GMRIT

Curriculum
2021

M. Tech.
Cyber Security
(Duration of Study : 2 years)

GMRIT
Training Tomorrow's Engineers Today

Department of Computer Science and Engineering
GMR Institute of Technology
Rajam, Andhra Pradesh
(An Autonomous Institute Affiliated to JNTU Kakinada, AP)
NBA Accredited and NAAC Accredited

Department of Computer Science and Engineering
M. Tech Specialization: Computer Science in Cyber Security

[Minimum Credits to be earned: 68]

No	Course Code	Course	POs	Periods			
				L	T	P	C
First Semester							
1	21MEX101	Advanced Optimization Techniques		4	-	-	4
2	21CCS101	Cryptography and Network Security		4	-	-	4
3		**Elective I**		4	-	-	4
4		**Elective II**		4	-	-	4
5		**Elective III**		4	-	-	4
6	21CCS102	Cryptography and Network Security Laboratory		-	-	3	1.5
7	21CCS103	Term Paper		-	-	3	1.5
			Total	**20**	**-**	**6**	**23**
Second Semester							
1	21CCS201	Principles of Secure Coding		4	-	-	4
2	21CCS202	Cybernet security		4	-	-	4
3		**Elective IV**		4	-	-	4
4		**Elective V**		4	-	-	4
5		**Elective VI**		4	-	-	4
6	21CCS203	Secure Coding Laboratory		-	-	3	1.5
7	21CCS204	Cybernet security Lab		-	-	3	1.5
			Total	**20**	**-**	**6**	**23**
Third Semester							
No	**Course Code**	**Course**	**POs**	**Periods**			
				L	**T**	**P**	**C**
1	21CCS301	Internship		-	-	-	4
2	21CCS302	Project Work		-	-	-	-
3		Research Methodology and IPR (Audit course)		-	-	-	0
			Total	-	-	-	**4**
Fourth Semester							
1	21CCS303	Project Work		-	-	-	18
			Total	-	-	-	**18**

List of Elective Courses

No	Course Code	Course	POs	Periods			
				L	T	P	C
Elective I							
1	21CCS001	Ethical Hacking and Counter Measures - 1		4	-	-	4
2	21CCS002	Computer Hacking and Forensic Investigator - 1		4	-	-	4
3	21CCS003	Incident Handler - 1		4	-	-	4
Elective II							
1	21CCS004	Managing and Securing networks		4	-	-	4
2	21CCS005	TCP/IP		4	-	-	4
3	21CCS006	Wireless Adhoc Networks		4	-	-	4
Elective III							
1	21CCS007	Fundamentals of Computer Science and Engineering		4	-	-	4
2	21CCS008	Fundamentals of Wireless sensor networks		4	-	-	4
3	21CCS009	Network Intrusion and Incidence Response		4	-	-	4
Elective IV							
1	21CCS010	Ethical Hacking and Counter Measures - 2		4	-	-	4
2	21CCS011	Computer Hacking and Forensic Investigator – 2		4	-	-	4
3	21CCS012	Incident Handler - 2		4	-	-	4
Elective V							
1	21CCS013	Penetration Testing and Vulnerability Assessment		4	-	-	4
2	21CCS014	Practical Vulnerability Management		4	-	-	4
3	21CCS015	Intrusion Detection and Prevention		4	-	-	4
Elective VI							
1	21CCS016	Cloud Architecture and Security		4	-	-	4
2	21CCS017	Protocols and Architectures for Wireless Sensor Networks		4	-	-	4
3	21CCS018	Fundamentals of 5G Mobile Networks		4	-	-	4

21MEX101 Advanced Optimization Techniques

4 0 0 4

Course outcomes

1. Design of mechanical systems and interdisciplinary engineering applications and business solutions using suitable optimization technique
2. Apply numerical or iterative techniques in power systems for optimal power flow solutions
3. Optimize the parameters in control systems for desired steady state or transient response
4. Optimize the cost function in deciding economic factors of power systems
5. Design of electrical systems optimally using suitable techniques like univariate method, steepest descent method etc
6. Design of electrical systems optimally using, steepest and descent method etc

Unit I
Linear programming and Assignment Problem

Linear programming-Two-phase simplex method, Big-M method, duality, interpretation, applications, Assignment problem- Hungarian's algorithm, Degeneracy, applications, unbalanced problems, traveling salesman problem

