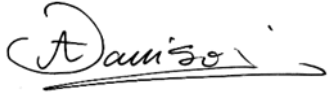


Approved by Chair:

A handwritten signature in black ink, appearing to read "Damiso", written over a horizontal line.

Dec 24, 2023

Signature

COMP3134 - Introduction to Cyber Security

Course Description

This course covers the fundamentals of Cyber Security. Students learn about various concepts and recommended steps in securing web-based applications from potential threats. It introduces how to seek and test for vulnerabilities using different attacking techniques. The students explore different types of cyber-attacks and learn about the procedures and the best practices to protect an application from those attacks by taking appropriate preventative measures.

Course Outcomes

At the end of this course, the student will reliably demonstrate the ability to:

1. Recall security fundamental terms and diagrams
2. Apply and classify network discovery and security auditing techniques
3. Identify & baseline network traffic using network monitoring tools
4. Identify and filter various protocols and network ports
5. Implement various tactics to attack a network or application
6. Classify levels of database insecurities
7. Compare and differentiate SQL injections
8. Critique and execute mitigation techniques

LIST OF TEXTBOOKS AND OTHER TEACHING AIDS:

Required:

- None

Recommended Resources:

- Certified Ethical Hacker (CEH) Version 10 Cert Guide (3rd Edition) Author: Omar Santos and Michael Gregg Publisher: Pearson IT Certification; 3rd edition ISBN-10: 0789760525 ISBN-13: 978-0789760524

Assignment Policy:

- All assignments must be submitted on the due date based on an instruction given by the professor. Late assignment, will be penalized 10% per day to maximum of 5 days, weekend included unless the student has notified the professor (via e-mail,

phone or in person) ahead of the due date that he/she has a valid reason for late submission.

- Students are responsible for making sure their marks are up to date on the blackboard. No mark will change after two weeks from the time marks were posted on Blackboard.

Testing Policy:

- Students must complete tests and the final exam on the assigned day. If unable to complete the test/exam as scheduled, students are required to notify the professor at least three days prior to the date, so alternative arrangements can be made. Failure to comply with this policy may result in a zero grade.
- Lab tests must be completed based on given instructions and must be completed during the lab hours. There will be no partial marks awarded for any of the lab tests if they are not complete.
- There will be no makeup quiz and lab exercises, for medical or other reasons. If you anticipate missing more than 2 quizzes or lab exercises for serious, major reasons, see your professor beforehand.

EVALUATION SYSTEM:

The passing grade for this course is: D (50%)

Assessment Tool:	Description:	Outcome(s) assessed:	EES assessed:	Date / Week:	% of Final Grade:
Quiz 6 x 2	The best 6 out of 8 quizzes will count	1, 3,4,6,7,8	3,5,11	TBA	12
Assignments x4	Group assignments	2,3,4,5,6,7,8	3,4,5,7,10	TBA	30
Lab Exercises	Hands-On lab exercises	1,2,3,4,5,6,7,8	3,4,5,7, 9,10, 11	TBA	8
Mid-Term Exam	Comprehensive mixed-question test	1,3,4,8	3,6,8,11	9	20
Final Exam	Comprehensive mixed-question test	1,3,4,6,7,8	3,6,8,11	15	30
TOTAL:					100%

Topical Outline

Learning Schedule / Topical Outline (subject to change with notification)

Week	Topic	Outcomes	Content / Activities	Resources
------	-------	----------	----------------------	-----------

