BCS302: Cyber-Defense and Ethical Hacking

Semester 1, 2025

Assessment	: Assignment 1
Due Date	: 20th February 2025 by 23.59PM
Release Date	: 20th January 2025
Value	: 30%
Assessment Type	: Group of Two/Three

Course Learning Outcomes
This final project assesses the following learning outcomes:

CLO1: Explain the concepts and practices used in computer security (C4, PLO1, MQF1)

Use of AI generative tools	1. Utilizing AI generative tools should be seen to augment creativity, problem-solving, and productivity while maintaining the integrity of the subject matter and upholding academic and professional standards. 2. Students must demonstrate their own knowledge, skills, and understanding of the subject matter in their work. 3. Where an assignment requires ChatGPT to be cited, you must reference all the content from Generative AI tools that you include. Failure to reference externally sourced, non-original work can result in Academic misconduct. 4. Students are to apply **APA Style** for any AI content generated that is utilized and integrated into the final work. This acknowledgment is to be added to the **footnote** of the respective pages. • **To cite AI-generated work that you did not edit or revise:** Name of AI Tool. (Year, Month Day you generated the content). Exact text of question or prompt you entered [AI-generated text/image/video, etc.]. Name of Company/Developer if different than name of AI tool. URL. Example: ChatGPT. (2023, June 3). "Steps of creating a running website using XAMPP?" [AIgenerated text]. OpenAI. https://chat.openai.com.

	• **To cite AI-generated work that you edited or revised:** Name of AI Tool & Your Last Name, First Initial. (Year, Month Day you generated the content). Exact text of question or prompt you entered [AI-generated text/image/video, etc.]. Name of Company/Developer if different than name of AI tool. URL. Example: ChatGPT & Chong, L.Y. (2023, July 19). How to setup cloud based CI/CD for a website deployment? [AI-generated text]. OpenAI. https://chat.openai.com/c/9bb6771b-209b-4c8c-ac79-6a8a9f39604a • **General Format for In-Text Citations** Examples: To make fluffy basmati rice, "rinse the rice twice in cold water" (ChatGPT, 2023) Cloud-based CI/CD requires the following steps to be applied (ChatGPT & Chong, L.Y., 2023) 5. Any violation of this policy will result in appropriate academic sanctions, which may include penalizing your grades, failing the course, and other disciplinary actions.

Submission Instructions

Submission	No resubmission allowed
Late Submission	Please fill out the Late Submission Form to be considered for extension. Penalty of 5 marks per working day will be imposed if: • late submission form is not included; • reason for extension is not given; • extension is not granted.
Cover Sheet & Marking Rubrics	Include the Assignment Cover Sheet & Marking Rubrics in the report
Academic Integrity	You are expected to adhere to the Academic Integrity Policy. All referencing and citation should use APA Style 7th Edition. You do not need to submit the similarity report. Turnitin similarity reports will be generated by the lecturer and penalties imposed for similarity exceeding 15%. You may be subject to additional penalties according to the Academic Integrity Policy.

Note: The marks below will be graded based on the viva or defense of your work.

Tasks:

Information Gathering is a crucial phase in ethical hacking methods that involves collecting as much data as possible about the target system or organization. This phase helps in identifying potential entry points and understanding the environment better. Among various techniques for information gathering, Capture The Flag (CTF) competitions are a notable and engaging method.

Capture The Flag (CTF) is a popular cybersecurity competition that challenges participants to solve a variety of tasks, puzzles, and challenges to find hidden "flags" within software, systems, or files. These flags are usually strings of text that serve as proof of solving a particular challenge. CTFs are designed to test and improve participants' skills in areas such as cryptography, reverse engineering, web exploitation, binary analysis, and more. They simulate real-world cybersecurity scenarios and provide a platform for learning and honing practical security skills.

In this group assignment consisting of two participants: you are tasked with completing four different Capture The Flag challenges, each focusing on a specific aspect of cybersecurity. The challenges include:

1. Compare and contrast different methodologies used in ethical hacking and explain the significance of Capture The Flag (CTF) competitions in cybersecurity. (10 Marks)

2. Capture The Flag 1 (Secret Message): This challenge likely involves extracting a hidden message or solving a puzzle within the provided Excel file **'CTF_WarmUp_Secret Message.xlsx'**. (10 Marks)

3. Capture The Flag 2 (X-Files): This challenge requires analyzing the **'X-Files.exe'** executable file to uncover hidden information, potentially involving reverse engineering or understanding the behaviour of the program. (15 Marks)

