Course Code	Course Name	Teaching Scheme			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical/Oral	Tutorial	Total
TEITC603	System And Web Security	04 Hr/Week	02 Hr/Week	---	04	01	---	05

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
TEITC603	System And Web Security	20	20	20	80	25	---	25	150

Course Objectives

1. Understand the fundamental principles of access control models and techniques, authentication and secure system design
2. Apply methods for authentication, access control, intrusion detection and prevention
3. Identify and mitigate software security vulnerabilities in existing systems.
4. Understand the role of firewalls, IPSec, Virtual Private Networks and identity management, etc.
5. Understand Web Server vulnerabilities and their counter measures

Course Outcomes:

Upon successful completion of the course the student will be able to:

- Differentiate between authentication and authorization;
- Explain the basic idea behind access control and compare the various access control policies and models.

- Explain the need for security protocols in the context of use with Internet-based applications;
- Explain the basic idea behind firewalls and intrusion detection systems and how they work;
- Explain malicious software and typical software solutions used in dealing with viruses and worms;
- Understand and explain various issues related to program security and web security.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours
1	**Introduction to Computer Security**	Vulnerabilities, Threats and Attacks, Public Key Cryptography and Cryptanalysis, Knapsack cryptosystem	04
2	**Authentication**	Authentication Methods and Protocols, Password based authentication, Token Based Authentication, Biometric Authentication, Digital Certificates, X. 509 Directory Services, PKI, Needham Schroeder Authentication Protocol, Single sign on, Kerberos Authentication Protocol, Federated Identity Management.	08
3	**Access Control**	Access control Policies: DAC, MAC, RBAC, Access control Matrix, ACLs and Capability Lists, Multiple level security model: Biba and Bell La Padula Models, Multilateral security, Covert channel, CAPTCHA.	06
4	**Software security**	Software Flaws, Buffer Overflow, Incomplete Mediation, Race conditions, Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits, Miscellaneous Software Attacks: Salami attack, Linearization Attacks, Trusted Computing: Software reverse engineering, Digital Rights management	08

5	**Operating System Security**	Linux Security Model, File System Security, Linux Vulnerabilities, Windows Security Architecture, Windows Vulnerabilities	04
6	**Network Security**	Network security basics, TCP/IP vulnerabilities Layer wise: Packet Sniffing, ARP spoofing, port scanning, IP spoofing, TCP syn flood, DNS Spoofing, Internet Security Protocols: SSL, TLS, IPSEC, Secure Email and S/MIME, Denial of Service: Classic DOS attacks, Source Address spoofing, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial of Service Attacks. Firewalls, Intrusion Detection Systems: Host Based and Network Based IDS, Honey pots.	12
7	**Web Security**	User Authentication and session management, Cookies, Secure HTTP, SQL Injection Techniques, Cross Site Scripting, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, Web Services Security.	06

Text Books

1) Computer Security Principles and Practice, by William Stallings, Pearson Education.

2) Security in Computing by Charles P. Pfleeger , Pearson Education

3) Computer Security by Dieter Gollman, **3rd Edition,** Wiley India.

4) Cryptography and Network Security by Behrouz A. Forouzan, TATA McGraw hill.

Reference Books

1) Information security Principles and Practice by Mark Stamp, Wiley publication

2) OWASP TOP 10: https://www.owasp.org/index.php/Top_10_2013

3) Network security bible 2nd edition, Eric Cole, Wiley India.

Term Work: 25 Marks (Total marks) = 15 Marks (Experiment and Case Studies) + 5 Marks (Assignments) + 5 Marks (Attendance)

Suggested Practical List:

1. Design and implement the RSA cryptosystem.
2. Implement Digital signature scheme using RSA.
3. Simulate the Buffer overflow attack.
4. Simulate the Salami attack.
5. Design and implement a program for adding passwords to a file. The program should be able to filter out weak passwords (based on dictionary words or variants) and store the strong passwords by creating a hash of user ID and password.
6. Study of a packet sniffer like wireshark, or tcpdump. Use this tool to capture and analyze data in packets.
7. Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc
8. Detect ARP spoofing using open source tool ARPWATCH
9. Install an IDS (e.g. SNORT) and study the logs.
10. Use of iptables in linux to create firewalls.
11. Implement a simple SQL injection attack.

Theory Examination:

1. Question paper will comprise of 6 questions, each carrying 20 marks.
2. Total 4 questions need to be solved.
3. Q.1 will be compulsory, based on entire syllabus wherein sub questions of 2 to 3 marks will be asked.
4. Remaining question will be randomly selected from all the modules.
5. Weightage of marks should be proportional to number of hours assigned to each module.