

# **B5.3-R3: NETWORK MANAGEMENT & INFORMATION SECURITY**

Lectures	70
Practical / tutorials	50
Total	120

## **Detailed Syllabus**

### **1. Introduction to Information Security (4 Hrs.)**

Attributes of Information Security: Confidentiality, Integrity, Availability.

Threats & Vulnerabilities: Unauthorized Access, Impersonation, Denial of Service, Malicious Software; Trap Doors, Logic Bomb, Trojan Horses; Viruses, Worms & Bacteria; Security Strategies & Processes; Importance of Security Policies and Audits.

### **2. Identification & Authentication (5 Hrs.)**

Definitions, Types of authentication, Password Authentication, Password Vulnerabilities & Attacks: Brute Force & Dictionary Attacks.

Password Policy & Discipline, Single Sign-on - Kerberos, Alternate Approaches:

Biometrics: Types of Biometric Techniques: False Rejection, False Acceptance, Cross Over Error Rates.

### **3. Access Control (6 Hrs.)**

Background, Subjects and Objects, Access Control Techniques: Mandatory Access Control, Discretionary Access Control, Access Control Lists, Role Based Access Control.

Access Control Structures, Window NT & Unix Access Control methods, Access Control Method: Bell-La Padula Model, Biba Integrity Model

### **4. Security Policy Design (6 Hrs.)**

Definition: Security Policy Document

Risk Management: Risk Assessment: Identification of assets, Identification of Threats to assets, Risk Calculation: Annualized Loss Expectancy (ALE).

Security Policy Framework: Components of an enterprise Network, Elements of a Security Architecture.

Design and Implementation: Physical Security Controls, Logical Security Controls, Infrastructure' & Data Integrity, Policies and Procedures for Staff: Secure Backups, Equipment Certification, Audit Trails

Security Awareness Training.

Incident Handling: Preparation, Detection of an Incident, Responding to an Incident, Recovering from an Incident, Building an Incident Response Team.

## **5. Cryptography (6 Hrs.)**

Cryptography Basics: Plain Text, Cipher Text, Encryption Algorithm, Decryption Algorithm; Requirements for Cryptography.

Cryptanalysis and attacks, Conventional Symmetric Encryption Algorithms: Symmetric vs Asymmetric, Block and Stream ciphers, DES, Double and Triple DES, Cryptographic Modes.

Key Distribution, Link Encryption & End-End Encryption. Steganography,

## **6. Public Key Infrastructure & Message Authentication (6 Hrs.)**

Public Key Cryptography Principles & Applications, Algorithms: RSA, Diffe-Hellman Key Exchange, DSS, Elliptic-curve.

One way Hash Functions: Message Digest, MDS, SHA 1.

Digital Signatures: Public Key Infrastructure: Digital Certificates, Certificate Authorities.

## **7. Network Security (9 Hrs.)**

Overview of IPV4: OSI Model, Maximum Transfer Unit, IP, TCP, UDP, ICMP; ARP, RARP and DNS; Ping, Traceroute.

Network Attacks: Buffer Overflow, IP Spoofing, TCP Session Hijacking, Sequence Guessing, Network Scanning: ICMP, TCP sweeps, Basic Port Scans; Denial of Service Attacks: SYN Flood, Teardrop attacks, land, Smurf Attacks.

Virtual Private Network Technology: Tunneling, IPSEC: Traffic Protocols: Authentication Headers, ESP Internet Key Exchange (IKE), Security Association PPTP, L2TP.

## **8. Network Management (9 Hrs.)**

Network Management Architecture & Applications: Management Standards and Models

Network Management Functions - Configuration: Configuration Management, Configuration Database & Reports, ASN.1

Network Management Functions: Fault: Management, Identification and Isolation; Security: Protecting Sensitive Information, Host and User Authentication.

SNMP v1, SNMP, V3: Structure of Management Information, Std. Management Information Base, SNMPv1 Protocol

Network Management Accounting & Performance Functions: Accounting Management, Performance Management, Network Usage, Metrics and Quotas.

## **9. Web Security & Application Security (6 Hrs.)**

Web Servers & Browsers: Security features, server privileges, active pages, scripting, Security configuration setting for browsers, Security of active content: JAVA, JAVA Script, Active x, plug-ins, cookies.

SSL & SET, Secured Mail: PEM and PGP.

## **10. Firewalls & Intrusion Detection Systems (8 Hrs.)**

Firewall Characteristics & Design Principles, Types of Firewalls: Packet Filtering Router, Application Level Gateway or Proxy, Content Filters, Bastion Host.

Firewall Architectures: Dual Homed Host, Screening Router, Screened Host, Screened Subnet.

Firewall logs, Intrusion Detection Systems: Components of an IDS, Placement of IDS Components, Types of IDS: Network Based IDS, File Integrity Checkers, Host Based IDS; IDS Evaluation parameters.

## **11. Law & Investigation (5 Hrs.)**

IT Act 2000: Objectives, Provisions, Offences

Cyber crimes: Crimes against the computer, Crimes using a computer, Investigation Issues: Cyber Forensics

## **Recommended Books**

### **Main Reading**

William Stallings, "Network Security Essentials"

Gollmann, Dieter, "Computer Security"

Micki Krause, Harold F. Tipton, "Handbook of Information Security Management"

## **Supplementary Reading**

Debby Russell, T. Gangemi, Sr., "Computer Security Basics"

Simson Garfield, "Web Security, Privacy Commerce"

Dr. R.K. Tiwari, P.K. Sastri, K.V. Ravikumar, "Computer Crime and Computer Forensics"