

Branch Name:	Computer Engineering / Information Technology
Program Code:	ET404 / ET407
Course Title:	Network Security
Course Code:	2ET4040602
Pre-requisite Course:	Knowledge of Computer Network

Course Objectives:

1. To understand basics of Cryptography and Network Security.
2. To be able to secure a message over insecure channel by various means.
3. Learn about how to maintain the Confidentiality, Integrity and Availability of a data.
4. Understand various protocols for network security to protect against the threats in the networks.
5. Understanding the purpose and implementation of firewalls and intrusion detection/prevention systems.
6. Developing skills to troubleshoot network security issues and diagnose problems.

Teaching and Examination Scheme:

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

Course Contents:

Unit No	Topic	Total Hours	Weightage (%)
1	Introduction and Security Threats: 1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare Avenues of Attack, steps in attack 1.2 Security Basics –Confidentiality, Integrity, AvailabilityTypes of attack: Denial of service (DOS), backdoors and trapdoors, sniffing,spoofing, man in the middle, replay 1.3 TCP/IP Hacking, Phishing attacks, Distributed DOS, SQLInjection. Malware : Viruses, Logic bombs	6	15
2	Organizational Security 1.4 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software/hardware, Access by non employees. 1.5 People as Security Tool: Security awareness and Individual user responsibilities. 1.6 Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature 1.7 And writing patterns, keystrokes, Physical barriers. 1.8 Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.	6	15
3	Cryptography and Public key Infrastructure 3.1 Introduction to Symmetric encryption & Asymmetric encryption. 3.2 Encryption algorithm / Cifer, Encryption and Decryption using: Caesar's cipher, playfair cipher, shift cipher, shift cipher, Vigenere cipher, one time	14	32

	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		
4	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 4.5 code, spam, mail encryption	8	19
5	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

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-hark. (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

Text Books: Cryptography and Network Security Principles and Practices BY Williams Stallings

List of Open-Source Software/learning website:

1. www.securityplusolc.com.
2. <http://mercury.webster.edu/aleshunas/COSC%205130/COSC%205130%20Home.htm>
3. <http://williamstallings.com/Cryptography/>
4. <http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf>
5. <http://nptel.iitm.ac.in/courses.php?disciplineId=106>
6. Network Simulator Tool: GNS3 v0.8.5, NetSimK
7. <http://www.snort.org/docs>

Course Learning Outcomes (CLO):

1. Identify and describe the common types of security threats are risks to the Computer Systems and the nature of common Information hazards.
2. Identify the potential threats to confidentiality, integrity and availability of Computer Systems.
3. Describe the working of standard security mechanisms and applied to the external and internal network.
4. Define cryptography, describe the elements of the encryption process and select best algorithm to encrypt data and protocols to achieve Computer Security.
5. Apply accepted security policies; procedures are necessary to secure Operating Systems and applications.
6. The field of network security is constantly evolving, so courses often cover emerging threats and technologies.

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes(POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	L			L									H		
CLO2	M	M	L											M		
CLO3	H	H		M											H	
CLO4	H		M	M										H		
CLO5	H	M		L										H		
CLO6	H	M		L											M	

H:High, M:Medium, L:Low