Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Faculty of Computer Applications

NAAC A Grade Accredited University

FACULTY OF COMPUTER APPLICATIONS

Programme	BCA Honors	**Branch/Spec.**	Computer Applications
Semester	V	**Version**	1.0.0.0
Effective from Academic Year	2026-2027	**Effective for the batch Admitted in**	June 2024
Subject Code	U35B4NS	**Subject Name**	NETWORK SECURITY

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	4	-	-	-	4	Theory	50	50	100
Hours	4	-	-	-	4	Practical	-	-	-

Objective:

To provide in-depth theoretical knowledge of network security principles, threats, cryptography, authentication, firewalls, VPNs, intrusion detection, and web security, enabling students to understand and design secure communication systems.

Pre-requisites:

Basic knowledge of Computer Networks and Operating Systems.

Course Outcomes:

Name of CO	**Description**
CO1	Understand the fundamentals of network security and basic cryptographic concepts.
CO2	Identify and analyze common network and web-based security threats.
CO3	Apply authentication methods and hashing algorithms for secure communication.
CO4	Explain firewall types, VPNs, and design secure network architectures.
CO5	Understand IP security protocols and intrusion detection systems.
CO6	Analyze web security protocols, SSL/TLS, and secure web communication.

	Mapping of CO and PO											
Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	0	0	1	0	2	2	0	0	1	1

CO2	3	3	0	2	1	0	2	1	0	2	1	1
CO3	3	3	3	0	3	0	2	1	0	0	1	1
CO4	3	2	3	0	3	0	2	1	0	0	1	1
CO5	3	3	3	3	3	0	2	1	0	1	1	1
CO6	3	3	0	0	3	0	3	1	3	1	1	1

Content:

Unit		Hrs
1	**Introduction to Network Security** Need for Security; Security Attacks: Passive & Active; Security Services and Mechanisms; Network Security Model; Basic concepts of Cryptography; IT Security in Open Systems: Threats, Security Requirements, and How Security Works	10
2	**Network Security Threats and Issues** Protocol Vulnerabilities: DoS, DDoS, SYN Flooding, Session Hijacking, ARP Spoofing, DNS Attacks; Wireless LAN Threats: Frame Spoofing, MAC Violations; Software Vulnerabilities: Phishing, Buffer Overflow, Cross-site Scripting, SQL Injection; Viruses, Worms, Malware, Botnets, Eavesdropping, Password Snooping; Digital Signatures: Properties, Requirements, Elgamal, Schnorr, NIST Digital Signature Algorithm	10
3	**Authentication** Authentication Requirements and Functions; Message Authentication Codes (MAC); MD5 and Secure Hash Algorithm (SHA); User Authentication: Password, Certificate-based, Biometric Authentication; Kerberos Authentication Protocol	10
4	**Firewalls and Network Security Devices** Network Security Introduction; Firewalls: Types – Personal, Network, Software, Hardware, Packet Filtering; Design Principles of Firewalls; Trusted Systems; Detailed Working of Kerberos	10
5	**IP Security and VPN** IP Security: Uses, Components, IPsec Architecture; Virtual Private Network (VPN): Introduction and Architecture; Intrusion Detection: Concepts and Classification; Network-Based and Host-Based IDS	10
6	**Web Security and Transport Layer Security** Web Security Threats and Protection Approaches; SSL Architecture and Protocol; Transport Layer Security (TLS); HTTPS and Secure Web Communication	10

Practical Content:

NA	
Text Books:	
1	William Stallings. *Network Security Essentials: Applications and Standards*, 6th Edition, Pearson, 2017.
Reference Books:	
1	**Behrouz A. Forouzan.** *Cryptography and Network Security*, Special Indian Edition, McGraw Hill.
2	**William Stallings.** *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson.
3	**Charlie Kaufman, Radia Perlman, Mike Speciner.** *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall.
Web References / MOOC / Certification Course	
1	https://digitalcloud.training/free-aws-certification-training/
2	https://www.coursera.org/professional-certificates/aws-cloud-solutions-architect
3	https://www.coursera.org/specializations/gcp-professional-architect-course
4	https://cloud.google.com/learn/training
Question Paper Scheme:	
	End Semester Examination Duration: (2 Hours Theory Examination) **Note for Examiner:** - Q-1 Any Five out of Seven (25 Marks) Q-2 Any Two out of Three (06 Marks) Q-3 Mandatory question (05 Marks) Q-4 Any Two out of Three (08 Marks) Q-5 Any Two out of Three (06 Marks) *The question paper must comprehensively address all Course Outcomes (COs), align Taxonomy levels, and ensure complete syllabus coverage.*