Marks: 2

Sl. No.	Module	Question
1	1	Is there a difference between a cybercrime and cyberfraud? Explain.
2		How do we classify cybercrimes? Explain each one briefly.
3		Explain the difference between active and passive attack. Provide examples.
4		Explain social engineering.
5		What is cyber stalking? Is it a crime according to Indian IT Act?
6		Explain cyberwarfare.
7		Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number. - Classify it as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
8		Henry spoofs Julie's IP address to gain access to her computer. - Classify it as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
9		Write some tips to be secured in a cyber cafe from cyber crimes.
10		Differentiate between vishing and smishing attack.
11		Explain the significance of Confidentiality in the CIA Triad.
12		What is Availability in the context of the CIA Triad?
13		Explain the significance of Confidentiality in the CIA Triad.
14		Name a threat that affects Integrity in cybersecurity. - Explain in brief.
15		How does a Denial-of-Service (DoS) attack impact the CIA Triad?
16		How does multi-factor authentication (MFA) contribute to the CIA Triad?
17		What are the challenges in maintaining the CIA Triad in cloud computing environments?
18	2	What is Cryptography?
19		What is symmetric key encryption?
20		What is Asymmetric key encryption?
21		Distinguise between Symmetric key encryption and Asymmetric key encryption?
22		What is the nimber of rounds in DES?
23		What is the round-key size in DES?
24		How does cryptography help in achieving non-repudiation?
25		What is the significance of using cryptographic techniques for message authentication?
26		What are the key components of a digital signature?
27		Explain the purpose of a Certificate Authority (CA).

28		Why is PKI important for secure communication?
29		Why is SHA-256 considered more secure than MD5?
30		What is a digital signature?
31		What is a public-key certificate?
32		What are two common techniques used to protect a password file?
33		What is an access right?
34		Discuss about pseudorandom numbers.
35	3	What is Access Control?
36		Difference between authentication and authorization.
37		Discuss about multifactor authentication (MFA).
38		Explain the term “permission” in access control.
39		Define action in Role-based access control (RBAC)
40		Write the different key entities of RBAC.
41		What is privilege escalation?
42		Give one example of a privilege escalation attack.
43		Differentiate between vertical and horizontal privilege escalation.
44		Name two common vulnerabilities that lead to privilege escalation.
45		How can privilege escalation be prevented?
46		What is the impact of privilege escalation on system security?
47		What are two common techniques used to protect a password file?
48		In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.
49		In general terms, what are four means of authenticating a user’s identity?
50		List and briefly describe the principal physical characteristics used for biometric identification.
51		Explain the difference between a simple memory card and a smart card.
52	4	What is Phishing?
53		State the purpose of Proxy server.
54		What do you understand by Passwordcraking?
55		State the role of hardware and software keylogger.
56		What do you unstand by SQL injection attack?
57		What is DDOS attack?
58		How does browser interoperate with a web proxy when SSL is being used?
59		What protocols comprise TLS?

60		What services are provided by TLS Record Protocol?
61		What is the differnce between TLS Connection and TLS session?
62		What is the significance of Secure flag?
63		What is the difference between common status code 301 & 302?
64		What is SQL injection?
65		What is the impact of an SQL injection vulnerability
66		How can code be executed because someone prepends his input with a quote character?
67		Is SQL injection a new vulnerability?
68		Can every single Web application be vulnerable to SQL injection?
69	5	What is ethical hacking
70		Explain the difference between ethical hacking and malicious hacking
71		Define penetration testing
72		Define the term “social engineering toolkit” (SET)
73		Explain the concept of a security baseline
74		What do malicious hackers do?
75		Define the term “security architecture” and its components
76		Define the term “security through obscurity” and its limitation
77		Define the term “firewalking” in the context of ethical hacking
78		The C shell does not treat the IFS variable as a special variable. How might this affect the loadmodule exploitation?
79		Can the UNIX Bourne shell variable HOME be used to compromise a system? If so, how?
80		Why might an analyst care how similar two vulnerabilities are?
81		The NRL classification scheme has three axes: genesis, time of introduction, and location. Name two other axes that would be of interest to an analyst. Justify your answer.
82		In the NRL classification scheme for the “genesis” axis, how might one determine whether a vulnerability is “malicious” or “nonmalicious”?
83		In the NRL classification scheme for the “genesis” axis, can the classes “Trojan horse” and “covert channel” overlap? Justify your answer.
84		Consider the first example in Section 23.4.1. Why does the router not save time by opening a connection to the destination host before the pending connection completes its three-way handshake?
85		The Linux system uses the SYN cookie approach. How does the system recover the MSS from the ACK’s sequence number?
86	6	What are the primary characteristics of Trojans and how do they differ from worms

