



FINAL EXAMINATION

Semester	:	SEPTEMBER 2025 SEMESTER
Programme Name	:	DIPLOMA IN COMPUTER SCIENCE
Course Code & Name	:	DCS2333 ETHICAL HACKING AND INTRUSION PREVENTION
Duration	:	3 HOURS

INSTRUCTIONS TO CANDIDATES:

1. Please read the instructions given in the question paper **CAREFULLY**.
2. The question paper consists of **FOUR (4)** questions.
3. Answer **ALL** questions in the question paper.
4. Answers to the questions are to be written into the examination booklet.
5. Electronic dictionaries, lecture notes, files or any unauthorised materials except writing equipment are strictly prohibited.

This question paper must be submitted along with all used and/or unused rough papers and/ or graph papers (if any). Candidates are **NOT ALLOWED** to take any examination paper(s) used or unused out of the examination hall.

WARNING:

The Examination Board of Peninsula College Georgetown regards cheating as a very serious offence and will not hesitate to mete out the appropriate punitive actions according to the severity of the offence committed, and in accordance with the clauses stipulated in the Students' Handbook, up to and including expulsion from Peninsula College Georgetown.

(This booklet contains 3 printed pages including this page)

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE ALLOWED TO DO SO

Answer **ALL** questions on the separate sheet provided.

[100 marks]

1. a) Define "Ethical Hacking." (1 mark)
 - (i) Explain the apparent contradiction in the phrase "authorized attempt to gain unauthorized access." (2 marks)
 - (ii) State the primary goal of an ethical hacking engagement. (2 marks)

 - b) Compare and contrast the motivations, authorization and activities example of Black Hat Hackers and Grey Hat Hackers. Provide **THREE (3)** different for each. (12 marks)

 - c) A company's IT manager wants to understand the value of hiring an ethical hacker. Explain **TWO (2)** key knowledge areas or skill sets a competent ethical hacker must possess, and for EACH, provide a specific tool they would use and its purpose. (4 marks)

 - d) What are the any **TWO (2)** considerations should be taken into account when conducting ethical hacking in Attack and Protect? (4 marks)
- Total: [25 marks]

2. a) Phishing is a common type of cyber-attack.
 - (i) Briefly define what a phishing attack is. (2 marks)
 - (ii) Explain how a typical phishing attack is carried out. (2 marks)
 - (iii) Provide **ONE (1)** real-world example of a phishing scenario. (1 mark)

 - b) Modern cyber attacks can be categorized into several key types, each exploiting different vulnerabilities in a target's digital environment. List and explain any **FOUR (4)** main types of attacks with modern example to illustrate how the attack works. (12 marks)

 - c) Suggest **FOUR (4)** measures that can be taken to prevent the phishing attacks. (4 marks)

 - d) Brief any **TWO (2)** primary types of penetration testing. (4 marks)
- Total: [25 marks]

3. a) Explain the **FIVE (5)** phases of the hacking process. For each phase, provide a brief description of its core objective or the primary activities an attacker would perform. (10 marks)
- b) Explain **TWO (2)** different types of footprinting techniques that can be used in ethical hacking with their examples. (6 marks)
- c) Transport layer protocols are fundamental to network communication. Compare and contrast any **TWO (2)** between the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). (4 marks)
- d) Port scanning is a critical phase in active footprinting, allowing a security professional or attacker to discover network services and potential entry points.
- i) Explain the purpose and functionality of the ping command in networking. (1 mark)
- ii) Briefly explain any **TWO (2)** distinct tools used for port scanning. For each tool, state its primary purpose that makes it suitable for a specific scanning scenario. (4 marks)
- Total: [25 marks]
4. a) A company's legacy password policy, which relied on complex passwords changed every 90 days, has proven ineffective against modern attacks. As a security consultant, you are tasked with recommending a modernized and prioritized defence strategy. Recommend **THREE (3)** modern defences method with core function and their benefit. (9 marks)
- b) Based on the topic "Methods of Attack," propose **FOUR (4)** our methods of attack. (4 marks)
- (i) Briefly explain how the attack listed above works. (8 marks)
- (ii) Provide a simple example or scenario to illustrate the attacks. (4 marks)
- Total: [25 marks]

- END OF QUESTIONS -