Forensics
- Demonstrate knowledge of Corporate Investigations
- Critique the case
- Document and prepare evidence for Court
- Learn Court terminology and the Trial process
- Determine the guidelines to testifying
- Prepare Forensics evidence for Testimony

III. **TOPICS:**

1. Advanced Network Security
2. Secure Web and E-Mail Servers
3. Computer Forensics Environment and Tools
4. Data Acquisition, Analysis and Validation
5. Investigating Crime and Incident Scenes
6. Prepare Forensics Reports

IV. **REQUIRED RESOURCES/TEXTS/MATERIALS:**

Textbook: ***Guide to Computer Forensics and Investigations (4th Edition)***

ISBN: 1435498836

Authors: Nelson, Phillips and Stuart

Publisher: Course Technology

V. EVALUATION PROCESS/GRADING SYSTEM:

Tests (3 @ 15% each)	45 %
LMS Quizzes	20 %
Participation and Attendance	10 %
Lab Assignments	25 %

Note: This evaluation scheme is subject to change if circumstances warrant. Any changes will be discussed with students and reported in writing before implementation.

Missed Tests

Students are expected to be present to write all tests in class. If a student is unable to write a test because of illness or a legitimate emergency, that student must contact the professor prior to the class and provide an explanation, which is acceptable by the professor. Should the student fail to contact the professor, the student may receive a **grade of zero** for that test.

Once the test has commenced, the student is considered absent and may not be given the privilege of writing the test.

Any student who has missed a test and meets the following criteria may write the missed test at the end of the semester.

The following semester grades will be assigned to students:

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

Attendance:

Absenteeism will affect a student's ability to succeed in this course. Absences due to medical or other unavoidable circumstances should be discussed with the professor. Students are required to be in class on time and attendance will be taken within the first five minutes of class. A missed class will result in a penalty in your marks unless you have discussed your absence with the professor as described above. The penalty depends on course hours and will be applied as follows:

Course Hours	Deduction
5 hrs/week (75 hrs)	1% / hr
4 hrs/week (60 hrs)	1.5% /hr
3 hrs/week (45 hrs)	2% /hr
2 hrs/week (30 hrs)	3%/hr

Absentee reports will be discussed with each student during regular meetings with Faculty Mentors. Final penalties will be reviewed by the professor and will be at the discretion of the professor.

Contact Information:

Dan Kachur – Professor
 School of Business
 (705) 759-2554 Ext: 2648
dan.kachur@saultcollege.ca