National College of Ireland

BSC(Honors) in Computing – Full-Time Year 4 BSHCYB4
Terminal Assignment-Based Assessment

Release Date, Monday 7th April 2025
Submission Date, Monday 14th April 2025 23:55

BSHCYB4 Penetration Testing

Eugene McLaughlin
Mark Drinan
Dr. Takfarinas Saber

Answer all questions
Submit a word document with your answers to the Turnitin link on Moodle on or before 23:55 on the 14th of April 2025.
This document will be electronically screened for evidence of academic misconduct.
The Terminal Assignment-based Assessment is weighted at 50% of the overall module mark.

Q1 25%

“A letter of engagement is a vital part of a penetration test” do you agree with this statement, in your answer discuss what you would expect to see in such a letter.

The Expected content of your answer is 1000 words.
The marks will be broken down as follows, refer to the marking rubric.

Criteria	Marks
Clearly defined Objectives. Why is it important?	5%
The rules of engagement are explained.	5%
The importance of scope is understood.	5%
The handling of data and communication is described	5%
Clarity of Explanation.	5%

Q2 25%

Write a 1000-word essay based upon the **last digit** of your student number, if your student number is x2120123**4** then your essay topic will be How does an ethical hacker differ from a cracker?

Student Number	Topic
0 or 5	Describe the pros and cons of black-box Vs white-box testing
1 or 6	Red Team or Blue Team if an organization can only afford one team, in your opinion which one should it choose?
2 or 7	Distinguish between active and passive information gathering.
3 or 8	What is the purpose of the Open Web Application Security Project's top 10 list?
4 or 9	How does an ethical hacker differ from a cracker?

Table 1 student essay topic.

The marks will be broken down as follows, refer to the marking rubric.

Criteria	Marks
Clear concise introduction introducing the topic	5%
The essay covers all relevant sections of the topic	10%
The essay demonstrated a clear understanding of the topic	10%

Q3 25%

Student Number	Team
0, 2, 4, 6, 8	Red
1, 3, 5, 7, 9	Blue

Table 2 Team Selection

The Covid pandemic has brought about a fundamental shift in work patterns. There are a significant number of employees still working from home and using their own devices. Based on the **second last** digit of your student number in Table 2 determine which security team you have been assigned.

- As a member of a Red team, describe how you would approach testing the security of a home network.
- As a member of a Blue team provides recommendations that would improve the security of a home network.

The Expected content of your answer is 1000 words.
If your student ID is x212012**3**4 then you are assigned to the Blue Team.

The marks will be broken down as follows, refer to the marking rubric.

Criteria	Marks
Clear concise introduction discussing the problem	5%
The essay demonstrated a clear understanding of the issues involved	5%
The objectives of the report are clear and unambiguous	5%
The steps required to complete the task are detailed and well explained	10%

Q4 25%

Refer to the attached OpenVAS report for Metasploitable2.pdf. Select your assigned port based on the second last digit of your student number. If your student number is x21201 3**2**4 then you are required to research the highest vulnerability on port 6697.

Student Number	Vulnerability on port
0	8009
1	5432
2	6697
3	21
4	6200
5	80
6	3632
7	1524
8	8787
9	25

Table 3 Nessus Report

A penetration test report should provide vulnerability details and mitigation factors for each vulnerability on the port listed in table 3.
You are required to fill out the details for your assigned vulnerability. Research the vulnerability using the CVE or CWS number to provide greater detail.

Marks will be broken down as follows:

Title, Rating, CVE-CWS	[5%]
Protocol and versions on port	[5%]
Description.	[5%]
Impact.	[5%]
Remediation.	[5%]

OpenVAS report on Metasploitable2	
Title	
Rating	
CVE-CWS	
Protocol and Version	
Description	
Impact	
Recommended Remedial Measures	