87		Define malware and classify it based on its behaviour.
88		What are the key characteristics of a rootkit?
89		Differentiate between zero-day malware and metamorphic malware.
90		Explain how YARA rules help in signature-based detection.
91		Discuss the limitations of antivirus software in detecting advanced malware.
92		Identify the differences between spyware and adware.
93		What is heuristic-based malware detection?
94		Consider the following fragment: legitimate code if data is Friday the 13th; crash_computer(); legitimate code What type of malware is this?
95		State two advantages of dynamic malware analysis over static analysis.
96		What is a "logic bomb"?
97		What is a "drive-by-download" and how does it differ from a worm?
98		What is the difference between machine executable and macro viruses?
99		What is the difference between a backdoor, a bot, a keylogger, Can they all be present in the same malware?

100		What means can a worm use to access remote systems to propagate?

Marks: 5

Sl. No.	Module	Question
1	1	Consider a financial report publishing system used to produce reports for various Organizations. (a) Give an example of a type of publication in which confidentiality of the stored data is the most important requirement. (b) Give an example of a type of publication in which data integrity is the most important requirement. (c) Give an example in which system availability is the most important requirement.
2		Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.
3		Show that the three security services—confidentiality, integrity, and availability— are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation.
4		The aphorism “security through obscurity” suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.
5		Explain: (i) Cybersquatting (ii) Cyberspace (iii) Cyberwarfare (iv) Cyberpunk (v) Hackers
6		List and explain preventive measures against cybercrime.
7		A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?
8		Explain how Botnets can be used as a fuel to cybercrime.
9		How do laws protecting privacy impact the ability of system administrators to monitor user activity?
10		Explain information security objectives with diagram.
11		Write a note on objectives of Information Technology Act , 2000 in India.

12		Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof. a. John copies Mary's homework. b. Paul crashes Linda's system. c. Carol changes the amount of Angelo's check from $100 to $1,000. d. Gina forges Roger's signature on a deed. e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
13		Differentiate between active attack and passive attack.
14		Write a short note on Cyberstalking.
15	2	Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is full of surprises".
16		Use the Playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.
17		Define the Diffie-Hellman protocol and its purpose.
18		To understand the security of the RSA algorithm, find d if you know that e = 17 and n = 187.
19		Define the man-in-middle attack with an example.
20		How does cryptographic authentication contribute to ensuring data integrity and preventing unauthorized modifications?
21		How does a digital signature work? Explain the process step by step with an example.
22		Explain the process of how a message is converted into a hash value using SHA-256.
23		Explain how digital certificates are used in HTTPS to secure web communication.
24		Explain the role of PRNG in key generation for encryption algorithms. How does it enhance security?
25		List three approaches to message authentication.
26		In the context of access control, what is the difference between a subject and an object?
27		In the context of biometric user authentication, explain the terms, enrollment, verification, and identification
28		Discuss about pseudorandom numbers and it's significance.
29	3	Briefly discuss about Mandatory access control (MAC)
30		"It controls the access rights of users or processes against the resources of the system"- is correct for which model of access control and why.
31		Discuss about advantage and disadvantage of Mandatory access control (MAC).
32		Discuss about advantage and disadvantage of Discretionary access control (DAC).
33		What are the key differences between vertical and horizontal privilege escalation?

