Marwadi University

Syllabus for Bachelor of Technology

Computer Engineering

Subject Code: 01CE0605

Subject Name: Network Security

B.Tech. Year - III

Objective: Objective of this course is to provide necessary study of Network Security issues and methods in networking systems. Topics to be covered include review of networking, advanced cryptography, access control, distributed authentication, IPSec, Virtual Private Networks, intrusion detection systems, and advanced topics such as wireless security, identity management, etc.

Credits Earned:05

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

- Designing of relatively stronger access control mechanism for secure identification and authentication. (Apply)
- Analysis of various identity management protocols. (Analyze)
- Design and deployment of firewalls to secure a private network. (Analyze)
- Implementation of security techniques for developing safe end-to-end communication systems. (Apply)
- Designing and performance analysis of security monitoring system to defend intrusion and impersonation (Evaluate)
- Integration and synthesis of modern security concepts in contemporary new technologies. (Evaluate)

Pre-requisite of course: NA.

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)	
4	0	2	5	50	30	20	25	25	150

Contents

Unit	Topics	Contact Hours
1	**Fundamentals & Perimeter Security:** Overview of OSI 7-layer Model, Need for Security in Computer network, Principles of Security, Overview of security components and mechanisms - Network Security and Architecture- ITU's Recommendation X.800, Device security.	11
2	**Identity Management and Access Control:** AAA Security Services and Protocols, IDS and IPS, Authentication: Kerberos V 4 and V 5, X.509 Authentication Service. Electronic Mail Security, IEEE 802.1x protocol, PKI, key distribution, Smart cards, LDAP, OCSP.	11
3	**End-to-End Security:** Secure Routing, IP Security (IPSec),Overview of VPNs,- Secure Socket Layer (SSL), MPLS VPN, SSH, Security in wireless networks, WEP, WPA, IEEE 802.11 (WAP) Security, Security in GSM, Security in 3G.	12
4	**Security Monitoring and Management:** Network Intrusion and Prevention - Anomaly Detection & Mitigation - Security Monitoring & Correlation, DoS and DDoS Attack. **Security Management** - Security & Policy Management - Security Framework & Regulatory Compliance	11
5	**Advance Topics:**Web security: DNS security, Smartcards/Biometrics, Privacy, Reconnaissance and Social Attacks, Security in E-Services and Applications, Bluetooth Security, Mobile Terminal Security.	11
	Total Hours	56

References:

1. Cryptography And Network Security Principles And Practice Fourth Edition,William Stallings, Pearson Education.
2. Network Security:Current Status and Future Directions, By Christos Douligeris, Dimitrious N. Serpanos, IEEE Press Wiley-Interscience A JoHN Willey& Sons, Inc Publication.
3. Network Security Essentials: Applications and Standards, by William Stallings.Prentice Hall
4. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World, Prentice Hall, 2002*

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	Analyse	Evaluate	Create
5%	10%	30%	25%	25%	5%

Suggested List of Experiments:

1. Scan Network ports Traffic using NMAP port scanner.
2. Use Netcat and analyse TCP / UDP connectivity
3. Use OpenVAS to check Network vulnerability
4. Use DVWA for Web application testing
5. Vulnerabilities and Threats - How can networks be compromised.
6. Use trace Route for Scanning and Enumerating the Network for Targets and Address Spoofing.
7. Exploring Wireshark's packet analysis capabilities
8. Exploring Dsniff – a password sniffing and network traffic analysis tool
9. Exploring Ettercap - a free and open source network security tool for man-in-the-middle attacks on LAN
10. Detection and Response – How do we detect and respond to attacks Preparing for and Detecting Attacks
11. Identify and Mitigate Network Attacks.