Applications of assignment problems

11+4 Hours

Unit II
Classical and Numerical Optimization Techniques

Classical optimization techniques-Single variable optimization with and without constraints, multi–variable, optimization without constraints, multi–variable optimization with constraints–method of Lagrange multipliers, Kuhn-Tucker conditions.
Numerical methods for optimization-Nelder Mead's Simplex search method, Gradient of a function, Steepest descent method, Newton's method, types of penalty methods for handling constraints

Exterior penalty function method for handling constraint

11+4 Hours

Unit III
Genetic algorithm and Programming

Genetic algorithm (GA)-Differences and similarities between conventional and evolutionary algorithms, working principle, reproduction, crossover, mutation, termination criteria, different reproduction and crossover operators, GA for constrained optimization, draw backs of GA.
Genetic Programming (GP)-Principles of genetic programming, terminal sets, functional sets, differences between GA & GP, random population generation, solving differential equations using GP

Solving differential equations using GP

12+4 Hours

Unit IV
Multi-Objective GA

Multi-ObjPareto's analysis, Non-dominated front, multi–objective GA, Non-dominated sorted GA, convergencecriterion, applications of multi-objective problems

Basic Problem solving using Genetic algorithm, Genetic Programming & Multi Objective GA and simpleapplications of optimization for engineering systems

Simple applications of optimization for engineering systems

12+3 Hours
Total 45+15 Hours

Reading material

1. J. S. Arora, Introduction to Optimum Design, McGraw Hill International Ed., NY, 1989
2. K. Deb, Optimization for Engineering Design: Algorithms and Examples, 2nd Ed., PHI, 1995
3. S. S. Rao, Engineering Optimization: Theory and Practice, New Age International (P) Ltd., 2001
4. D. E. Goldberg, Genetic Algorithms in Search and Optimization, Pearson publication, 1990
5. J. R. Koza, Genetic Programming, MIT Press, 1993
6. K. Deb, Multi-Objective Optimization Using Evolutionary Algorithms, Wiley, 2001

21CCS101 Cryptography and Network Security

4 0 0 4

Course Outcomes

1. Identify common network security vulnerabilities/attacks.
2. Explain the foundations of Cryptography and network security.
3. Demonstrate detailed knowledge of the role of encryption to protect data.
4. Analyze security issues arising from the use of certain types of technologies.
5. Identify the appropriate procedures required to secure networks.
6. Analyze the possible security attacks in complex real time systems and their effective countermeasures.

Unit I

Introduction and Number Theory

Security trends, Attacks and services, Classical crypto systems, Different types ofciphers, LFSR sequences, Basic Number theory, Congruences, ChineseRemainder theorem, Modular exponentiation, Fermat and Euler's theorem, Legendreand Jacobi symbols
Finite fields, continued fractions

11+4 Hours

Unit II
Conventional and Public Key Cryptography

Simple DES, Differential cryptoanalysis, DES, Modes of operation, Triple DES, AES, RC4, RSA, Attacks, Primality test.
Factoring

12+3 Hours

Unit III
Hash Functions and Digital Signatures

Discrete Logarithms, Computing discrete logs, Diffie-Hellman key exchange, ElGamal Public key cryptosystems, Hash functions, Secure Hash, Birthday attacks, MD5, Digital signatures, RSA, ElGamal.
DSA.

11+4 Hours

Unit IV
Authentication Applications and System Security

Authentication applications, Kerberos, X.509, PKI, Electronic Mail security, PGP,S/MIME, IP security, WebSecurity, SSL, TLS, SET.System security, Intruders, Malicious software, viruses, Firewalls.
SecurityStandards.

Reading Material

1. Wade Trappe, Lawrence C Washington, “Introduction to Cryptography with coding theory”, 2nd Edition, Pearson, 2007.
2. William Stallings, “Cryptography and Network security Principles and Practices”, Pearson/PHI, 4th Edition, 2006.
3. W. Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, 2nd Edition, 2007.
4. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing 3rd Edition – Prentice Hall of India, 2006.

21CCS001 Ethical Hacking and Counter Measures-1

4 0 0 4

Course Outcomes

1. Understand key issues plaguing the information security world, incident management process, and penetration testing.
2. Understand various types of footprinting, footprinting tools, Network scanning techniques and apply countermeasures.
3. Understand Enumeration techniques and apply enumeration countermeasures.
4. Understand and apply System hacking methodology, steganography, steganalysis attacks, and covering tracks.
5. Understand Different types of Trojans analyze Trojans, and apply Trojan countermeasures.
6. Understand Social Engineering techniques, identify theft, and apply social engineering countermeasures.

