UCS727: NETWORK SECURITY

L	T	P	Cr.
3	0	2	4.0

Course objective: This course is designed to impart a critical theoretical and detailed practical knowledge of a range of computer network security technologies as well as network security tools.

Detail contents:

Introduction: Security Attacks, Security Services, Security Mechanisms and Principles, Security goals, malicious software, Worms, Viruses, Trojans, Spyware, Botnets

Basic of Cryptography: Symmetric and asymmetric cryptography, cryptographic hash functions, authentication and key establishment, Message Authentication Codes (MACs), digital signatures, PKI.

Security Vulnerabilities: DoS attacks, Buffer Overflow, Race Conditions, Access Control Problems, Spoofing and Sniffing attacks, ARP Poisoning, Social Engineering and countermeasures.

Internet Security: TCP/IP Security, Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH), IPsec, Email Security, DNS Security, DNSSEC, Authentication Protocols

Web Security: Phishing attack, SQL Injection, Securing databases and database access, Cross Site Scripting Attacks, Cookies, Session Hijacking, E-commerce security

System Security: Firewalls, Types: Packet filter (stateless, stateful), Application layer proxies, Firewall Location and Configurations, Intruders, Intrusion Detection System, Anomaly and misuse detection.

Wireless Network Security: IEEE 802.11i Wireless LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP End-to-End Security

Laboratory work: Insert malicious shell code into a program file and check its malicious or benign status, create Client Server program to send data across systems as two variants clear text data and encrypted data with different set of encryption algorithms, demonstrate Buffer Overflow and showcase EIP and other register status, perform ARP poisoning, SQL Injection and demonstrate its countermeasure methods, implement stateful firewall using IP Tables, showcase different set of security protocol implementation of Wireless LAN.

Course learning outcome (CLO):

On completion of this course, the students will be able to:

1. Comprehend and implement various cryptographic algorithms to protect the confidential data.
2. Identify network vulnerabilities and apply various security mechanisms to protect networks from security attacks.
3. Apply security tools to locate and fix security leaks in a computer network/software.
4. Secure a web server and web application
5. Configure firewalls and IDS

Text Books:

1. *Network Security Essentials, William Stallings, Prentice Hall (2013), 5th Ed.*

Reference Books:

1. *Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin, Addison-Wesley Professional (2003), 2nd Ed.*
2. *Cryptography and Network Security, W. Stallings, Prentice Hall (2010), 5th Ed.*

Evaluation Scheme:

Sr. No.	**Evaluation Elements**	**Weightage (%)**
1	MST	20
2	EST	40
3	Sessionals(Assignments/Projects/Tutorials/Quizzes/Lab Evaluations)	40