

**BOWEN UNIVERSITY IWO, OSUN STATE**  
**COLLEGE OF COMPUTING AND COMMUNICATION STUDIES**  
**CYBERSECURITY PROGRAMME**

**B. Sc. DEGREE SECOND SEMESTER EXAMINATION 2022/2023 SESSION**

**COURSE CODE: CYB 102 COURSE TITLE: FUNDAMENTALS OF CYBERSECURITY I**

**COURSE CREDITS: 3 DATE: SATURDAY 17<sup>TH</sup> JUNE 2023**

**DURATION: 2 HOURS**

**INSTRUCTION: ANSWER ALL QUESTIONS IN SECTIONS A, B, C AND TWO QUESTIONS FROM SECTION D**

---

---

**SECTION A (Objectives: Answer all the questions, each question carries 2 marks)**

1. .... is concerned with making cyberspace safe from threats, namely cyber-threats.  
A. Cybersecurity B. Spamming C. Sniffing D. Phishing
2. A ..... is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks.  
A. Spamming B. Sniffing C. DoS D. Cyberattack
3. .... is an act committed by an intruder by accessing your computer system without your permission..  
A. Spamming B. Sniffing C. Hacking D. Phishing
4. In a typical ..... attack, the hacker infects a web page with a malicious client-side script or program.  
A. XSS B. DoS C. phishing D. spamming
5. .... refers to protecting private information from eyes that should not have access to it.  
A. Authentication B. Confidentiality C. Integrity D. Password
6. .... is a service used to identify a user.  
A. Authentication B. Login C. Sign-in D. Password
7. System carries out the test of itself after a certain period of time again and again is known as .....  
A. Build In Self -Test B. Auto-build Self -Test C. Memory Check Self -Test D. Component Check Self -Test
8. .... security is the sum of the people, processes, and technology implemented within an organization to protect information assets.  
A. Data B. Network C. Information D. Access
9. .... testing is a type of Software Testing that uncovers vulnerabilities of the system, threats, risks in a software application and determines that the data and resources of the system are protected and prevents malicious attacks from possible intruders.  
A. Security B. Cybercrime C. Cyber breach D. Sniffing
10. .... allows software programs to communicate with each other, could also introduce a software vulnerability.  
A. API B. XSS C. CSS D. Adware



**SECTION B (Fill in the Gaps with the correction answers: Answer all the questions, each question carries 2 marks)**

1. .... is the protection of internet-connected systems such as hardware, software and data from cyber-threats.
2. .... is when the attacker used stolen credentials to gain unauthorized access to a user's account.
3. .... advertises malware with uninvited messages, which are automatically generated, clickable advertisements leading you to downloadable malicious software.
4. .... is an explicit attempt by attackers to deny service to intended users of that service.
5. Setting up of early warning system is a countermeasure against .....
6. .... is a service the system uses, together with a user pre-provided identification information such as a password, to determine who uses what of its services.
7. .... risk management is not simply the job of the security team; everyone in the organization has a role to play.
8. .... testing is the simulation of the attack from a malicious hacker.
9. .... break into the systems to steal or destroy data
10. In a ..... Box, tester is authorized to do testing on everything about the network topology and the technology.

**SECTION C (True or False: Answer all the questions, each question carries 2 marks)**

1. We live in a connected world in which we all depend on the Internet and several digital or computer -based system for survival and interactions, hence we are exposed to cyberattacks.
2. Cyberterrorism has capacity to disrupt national infrastructure of a nation and cause colossal loses.
3. Another name for logic bomb is slag code
4. In recovery blocks technique of fault tolerant system, redundant copies are generated using different algorithms only.
5. A cluster is a set of tightly coupled, independent computer systems, connected over a network that behaves as a single system.
6. Encryption protects the communications channel from sniffers.
7. Disaster recovery planning is a team work.
8. A sure way to deal with negligence and security mistakes by the employees is to educate them on why safety matters.
9. Vulnerability scanning is performed with the help of automated software to scan a system to detect the known vulnerability patterns.
10. Many programmers use third-party code libraries, rather than try to write all software from scratch. This can be a real time-saver, but it can also be dangerous if the library has any vulnerabilities.

**SECTION D (Theory Answer any two questions, each question carries 20 marks)**

**Question One**

- |   |                |
|---|----------------|
| a. Why is cloud security important in this present-day computer network infrastructure? | <b>5 marks</b> |
| b. Who are the unskilled script kiddies?  | <b>5 marks</b> |
| c. What is a fault-tolerant system?   | <b>2 marks</b> |
| d. Explain what you understand by Bad Bots and highlight the safety tips against them?  | <b>8 marks</b> |

### **Question Two**

- a. Briefly state what you know about Software Piracy and its effect on Software Developers. **6 marks**
- b. State the focus of cryptography. **4 marks**
- c. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyberattacks, explain. **6 marks**
- d. Explain what you understand by social engineering and state a typical form of it? **4 marks**

### **Question Three**

- a. Discuss visual event monitoring as a hardware access control system. **6 marks**
- b. Who are identity thieves? **4 marks**
- c. How are the passive servers used in a fault tolerant cluster? **4 marks**
- d. What is a security policy? **2 marks**
- e. State what should be kept in mind when writing a security policy. **4 marks**

### **Question Four**

- a. Identify the key elements of Disaster Recovery Planning. **6 marks**
- b. List the six (6) basic principles of security testing. **6 marks**
- c. State the purpose of ethical hacking. **2 marks**
- d. Explain what you understand by Software Vulnerability? **2 marks**
- e. Highlight how a Software Vulnerability Works. **4 marks**