Unit I

Introduction to Ethical hacking, Footprinting & Reconnaissance and Scanning Networks

Introduction to Ethical hacking: Information Security Overview – Information Security Threats and Attack Vectors – Hacking Concepts, Types, and Phases – Ethical Hacking Concepts and Scope – Information Security Controls – Information Security laws and Standards.
Footprinting and Reconnaissance: Footprinting Concepts – Footprinting Methodology – Footprinting Tools – Footprinting Countermeasures – Footprinting penetration Testing.
Scanning Networks: Check for Live systems – Check for Open Ports – Scanning Beyond IDS - Banner Grabbing – Scan for Vulnerability – Draw Network Diagrams – Prepare Proxies – Scanning Pen Testing

12+4 Hours

Unit II
Enumeration and System hacking

Enumeration: Enumeration Concepts – NetBIOS Enumeration – SNMP Enumeration – LDAP Enumeration – NTP Enumeration – SMTP and DNS Enumeration – Enumeration Countermeasures – Enumeration Pen Testing.
System hacking: Cracking Passwords – Escalating Privileges – Executing Applications - Hiding files – Covering Tracks – Penetration Testing

11+4 Hours

Unit III
Malware Threats and Sniffing

Malware Threats: Introduction to malware – Trojan Concepts – Virus and Worm Concepts – malware Reverse Engineering – Malware detection - Countermeasures – Anti-Malware Software – Penetration Testing.
Sniffing: Sniffing Concepts – MAC Attacks – DHCP Attacks – ARP Poisoning – Spoofing Attack – DNS Poisoning – Sniffing Tools – Countermeasures – Sniffing Detection Techniques – Sniffing Pen Testing.

11+4 Hours

Unit IV
Social Engineering and Denial-of-Service

Social Engineering: Social Engineering Concepts – Social Engineering Techniques – impersonation on Social Networking Sites – Identity Theft – Social Engineering Countermeasures – Penetration Testing.
Denial-of-Service: DoS/DDoS Concepts – DoS/DDoS Attack Techniques – Botnets – DDoS Case Study – DoS/DDoS Attack Tools – Countermeasures – DoS/DDoS Protection Tools – DoS/DDoS Penetration Testing.

11+3 Hours

Total: 45+15 Hours

Reading Materials

1. ”CEH Study Guide” by EC-Council, 2016.
2. Kimberly Graves, ”CEH Study Guide”, SYBEX publishers, 2015.

21CCS002 Computer Hacking and Forensic Investigator-1

4 0 0 4

Course Outcomes

1. Perform incident response and forensics, Perform electronic evidence collections.
2. Perform digital forensic acquisitions, Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.
3. Examine and analyze text, graphics, multimedia, and digital images and also recover information and electronic data from computer hard drives and other data storage devices.
4. Work on technical examination, analysis and reporting of computer-based evidence.
5. Support the generation of incident reports and other collateral.
6. Plan, coordinate and direct recovery activities and incident analysis tasks.

Unit I

Computer Forensics in Today's World and Computer Forensics Investigation Process

Forensics Science - Computer Forensics - Security Incident Report - Aspects of Organizational Security - Evolution of Computer Forensics - Objective of Computer Forensics - Need for Compute Forensics - Forensics Readiness - Cyber Crime - Cyber Crime Investigation - Corporate Investigations

Investigating Computer Crime - Before the Investigation - Build a Forensics Workstation - Building the Investigation Team - People Involved in Computer Forensics - Review Policies and Laws - Forensics Laws - Notify Decision Makers and Acquire Authorization - Risk Assessment - Build a Computer Investigation Toolkit - Steps to Prepare for a Computer Forensics Investigation

Reporting a Cyber Crime.Computer Forensics Investigation Methodology

12+3 Hours

Unit II

Searching and Seizing Computers and Digital Evidence

Searching and Seizing Computers without a Warrant - Searching and Seizing Computers with a Warrant - The Electronic Communications Privacy Act - Electronic Surveillance in Communications Networks – Evidence.

Digital Data - Definition of Digital Evidence - Increasing Awareness of Digital Evidence -Challenging Aspects of Digital Evidence - The Role of Digital Evidence - Characteristics of Digital Evidence - Fragility of Digital Evidence - Anti-Digital Forensics (ADF) - Types of Digital Data - Rules of Evidence - Electronic Devices: Types and Collecting Potential Evidence - Digital Evidence Examination Process - Electronic Crime and Digital Evidence Consideration by Crime Category.

