DEPARTMENT OF COMPUTER ENGINEERING

Subject Code: 10CE0102

Subject Name: Advance Network Security

M.Tech. Year - I

Objective: This course provides a comprehensive view of the network security principles and measures to prevent vulnerabilities and security attacks in the networks including security policies, access controls, IP security, authentication mechanisms, and intrusion detection and protection, Cyber Security topics.
.

Credits Earned: 4 Credits

Course Outcomes: After completion of this course, student will be able to

- Understand the basic concepts of networks, networking devices and various
- Understand various cryptographic algorithm
- Explore Various tools for web security and analysis

Pre-requisite of course: Computer Network, Web Technology

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Term work (TW)	
3	0	2	4	50	30	20	25	25	150

Contents:

Unit	Topics	Contact Hours
1	Review of computer security, Public Key cryptography, RSA. Review of Cryptography Basics, On-line Shopping, Payment Gateways, Digital Certificates, Hashing, Message Digest, & Digital Signatures. Introduction to cyber crime and cyber law, cyber space and information technology, Nature and scope of cyber crime, Jurisdiction of cyber crime. Systems Vulnerability Scanning, Overview of vulnerability scanning,	6
2	Introduction- A web security forensic lesson, Web languages, Introduction to different web attacks. Overview of N-tier web applications, Web Servers: Apache, IIS, Database Servers. Web Hacking Basics HTTP & HTTPS URL, .	7

3	Web Under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS, Basics, Securing databases, Secure JDBC, Securing Large Applications, Cyber Graffiti, Network Defense tools, Web Application Tools	5
4	Secure System Planning and administration, Information security policies and procedures nformation security: fundamentals-Employee responsibilities-information classification-Information handling- Tools of information security-Information processing-secure program administration. Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.	6
	Total Hours	**32**

References:

1. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, Raghu Santanam, M. Sethumadhavan, Information Science Reference
2. Pfleeger, Charles P. and Shari L. Pfleeger. Security in Computing, 4th Edition. Upper Saddle River, NJ: Prentice Hall, 2008
3. Rice, David. Geekonomics: The Real Cost of Insecure Software. Upper Saddle River, NJ: Pearson Education, 2008
4. Cyber Security Essentials,James Graham, Ryan Olson, Rick Howard, CRC Press
5. Cybercrime: Security and Surveillance in the Information Age, Douglas Thomas; Brian Loader
6. Computer Crime: A Crime-Fighters Handbook by David Icove Grabosky
7. Mark F Grady, FransescoParisi, “The Law and Economics of Cyber Security”, Cambridge University Press, 2006
8. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking:attacks and defense. Addison Wesley. 2003.
9. Garms, Jess and Daniel Somerfield. Professional Java Security. Wrox. 2001.

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyze	Evaluate	Create
5%	10%	15%	30%	20%	30%

Suggested List of Experiments:

1. Networking Basics - How do networks work Security Lab Setup and
2. Vulnerabilities and Threats - How can networks be compromised Scanning and Enumerating the Network for Targets and Address Spoofing
3. Denial of Service Attacks and Network Applications Exploits
4. Malware Analysis and Botnets
5. Escalating Privilege – Sniffing, Keylogging, Password Cracking and Man in the Middle Attacks
6. Security in Wireless Systems
7. Prevention - How do we prevent harm to the networks Firewalls
8. Hardening the Host Computer and Securing Network Communications
9. Detection and Response – How do we detect and respond to attacks Preparing for and Detecting Attacks
10. Identify and Mitigate Network Attacks

Instructional Method:

a. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

b. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

c. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

d. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory

Supplementary Resources:

1. http://nptel.ac.in/courses/108108076/
2. http://nptel.ac.in/downloads/108105053/
3. http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-002-circuits-and-electronics-spring-2007/video-lectures/
4. https://www.facstaff.bucknell.edu/mastascu/eLessonsHTML/EEIndex.html
5. http://www.electrical4u.com/nature-of-electricity/
6. http://vlab.amrita.edu/index.php