RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science & Information Technology, VI-Semester

Open Elective CSIT- 604 (A) Cryptography and Network Security

Course Objectives:

This Course focuses towards the introduction of network security using various cryptographic algorithms. It also focuses on the practical applications that have been implemented and are in use to provide email and web security.

Course Outcomes:

1. Analyze and evaluate the cyber security needs of an organization.
2. Analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
3. Measure the performance and troubleshoot cyber security systems.
4. Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools.
5. Design and develop security architecture for an organization.
6. Design operational and strategic cyber security strategies and policies.

Course Contents:

UNIT I:

Introduction to Network Security, Computer Securit y and Cyber Security. Security Terminologies and Principle, Security Threats, Types of attacks (Operating System, application level, Shrink Wrap code, Misconfiguration attacks etc.). Introduction to Intrusion, Terminologies, Intrusion Detection System (IDS), Types of Intrusion Detection Systems, System Integrity Verifiers (SIVS).Indication of Intrusion: System Indications, File System Indications Network Indications. Intrusion Detection Tools ,Post attack IDS Measures & Evading IDS Systems. Penetration Testing, Categories of security assessments, Vulnerability Assessment, Types of Penetration Testing. Risk Management.

UNIT II:

Cryptography, Classical Cryptographic Techniques, Encryption, Decryption, Code Breaking: Methodologies, Cryptanalysis, Cryptography Attacks, Brute-Force Attack, Use of Cryptography. Public key cryptography, Principles of Public key Cryptosystems, Cryptographic Algorithms RSA, Data Encryption Standard (DES), RC4, RC5, RC6, Blowfish, Key Management, Diffie- Hellman key exchange, elliptic curve cryptography.

UNIT III:

Hash Functions, One-way Hash Functions, SHA (Secure Hash Algorithm), Authentication Requirements, Authentication Functions, Kerberos. Message Authentication codes, Message Digest Functions, MD5, SSL (Secure Sockets Layer), SSH (Secure Shell), Algorithms and Security, Disk Encryption, Government Access to Keys (GAK) Digital Signature: Analysis, Components, Method, Applications, Standard, Algorithm: Signature Generation/Verification, ECDSA, EIgamal Signature Scheme, Digital Certificates.

UNIT IV:

Trojans and Backdoors: Overt and Covert Channels, Working, Types (Remote Access Trojans, Data-Sending Trojans, Destructive Trojans, Trojans, Proxy Trojans, FTP Trojans, Security Software Disablers). **Viruses and Worms:** Characteristics, Working, Infection Phase, Attack Phase. Sniffers: Definition, spoofing, Sniffing, Vulnerable Protocols, Types.**Phishing:** Methods, Process, Attacks Types (Man-in-the-Middle Attacks, URL Obfuscation Attacks, Hidden Attacks, Client-side Vulnerabilities, Deceptive Phishing, Malware-Based Phishing, DNS Based Phishing, Content-Injection Phishing, Search Engine Phishing). **Web Application Security-** Secured authentication mechanism, secured session management, Cross-site Scripting, SQL Injection and other vulnerabilities **Denial-of Service Attacks:** Types of Attacks (Smurf Attack, Buffer Overflow Attack, Ping of Death Attack, Teardrop Attack, SYN Attack, SYN Flooding), DDoS Attack(Distributed DoS Attack.), Session Hijacking, Spoofing v Hijacking, TCP/IP hijacking, CAPTCHA Protection.

UNIT V:

IP Security, Web Security, Firewalls: Types, Operation, Design Principles, Trusted Systems. Computer Forensics, Need, Objectives,Stages & Steps of Forensic Investigation in Tracking Cyber Criminals, Incident Handling. Hacking, Classes of Hacker (Black hats, grey hats, white hats, suicide hackers), Footprinting, Scanning (Types-Port, Network, Vulnerability), E-Mail Spiders, Overview of System Hacking Cycle.

Recommended Books:

1. William Stallings, “Cryptography and Network Security: Principles and Practice” Pearson Charlie Kaufman, Radia Perlman, Mike Speciner, Michael Speciner, “Network Security - Private communication in a public world” TMH
2. Fourozon, “Cryptography & Network Security” TMH.
3. Joseph Migga Kizza, Computer Network Security, Springer International Edition.
4. Atul Kahate, “Cryptography and Network Security” Mc Graw Hill
5. Carl Endorf, Eugene Schultz, Jim Mellander “Intrusion Detection & Prevension” TMH.
6. Neal, Krawetz, Introduction to Network Security,Cengage Learning.