12+3 Hours

Unit III

First Responder Procedures

Electronic Evidence - First Responder - Roles of First Responder - Electronic Devices: Types and Collecting Potential Evidence - First Responder Toolkit - Creating a First Responder Toolkit -Evidence Collecting Tools and Equipment - First Response Basics - Securing and Evaluating Electronic Crime Scene - Conducting Preliminary Interviews - Documenting Electronic Crime Scene - Collecting and Preserving Electronic Evidence - Packaging and Transporting Electronic Evidence - Reporting the Crime Scene - Note Taking Checklist

First Responder Common Mistakes.

12+3 Hours

Unit – 4

Understanding Hard Disks and File System

Hard Disk Drive Overview - Disk Drive Overview - Hard Disk Drive - Solid-State Drive – (SSD) - Physical Structure of a Hard Disk - Logical Structure of Hard Disk - Types of Hard Disk Interfaces -Hard Disk Interfaces - Disk Platter – Tracks – Sector – Cluster - Bad Sector - Hard Disk Data Addressing - Disk Capacity Calculation - Measuring the Performance of the Hard Disk - Disk Partitions and Boot Process - Understanding File Systems - RAID Storage System.

File System Analysis Using The Sleuth Kit (TSK)

12+3 Hours

Total: 45+15 Hours

Reading Materials

1. "CHFI Study Guide" by EC-Council, 2016.

21CCS003 Incident Handler-1

4 0 0 4

Course Outcomes

1. Understand various incident responses
2. Analyze Different type of Risk policies
3. Identify an incident and apply various incident handling methods
4. Analyze the response of various of roles incident response teams and its services
5. Understand and implement the various policies and procedures of incident response
6. Identify various DoS incidents

Unit I

Module 01: Introduction to Incident Response and Handling

Cyber Incident Statistics - Computer Security Incident - Information as Business Asset - Data Classification - Common Terminologies - Information Warfare - Key Concepts of Information Security - Vulnerability, Threat, and Attack - Types of Computer Security Incidents - Examples of Computer Security Incidents - Verizon Data Breach Investigations Report – 2008 - Incidents That Required the Execution of Disaster Recovery Plans - Signs of an Incident- Incident Categories - Incident Prioritization - Incident Response - Incident Handling - Use of Disaster Recovery Technologies - Impact of Virtualization on Incident Response and Handling - Estimating Cost of an Incident - Key Findings of Symantec Global Disaster Recovery Survey – 2009 - Incident Reporting - Incident Reporting Organizations - Vulnerability Resources.

12+4 Hours

Unit II

Risk Assessment and Incident Response & Handling Steps

Risk Assessment: Risk - Risk Policy - Risk Assessment - NIST's Risk Assessment Methodology -Steps to Assess Risks at Work Place - Risk Analysis - Risk Mitigation - Cost/Benefit Analysis - NIST Approach for Control Implementation - Residual Risk - Risk Management Tools.

Incident Response and Handling Steps: How to Identify an Incident - Handling Incidents - Need for Incident Response - Goals of Incident Response - Incident Response Plan - Incident Response and Handling Steps - Training and Awareness - Security Awareness and Training Checklist - Incident Management - Incident Response Team - Defining the Relationship between Incident Response, Incident Handling, and Incident Management - Incident Response Best Practices - Incident Response Policy - Incident Response Plan Checklist - Incident Handling System: RTIR - RPIER 1st Responder Framework.

12+4 Hours

Unit III

CSIR

What is CSIRT? - What is the Need of an Incident Response Team (IRT) - CSIRT Goals and Strategy - CSIRT Vision - Common Names of CSIRT - CSIRT Mission Statement - CSIRT Constituency - CSIRT Place in the Organization - CSIRT Relationship with Peers - Types of CSIRT Environments - Best Practices for creating a CSIRT - Role of CSIRTs - Roles in an Incident Response Team - CSIRT Services - CSIRT Policies and Procedures - How CSIRT Handles a Case - CSIRT Incident Report Form - Incident Tracking and Reporting Systems – CERT - CERT-CC - CERT(R) Coordination Center: Incident Reporting Form - CERT:OCTAVE - World CERTs - http://www.first.org/about/organization/teams/

http://www.apcert.org/about/structure/members.html - IRTs Around the World.

