A POLYTECHNIC INSTITUTION

Course Outline

School of Computing and Academic Studies
Program: Computer Systems Technology
Option: Bachelor of Technology, Computer Systems

Course Number: **COMP 8006**
Course Name: **Network Security and Administration Level 2**

Start Date: January 8, 2018 **End Date:** April 20, 2018

Total Hours: **Total Weeks:** **Term/Level: 1** **Course Credits: 3**
Hours/Week: 3.75 **Lecture: 1.25** **Lab: 2.5**

Prerequisites:

1. Comp 7006 or
2. Permission of instructor and Program Head

Course No.	**Course Name**	**Course No.**	**Course Name**

- **Course Description:**

This course builds on the foundations established in Comp 7006 and covers more advanced topics in network security and intrusion detection. In-depth coverage of perimeter protection and firewall designs. Advanced intrusion detection and IDS/IPS design and implementation. Introduction to privacy and Cyberwarfare issues and vulnerabilities. Students will be familiarized with network monitoring and security tools, and use them to perform traffic and IDS signature analysis, and network forensics.

- **Evaluation**

Theory Final Examination:	30%	Comments:
Practical Final Project:	35%	
Labs & Assignments:	35%	
TOTAL	100%	

- **Course Learning Outcomes/Competencies**

Upon successful completion, the student will be able to:

1. Configure and set-up TCP/IP security applications on Linux-based LANs.
2. Design and implement complete and functional Linux firewalls.
3. Deploy Intrusion detection tools in a network.
4. Conduct detailed and extensive tests to verify firewall and IDS functionality
5. Be able to use logs produced by various security tools to conduct security audits on a network.
6. Design a defensive Perimeter solution (defence-in-depth) for a Network.
7. Configure a custom Linux kernel for security and deploy it.
8. Take measures to protect against information theft and Cyberwarfare.

- **Verification**

I verify that the content of this course outline is current.

Aman Abdulla — January 2, 2018

Authoring Instructor	Date

I verify that this course outline has been reviewed.

Program Head/Chief Instructor	Date

I verify that this course outline complies with BCIT policy.

Dean/Associate Dean	Date

Note: Should changes be required to the content of this course outline, students will be given reasonable notice.

- **Instructor(s)**

Aman Abdulla	Office Location:	SW2-323	Office Phone:	604-432-8837
	Office Hrs.:		E-mail Address:	aabdulla@milliways.bcit.ca

- **Learning Resources**

Required:

Linux Firewalls, 3rd Edition
Robert Ziegler

Recommended:

TCP/IP Illustrated, Volume 1 (Highly recommended)
Richard W. Stevens
Prentice-Hall

Network Intrusion Detection, 3rd Edition
By Stephen Northcutt and Judy Novak

Assignments: Late assignments, lab reports or projects will **not** be accepted for marking. Assignments must be done on an individual basis unless otherwise specified by the instructor.

Makeup Tests, Exams or Quizzes: There will be **no** makeup tests, exams or quizzes. If you miss a test, exam or quiz, you will receive zero marks. Exceptions may be made for **documented** medical reasons or extenuating circumstances. In such a case, it is the responsibility of the student to inform the instructor **immediately**.

Ethics: BCIT assumes that all students attending the Institute will follow a high standard of ethics. Incidents of cheating or plagiarism may, therefore, result in a grade of zero for the assignment, quiz, test, exam, or project for all parties involved and/or expulsion from the course.

Attendance: The attendance policy as outlined in the current BCIT Calendar will be enforced. Attendance will be taken at the beginning of each session. Students not present at that time will be recorded as absent.

Illness: A doctor's note is required for any illness causing you to miss assignments, quizzes, tests, projects, or exam. At the discretion of the instructor, you may complete the work missed or have the work prorated.

Attempts: Students must successfully complete a course within a maximum of three attempts at the course. Students with two attempts in a single course will be allowed to repeat the course only upon special written permission from the Associate Dean. Students who have not successfully completed a course within three attempts will not be eligible to graduate from the appropriate program.

Course Outline Changes: The material or schedule specified in this course outline may be changed by the instructor. If changes are required, they will be announced in class.

Labs: Lab attendance is mandatory. Lab exercises are due at the end of the lab period.

I.D. Required in Examination Centres: Effective December 2000, in order to write exams, students will be required to produce photo-identification at examination centres. Photo I.D. must be placed on the desk before an exam will be issued to the student. The I.D. must remain in view on the desk while writing the exam, for inspection by invigilators. Students should bring a BCIT OneCard or alternatively two pieces of identification, one of which must be government photo I.D. such as a driver's licence. Please see BCIT Policy #5300, Formal Invigilation Procedures.

Computer Use Policy: BCIT has an Institute-wide policy (#3501) pertaining to information technology and services and to the resources available in support of the Institute mission. Computer Systems Technology students are expected to exercise the highest degree of professionalism and ethical behaviour related to information technology. Violations of BCIT Policy #3501 will result in disciplinary action which may include suspension or expulsion of students. Also refer to the Computer Systems Technology Student Conduct Guidelines.

- **Assignment Details:** Will be provided in class

Schedule

Topic Number	Outcome/Material Covered
1	**Configuring TCP/IP Networking (Review):** • Setting the Hostname & assigning IP Addresses • Creating Subnets • Configure hosts and networks Files • Network configuration (IP, DNS, ARP, etc)
2	**TCP/IP Firewalls:** • Methods of Attack • Firewalls and IP Filtering • Setting Up Linux for Firewalling • Netfilter and *iptables* • Testing a Firewall Configurations
3	**IP Accounting:** • Configuring IP Accounting • Resetting the Counters • Flushing the Ruleset • Passive Collection of Accounting Data
4	**Network Intrusion Detection:** • "Real world" packet dump analysis • Configuration/Deployment of snort and writing snort filters • Configuration/Deployment of Suricata • Detection of Intelligence gathering • IPS design and implementation
5	**Network Traffic Analysis** • Network traffic analysis • Network traffic forensics
6	**Advanced Issues:** • Network Penetration Testing • Perimeter Networks • Social Network Privacy • Cyberwarfare Basics • Malware Cyber threats

****Topics may be omitted, replaced or added at the discretion of the instructor.**

- Notes will be posted on my Web server which you may access using the following URL:

  http://milliways.bcit.ca/c8006/

CST/PTS Student Conduct Guidelines

The School of Computing and Academic Studies expects the highest level of professional conduct and ethical behaviour from all students enrolled in Computer Systems Technology (CST) courses and programs.

All students are reminded of the following BCIT policies related to student conduct:

- Policy 5250 Cheating and Plagiarism www.bcit.ca/~presoff/5250.htm
- Policy 5251 Student Conduct www.bcit.ca/~presoff/5251.htm
- Policy 3501 Responsible Use of Information Technology at BCIT www.bcit.ca/~presoff/3501.htm

CST students are especially reminded that the Computing and IT knowledge and skills acquired in the course of their studies confer upon them, as with all IT professionals, a special responsibility to use this knowledge in a responsible, professional and ethical manner.

Given that misuse of computer facilities at BCIT can have significant legal and/or economic impacts, upon evidence of any violation of Policy 3501, the School may recommend immediate suspension, even for first offences.

By attending this course, every student has been made aware of these policies and the actions that will be taken. Please follow the links provided, each student is responsible to read and comply with these policies.