34		How can an attacker exploit weak file permissions to gain elevated privileges?
35		What is the significance of SUID binaries, and how can they be misused for privilege escalation?
36		What risks are associated with writable /etc/sudoers files, and how can they be exploited?
37		How does a weakly configured PATH variable lead to privilege escalation?
38		Why should a time-based authentication system invalidate the current password on a successful authentication?
39		Let the expected time required to guess a password be T. Then T is a maximum when the selection of any of a set of possible passwords is equiprobable. Prove this theorm.
40		What complications arise in dynamic keystroke monitoring as a biometric authentication mechanism when the user's keystrokes are sent over the Internet? In particular, what characteristics of the keystroke sequences are valid, and which ones are distorted by the network?
41		The example describing S/Key stated that "for MD4 and MD5, dictionary attacks are not a threat provided the seeds are chosen randomly." Why? How realistic is this assumption?
42		Classify the following proposed passwords as good choices or poor choices, and justify your reasoning. a. Mary b. go2work c. cat&dog d. 3.1515pi
43	4	Why are stack-based buffer overflows generally easier to exploit than heap-based overflows?
44		What is Buffer Overflow Vulnerabilities? Explain with suitable example.
45		Elaborate the techniques to minimise the Buffer overflow attack.
46		Write a short note on Malware.
47		Explain how a Backdoor work?
48		List and briefly define the parameters that define a TLS Session State.
49		List and briefly define the parameters that define a TLS Session Connection.
50		What are the steps involved in TLS REcord Protocol Transmission?
51		What standard "Signature" in an applications behavior can be used to identify most instances of XSS Vulnerabilities?
52		Name three possible attack payloads for XSS exploits.
53		I observe a weird behavior in a Web application when I insert a single quote in the search functionality. However, I don't get any errors. Can the application be exploited?

54		Can every single Web application be vulnerable to SQL injection?
55		What is the main reason for the presence of SQL injection vulnerabilities?
56		Is it necessary to always start the attack by fingerprinting the database?
57	5	What are the challenges in creating an Enterprise Information Security Architecture (EISA)?
58		Describe the steps involved in a typical threat hunting process
59		How do you approach incident response in the case of a security breach?
60		Describe the steps involved in a typical brute force attack.
61		What is the role of a virtual private network (VPN) in network security?
62		Describe the steps involved in a typical malware analysis.
63		What are the different threat modeling methodologies?
64		Classify the vulnerabilities in Exercise 1 using the PA model. Assume that the classification is for the implementation level. Justify your answer.
65		A common error on UNIX systems occurs during the configuration of bind. Classify this vulnerability using the RISOS model and justify your answer.
66		An attacker breaks into a web server running on a Windows 2000-based system. He concludes that Windows 10 has poor security features. Is his conclusion reasonable? Why or why not?
67		Identify and describe additional security weaknesses that could be exploited in a computer system. Provide explanations for each identified vulnerability and their potential impact.
68		Assume that an attacker has found a technique for sending packets through the outer firewall to the DMZ without the packets being checked. How can the attacker arrange for a packet to be sent to the WWW server in the DMZ without the firewall checking it?
69		The organization of the network provides a DMZ to which the public has controlled access. Explain how the principle of least privilege is relevant to the creation of the DMZ. Justify your answer.
70		A security analyst wishes to deploy intrusion detection monitors. Where should the intrusion detection monitors be placed in the network's topology, and why?
71	6	Discuss the limitations of static analysis and how attackers bypass it.
72		Explain how command-and-control (C2) servers facilitate malware operations.

73		Apply memory forensics to detect a malware-infected process in a system.
74		Create a comparative table showing differences between traditional and next-gen antivirus.
75		Compare different malware persistence techniques used by attackers.
76		Evaluate why behavioral detection techniques are necessary for APTs.
77		Create a flowchart for the execution process of ransomware.
78		Evaluate the strengths and weaknesses of behavioral detection techniques.
79		Compare and contrast static and dynamic malware analysis with examples.
80		Analyze the role of artificial intelligence in malware detection.

