



Paper Code : NIS 602

Paper Name: Networks and Information Security

Teaching Hours (Per Week)		Examination Scheme		
TH. (hours)	Pr. (hours)	Internal	External	Total
		Th. (marks)	Th. (marks)	
4		30	70	100 (marks)

Lectures = 68 hours

UNIT I: [15]

Introduction to Information Security

Need of Information Security, Attributes of Information Security, Authentication, Confidentiality, Integrity, Availability, Non Repudiation, Access Control.

Threats and Vulnerabilities, Security Attacks, Unauthorized Access, Impersonation, Denial of Service.

Malicious Software, Viruses, Worms, Trojan Horses.

Identification and Authentication, Password Authentication, Password Vulnerabilities and attacks, Password Policy, Single Sign-on, Kerberos, Biometrics Authentication.

UNIT II: [16]

Cryptography

Cryptography Basics: Plain Text, Cipher Text, Encryption Algorithm, Decryption Algorithm, Cryptanalysis, Symmetric and Asymmetric Encryption, Substitution Cipher, Transposition Cipher, One time Pad, Block and Stream Ciphers, Data Encryption Standard (DES).

Message Authentication and Hash Function.

Public Key Cryptography principles and application, RSA, Public Key Encryption Algorithm.

Digital Signatures, Digital Certificate, Certificate Authorities.

UNIT III: [15]

Network Security

Network Devices: Switches, Routers, Firewalls, VPN Concentrators, Load Balancers, Proxies, Network Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS).

Network Protocol: Overview of IPV4 and IPV6, OSI Model, Maximum Transfer Unit, Internet Protocol (IP), Transport Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Domain Name System (DNS).

Network Design: Network Address Translation (NAT), Demilitarized Zone (DMZ), Subnetting, Switching, Virtual Local Area Network (VLAN).

Network Attack: Buffer Overflow, TCP Session, Hijacking, Sequence Guessing, Network Scanning.

IP Security overview and architecture.



UNIT IV:

Web and E-mail Security

[12]

Web Servers and Browsers, HTTP, Cookies, Caching, Plug-in, ActiveX, Java, JavaScript, Secure Socket Layer (SSL), Secure Electronic Transaction (SET).

E-mail Risks, Spam, E-mail Protocols, Simple Mail Transfer Protocol (SMTP), Post office Protocol (POP), Internet Access Message protocol (ICMP).

Secured Mail: Pretty Good Privacy (PGP), *S/MIME* (Secure/Multipurpose Internet Mail Extensions)

UNIT V:

Firewall

[10]

Firewall Design principles, Firewall Characteristics, Types of Firewalls, Packet Filtering Router, Stateful Inspection Firewall, Application Level Gateway or Proxy, Circuit Level Gateway, Bastion Host.

Firewall Configuration, Screened Host Firewall System, Screened Subnet Firewall System.

Text Books:

1. William Stallings "Cryptography and network security, principles and practices", Pearson
2. Gollmann, Dieter, "Computer Security", John Wiley & Sons Ltd.

Reference Books:

1. Debby Russell, T. Gangemi, Sr., "Computer Security", O'Reilly publications.
2. Simson Garfied, "Web security, Privacy Commerce,", O'Reilly Publications.
3. Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Edition