

Subject Code: 1ET4040602	Subject Title: NETWORK SECURITY
Pre-Requisite	Knowledge of Computer Network

RATIONALE:

Present computing era is based on internet and hence networking is an essential part of course. Prime concern is that in current advanced digital world various security threats are increasing day by day posing problems to data confidentiality, integrity and availability. This course aims at learning basic cryptography techniques and applying security mechanisms for operating systems as well as private and public network to protect them from various threats.

COURSE OBJECTIVE:

To understand basics of Cryptography and Network Security. To be able to secure a message over insecure channel by various means. learn about how to maintain the Confidentiality, Integrity and Availability of a data. Understand various protocols for network security to protect against the threats in the networks.

TEACHING AND EVALUATION SCHEME:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				Total (Marks)
Lecture	Tutorial	Practical	Credit	Theory		Practical		
				University Assessment	Continuous Assessment	University Assessment	Continuous assessment	
3	0	2	4	60	40	20	30	150

DETAILS OF COURSE CONTENTS:

SR. NO.	Topic and Sub-Topics	Total Hrs.	Weightage %
Unit – I	Introduction and Security Threats: 1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare 1.2 Avenues of Attack, steps in attack 1.3 Security Basics –Confidentiality, Integrity, Availability 1.4 Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs	6	15
Unit – II	Organizational Security 2.1 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non employees. 2.2 People as Security Tool: Security awareness, and Individual user responsibilities. 2.3 Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature And writing patterns, keystrokes, Physical barriers. 2.4 Password Management, vulnerability of password, password	6	15

	protection, password selection strategies, components of a good password.		
Unit – III	Cryptography and Public key Infrastructure 3.1 Introduction to Symmetric encryption & Asymmetric encryption. 3.2 Encryption algorithm / Cipher, Encryption and Decryption using: Caesar's cipher, playfair cipher, shift cipher, shift cipher, Vigenere cipher, one time pad (vermin cipher), hill cipher (for practice use small matrix and apply encryption only). 3.3 Transposition techniques (rail fence), steganography 3.4 Hashing function : SHA1 (only) 3.5 Asymmetric encryption: Digital Signatures, Key escrow 3.6 Public key infrastructures : basics, digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate 3.7 Centralized or decentralized infrastructure, private key protection 3.8 Trust Models: Hierarchical, peer to peer, hybrid	14	32
Unit – IV	Network security 4.1 Firewalls: working, design principles, trusted systems, Kerberos. 4.2 Security topologies – security zones DMZ, Internet, Intranet, VLAN, security implication, tunneling 4.3 IP security : overview, architecture, IPSec configurations, IPSec security 4.4 Email security : security of email transmission, malicious code, spam, mail encryption	8	19
Unit - V	Web Security 5.1 Intruders, Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, network IDS components, advantages and disadvantages of NIDS, host based IDS components, advantages and disadvantages of HIDS. 5.2 Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL) & Transport Layer Security(TLS), Concepts of secure electronic transaction	8	19

COURSE OUTCOME:

The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning outcomes in cognitive, psychomotor and affective domain to demonstrate following course outcomes.

- Identify and describe the common types of security threats and risks to the Computer Systems and the nature of common Information hazards.
- Identify the potential threats to confidentiality, integrity and availability of Computer Systems.
- Describe the working of standard security mechanisms and applied to the external and internal network.

- iv. Define cryptography, describe the elements of the encryption process and select best algorithm to encrypt data and protocols to achieve Computer Security.
- v. Apply accepted security policies, procedures are necessary to secure Operating Systems and applications.

SUGGESTED LIST OF EXERCISES/PRACTICAL/EXPERIMENTS:

S. No.	Exercises (Course Outcomes in Psychomotor Domain according to NBA Terminology)
1	List and practice various “net” Commands on DOS & Linux.
2	Configure a system for various security experiments.
3	Configure Web browser security settings.
4	Draw Diagram of DoS, backdoors, trapdoors.
5	Draw diagrams of sniffing, spoofing, man in the middle & replay attacks.
6	Draw diagram for Confidentiality, Integrity & Availability.
7	Write Ceaser’s Cipher algorithm & Solve various examples based on Encryption & Decryption.
8	Write, test and debug Ceaser cipher algorithm in C/C++/Java/Python/Matlab.
9	Write algorithm/steps for Shift Cipher & solve various examples on it.
10	Write algorithm/steps for Hill Cipher and solve examples on it.
11	Write algorithm/steps for playfair cipher and solve examples on it.
12	Write algorithm/steps for Verman Cipher & solve
13	List and practice various “net” Commands on DOS & Linux. various examples on it.
14	Draw various Security Topologies.
15	Demonstrate traffic analysis of different network protocols using tool. i.e. Wire-shark. (Atleast one of them should be recorded and included in term work.)
16	Demonstrate Sniffing using packet tool i.e. snort.
17	Configure your e-mail account against various threats. i.e. spam attack, phishing, spoofing etc.
18	Draw diagram Host-based Intrusion Detection System
19	Draw diagram Network-based Intrusion Detection System
20	Demonstration of SQL-Injection.
21	Demonstration of readymade encryption/decryption code

LIST OF REFERENCES:

Reference Books

S. No.	Title of Book	Author
1	Principles Of Computer SecurityCompTIA Security+ And Beyond (Exam SY0-301), 3 rd Edition Books	Conklin, Wm. Arthur Gregory White, Dwayne Williams, Roger Davis, Chuck Cothren, Corey Schou

2	Cryptography and Network Security Principles and Practices	Williams Stallings
3	Principles of Computer Security CompTIA Security+ and Beyond Lab Manual	Vincent Nestler, Gregory White, Wm.Arthur Conklin, Matthew Hirsch, Corey Schou
4	Cryptography and Network Security Principal and Practices	Atul Kahate
5	Cryptography and Network Security	B A Forouzen
6	Computer Security Basics	Deborah Russell G.T. Gangenisr
7	Computer Security	Dieter Gollman

E- Learning References

- i. Software: Wireshark Traffic Analysis/Packet Sniffing Tool, Snort Packet Sniffing tool
- ii. www.securityplusolc.com.
- iii. <http://mercury.webster.edu/aleshunna/COSC%20130/COSC%20130%20Home.htm>
- iv. <http://williamstallings.com/Cryptography/>
- v. <http://mercury.webster.edu/aleshunna/COSC%20130/Chapter-22.pdf>
- vi. <http://nptel.iitm.ac.in/courses.php?disciplineId=106>
- vii. Network Simulator Tool: GNS3 v0.8.5, NetSimK
- viii. <http://www.snort.org/docs>