

**Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,**  
**Department Of CMPN, INFT, AIDS, ETRX, EXTC, INST**  
**Year:2023-24 (Odd Sem)**  
**Mid Term Test**

<b>Class : BE</b>	<b>Division: All</b>
<b>Semester: VII</b>	<b>Subject: Cyber Security and Laws</b>
<b>Date: 8/9/2023</b>	<b>Time: 1:30pm -2:30pm</b>

<b>Q.1)</b>		<b>(Attempt any five of the following )</b>	<b>Marks (20)</b>	<b>CO's Mapped</b>	<b>BL</b>
	a)	List the features of Indian IT Act 2000.	2M	1	1
	b)	Classify the cybercrimes and explain any one briefly.	2M	1	2
	c)	Explain various types of key-loggers in brief.	2M	3	2
	d)	What are the different ways of password cracking? Explain in brief.	2M	3	2
	e)	Enumerate, work from home cyber security tips and risks.	2M	2	2
	f)	List various threats associated with cloud computing.	2M	2	1
<b>Q.2)</b>	a)	Explain how criminals plan the cyber attack? Discuss various steps involved.	5M	1	3
		<b>OR</b>			
	b)	Compare Vishing, Phishing and Smishing in cyber security.	5M	3	3
<b>Q.3)</b>	a)	What is social engineering? Explain with the help of an example.	5M	2	3
		<b>OR</b>			
	b)	Explain DoS and DDoS attacks methods used in cybercrime.	5M	3	3

**Answer Key**

**Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,**  
**Department Of CMPN, INFT, AIDS, ETRX, EXTC, INST**  
**Year:2023-24 (Odd Sem)**  
**Mid Term Test**

<b>Class : BE</b>	<b>Division: All</b>
-------------------	----------------------

Semester: VII	Subject: Cyber Security and Laws
Date: 8/9/2023	Time: 1:30pm -2:30pm

Q.1)		(Attempt any five of the following )	Marks (20)	CO's Map ped
	a)	<p>List the features of Indian IT Act 2000.</p> <ul style="list-style-type: none"> <li>• It provides legal recognition to records in the electronic form.</li> <li>• It provides legal recognition to e-commerce and electronic transactions in India.</li> <li>• It provides legal recognition to digital signatures issued and authenticated by the certifying authorities.</li> <li>• It is applicable to cybercrimes and contraventions committed in India and outside India by any person, irrespective of nationality, if the cybercrime is committed in India or involves any computer based in India.</li> <li>• It has appointment of adjudicating officers for holding inquiries under the Act.</li> </ul> <p>(Any 4)</p>	2M	1
	b)	<p>Classify the cybercrimes and explain any one briefly.</p> <ol style="list-style-type: none"> <li>1. Cybercrime against an individual</li> <li>2. Cybercrime against property</li> <li>3. Cybercrime against organization</li> <li>4. Cybercrime against Society</li> <li>5. Crimes emanating from Usenet newsgroup</li> </ol> <p>(Explain any one in short and give examples.)</p>	2M	1
	c)	<p>Explain various types of key-loggers in brief.</p> <ul style="list-style-type: none"> <li>• Software-based keyloggers</li> <li>• Hardware keyloggers</li> </ul> <p>(explain in short and give examples)</p>	2M	3
	d)	<p>What are the different ways of password cracking? Explain in brief.</p> <ol style="list-style-type: none"> <li>1. Rainbow table approach</li> <li>2. Dictionary attack</li> <li>3. Brute force attack</li> <li>4. Social engineering approach</li> <li>5. Shoulder surfing attack</li> </ol> <p>(explain any 4 methods in short)</p>	2M	3
	e)	<p>Enumerate, work from home cyber security tips and risks.</p> <ol style="list-style-type: none"> <li>1. Use antivirus and internet security software at home</li> <li>2. Keep family members away from work devices</li> <li>3. Invest in a sliding webcam cover</li> <li>4. Use a VPN</li> <li>5. Use a centralized storage solution</li> </ol>	2M	2

		6. Secure your home Wi-Fi 7. Beware of Zoom and video conferencing 8. Make sure your passwords are strong and secure 9. Protect your online banking 10. Be wary of email scams and your email security  (List any 4)		
	f)	List various threats associated with cloud computing. <ul style="list-style-type: none"> <li>• Elevated user access</li> <li>• Regulatory compliance</li> <li>• Location of data</li> <li>• Segregation of data</li> <li>• Recovery of data</li> <li>• Information security violation reports</li> <li>• Long term viability</li> </ul> (List any 4 and explain in short)	2M	2
Q.2)	a)	Explain how criminals plan the cyber attack? Discuss various steps involved.  1. Reconnaissance (information gathering) 2. Scanning and scrutinizing the gathered information (validity of information and identify proneness/sensitivity) 3. Launching an attack (gaining and maintaining the system access) (Explain each step in detail and mention tools used in each step)	5M	1
		<b>OR</b>		
	b)	Compare Vishing, Phishing and Smishing in cyber security. Smishing: <ul style="list-style-type: none"> <li>• Sms-phishing</li> <li>• Sms can be abused as pretexting, VoIP to gather information</li> </ul> Vishing: <ul style="list-style-type: none"> <li>• Social engg on phone</li> <li>• V-voice and phishing</li> <li>• To get PI</li> <li>• Includes Id theft, money transfer, ....</li> </ul> Phishing: <ul style="list-style-type: none"> <li>• Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.</li> </ul> (Explain above mentioned points in detail.)	5M	3
Q.3)	a)	What is social engineering? Explain with the help of an example. <ul style="list-style-type: none"> <li>• Social engineering involves gathering secret information as well as unauthorized access to the network.</li> <li>• Classification of social engineering.</li> </ul> 1. Human Based 2. Computer Based.	5M	2

		(Block diagram is required to show the steps of conducting a social engineering attack.  Explain the above mentioned types in detail.)		
		<b>OR</b>		
	b)	<p>Explain DoS and DDoS attacks methods used in cybercrime.</p> <ul style="list-style-type: none"> <li>• In computing, a <b>denial-of-service (DoS)</b> or distributed <b>denial-of-service (DDoS) attack</b> is an attempt to make a machine or network resource unavailable to its intended users.</li> <li>• A <b>DoS attack</b> generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.</li> </ul> <p>(Explain how it will affect the victim's system, also list different types of DoS and DDoS attacks and how to prevent this attack.)</p>	5M	3