4. **Network Layout Task 4:** Bambinos, a reputable nasi-lemak delivery service, has gained recognition for its delectable menu offerings and swift delivery services across multiple locations. Despite its success in the culinary sphere, recent assessments have unveiled vulnerabilities within its network infrastructure, exposing critical data and communication channels to potential cybersecurity risks. As depicted in the network diagram, **Bambinos.doc**, they operate a complex network architecture involving Peplink Load Balancers, SonicWalls, and Network Load Balancers (NLB) to facilitate a seamless flow of

data and communication within its operations. The diagram highlights key data transfer pathways from its headquarters to various stores, emphasizing the interconnection of critical components such as DOTS order taking systems, web-based ordering platforms, and store servers. However, the diagram also sheds light on potential vulnerabilities, including a data transfer flow from the store to the headquarters that may be susceptible to unauthorized access. Additionally, the incoming call handling process from Telekom Malaysia to the customer service center (CSC) raises concerns about the security and privacy of customer data and communication channels. Considering these vulnerabilities, there is an urgent need for Bambinos to fortify its network infrastructure and implement robust cybersecurity measures to safeguard sensitive information, ensure uninterrupted service delivery, and maintain customer trust and confidence in its services.

Based on the network diagram, provide a comprehensive report that maintains professional standards with pertinent screenshots, and offers in-depth analysis of the findings. Additionally, thoroughly discuss the security implications stemming from the identified vulnerabilities and propose effective mitigation strategies. (40 Marks)

5. Capture The Flag 5 (Where is Waldo): This challenge might involve locating a hidden item or information within the 'IMG_134.jpg' image file, possibly using steganography techniques or analyzing the image data. (25 Marks)

To facilitate the process of tracking and managing your progress, a GUI application named **'CTF.exe'** and **Bambinos.doc** have been provided, allowing you to check your scores for each of the CTF challenges. Happy Hacking!

Details of the challenges:

Capture The Flag 2 (Secret Message): This challenge is worth 10 points.

The flag is hidden in an encrypted message given in the excel file as shown below:

Guidelines

* Secret message is in the Encoded Message

* Flag consist of 6 alphabets, two words, pertaining to an institute of higher learning in Malaysia

Encoded Message (to be decoded)

Hello!, Everyoe gone already. Lots of things to do here. Please remember to feed my bird. Maybe you can send me a picture. Everyone here is nice.

Decoded Message

(Type the coded message here, e.g. TAR IT)

Paste the decoded message in the GUI to see if you have succesfully captured the flag

Fig. 1: CTF (Secret Message)

Paste the flag in the GUI to check if it is correct to collect your reward.

Provide the solution in detail, source code if any, and a screenshot as proof.

<u>Capture The Flag 3 (X-Files):</u> This challenge is worth 15 points.

Click on the **X-Files.exe** to perform a username and password registration:

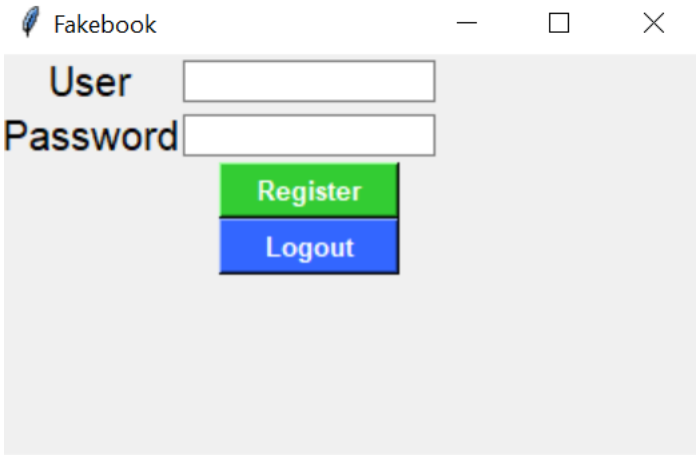

Fig. 2: X-Files

'Logout' will terminate the program.

'Register' will perform the registration.

Upon completion, the flag is contained in the registration text database.

Paste the result in the GUI to check if it is correct to collect your reward.

Provide the solution in detail, source code if any, and a screenshot as proof.

Capture The Flag 5 (Where is Waldo?): This challenge is worth 25 points.

Somewhere in this picture with the President of Portugal from IMG_134.jpg, there contains the flag of twelve characters long beginning with IEC.

Fig 3: **image.jpg**

Colonize it!

Hint: Perform file handling method.

Paste the flag in the GUI to check if it is correct to collect your reward.

Provide the solution in detail, source code if any, and a screenshot as proof.

Submission Instructions

Submission	Submit all your work through the Turnitin activity on the LMS. Submission to LMS by 23.59 PM. No resubmission allowed.
Late Submission	Please fill out the Late Submission Form to be considered for extension. Penalty of 5 marks per working day will be imposed if:

	- late submission form is not included; - reason for extension is not given; - extension is not granted.
Cover Sheet	Include the Assignment Cover Sheet
Academic Integrity	You are expected to adhere to the Academic Integrity Policy. All referencing and citation should use APA Style (7th Edition preferred). You do not need to submit the similarity report. Turnitin similarity reports will be generated by the lecturer and penalties imposed for similarity exceeding 15%. You may be subject to additional penalties according to the Academic Integrity Policy.
Format	Font type: Times New Roman Font size: 12 Spacing: Double space Text alignment: Justify Please submit the final report and codes to the HLMS

BCS302: Cyber-Defense and Ethical Hacking

Faculty of Computing and Digital Technology

HELP University

Note: The marks below will be graded based on the viva or defense of your work.

