Darshan Institute of Engineering and Technology

Bachelor of Technology – Semester VI

Mid Semester Examination: II – MARCH 2024

Course Code	: 2101CS632	**Exam Date**	: 07/03/2024
Course Name	: Cyber Security	**Total Marks**	: 30
Time	: 08:15 am to 09:30 am	**Enrollment No.**	:_____

Instructions

1. Attempt **all** the questions.
2. Figure to the right indicate maximum **marks**.
3. Don't do any kind of **rough** work or **calculation** in Question Paper.
4. **Make** suitable assumptions whenever necessary.
5. The text to the right-side of the marks indicates the Bloom's Level **(BL*)** of the question followed by the Course Outcome**(CO).**
   i.e. R: Remembrance, **U:** Understanding, **A:** Application, **N:** Analyze, **E:** Evaluate, **C:** Create.

Course Outcomes (COs)	At the end of this course, students will be able to: CO 1: Describe Cyber Crime and Offense CO 2: Explain on Cyber Attacks and Techniques CO 3: Discuss Cyberlaw and Amendment of IT Act CO 4: Perform system Vulnerability and Web Vulnerability scanner Tools CO 5: Classify the functionality of antivirus and Firewalls

Q. No.		Question	Marks	BL*	CO
Q. 1	(A)	Define DOS & DDOS using an example.	3	R	CO2
Q. 1	(B)	Consider a situation where a hacker has attacked an organization through the vulnerability of BUFFER OVERFLOW. Explain BUFFER OVERFLOW using the example of Heart Bleed. **OR** You are a legal advisor for a technology company operating in a country with laws governing electronic communications and cybercrime. The company provides a social media platform where users can share content and interact with each other. Recently, there has been an incident involving the misuse of the platform, resulting in the dissemination of offensive and defamatory content targeting certain individuals and communities. Describe what the section 66E, 66F and 67 of IT ACT.	3	U	CO2
Q. 1	(C)	You are a cybersecurity analyst tasked with conducting a penetration test on a target system (Victim Machine) to assess its security posture. The target system is known to have multiple open ports, and your objective is to exploit one of these ports to gain remote access and deliver a shell named "fail.txt" to the Victim Machine using netcat.	4	A	CO4

		Given the scenario, Carry out the steps you would take to identify open ports on the Victim Machine and subsequently deliver the "fail.txt" shell using netcat. Use the commands and techniques you would employ to achieve this objective while minimizing the risk of detection. **OR**			
	(C)	As a cybersecurity analyst, you discover a situation where an attacker is attempting to launch a Denial of Service (DoS) attack against a victim system by sending 1000 UDP packets with a spoofed source IP address of 1.1.1.1 using the hping3 tool. Given this scenario, Solve and demonstrate the command syntax the attacker likely used to execute the DoS attack using hping3?	**4**	**A**	**CO2**
Q. 2	**(A)**	Define PORTS and also write the use of ports 22, 25 and 21.	**3**	**R**	**CO4**
Q. 2	**(B)**	How would you threat model around SQL Injection Vulnerabilities in an organisation. **OR**	**7**	**U**	**CO2**
	(B)	You are the cybersecurity manager at a large e-commerce company that relies heavily on secure online transactions. Recently, there has been a breach in which attackers successfully intercepted sensitive customer data during transmission. As part of your investigation, you discover that the SSL/TLS certificates used to secure the company's website were compromised. In light of this breach, indicate how the Certifying Authority helps in securing the communication between your users and the company?	**7**	**U**	**CO2**
Q. 3	**(A)**	Define GDPR, HIPAA and PCIDSS and where is it used?	**3**	**R**	**CO3**
Q. 3	**(B)**	Explain the XSS with an example. **OR**	**3**	**U**	**CO4**
	(B)	Explain the INSECURE DESERIALISATION with an example.	**3**	**U**	**CO4**
Q. 3	**(C)**	Analyse the code and articulate each line of it	**4**	**A**	**CO3**

```
const jwt = require('jsonwebtoken');
const secretKey = 'my_secret_key';
const payload = {
   userId: 123456,
   username: 'example_user'
};
const token = jwt.sign(payload, secretKey, { expiresIn: '1h' });
console.log ('Generated Token:', token);
```

OR

Analyse this code and find the Vulnerability in it and write how will you exploit it.

```
#include <stdio.h>
#include <string.h>

void greet(char *name)
 {
   char greetings[10];
   strcpy(greetings, name);
   printf("Hello, %s!\n", greetings);
}

int main()
{
   char username[20];
   printf("Enter your name: ");
   scanf("%s", username);
   greet(username);
   return 0;
}
```

(C) **4** **A** **CO2**

* * * * * * * * * * *