



NAME OF THE SCHOOL
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: F1+TF1

Programme Name & Branch : B.Tech
Course Code and Course Name : BCSE410L - Cyber Security
Faculty Name(s) : Common for all
Class Number(s) : Common for all
Date of Examination : 18.10.2024
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

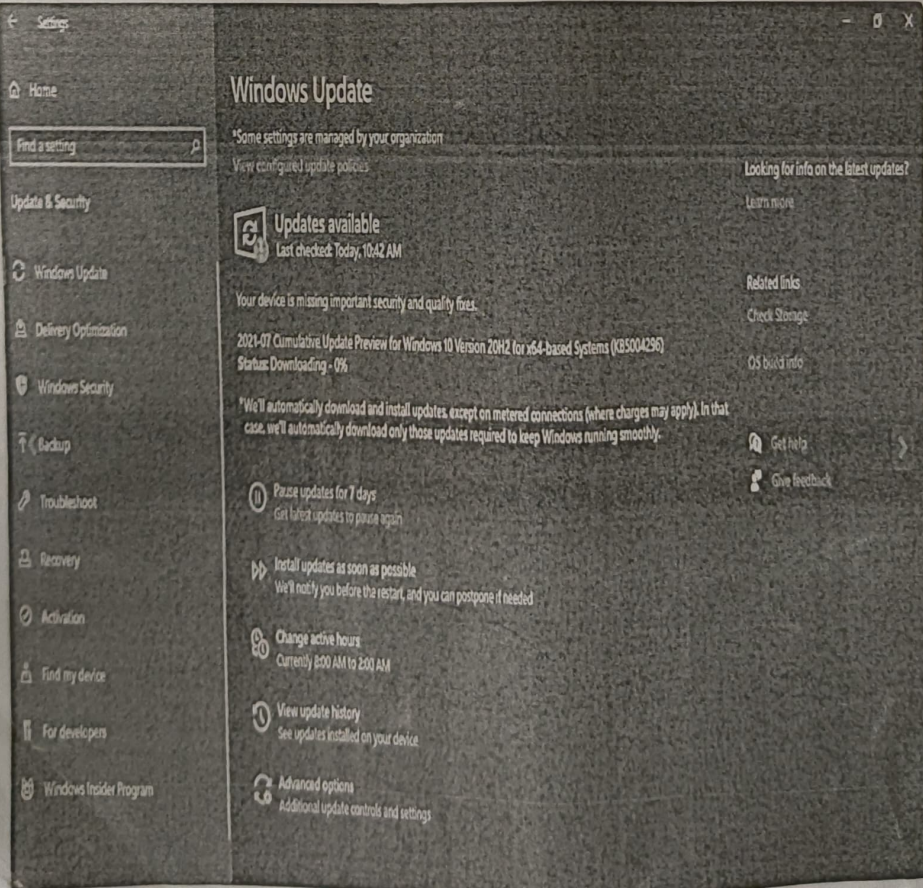
- Answer All Questions
- M - Max mark; CO - Course Outcome; BL - Blooms Taxonomy Level (1 - Remember, 2 - Understand, 3 - Apply, 4 - Analyse, 5 - Evaluate, 6 - Create)
- Course Outcomes
CO2: Identify the emerging vulnerabilities and attacks and countermeasures in cyber-physical system
CO3: Comprehend the need for ethical hacking to minimize the security risk.

Q. No.	Question	Marks	CO	BL
1	Alice has received a password reset email for her Instagram account from the genuine sender. After she resets her password, suddenly she finds in her Instagram account unrelated pictures and stories are posted. Fortunately, the password is not reset again later. What was the attack happened and how? How Alice should react for this attack? As a cyber security personnel, what are the recommendations you will give to Alice so that this attack not to happen again?	10	2	4
2	Assume you are appointed as a cyber security admin in a software company. You have to ensure the strength of employee passwords. The following guidelines are recommended by the Security manager. The password ❖ length should be more than 8 ❖ should have at least one capital letter ❖ should have at least one digit ❖ should have at least one special character from the set { @, #, \$, %, &, * } Write a pseudo algorithm to implement these guidelines while the employee signup and/or change his/her password.	10	2	4
3	Hikvision (Hangzhou Hikvision Digital Technology) is a Chinese state-owned manufacturer of video surveillance equipment. Their customers span over 100 countries (including the United States, despite the FCC labelling Hikvision "an unacceptable risk to U.S. national security" in 2019). During 2021 fall, Hikvision cameras was reported CVE-2021-36260 to the world. The exploit was given a "critical" 9.8 out of 10 rating by NIST. Despite the severity of the vulnerability, nearly 80,000 affected devices remain compromised. The extent of the damage done already is unclear. The authors of the report could only speculate that "Chinese threat groups such as MISSION2025/APT41, APT10 and its affiliates, as well as unknown Russian threat actor groups could	10	3	5



NAME OF THE SCHOOL
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: F1+TF1

	potentially exploit vulnerabilities in these devices to fulfil their motives (which may include specific geo-political considerations).” What are the attacks involved in this exploit and what are the vulnerabilities existed? Which is played a major role and how? Recommend some appropriate reactive and proactive measures for these vulnerabilities.			
4	Demonstrate how MAC spoofing can be used to host a) Man-in-the-middle attack b) ARP spoofing attack	5 5	3	4
5	a) There are two commands commonly used to test null sessions (in 192.30.20.10): net use \\192.30.20.10\IPC\$ "" /user: net use \\192.30.20.10\IPC\$ what is the difference? b) When I try to update my Windows 10 OS the following message popped up. “Windows Update error (Your device is missing important security and quality fixes)” Cumulative update preview for windows 10 version 20H2 for x64 - based systems (KB5004296)	5		
			3	4
	State the reasons for this error.	5		