Assignment 1 Marking Scheme
Student Name:
Student ID:
Worth: 30% (full mark:100)

Topic			**Marks awarded**
Comparing Hacking Method and importance of CTF			
Level C – Provides a basic explanation of some ethical hacking methods and importance of CTF (0-3)	Level B – Provides a clear explanation of several ethical hacking methods and importance of CTF (4-6)	Level A –Provides a detailed and thorough explanation of multiple ethical hacking methods and importance of CTF (7-10)	
Capture The Flag 2: Secret Message			

Level C – Little to no analysis perform with confusing explanation and no screenshots provided (0-2)	Level B - Acceptable analysis of the encrypted message and its encryption technique. Little explanation of the steps taken to decrypt the message with blurry screenshots. (3-6)	Level A - Detailed analysis of the encrypted message and its encryption technique. Clear explanation of the steps taken to decrypt the message with good screenshots. (7-10)	
Capture The Flag 3: X-Files			
Level C – Little to no analysis of the program, without any understanding of the registration process and how it interacts with the database. Confusing demonstration of the steps taken to extract the flag with blurry screenshots. (0-5)	Level B – Moderate analysis of the program, including some understanding of the registration process and how it interacts with the database. Missing demonstration the steps taken to extract the flag with acceptable screenshots. (6-10)	Level A – Comprehensive analysis of the program, including a detailed understanding of the registration process and how it interacts with the database. Clear demonstration of the steps taken to extract the flag with vivid screenshots. (11-15)	
Network Layout Task 4: Bambinos.doc			
Level C – Analysis shows incorrect outputs and includes an irrelevant interpretation of the data, resulting in inadequate conclusions and understanding (0-13)	Level B – Analysis presents findings that are appropriate and supported, with an acceptable interpretation that demonstrates a reasonable understanding of the data and its implications (14-27)	Level A –Analysis provides accurate outputs and includes a precise and insightful interpretation of the data, demonstrating a comprehensive understanding of the vulnerabilities and their potential impact (28-40)	
Capture The Flag 5: Where is Waldo			

Level C – Litte to no examination of the image's content and metadata. Confusing explanation of the steps taken to locate and extract the flag. Utilization of ineffective file handling methods, with poorly documented source code and screenshots. (0-8)	Level B – Sufficient examination of the image's content and metadata. An acceptable explanation of the steps taken to locate and extract the flag. Utilization of basic file handling methods, with adequate documented source code and screenshots. (9 -17)	Level A – Detailed examination of the image's content and metadata. Clear explanation of the steps taken to locate and extract the flag. Utilization of effective file handling methods, with well documented source code and screenshots. (18-25)	
TOTAL MARKS			
Late submission (deduction of 5 marks per day)			
Penalty will be given for Turnitin similarity score above 15%			
FINAL TOTAL MARKS			

HELP University
university of achievers

Assignment Cover Sheet

Student Information (For group assignment, please state names of all members)		Grade/Marks
Name	**ID**	

Module/Subject Information		Office Acknowledgement
Module/Subject Code	BCS302	
Module/Subject Name	Cyber-Defense and Ethical Hacking	
Lecturer/Tutor/Facilitator	Dr Shapla Khanam	
Due Date	20/02/2025	
Assignment Title/Topic	Assignment	
Intake (where applicable)		
Word Count	n/a	**Date/Time**

Declaration

- I/We have read and understood the Programme Handbook that explains on **plagiarism**, and I/we testify that, unless otherwise acknowledged, the work submitted herein is entirely my/our own.
- I/We declare that no part of this assignment has been written for me/us by any other person(s) except where such collaboration has been authorized by the lecturer concerned.
- I/We authorize the University to test any work submitted by me/us, using text comparison software, for instances of plagiarism. I/We understand this will involve the University or its contractors copying my/our work and storing it on a database to be used in future to test work submitted by others.

Note: 1) The attachment of this statement on any electronically submitted assignments will be deemed to have the same authority as a signed statement.
2) The Group Leader signs the declaration on behalf of all members.

Signature:	Date:
E-mail:	

Feedback/Comments*
Main Strengths
Main Weaknesses
Suggestions for improvement

	Student acknowledge feedback/comments
Grader's signature	Student's signature:
Date:	Date:

Note:

1) A soft and hard copy of the assignment shall be submitted.
2) The signed copy of the assignment cover sheet shall be retained by the marker.
3) If the Turnitin report is required, students have to submit it with the assignment. However, departments may allow students up to **THREE** (3) working days after submission of the assignment to submit the Turnitin report. The assignment shall only be marked upon the submission of the Turnitin report.