Seat No.: Enrolment No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

Diploma Engineering – SEMESTER – 6 (NEW) – EXAMINATION – Summer-2024

Subject Code: 4360705 **Date: 21-05-2024**

Subject Name: Network Forensics

Time: 10:30 AM TO 01:00 PM **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make Suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Use of programmable & Communication aids are strictly prohibited.**
5. **Use of non-programmable scientific calculator is permitted.**
6. **English version is authentic.**

Q.1	**(a)**	List out full forms of IP, TCP and DNS.	**03**
પ્રશ્ન.1	(અ)	IP, TCP અને DNS નું પૂરું નામ લખો.	૦૩
	(b)	Explain Network Threats with example.	**04**
	(બ)	નેટવર્ક થ્રેટ્સને ઉદાહરણ સાથે વિગતવાર સમજાવો.	૦૪
	(c)	Explain the OSI reference model with the function of each layer.	**07**
	(ક)	દરેક લેયર ના કાર્ય સાથે OSI મોડેલ સમજાવો.	૦૭
		OR	
	(c)	Explain TCP/IP model with function of each layer.	**07**
	(ક)	દરેક લેયર ના કાર્ય સાથે TCP/IP મોડેલ સમજાવો.	૦૭
Q.2	**(a)**	Describe Network Forensics and its Application.	**03**
પ્રશ્ન.2	**(અ)**	નેટવર્ક ફોરેન્સિક્સ અને તેની એપ્લિકેશનનું વર્ણન કરો.	**૦૩**
	(b)	Explain the process of Proactive Investigation.	**04**
	(બ)	પ્રોએક્ટિવ ઇન્વેસ્ટિગેશનની પ્રક્રિયા સમજાવો.	૦૪
	(c)	Explain Cross-site scripting, DNS Spoofing and ARP Poisoning.	**07**
	(ક)	ક્રોસ-સાઇટ સ્ક્રિપ્ટીંગ, DNS સ્પુફિંગ અને ARP પોઇઝનિંગ વિગતવાર સમજાવો.	૦૭
		OR	
Q.2	**(a)**	Write Advantages and Disadvantages of Network Forensics.	**03**
પ્રશ્ન.2	**(અ)**	નેટવર્ક ફોરેન્સિક્સના ફાયદા અને ગેરફાયદા લખો.	૦૩
	(b)	Explain Incident Response.	**04**
	(બ)	ઇન્સીડન્ટ રિસ્પોન્સ વિગતવાર સમજાવો.	૦૪
	(c)	Explain Social Engineering Attack and its types.	**07**
	(ક)	સોશિયલ એન્જિનિયરિંગ એટેક અને તેના પ્રકારો સમજાવો.	૦૭
Q. 3	**(a)**	List the sources of evidence for Network forensics.	**03**
પ્રશ્ન.3	**(અ)**	નેટવર્ક ફોરેન્સિક્સ માટે પુરાવાના સ્ત્રોતોની યાદી બનાવો.	૦૩
	(b)	Explain Network traffic capture.	**04**
	(બ)	નેટવર્ક ટ્રાફિક કેપ્ચર સમજાવો.	૦૪
	(c)	Write a short note on Deep packet inspection (DPI).	**07**
	(ક)	ડીપ પેકેટ ઇન્સ્પેક્શન (DPI) પર ટૂંકી નોંધ લખો.	૦૭
		OR	
Q. 3	**(a)**	List the Data acquisition methods.	**03**
પ્રશ્ન.3	**(અ)**	ડેટા એક્વિઝીશન પધ્ધતિઓની ની યાદી બનાવો.	૦૩
	(b)	Explain Write-blocking and Data hashing preservation techniques.	**04**
	(બ)	રાઇટ-બ્લોકીંગ અને ડેટા હેશીંગ પ્રિઝર્વેશન ટેકનિક સમજાવો.	૦૪

	(c)	List Network Traffic Analysis Methods. Explain Network behavior analysis.	**07**
	(ક)	નેટવર્ક ટ્રાફિક એનાલિસિસ મેથડ્સ ની યાદી બનાવો. નેટવર્ક બિહેવિયર એનાલિસિસ સમજાવો.	૦૭
Q. 4	**(a)**	Describe the Wireless communication.	**03**
પ્રશ્ન.4	(અ)	વાયરલેસ સંચારનું વર્ણન કરો.	૦૩
	(b)	Differentiate WEP and WPA.	**04**
	(બ)	WEP અને WPA નો તફાવત લખો.	૦૪
	(c)	Explain attacks on wireless network. Explain how do you protect Wireless Network?	**07**
	(ક)	વાયરલેસ નેટવર્ક પર થતા એટેકસ સમજાવો. તમે વાયરલેસ નેટવર્ક ને કેવી રીતે સુરક્ષિત કરશો તે સમજાવો.	૦૭
		OR	
Q. 4	**(a)**	Describe the security challenges of wireless communication.	**03**
પ્રશ્ન.4	(અ)	વાયરલેસ કોમ્યુનિકેશનના સિક્યુરિટી ચેલેન્જીસ નું વર્ણન કરો.	૦૩
	(b)	Explain WPA and WPA-2 Encryption.	**04**
	(બ)	WPA અને WPA-2 એન્ક્રિપ્શન સમજાવો.	૦૪
	(c)	Explain Man-in-the-middle (MITM) attack and Rogue access points.	**07**
	(ક)	મેન-ઇન-ધ-મિડલ (MITM) એટેક અને Rogue એક્સેસ પોઈન્ટ્સ સમજાવો.	૦૭
Q.5	**(a)**	Describe Authorization and Data Preservation.	**03**
પ્રશ્ન.5	(અ)	ઓથોરાયજેશન અને ડેટા પ્રિઝર્વેશન નું વર્ણન કરો.	૦૩
	(b)	Explain Metadata preservation.	**04**
	(બ)	મેટાડેટા પ્રિઝર્વેશન વિગતવાર સમજાવો.	૦૪
	(c)	Write short note on Role of Artificial intelligence in Intrusion Detection and Network Forensics.	**07**
	(ક)	ઇન્ટ્રુઝન ડિટેક્શન અને નેટવર્ક ફોરેન્સિક્સમાં આર્ટીફિસિયલ ઇંટેલિજન્સની ભૂમિકા પર ટૂંકી નોંધ લખો.	૦૭
		OR	
Q.5	**(a)**	Describe Data and Personal Data Breach.	**03**
પ્રશ્ન.5	(અ)	ડેટા અને પર્સનલ ડેટા બ્રિચ નો વર્ણન કરો.	૦૩
	(b)	Explain Evidence Handling procedure.	**04**
	(બ)	ઈવિડેન્સ હેન્ડલિંગ ની પ્રક્રિયા સમજાવો.	૦૪
	(c)	Explain Internet of Things (IoT) forensics, components and challenges.	**07**
	(ક)	ઈન્ટરનેટ ઓફ થિંગ્સ (IoT) ફોરેન્સિક્સ, ઘટકો અને પડકારો સમજાવો.	૦૭