00093

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree/Diploma

in

Information Technology

(Specialized in Cyber Security)

Final Examination

Year 3, Semester I (2023)

IE3022 – Applied Information Assurance

Duration: 2 Hours

May, 2023

Instructions to Candidates:

- This paper has 10 minutes of reading time followed by 2 hours for answering the questions
- This paper contains 4 questions
- Answer all questions in the booklet given.
- The entire exam is worth **100 marks** that contributes to **50%** of the final grade.
- This paper contains 5 pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed
- Exam paper is to be collected back with the answer booklet.

Question 1 **(25 Marks)**

a. Explain the concept of buffer overflow and its potential consequences.

(4 marks)

b. Provide two examples of buffer overflow incidents?

(2 marks)

c. Criticize safeguards used to mitigate BoF?

(5 marks)

d. What are the implications of Common Vulnerability Exposure (CVE) in the cybersecurity landscape?

(4 marks)

e. Analyze the significance of CVE in identifying and managing software vulnerabilities and its impact on the software industry. Provide examples to support your arguments.

(3 marks)

f. What are some of the limitations and criticisms of the OWASP Top 10? Analyze the potential drawbacks of relying solely on the OWASP Top 10 to manage web application security, and suggest alternative approaches to complement or improve upon it.

Your answer should demonstrate a critical understanding of the limitations of the OWASP Top 10, as well as provide thoughtful analysis and relevant examples to support your arguments

(7 marks)

Question 2 **(25 Marks)**

a. List the main objectives of penetration testing.

(4 marks)

b. Compare the approaches of Red Team vs Purple Team?

(5 marks)

c. Criticize the importance of pre-engagement phase in penetration testing?

(10 marks)

d. Google hacking is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Explain the purpose of the following queries.

(6 marks)

i. **"intitle:index.of" site:example.com-**

ii. **"filetype:sql" site:example.com. –**

iii. **"inurl:/wp-admin/" site:example.com–**

Question 3 (25 Marks)

a. What are the goals and objectives of scanning a network?

(3 marks)

b. Recommend mitigations against scanning a network.

(3 marks)

c. List three tools which can be used to scan a network.

(3 marks)

d. Case Study: Digitech's Cybersecurity Breach

Digitech Inc. is a medium-sized e-commerce company that sells products online. They store sensitive customer data, including personal and financial information. In recent years, the company has grown rapidly and has expanded its operations, including its online presence. As a result, they have become a target for cybercriminals looking to steal customer data.

In early 2022, the company discovered that its website had been hacked, and sensitive customer information had been stolen. The company's IT department investigated the breach and found that the hackers had gained access to the company's servers by exploiting a vulnerability in the website's software. The breach had gone undetected for several weeks, during which time the hackers had stolen over 100,000 customer records.

After discovering the breach, the company immediately took action to secure its systems and notified affected customers. The company also worked with law enforcement and cybersecurity experts to investigate the breach and identify the perpetrators. The investigation revealed that the hackers were a group of organized criminals based in Eastern Europe.

The breach had a significant impact on Digitech's reputation and financials, resulting in lost revenue, legal fees, and damage to customer trust. The company learned several lessons from the breach and implemented new cybersecurity measures to prevent similar incidents from occurring in the future.

i. What was the cause of the breach in Digitech's cybersecurity system?

(2 marks)

ii. What was the impact of the breach on Digitech's operations and reputation?

(3 marks)

iii. How did Digitech respond to the breach, and what measures did they take to prevent similar incidents in the future?

(4 marks)

iv. What legal and regulatory implications did the breach have for Digitech?

(3 marks)

v. How can other businesses learn from Digitech's experience and improve their cybersecurity measures?

(4 marks)

Question 4 **(25 Marks)**

a) Define what an exploit is and how it works in the context of Metasploit?

(5 marks)

b) List five reasons why web application security is important in current global economy.

(5 Marks)

c) Provide three examples for Common Web Application attacks?

(3 Marks)

d) Criticize the importance of session management in Web Application Security?

(3 Marks)

e) Name the three types of SQL injection attacks.

(3 Marks)

f) Interpret the following SQL statements.

i. SELECT * FROM Items WHERE item_id = 20; DROP TABLE Items;

ii. SELECT * FROM Users WHERE username = "invalid_user" OR "1"="1" AND password = "invalid_pass" OR "1"="1"

(6 Marks)

End of the Question Paper