PENINSULA COLLEGE GEORGETOWN DK266-03(P)

FINAL EXAMINATION

Semester	:	**JANUARY 2026 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 4 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. An ethical hacker is hired by a company called **DataSecure Sdn. Bhd.** to perform the **reconnaissance phase** of a penetration test. The hacker begins by collecting publicly available information about the organisation using various **footprinting techniques**, including Whois lookups and network path analysis using Tracert.

   Based on the scenario, answer the following questions.

   a) Describe **FOUR (4)** types of information that can be gathered during the footprinting phase of a penetration test. (8 marks)

   b) i) List **THREE (3)** types of information that can be obtained using a Whois query. (3 marks)

   ii) Explain information obtained from Whois can assist an attacker in planning further attacks. (4 marks)

   c) i) List **THREE (3)** purposes of using the Tracert command during network reconnaissance. (3 marks)

   ii) Explain the role of TTL (Time To Live) in the operation of the Tracert command. (2 marks)

   d) List **FIVE (5)** security measures organisations can implement to reduce information exposure during footprinting activities. (5 marks)

   Total: [25 marks]

2. A logistics company requested a security assessment of its internal network. During the penetration test, the ethical hacker performs network discovery and fingerprinting to identify devices connected to the network and determine their operating systems and running services.

   Based on the scenario, answer the following questions.

   a) Describe **FOUR (4)** techniques used for network discovery in ethical hacking. (8 marks)

   b) i) List **THREE (3)** examples of network infrastructure devices that may be identified during network scanning. (3 marks)

   ii) Explain **TWO (2)** fingerprinting techniques help determine the operating system of a target device. (4 marks)

c) List **FIVE (5)** tools commonly used for network discovery and fingerprinting. (5 marks)

d) Describe **TWO (2)** security measures organisations can implement to protect network infrastructure devices from hacking attempts. (4 marks)

e) List **ONE (1)** reason for attackers attempt to compromise network infrastructure devices such as routers or switches. (1 mark)

Total: [25 marks]

3. A private college in Malaysia recently experienced a security alert in its campus network. A diploma student named **Alex** developed a script to scan the college network while connected to the **campus guest Wi-Fi** using his personal laptop. The script performed automated scanning to identify **live hosts, open ports, and outdated service versions** on several servers within the campus network.
The activity triggered an alert in the college's **Intrusion Detection System (IDS)**, and the IT department launched an investigation. Alex explained that he was only experimenting and learning about network security techniques for educational purposes, but he had **not obtained permission** from the college IT department before conducting the scan.
Based on the scenario, answer the following questions.

a) List **FIVE (5)** cybercrime activities that are prohibited under the Computer Crimes Act 1997. (5 marks)

b) Explain **FOUR (4)** reasons for Alex's network scanning activity could be considered unauthorised access or misuse of computer systems under Malaysian cyber laws. (8 marks)

c) Explain **THREE (3)** differences between Alex's actions as a student experimenting with security tools and the behaviour of a malicious hacker. (6 marks)

d) Explain **THREE (3)** ethical responsibilities Alex should have followed before conducting any network scanning activities. (6 marks)

Total: [25 marks]

4. A financial institution detected unusual activity in its internal network. The security monitoring system recorded multiple failed login attempts, abnormal network traffic, and unusual system behaviour.

The security team suspects that attackers are attempting to exploit system vulnerabilities and bypass the organisation's intrusion detection system.

Based on the scenario, answer the following questions.

a) List **FIVE (5)** common types of cyberattacks that exploit system vulnerabilities. (5 marks)

b) Explain **FOUR (4)** indicators that may suggest a network intrusion is occurring. (8 marks)

c) List **THREE (3)** types of Intrusion Detection Systems (IDS) used in network security. (3 marks)

d) Explain **TWO (2)** differences between Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). (4 marks)

e) List **FIVE (5)** methods used by ethical hackers to identify vulnerabilities in a system during penetration testing. (5 marks)

Total: [25 marks]

- END OF QUESTIONS -