1	1	1	<ul style="list-style-type: none"> - Security fundamentals - Defining & evaluating Assets, Vulnerabilities, Threats, Counter-Measurements & Risks 	Ch 1, Section 1 Ch 1, Section 2 Ch 1, Section 3
2	2	1, 2	<ul style="list-style-type: none"> - OSI Model - Intro to Anatomy of TCP/IP protocols - Anatomy of TCP/IP protocols <ul style="list-style-type: none"> - Application layer - Transport layer - Transmission control protocol - Information Gathering <ul style="list-style-type: none"> - Passive Information Gathering - Active Information Gathering 	Ch 2, Section 1 Ch 2, Section 2 Ch 2, Section 3
3	3	3,4	<ul style="list-style-type: none"> - Passive and Active Sniffing - Introduction to Wireshark - Address Resolution protocol (ARP) - ARP poisoning - Media Access Control (MAC) flooding Assignment 1	Ch 6, Section 1
4	4	5, 8	<ul style="list-style-type: none"> - Transport layer hijacking <ul style="list-style-type: none"> - Identify and find an active session - Predict the sequence number - Take one of the parties offline - Application layer hijacking <ul style="list-style-type: none"> - Predictable session token ID - Man-In-The-Middle (MITM) attacks 	Ch 6, Section 2
5	5	4, 5	<ul style="list-style-type: none"> - Denial of Service (DoS) - DoS attack techniques - Volumetric Attacks - SYN flood attacks - Internet Control Message Protocol (ICMP) attacks - Application-level attacks 	Ch 6, Section 3

			<ul style="list-style-type: none"> - Permanent DoS attacks - Distributed Denial of Service (DDoS) 	
6	6	5	<ul style="list-style-type: none"> - Web server hacking <ul style="list-style-type: none"> - Scanning Web Servers - Banner Grabbing and Enumeration - Web Server Vulnerability Identification <p>Midterm Exam Review Assignment 2</p>	Ch 7, Section 1
7	Mid-Term Exam			
8	Intersession Week			
9	7	5, 8	<ul style="list-style-type: none"> - Attacking the Web Server <ul style="list-style-type: none"> - DNS Server Hijacking and DNS Amplification Attacks - Directory Traversal - Website Defacement - Application Error Handling - Cookie Manipulation Attacks - Web Server Password Cracking - Comments in Source Code - Lack of Error Handling & Overly Verbose Error Handling - Race Conditions - Hidden Elements 	Ch 7, Section 2

10	8	8	<ul style="list-style-type: none"> - Securing Web Servers <ul style="list-style-type: none"> - Harden Before Deploying - Disable Unneeded Services - Lock Down the File System - Log and Audit - Provide Ongoing Vulnerability Scans 	Ch 7, Section 3
11	9	5, 8	<ul style="list-style-type: none"> - Web Application Hacking <ul style="list-style-type: none"> - Unvalidated Input - Parameter/Form Tampering - Injection Flaws - Cross-site Scripting (XSS) <ul style="list-style-type: none"> - Understanding XSS Vulnerabilities - Reflected XSS - Stored XSS - DOM-based XSS - XSS Evasion Techniques - XSS Mitigations <p>Assignment 3</p>	Ch 7, Section 4
12	10	5,8	<ul style="list-style-type: none"> - Fraudulent Activities <ul style="list-style-type: none"> - Cross-site Request Forgery - Clickjacking - Verifying Authentication <ul style="list-style-type: none"> - Password Cracking - Understanding What Cookies Are and Their Use - URL Obfuscation 	Ch 7, Section 5
13	11	6, 7, 8	<ul style="list-style-type: none"> - Database Hacking <ul style="list-style-type: none"> - SQL Injection Categories - In-Band SQL Injection - Out-of-Band SQL Injection - Blind SQL Injection - Fingerprinting the Database - SQL Injection Mitigations <p>Assignment 4</p>	Ch 7, Section 6
14	12		<ul style="list-style-type: none"> - Review / Catch-Up Week 	

For information on withdrawing from this course without academic penalty, please refer to the College Academic Calendar: <http://www.georgebrown.ca/Admin/Registr/PSCal.aspx>

Policy on Academic Dishonesty:

The *minimal* consequence for submitting a plagiarized, purchased, contracted, or in any manner inappropriately negotiated or falsified assignment, test, essay, project, or any evaluated material will be a grade of zero on that material.

To view George Brown College policies please go to www.georgebrown.ca/policies