Name: **Enrolment No:**	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2022

Course: Introduction to Cyber Security **Semester: I**
Program: MCA **Time: 03 hrs.**
Course Code: CSCS7006P **Max. Marks: 100**

Instructions: Attempt all Questions

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Illustrate the distinguishing characteristics of viruses written in interpreted languages.	**4**	**CO1**
Q 2	State the disadvantage of using the same secret key K in all issued phone cards and suggest a way around this.	**4**	**CO2**
Q 3	Suppose A and B are two frames in a browser that are loaded from different origins. Why is it a reasonable security policy to allow A to navigate B to another origin based only on whether the display area of A contains the display area of B and A has control over that area?	**4**	**CO3**
Q 4	A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do? List major risks associated with this scenario.	**4**	**CO4**
Q 5	Demonstrate the use of latency in anonymous communications. What limits or costs does low latency impose?	**4**	**CO1**

SECTION B
(4Qx10M= 40 Marks)

Q 6	You're sitting in a coffee shop enjoying a latte and doing some relaxing computer security reading at http://awesome-security-stuff.com. You're connected on the coffee shop's Wi-Fi network. You notice that each article has a Facebook Like button, loaded as such: 	**10**	**CO2**

	allowing you to indicate on Facebook that you enjoyed this article. If Facebook wanted to, could it track what articles you are visiting, if you don't click on the Like button? Justify your answer.		

Q 7	Consider a Web site xyz.com that implements a phone dialer. When the user enters a phone number to call, the browser opens a new window to xyz.com/call.html containing the following JavaScript that defines a postMessage event listener:
	
	function receiveMessage (event) {
	// event.data is a phone number from sender
	initiatePhoneCallTo(event.data)
	}
	window.addEventListener('message', receiveMessage)
	
	The parent page then sends a postMessage to this window to initiate the call. This activates the receiveMessage function which makes the call. Explain how an attacker website can cause a visitor to initiate phone calls to arbitrary phone numbers. Assume the visitor is logged in to his/her xyz.com account but does not have xyz.com open in a window.
		10	**CO3**

	OR		
Q 7	A rapidly growing online crime is phishing, in which victims are lured by an e-mail to log on to a website that appears genuine but that steals their passwords. You have been hired by a bank to help them harden their online banking service against phishing attacks. Briefly explain the strengths and weaknesses of the following four possible countermeasures: 1. SSL/TLS client certificates issued to each customer. 2. A handheld password calculator issued to each customer. 3. Displaying a unique picture to each customer during the login process. 4. Requiring that large payments, or payments to new recipients, be authorized by telephone or SMS as well as online.	**10**	**CO3**
Q 8	Request: GET /view? Filename=hello.txt HTTP/1.1 Host: localhost:4000 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) Response: HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Date: Tue, 10 Dec 2019 00:00:00 GMT Hello, world!	**10**	**CO4**

	There is a glaring security vulnerability in this server. What is the issue? How could the issue be fixed?		
Q 9	Name and briefly explain four techniques that the designers of C compilers and operating system kernels can implement to reduce the risk of stack-based buffer-overflow attacks.	**10**	**CO1**
SECTION-C (2Qx20M=40 Marks)			

Q 10	The route handler below implements the "delete account" functionality which is common on most websites. This allows the user to completely delete their account. The actual deletion logic is in the deleteAccount function, which is not shown here. To confirm that the request came from the actual user, the request must include the user's password which is validated before the account is deleted.
	
	app.get('/delete', (req, res) => {
	const {username, password} = req.body
	if (!isAuthValid(username, password)) {
	res.send('Invalid username or password.')
	}
	deleteAccount(username)
	res.send('Account deleted.')
	})
	
	There are two severe security issues in the route handler. Identify the two issues.
		20	**CO2**

Q 11	You're a web developer working for a national newspaper. The product manager informs you that a decision has been made to ban users of the Brave web browser because of its ad-blocking capabilities which are negatively affecting revenue. It is your responsibility to implement this functionality. Brave uses the same User-Agent header value as the Chrome browser, so it's not possible to distinguish Brave users by merely looking at this header value. Propose a fingerprinting method you could use to distinguish Brave users from other browser users. It's okay if your method has some false positives if it recognizes all Brave users.	**20**	**CO3**
	OR		
Q 11	You have been hired by a company which is bidding to take over the National Lottery when Camelot's franchise expires, and your responsibility is the security architecture. State the security policy you	**20**	**CO3**

	would recommend and outline the mechanisms you would implement to enforce it.		