

Nirma University
Institute of Technology, School of Technology
MTech Computer Science and Engineering / MTech Computer Science and
Engineering (Information and Network Security)
Semester – II

L	T	P	C
3	0	2	4

Course Code	3CS12D306
Course Title	Secured Software Design and Enterprise Computing

Course Learning Outcomes (CLOs):

At the end of the course, students will be able to

1. differentiate between various software vulnerabilities
2. identify software process vulnerabilities for an organization
3. monitor resources consumption in a software
4. interrelate security and software development process

Syllabus:

Teaching Hours:

Unit-I

Secure Software Design: Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.

8

Unit – II

Enterprise Application Development: Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Present software solution.

7

Unit – III

Enterprise Network Management: Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them, Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum Vulnerabilities and flaws.

8

Unit – IV

Enterprise Systems Administration: Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).

8

Unit – V

8

Software Security in Business Enterprise: Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, Access control models, Kerberos protocol, Protocols specially designed for e-commerce and web applications, firewalls and VPNs. Management issues, technologies, and systems related to information security management at enterprises.

Unit – VI

6

Case Studies: Case study of DNS server, Case study on DHCP configuration and Case study on SQL injection attack, Case study on Terminal services

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Above concepts are to be implemented and at least 6 experiments are to be carried out.

Suggested Readings[^]:

- 1 Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
- 2 Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley
- 3 W. Stallings, Cryptography and network security: Principles and practice, Prentice Hall.
- 4 C. P. Pfleeger, S. L. Pfleeger, Security in Computing, Prentice Hall
- 5 Gary McGraw, Software Security: Building Security In, Addison-Wesley

L=Lecture, T=Tutorial, P=Practical, C=Credit

[^]this is not an exhaustive list