3	2	2	1	1	2	-	-	-	-	-	-	1	3	-
4	-	-	-	-	-	-	1	2	-	-	-	1	-	2
5	-	3	-	2	-	-	1	1	-	-	-	2	2	1
AVg.	2	2	1	2	2	-	1	1	-	-	-	2	2	2

1 - low, 2 - medium, 3 - high, '-' - no correlation

CB3602 NETWORK SECURITY

L	T	P	C
3	0	2	4

COURSE OBJECTIVES:

- To understand the basic concepts of security
- To understand the concept of authentication protocols and digital signatures.
- To learn various methods and protocols to understand the cryptography.
- To learn various network security attacks.
- To understand the IP and Web security.

UNIT I FUNDAMENDALS OF NETWORKING SECURITY 9

Overview of networking security- Security Services -Confidentiality, Authentication, Integrity, Non-repudiation, access Control - Availability and Mechanisms- Security Attacks -Interruption, Interception ,Modification and Fabrication.

UNIT II AUTHENTICATION AND SECURITY 9

Authentication overview - Authentication protocols - Authentication and key establishment - key exchange - mediated key exchange - User Authentication –password based authentication - password security - Certificate Authority and key management - digital signatures - digital Certificates.

UNIT III PUBLIC-KEY CRYPTOGRAPHY AND MESSAGE AUTHENTICATION 9

Basics of cryptography -cryptographic hash functions - symmetric and public-key encryption - public key cryptography principles & algorithms - cipher block modes of operation - Secure Hash Functions – HMAC

UNIT IV SECURITY ATTACKS 9

Buffer overflow attacks & format string vulnerabilities - Denial-of-Service Attacks -Hijacking attacks : exploits and defenses - Internet worms – viruses – spyware –phishing – botnets - TCP session hijacking - ARP attacks - route table modification - UDP hijacking - man-in-the-middle attacks.

UNIT V IP SECURITY AND WEB SECURITY 9

Network defense tools: Firewalls,VPNs, Intrusion Detection, and filters - Email privacy: Pretty Good Privacy (PGP) and S/MIME - Network security protocols in practice- Introduction to Wireshark – SSL - IPsec, and IKE -DNS security- Secure Socket Layer (SSL) and Transport Layer Security (TLS) - Secure Electronic Transaction (SET)

45 PERIODS

PRACTICAL EXERCISES:

1. Using Wireshark explore the different layer protocol headers.
2. Demonstrate two different Certificates producing the same MD5 hash
3. Computing MACs, HASH and HMAC for messages

4. Implement and demonstrate Buffer overflow attack
5. Implement and demonstrate Denial of service attacks (DoS) and DDoS
6. Implement the ARP attack and MITM
7. Implement the Botnet attack detection using publically available dataset
8. Explore and install Snort intrusion detection tool
9. Implement Firewall rules using snort
10. Generate the network attack and Detect the attack using Snort

30 PERIODS
TOTAL: 75 PERIODS

COURSE OUTCOMES:

On Completion of the course, the students should be able to:

CO1: Describe computer and network security fundamental concepts and principles.

CO2: : Acquire the knowledge of various authentication protocols, key exchange mechanism, and digital certificates.

CO3 : To get better knowledge on fundamental concepts of cryptography, encryption and hashing techniques.

CO4: Identify and assess different types of threats and attacks such as social engineering, rootkit, and botnets,etc.

CO5: Acquire Demonstrate the ability to select among available network security technology and protocols such as IDS, firewalls, SSL , TLS, etc.

TEXT BOOKS

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.

REFERENCES

1. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal
Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, Wiley Dreamtech

2. Cryptography and network Security, Third edition, Stallings, PHI/Pearson

3. A look back at Security Problems in the TCP/IP Protocol Suite, S. Bellovin, ACSAC 2004.

CO's- PO's & PSO's MAPPING

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	2	**1**	1	1	-	-	-	**1**	-	-	1	1	3
2	3	3	3	3	3	-	-	-	2	-	-	1	3	3
3	3	3	3	3	3	-	-	-	2	-	-	1	3	3
4	3	3	2	3	2	-	-	-	3	-	-	3	3	3
5	3	3	3	3	3	-	-	-	3	-	-	2	**3**	3
AVg.	**3**	**2.8**	**2.4**	**2.6**	**2.4**	**-**	**-**	**-**	**2.2**	**-**	**-**	**1.6**	**2.6**	**3**

1 - low, 2 - medium, 3 - high, '-' - no correlation