GANPAT UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

Programme	Diploma Engineering		Branch	COMPUTER ENGINEERING	
Semester	V		Version	1.0.0.0	
Effective from Academic Year	2020-21		Effective for the batch Admitted in	JULY 2018	
Subject code	1IT2501	Subject Name	NETWORK SECURITY		

Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	0	4	Theory	40	60	100
Hours	3	0	2	0	5	Practical	30	20	50

Pre-requisites:
Basic knowledge of computer hardware and software, different operation system and Computer network and Data Communication Network.

Course Learning Outcomes:
The course content should be taught and implemented with an aim to develop different skills leading to the achievement of the following competencies and course learning outcomes: T1. Identify and describe the common types of security threats and risks to the Computer Systems. T2. Identify the potential threats to Security Services like confidentiality, integrity and availability. T3. Describe the working of standard security mechanisms and applied to the external and internal network. T4. Define cryptography, describe the elements of the encryption process and select best algorithm to encrypt data and protocols to achieve Computer Security. T5. Apply accepted security policies; procedures are necessary to secure Operating Systems and applications. The practical should be carried out in such a manner that students are able to acquire different learning out comes in cognitive, affective domain to demonstrate course learning outcomes.

Course Content				
Name of UNIT	Unit Content	Unit Learning Outcomes	Marks	Hrs
UNIT – 1 Introduction to Security and Threats:	1.1 Introduction to Security 1.2 Threats to security: Viruses and Worms, Intruders, Insiders, Information warfare 1.3 Security Basics – Confidentiality, Integrity, Availability 1.4 Authentication and Authorization 1.5 Types of attack: Active attack and Passive attack 1.6 Other Attack: Backdoors and trapdoors, sniffing, spoofing, man in the middle, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs	1a. List and discuss various security terms, recent trends in computer security. 1b.Describe various types of threats that exist for computers and networks. 1c. Describe Security Services 1d.Describe various types of computer and network attacks 1e.Describe physical security components that can protect any computer and network. 1f.explain characteristics of a strong password.	10	10

	1.7 Physical security: Biometrics: finger prints, hand prints, Retina, voice patterns. 1.8. Describe Good Password.			
UNIT – 2 Cryptography	2.1 Introduction to Encryption Scheme: Symmetric encryption & Asymmetric encryption 2.2 Symmetric Encryption algorithm / Cipher-Encryption and Decryption using: Caesar's cipher, shift cipher, playfair cipher, Vigenere cipher, one time pad (vernam cipher), hill cipher (encryption only) Transposition techniques: rail fence 2.3 steganography 2.4 Hashing function : SHA1 2.5 Asymmetric encryption: 2.5.1 Maintain Confidentiality 2.5.2 Maintain Authentication 2.5.3 Maintain Authentication And Confidentiality 2.6 Digital Signatures, Key escrow	2a. Identify and describe types of cryptography. 2b.List and describe various Encryption Algorithms. 2c. Understand Hashing using SHA1 mechanism. 2d. Describe how authentication is achieve using digital signature 2e. State the advantage of Asymmetric encryption over symmetric	14	10
UNIT – 3 Public key Infrastructure	3.1 Basics of PKI 3.2 Digital certificates: 3.2.1 Role of Certificate Authority 3.2.2 Role of Registration Authority 3.2.3 Steps for obtaining a digital certificate 3.2.4 Steps for verifying authenticity and integrity of a certificate 3.3 Centralized or decentralized infrastructure, private key protection 3.4 Trust Models: Hierarchical, peer to peer, hybrid	3a. List the basics of public key infrastructures. 3b. Describe the roles of certificate authorities and certificate repositories. 3c. Explain the relationship between trust and certificate verification 3d. Explain use of digital certificates. 3e.Distinguish centralized and decentralized infrastructures. 3f. List and describe trust models	12	8
UNIT – 4 Network security	4.1 Firewalls: working, types design principles, 4.2 Kerberos 4.3 Security topologies – security zones, DMZ, Internet, Intranet, VLAN, tunnelling. 4.4 IP security: Architecture and security	4a. Explain working principle of FIREWALLs 4b.Classify and describe various security topologies. 4c.Describe various security topologies.	12	8
UNIT – 5 Web Security	5.1 Intruders, Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS	5a. List & Explain Web Security Threats. 5b. Explain securities in SSL and TLS. 5c. Explain concept of secure electronic transaction	12	9

	5.2 signature based IDS, anomaly based IDS 5.3 Advantages and disadvantages of NIDS and HIDS 5.4 Transport Layer Security: Secure Socket Layer/TLS 5.5 Application Layer Security: Secure Electronic Transaction (SET)			

List of Practical		
No.	Unit	Name of Practical
1	I	List and practice various “net” Commands on DOS & Linux
2	I	Configure Web browser security settings.
3	I	To study about various threat: DoS, backdoors, trapdoors, sniffing, spoofing, man in the middle & replay attacks.
4	I	To understand Security services and its related security mechanism.
5	II	Write, test and debug Ceaser cipher algorithm in C/C++/Java/Python.
6	II	Write Ceaser’s Cipher algorithm & Solve various examples based on Encryption & Decryption.
7	II	Write algorithm/steps for Shift Cipher & solve various examples on it
8	II	Write algorithm/steps for Verman Cipher & solve.
9	II	Write algorithm/steps for playfair cipher and solve examples on it
10	II	Write algorithm/steps for Hill Cipher and solve examples on it(only encryption)
11	II	Write algorithm/steps for Shift Cipher & solve various examples on it
12	II	Write algorithm/steps for Vignere Cipher & solve various examples on it.
13	III	To study about Public Key Infrastructure.
14	III	Demonstrate traffic analysis of different network protocols using tool. i.e. Wire-shark
15	IV	To study about various Security Topologies.
16	V	Host-based Intrusion Detection System
17	V	Network-based Intrusion Detection System
18	V	Give presentation on any recent trend of security.
19	V	Prepare poster on any recent trend of security.

List of Instruments / Equipment / Trainer Board	
1	Wireshark Traffic Analysis
2	Packet Sniffing Tool, Snort Packet Sniffing tool

List of Text Books			
No	Title of Text Books	Authors	Publication
1	Cryptography and Network Security Principal and Practices	Atul Kahate	Tata-McGraw-Hill

List of Reference Books			
No	Title of Reference Books	Authors	Publication
1	Cryptography and Network Security Principles and Practices	Williams Stallings	Pearson Education
2	Cryptography and Network Security	B A Forouzen	Tata-McGraw-Hill

Link of Learning Web Resource

1	http://www.cse.iitm.ac.in/~chester/courses/16e_cns/slides/01_Introduction.pdf
2	https://www.wireshark.org/docs/wsug_html_chunked/
3	https://www.wireshark.org/download.html
4	https://www.snort.org/docs