Marks: 10

Sl. No.	Module	Question

1	1	For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers. a. A student maintaining a blog to post public information. b. An examination section of a university that is managing sensitive information about exam papers. c. An information system in a pathological laboratory maintaining the patient's data. d. A student information system used for maintaining student data in a university that contains both personal, academic information and routine administrative information (not privacy related). Assess the impact for the two data sets separately and the information system as a whole. e. A University library contains a library management system which controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.
2		Consider a company whose operations are housed in two buildings on the same property; one building is headquarters, the other building contains network and computer services. The property is physically protected by a fence around the perimeter, and the only entrance to the property is through this fenced perimeter. In addition to the perimeter fence, physical security consists of a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services' LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes.
3		Consider a very high-assurance system developed for the military. The system has a set of specifications, and both the design and implementation have been proven to satisfy the specifications. What questions should school administrators ask when deciding whether to purchase such a system for their school's use?
4		Is it possible to design and implement a system in which no assumptions about trust are made? Why or why not?

5		Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad. a. The electronic mail sending and receiving programs are disabled. b. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.) c. The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.
6		Computer viruses are programs that, among other actions, can delete files without a user's permission. A U.S. legislator wrote a law banning the deletion of any files from computer disks. What was the problem with this law from a computer security point of view? Specifically, state which security service would have been affected if the law had been passed.
7		The president of a large software development company has become concerned about competitors learning proprietary information. He is determined to stop them. Part of his security mechanism is to require all employees to report any contact with employees of the company's competitors, even if it is purely social. Do you believe this will have the desired effect? Why or why not?
8		An organization makes each lead system administrator responsible for the security of the system he or she runs. However, the management determines what programs are to be on the system and how they are to be configured. a. Describe the security problem(s) that this division of power would create. b. How would you fix them?
9		Users often bring in programs or download programs from the Internet. Give an example of a site for which the benefits of allowing users to do this outweigh the dangers. Then give an example of a site for which the dangers of allowing users to do this outweigh the benefits.

10		Identify mechanisms for implementing the following. State what policy or policies they might be enforcing. a. A password-changing program will reject passwords that are less than five characters long or that are found in the dictionary. b. Only students in a computer science class will be given accounts on the department's computer system. c. The login program will disallow logins of any students who enter their passwords incorrectly three times. d. The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it. e. When World Wide Web traffic climbs to more than 80% of the network's capacity, systems will disallow any further communications to or from Web servers. f. Annie, a systems analyst, will be able to detect a student using a program to scan her system for vulnerabilities. g. A program used to submit homework will turn itself off just after the due date.
11	2	In AES, the size of the block is the same as the size of the round key (128 bits); in DES, the size of the block is 64 bits, but the size of the round key is only 48 bits. What are the advantages and disadvantages of AES over DES with respect to this difference?
12		Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can use the chosen-ciphertext attack if she has access to Bob's computer to find the plaintext.
13		In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 5. a) What is the value of the symmetric key? b) What is the value of R1 and R2?
14		In the Diffie-Hellman protocol, what happens if x and y have the same value, that is, Alice and Bob have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.
15		Discuss how message authentication codes (MACs) and digital signatures contribute to integrity and authenticity. Compare their working mechanisms with appropriate diagrams.
16		A message M = "HELLO" is given. Convert this message into its ASCII representation, and then compute its MD5 hash (simplified steps). Explain how the hash function ensures integrity.
17		Explain the differences between MD5 and SHA-256 in terms of security, output size, and collision resistance. Demonstrate with a simple hash calculation for a given input.
18		Is the identity function, which outputs its own input, a good cryptographic checksum function? Why or why not?
19		Is the sum program, which exclusive or's all words in its input to generate a one-word output, a good cryptographic checksum function? Why or why not?
20		Prove the fundamental laws of modular arithmetic: a. (a + b) mod n = (a mod n + b mod n) mod n b. ab mod n = ((a mod n)(b mod n)) mod n

21	3	Analyze the role of vulnerabilities in operating systems and applications in enabling privilege escalation. How can organizations prevent such attacks?
22		Describe the impact of privilege escalation attacks on cybersecurity. Discuss detection and prevention strategies in detail.
23		How can sudoedit misconfigurations lead to privilege escalation, and how can organizations prevent this?
24		Discuss about basic needs of access control is a security strategy.
25		“Login credentials” is a relevant to which of the following categories justify. –identification, authentication, authorization of users and entities.
26		Briefly discuss about components of Access Control.
27		Write about the different models of access control.
28		A system allows the user to choose a password with a length of one to eight characters, inclusive. Assume that 10,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of having been guessed. Determine the expected time to meet this probability under each of the following conditions. a. Password characters may be any ASCII characters from 1 to 127, inclusive. b. Password characters may be any alphanumeric characters (“A” through “Z,” “a” through “z,” and “0” through “9”). c. Password characters must be digits.
29		A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions. a. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system. b. The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends a “yes” or “no” to the system indicating whether or not the user has been authenticated.

