Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Faculty of Computer Applications

NAAC A Grade Accredited University

Programme	B.Sc. IT Honours (Cyber Security)	**Branch**	Computer Applications
Semester	VI	**Version**	1.0.0.0
Effective from Academic Year	2026-27	**Effective for the batch Admitted in**	June 2024
Subject code	U66A1NS	**Subject Name**	NETWORK SECURITY

Teaching scheme						**Examination scheme(Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CCE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	2	-	2	-	4	Theory	50	50	100
Hours	2	-	4	-	6				

Objective:

To develop skills for securing networks using protocols, tools, and emerging technologies.

Pre-requisites:

Basic knowledge of computer networks and operating systems.

Learning Outcome:

Name of CO	Description
CO1	To understand the principles of network security and the use of IPsec.
CO2	To identify network threats, attacks, and use appropriate detection tools.
CO3	To apply authentication techniques and secure email protocols for communication security.
CO4	To analyze the role of firewalls and web security applications in protecting networks.
CO5	To design secure network solutions using advanced and emerging security technologies.

Mapping of CO and PO:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	2	2	1	1	1	1	1	1
CO2	3	3	2	2	3	2	1	1	2	2	1	1
CO3	2	2	2	2	3	3	2	1	2	2	1	1
CO4	2	3	3	2	3	2	2	1	2	2	1	1
CO5	2	3	3	2	3	2	2	2	2	2	2	2

Content:

Unit	Content	Hrs.
1	**Network Security Principles and IPsec**: Fundamentals of Network Security and Common Threats, Models for Network and Access Security, Security in Real-time Communication Systems, TCP/IP Stack and Layer-wise Security Mapping, Overview of IPsec, Authentication Header (AH), Encapsulating Security Payload (ESP), IPsec Key Management and IKE.	06
2	**Threats, Attacks, and Detection Tools:** Network and Device Vulnerabilities, Protocol-based Attacks (DNS Spoofing, ARP Poisoning, Hijacking), Network Attacks (DoS, MITM, Replay), Introduction to DMZ, NAC, and Proxy Servers, Fundamental of IDS, Introduction to IPS, IDS/IPS Tools.	06
3	**Authentication and Secure Email Systems**: Overview of Kerberos and X.509 Authentication, Port Scanning & Port Knocking, P2P Network Security, Email Security Requirements and Protocols (PGP, S/MIME), Properties of Secure Communication (Integrity, Privacy, Non-repudiation).	06

4	**Firewalls and Web Security Applications:** Types of Firewalls (Packet, Proxy, Stateful), Secure Web Practices (Cookies, HTTPS, Sessions), Security in Wireless Sensor Networks, Security in Mobile Networks, Proxy-based Filtering and Secure Tunnels.	06
5	**Secure Network Design and Emerging Technologies:** Network Security Architecture and Best Practices, Zero Trust Architecture (ZTA), Secure LAN/WAN Design, Network Logging, Auditing, and Policy Compliance, Introduction to Threat Hunting, Emerging Trends in Cybersecurity.	06

Practical Content:	
List of practical specified by subject teacher based on above mentioned topics	
Reference Books:	
1	William Stallings, "Cryptography and Network Security – Principles and Practices", Prentice Hall of India, Third Edition, 2003.
2	Network Security Essentials: Applications and Standards by William Stallings, 6th Edition, Pearson, 2023.
3	Network Security and Cryptography by Bernard Menezes, 1st Edition, Cengage Learning, 2010.
4	C. Kaufman, R. Perlman, M. Speciner, R. Perlner, "Network Security: Private Communication in a Public World",Pearson Education, 3rd edition, 2024
Web Reference:	
1	https://www.open.edu/openlearn/digital-computing/network-security/content-section-0?active-tab=description-tab
2	https://www.tutorialspoint.com/network_security/index.htm
3	https://www.geeksforgeeks.org/computer-networks/computer-network-tutorials/
MOOC/Certificate Course:	
1	https://onlinecourses.nptel.ac.in/noc25_ee54/preview.
2	https://www.coursera.org/learn/-network-security
3	https://www.open.edu/openlearn/digital-computing/network-security/content-section-0?active-tab=description-tab
4	https://www.coursera.org/learn/networks-and-network-security
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 with Bloom's Taxonomy levels, and ensure complete syllabus coverage