Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	**T**	**P**	**L**	**T**	**P**	**Total**
ET921	**Network Security**	**4**	**--**	**--**	**4**	**--**	**--**	**4**
		Examination Scheme						
		Theory Marks						
		ISE		**MSE**		**ESE**		
		10		**30**		**100 (60% Weightage)**		

Pre-requisite Course Codes		--
Course Outcomes	CO1	Describe security threats and apply security techniques using cryptosystems.
	CO2	Explain the key terms and concepts in cyber law, intellectual property and cyber crimes, trademarks and domain theft
	CO3	Build and configure firewall and intrusion detections systems' using GNU open source security tools.
	CO4	Incorporate approaches for incident analysis and response, for risk management and best practices and digital evidence collection, and evidentiary reporting in forensic acquisition

Module No.	Unit No.	Topics	Ref.	Hrs.
1		**Introduction to Network and Cybersecurity:** Recap: • Need for network security, Attacks and Their classification • Network Vulnerabilities and control • Security services and mechanisms, • Impact of Security on Enterprises • Risk Factors and Cost Analysis.	1,2,3	8
2		Cryptography and Cryptosystems: Recap: • Classical and modern cryptography, stream and block ciphers, • Message digest,digital signature, digital certificate, certificate authority, cryptanalysis • DES/AES/RSA/RC4/MD5/SHA algorithms • Secure protocols SSL, IPSec, VPN,PKI Implementing security using symmetric and Public-Key crytography.	1	10
3		Ethical Hacking and Network defences • Cybercrimes, Cybercriminals, Cyberoffences, Cybercrimes in Mobile and Wireless Devices, Tools and Methods used in Cybercrimes • Network reconnaissance, scanning and sniffing, gaining	6, 7	10

		access. • Security Technologies:Firewall, IDS and Antivirus, Reverse proxy • L7 content filtering firewall, NAT & reverse proxy, Firewall deployment and limitations, selection of firewalls. Performance analysis of firewall. • Signature and Anamoly based IDSs, IDS deployment, zone diagram, performance analysis of IDS, strengths and limitations of IDS. Biometrics for security		
4		Cybersecurity principles and best practices: • Layered Defense,Surveillance and Reconnaissance Outsider/Internal Threat Protection, Privacy,Intellectual Property,Professional Ethics,Freedom of Speech ,Fair User and Ethical Hacking,Trademarks ,Internet Fraud ,Electronic Evidence.	2,7	10
5		Cybersecurity implications on Organizations, standards and Cyber laws: • Risk Management: Asset Evaluation and Business Impact Analysis, Risk Identification ,Risk Quantification ,Risk Response Development and Control Security Policy, Compliance, and Business Continuity. • Cyber Incident Preparation: Incident Detection and Analysis, Containment, Eradication, and Recovery ,Proactive and Post-Incident Cyber Services • Forensics: Forensic Technologies ,Digital Evidence Collection ,Evidentiary Reporting The Indian IT Act and new amendments.	6,7	10
6		System Security and Case-Study: • Security Operations Center (SOC), Network Operations Center (NOC) • Network Security Audit • SET, Biometric Security, Digital Immune System Cloud Security. Wi-Fi Security, Mobile and Cellular Security	6	10
			Total	**48**

References:

[1] Cryptography and Network Security by Behrouz Forouzan McGrawHill Publications

[2] Security in Computing by Pfleeger and Pfleeger, Pearson Publications

[3] Management of Information Security by M. Whitman Cengage Publications

[4] Cryptography and Network Security by B. Menzanes, Elsevier

[5] Computer Security by Matt Bishop, Pearson Publication

[6] Cryptography and Network Security by William Stallings, Pearson publications.

[7] Cyber Security by Nina Godbole, John Wiley Publications

[8] Information Security: Principles and Practice, 2nd edition by Mark Stamp and Deven Shah

[9] Data Communication & Network Security by Houston Carr and Charles Snyder, McGraw-Hill Publication