30		The designers of the UNIX password algorithm used a 12-bit salt to perturb the first and third sets of 12 entries in the E-table of the UNIX hashing function (the DES). Consider a system with 224 users. Assume that each user is assigned a salt from a uniform random distribution and that anyone can read the password hashes and salts for the users. a. What is the expected time to find all users' passwords using a dictionary attack? b. Assume that eight more characters were added to the password and that the DES algorithm was changed so as to use all 16 password characters. What would be the expected time to find all users' passwords using a dictionary attack?
31	4	Explain various types of Buffer Overflow with suitable example. How such types attacks can be mitigated?
32		Explain various steps of SQL injection attack. Elaborate how the method of preventing SQL injection attack.
33		Elaborate the steps to prevent DoS/DDoS attack.
34		Explain various types of DOS attacks
35		What three defensive messures can be used to prevent javascript hijacking attacks and what main precondition must exist to enable a CSRF attack against a sensetive function of an application?
36		" We are safe from clickjacking attacks, because we dont use frames". What, if anything, is wrong with the statement? Explain.
37		You discover an application function where the contents of a query string parameters are inerted into the location header in an HTTP redirect. What types of attack can this behaviour potentialy be exploited to perform?
38		Derive the code that contains JavaScript Malware that automatically reconfigures your company's routers or firewalls, from the inside, opening the internal network up to the whole world.
39		How exploit process works using Javascript Malware for an unassuming web surfer.
40		Derive the code for the attacker wanting to update the demilitarized zone (DMZ) setting in the device, and pointing all network traffic to the victim's machine.
41	5	Analyze a case study of 'The Marriott hotel chain cyber breach' that mentions different phases of ethical hacking
42		Elaborate on a case study where Denial of Service is used as an attack vector
43		Elaborate on a case study where Phishing is used as an attack vector
44		Analyze a case study of 'The ChatGPT data leak case' that mentions different phases of ethical hacking
45		Analyze a case study of an 'Aadhaar data breach' that mentions different phases of ethical hackin

46		Classify the following vulnerabilities using the RISOS model and justify your answer: The presence of the “wiz” command in the sendmail program. The failure to handle the IFS shell variable by loadmodule. The failure to select an Administrator password that was difficult to guess. The failure of the Burroughs system to detect offline changes to files.
47		Consider the scheme used to allow customers to submit their credit card and order information. Why is the file inaccessible to the Web server?
48		The Drib hired Dewey, Cheatham, and Howe to audit their networks. The analyst provides a floppy disk with a scanning tool. Should the Drib security officers trust this scan? Suggest four questions they should ask.
49		Suppose the Drib wished to allow employees to telecommute. Discuss the required changes in the network infrastructure, particularly regarding SSH security.
50	6	Perform a penetration test on a system after you obtain authorization to do so. Apply the Flaw Hypothesis Methodology to obtain a meaningful assessment of the system’s security.
51	6	Analyze a real-world case study of malware and describe how it was detected and mitigated.
52		Apply network traffic analysis to detect a malware-infected host in an enterprise network.
53		Discuss how heuristic analysis is used to detect new and previously unknown malware. How does it differ from traditional signature-based detection?
54		Discuss the differences between anomaly-based and signature-based detection techniques.
55		Compare different static analysis tools and their functionalities in malware detection.
56		Define static malware analysis and dynamic malware analysis. Explain the differences between these two approaches, highlighting their advantages and limitations.

57		Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your e-mail client, Web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?
58		Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?
59		Compare signature-based and behavior-based malware detection techniques. Explain the strengths and weaknesses of each approach.
60		Explain different types of malware (such as viruses, worms, trojans, ransomware, spyware, rootkits, and botnets) and describe their key characteristics.