LAIKIPIA UNIVERSITY

UNIVERSITY EXAMINATIONS

1ST SEMESTER 2022/2023 ACADEMIC YEAR

THIRD YEAR EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE (ICT)

BICT 412: INFORMATION SECURITY AUDIT AND ASSURANCE

STREAM: R ***TIME: 2 HRS***

DAY: TUESDAY [8.30AM – 10.30AM] ***DATE: 06/12/2022***

THIS QUESTION PAPER CONSISTS OF FIVE (5) PAGES

PLEASE DO NOT OPEN UNTIL THE INVIGILATOR SAYS SO.

SECTION A (30 marks)

INSTRUCTIONS: - Answer ALL Questions in this section

QUESTION ONE (40 Marks)

(a) Read the following article from a local daily and answer the questions that follow

From the ongoing debate on mobile banking involving Safaricom's M-Pesa service and Zain's proposed service, one can draw parallels with concerns raised elsewhere about the security of these new technological phenomena. Shocking revelations of security breaches and the vulnerabilities of mobile communications is not encouraging enough to provide a complete assurance about the security of customers' cash. For instance, technology experts have recently detected a new malicious programme that infected customers of an Indonesian telecom operator. This SMS-based programme targeted the SMS credit transfer service with instructions to transfer part of the money in the customer's account to the perpetrator's account.

i). What is a security breach and how does it differ from a security violation? (3 marks)

ii). What are vulnerabilities and how do they differ from exploits? (3 marks)

iii). Identify an exploit from the article (1 mark)

(b) For each of the following Human Threats-Sources, state any TWO Motivations and TWO Threat Actions. (6 marks)

Threat Source	Motivation	Threat action
i) Hacker /cracker		
ii) Terrorist		
iii) Industrial espionage (companies, foreign governments, other government interests)		
iv) Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)		

(c)

(i) Explain the meaning of the terms Ethical Hacking and Penetration testing. (4 marks)

(ii) Identify and distinguish between the three penetration testing methodologies (4 marks)

(d)

(i) Outline the FIVE stages that constitute the anatomy of an attack (5 marks)

(ii) Explain the role of law and ethics in information security (4 marks)

SECTION B (40 Marks)

Answer ANY TWO Questions in this section

QUESTION TWO (20 marks)

(a) In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC.

(i) In the context of information security, define the term *"risk"* (3 marks)

(ii) Describe FOUR information-gathering techniques that you would use to gather information relevant to the IT system within its operational boundary: (7 marks)

(b)

i). Explain the TWO components that constitute vulnerability assessment in qualitative risk assessment for IT systems (4 marks)

ii). Explain what a threat assessment entails (4 marks)

iii). What is Vulnerability Assessment? (2 marks)

QUESTION THREE (20 marks)

(a) The legal system faces challenges in offering protection from the misuse of computer technology. Identify and explain any FIVE such challenges (10 marks)

(b) With regard to the design of security architecture explain the following guiding principles and state their roles in the security architecture

(i) Defense in depth (2 marks)
(ii) The Separation of Duties (3 marks)
(iii) The Principle of Least Privilege (3 marks)
(iv) Data classification (2 marks)

QUESTION FOUR (20 marks)

(a) Distinguish between eavesdropping and snooping. (4 marks)

(b)

i). What is social engineering? (2 marks)

ii). Consider the attack dialog below and identify the human behavior vulnerability exploited by the attacker in the dialogue? (1 mark)

Attacker: *"Hi Ms. Lee, this is Steven from the IS Department. I've found a virus stuck in your mailbox and would like to help you remove it. Can I have the password to your email? "*

Ms. Lee (the secretary): *"A virus? That's terrible. My password is the magnum. Please help me clean it up"*

iii). Identify any other FOUR human behavior vulnerabilities exploited by social engineers (2 marks)

(c)Read the following article from an internet user and answer the questions that follow

I'm very computer illiterate. We got high-speed net with Verizon and we downloaded the security system in and it found so many spyware things on different sites I was on. The list was so long. We deleted all of them. WOW, Thank God I never used a credit card online. I was always afraid to because I heard so much about this theft. But, one of the spywares came on Web MD when I used it. Even Web MD?

i). What is spyware? (1 mark)

ii). Explain the danger posed by spyware to online shoppers. (2 marks)

(d)For each of the threat types listed state any TWO prevention measures you can take

i) Backdoor (2 marks)

ii) Denial of service attack (2 marks)

iii) Password guessing (2 marks)

iv) Buffer overflow (2 marks)

QUESTION FIVE (20 marks)

ACME is an insurance and investment company that grew from a mainframe-only shop ten years ago to now integrating a client-server model. The integration of other architectural components like data, applications, and infrastructure came after expanding and integrating different

applications and systems in the client-server environment. Security was not an integral component from an architectural perspective. As such, many security components were either missing or lacking in security design and implementation, such as IDS, DMZ, VPN implementation, web architecture, the system builds, patch management, hardware and software directions, data classifications, encryption policy and standards, firewalls design, operating systems security, etc.

(a) Explain the roles of the following in network security

(i) IDS (3 marks)

(ii) DMZ (3 marks)

(iii) VPN (3 marks)

(b) Explain how the firewall limits the functionality of the IDS (4 marks)

(c) You are asked to configure a DMZ in your company network with the web server as the gateway or the front door to the company network. Explain how you will do this (3 marks)

(d)

(i) What is a Security perimeter? (1 mark)

(ii) Usually, user password or password file is essential to intruder describe TWO methods you can use to protect password file. (3 marks)