[CRT07]

UNIVERSITY OF GREATER MAMCHESTER

SCHOOL OF ART & CREATIVE TECHNOLOGIES

BSC (HONS) CYBER SECURITY

SEMESTER 2 EXAMINATION 2024/2025

ETHICAL HACKING AND DIGITAL FORENSICS

MODULE NUMBER: SEC6202

Date: Thursday 15 May 2025 **Time: 14:00 – 16:00**

INSTRUCTIONS TO CANDIDATES:

- This examination consists of **four** questions.
- Candidates must **answer all questions**.
- All questions carry equal marks.
- Individual marks are allocated within each question.
- Answers should be structured in an academic manner, supported by theoretical and practical evidence where applicable.

School of Art & Creative Technologies
B.Sc. Cyber Security
Semester Two Examination 2024-2025
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 1

(a) Critical Analysis of Cybersecurity Risk Concepts

Provide a critical assessment of the distinctions between **risk, threat, and vulnerability** within the context of cybersecurity. Additionally, analyse the difference between **residual risks** and **secondary risks**, highlighting their implications in risk management.

(10 marks)

(b) Business Continuity and Disaster Recovery Assessment

ABC Company has implemented a **Business Continuity (BC) and Disaster Recovery (DR)** plan. On **Monday at 10:00 AM**, an incident occurred. The **Maximum Tolerable Downtime (MTD)** is **7 hours**. The **Recovery Time Objective (RTO)** was achieved in **3 hours and 30 minutes**, while the **Recovery Point Objective (RPO)** requires **3 hours**.

- Critically evaluate the **definitions and significance** of **MTD, RTO, RPO, and SDO (Service Delivery Objective)** in business continuity planning.
- Assess whether the company successfully met its **MTD** and discuss the implications of the given recovery metrics.

(15 marks)

Total 25 marks

Please turn the page

School of Art & Creative Technologies
B.Sc. Cyber Security
Semester Two Examination 2024-2025
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 2

(a) Quantitative Risk Assessment and Financial Analysis

An organisation has an asset valued at £20,880 with an Exposure Factor (EF) of 40%.

Calculate the Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE).

If the implementation of a security safeguard reduced the Annual Rate of Occurrence (ARO) from 4 to 2, and the cost of the safeguard is £20,000, calculate the Return on Security Investment (ROSI).

(15 marks)

(b) Critically evaluate the role of the Metasploit Framework (MSF) in penetration testing. Your answer should include:

1. A clear explanation of what Metasploit is and its core components.
2. The typical workflow used when exploiting vulnerabilities using MSF.
3. An example of a specific module and how it might be used in practice.

(10 marks)

Total 25 marks

Please turn the page

School of Art & Creative Technologies
B.Sc. Cyber Security
Semester Two Examination 2024-2025
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 3

(a) Digital Forensic Memory Analysis

Conduct a **critical evaluation** of **digital forensic memory analysis**, with a focus on key forensic processes, including:

- **Active process identification**
- **Network connections**
- **Connscan**
- **Atom analysis**
- **Clipboard analysis**
- **Crashinfo analysis**

(10 marks)

(b) Digital Forensic Techniques and Legal Compliance

Assess the role of **digital forensic techniques** in cyber investigations, including:

- **Imaging**
- **Digital investigations**
- **Evidence analysis tools**

Explain in detail how these techniques are used to **collect, preserve, and present forensic evidence** in accordance with **legal frameworks**.

(15 marks)

Total 25 marks

Please turn the page

School of Art & Creative Technologies
B.Sc. Cyber Security
Semester Two Examination 2024-2025
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 4

(a) Fuzzing in Python

Fuzz testing (fuzzing) is a software testing technique used to identify vulnerabilities and unexpected behaviours in programs by providing invalid, unexpected, or random data as input.

I. Explain the purpose and benefits of fuzz testing in software development.

II. Describe how fuzz testing can be implemented in Python, mentioning at least one Python library that supports fuzzing.

III. Write a Python script that performs basic fuzz testing on a simple function that processes user input. Ensure the script demonstrates how fuzzing can uncover potential errors.

(15 marks)

(b) Network Attack Analysis

Analyse the **differences** between **SYN flooding attacks** and **SYN spoofing attacks**, detailing their **impact on network security**. Furthermore, discuss the **objectives and mechanisms** of an **HTTP flood attack** and its implications for **cybersecurity defence strategies**.

(10 marks)

Total 25 marks

END OF EXAMINATION