A POLYTECHNIC INSTITUTION

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

Course Number: *COMP 8506*
Course Name: *Selected Topics in Network Security and Design*

Start Date: September 3, 2018 **End Date:** December 13, 2018

Total Hours: **Total Weeks:** **Term/Level:** 1 **Course Credits:** 3
Hours/Week: 3 **Lecture:** 1 **Lab:** 2

Prerequisites: **Dip. Of Tech in Computer Systems (or equivalent) or instructor and Program Head** **Permission of instructor and Program Head**

Course No.	Course Name	Course No.	Course Name
COMP 8006	Network Administration and Security Level 2		

- **Course Description:**

This course is a study of topics of particular interest to advanced B. Tech students in the area of network security. The focus will be on understanding and identifying network vulnerabilities and how they can be exploited. Penetration testing frameworks and tools will be covered. The use of malicious devices and social engineering techniques will be covered. The use of Honeynets and wargames in understanding how to mitigate network threats and vulnerabilities will be covered.

- **Course Goals**

- To get hands-on experience with network penetration tools and frameworks.
- Understand and use threat mitigation techniques to protect networks and systems.
- This course will get students to apply all the knowledge and skills acquired in Comp 7006 and Comp 8006 in a practical, hands-on manner.
- Conduct an in-depth study of specific and highly specialized areas in Network Vulnerabilities and Exploits.
- Implement a substantial project in the selected area, and produce an application or project report or both upon completion.

- **Evaluation**

Final Exam:	20%	Comments: The breakdown of evaluation components will be discussed in class.
Assignments:	30%	
Project:	40%	
Presentation:	10%	
TOTAL	100%	

- **Course Learning Outcomes/Competencies**

Upon successful completion, the student will be able to:

1. Understand how exploits can be used to compromise networks and evaluate the threat they pose to systems and networks.
2. Conduct network audits and penetration testing for networks.
3. Analyze networks and identify potential vulnerabilities that could be exploited.
4. Design and implement customized network security solutions that would mitigate threats and vulnerabilities.

- **Verification**

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

Aman Abdulla — August 31, 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

Aman Abdulla

Office Location: SW2-323 Office Phone: 604-432-8837

Office Hrs.: E-mail Address: abdulla@milliways.bcit.ca

ν Learning Resources

Required:

Given the rapidly changing nature of this field of study the best resources are on the Internet. You will be required to seek out sites that provide exploits and current information in the area of network security.

Recommended:

Know Your Enemy
Revealing The Security Tools, Tactics, and Motives of the Blackhat Community - By The Honeynet Project
Addison-Wesley Publishers

Students may be required to purchase special software related to lab experiments and projects.

Access to older PCs that can be used as test machines will be very useful.

ν Information for Students

By attending this course and receiving this course outline, you have been made aware of the following policies. Please follow the links provided as each student is responsible for reading and complying with these policies.

The following statements are in accordance with the *BCIT Student Regulations Policy 5002*. To review the full policy, please refer to http://www.bcit.ca/files/pdf/policies/5002.pdf.

Attendance/Illness:
In case of illness or other unavoidable cause of absence, the student must communicate as soon as possible with his/her instructor or Program Head or Chief Instructor, indicating the reason for the absence. Prolonged illness of three or more consecutive days must have a BCIT medical certificate sent to the department. Excessive absence may result in failure or immediate withdrawal from the course or program.

Academic Misconduct:
Violations of academic integrity, including dishonesty in assignments, examinations, or other academic performances are prohibited and will be handled in accordance with the *Violations of Standards of Conduct* section of Policy 5002.

The School of Computing and Academic Studies expects the highest level of professional conduct and ethical behaviour from all students enrolled in part time studies courses and programs. All students are reminded of the BCIT policy related to the *Responsible Use of Information Technology*. Read the full policy here: http://www.bcit.ca/files/pdf/policies/3501.pdf.

The Computing and IT knowledge and skills acquired by students in the course of their studies confers upon them, as with all professionals, a special responsibility to use their knowledge in a responsible, professional and ethical manner. Further, given that misuse of computer facilities at BCIT can have significant legal and/or economic impacts, upon evidence of any such misconduct, the School may recommend immediate suspension, even for first offences.

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 their respective program.

Accommodation:
Any student who may require accommodation from BCIT because of a physical or mental disability should refer to BCIT's Policy on Accommodation for Students with Disabilities (http://www.bcit.ca/files/pdf/policies/4501.pdf), and contact BCIT's Disability Resource Centre (SW1-2300, 604-451-6963, http://www.bcit.ca/drc/) at the earliest possible time. Requests for accommodation must be made to the Disability Resource Centre, and should not be made to a course instructor or Program area.

Any student who needs special assistance in the event of a medical emergency or building evacuation (either because of a disability or for any other reason) should also promptly inform their course instructor(s) and the Disability Resource Centre of their personal circumstances.

Course Notes:

- You will be required to work in teams that will be established on the first day of class.
- Each team will be required to do significant research into setting up a Honeypot for the Windows and Linux operating systems.
- Notes will be posted on my Web server which you may access using the following URL:

  http://milliways.bcit.ca/c8506/

- The final project will be the main focus of the entire term. Each week you will provide me with project updates.
- Throughout the term we will hold periodic project review meetings. Further details to be discussed in class.

ν Assignment Details :

- The main component of this course will be the "war games" project. Students will be required to submit a detailed report outlining their design of the Honeypot, the vulnerabilities used and the exploits used to test each exploit.
- There will be some smaller assignments, but they will all address the larger project. That is, the assignments will be smaller components to be used in the final project.
- There is considerable latitude in topics and the nature of the assignments and final project given the nature of this field of study. We will discuss and select these topics as part of our class discussions.

Note: The final project format will most likely be modified for this running of the course. Details will be provided in class.

Schedule

Module Number	Outcome/Material Covered	Approximate Duration
1	**Exploits and the Attackers' Process**: • The purpose of exploits. • The Attacker's process. • Reconnaissance and System Exploits. • Types of Attacks and Exploits	**(1 Week)**
2	**Attack Routes**: • Ports and Services • Third-Party Software • Trojans	**(1 Week)**
3	**Network Mapping and Reconnaissance Tools & Techniques** • Network Mapping tools (hping3, traceroute, nmap) • Port Scanners (Nmap, hping3)	**(1 Week)**
4	**Local Area Network Exploits and Tools** • ARP poisioning • Switched Packet Sniffing • Tools: Dsniff and Ettercap	**(1 Week)**
5	**Network Tools – Interactive sessions** • Using netcat to penetrate systems • Scanning using netcat	**(1 Week)**
6	**Covert Channels & Steganography** • TCP/IP Covert channels • Steganography tools	**(1 Week)**
7	**Metasploit Framework and Kali** • Armitage exploits • Social Engineering tools	**(1 Week)**
8	**Password Security** • Password attacks • Windows and Linux password crackers	**(1 Week)**
9	**Wireless Network Vulnerabilities and Attacks** • Wireless Vulnerabilities • Wireless Attacks • Reconnaissance and Sniffing Tools • WEP/WPA Encryption Cracking	**(1 Week)**

Module Number	Outcome/Material Covered	Approximate Duration
10	**Network Penetration Techniques** • Packet Crafting & Fuzzing • Network auditing	**(1 Week)**
11	**Network Penetration Tools and Devices** • Malicious Devices • Social Engineering Devices & Tools	**(1 Week)**
12	**Project Topics:** • Honeynet • War Games	**Meetings and preparation throughout the course.** **Presentation: 1 Week**

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

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.