12+4 Hours

Unit IV
Handling Network Security Incidents

Denial-of-Service Incidents - Distributed Denial-of-Service Attack - Detecting DoS Attack - Incident Handling Preparation for DoS - Unauthorized Access Incident - Inappropriate Usage Incidents - Multiple Component Incidents - Network Traffic Monitoring Tools - Network Auditing Tools - Network Protection Tools.

9+3 Hours
Total: 45+15 Hours

Reading Materials

1. "ECIH Study Guide" by EC-Council, 2016.

21CCS004 Managing and Securing networks

4 0 0 4

Course outcomes

1. Determine appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies.
2. Troubleshoot their network for various network problems.
3. Identify various threats on organization network.
4. How to design and implement various security policies for their organizations.
5. Learn the importance of physical security and able to determine and implement various physical security controls for their organizations.
6. Choose appropriate firewall solution, topology, and configurations to harden security through firewall.

Unit I

Network Defense, security Fundamentals

Computer Network and Defense Fundamentals: Network Fundamentals - Network Components- TCP/IP Networking Basics- TCP/IP Protocol Stack – IPAddressing - Computer Network Defense (CND) – CND Triad – CND Process – CND Actions – CND Approaches.

Network Security Threats, Vulnerabilities, and Attacks: Essential Terminologies - Network Security Concerns- Network Security Vulnerabilities - Network Reconnaissance Attacks - Network Access Attacks- Denial of Service (DoS) Attacks - Distributed Denial-of-Service Attack (DDoS) - Malware Attacks

Network Security Controls, Protocols, and Devices: Fundamental Elements of Network Security - Network Security Controls – User Identification, Authentication, Authorization and Accounting - Types of Authorization Systems - Authorization Principles – Cryptography - Security Policy - Network Security Devices - Network Security Protocols

11+4 Hours

Unit II
Network Security Policy Design & Implementation and Physical Security

Network Security Policy Design & Implementation

What is Security Policy - Internet Access Policies - Acceptable-Use Policy - User-Account Policy - Remote-Access Policy - Information-Protection Policy - Firewall-Management Policy - Special-Access Policy - Network-Connection Policy - Business-Partner Policy - Email Security Policy - Passwords Policy - Physical Security Policy - Information System Security Policy - Bring Your Own Devices (BYOD) Policy - Software/Application Security Policy - Data Backup Policy - Confidential Data Policy - Data Classification Policy - Internet Usage Policies - Server Policy - Wireless Network Policy - Incidence Response Plan (IRP) - User Access Control Policy - Switch Security Policy - Intrusion Detection and Prevention (IDS/IPS) Policy - Personal Device Usage Policy - Encryption Policy - Router Policy - Security Policy Training and Awareness - ISO Information Security Standards - Payment Card Industry Data Security Standard (PCI-DSS) - Health Insurance Portability and Accountability Act (HIPAA) - Information Security Acts: Sarbanes Oxley Act (SOX) - Information Security Acts: Gramm-Leach-Bliley Act (GLBA) - Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal - Information Security Management Act (FISMA) - Other Information Security Acts and Laws

Physical Security

Physical Security - Access Control Authentication Techniques - Physical Security Controls - Other Physical Security Measures - Workplace Security - Personnel Security: Managing Staff Hiring and Leaving Process - Laptop Security Tool: EXO5- Environmental Controls - Physical Security: Awareness /Training - Physical Security Checklists.

12+4 Hours

Unit III
Host Security and Secure Firewall Configuration & Management

Host Security: Host Security - OS Security- Linux Security - Securing Network Servers - Hardening Routers and Switches - Application/software Security - Data Security- Virtualization Security
Secure Firewall Configuration and Management: Firewalls and Concerns - What Firewalls Does? - What should you not Ignore?:Firewall Limitations - How Does a Firewall Work? - Firewall Rules - Types of Firewalls - Firewall Technologies - Firewall Topologies - Firewall Rule Set & Policies - Firewall Implementation - Firewall Administration - Firewall Logging and Auditing - Firewall Anti-evasion Techniques - Why Firewalls are Bypassed? - Full Data Traffic Normalization - Data Stream-based Inspection - Vulnerability-based Detection and Blocking - Firewall Security Recommendations and Best Practices - Firewall Security Auditing Tools.

12+4 Hours

Unit IV
Secure IDS and VPN Configuration and Management

Secure IDS Configuration and Management: Intrusions and IDPS - IDS - Types of IDS Implementation - IDS Deployment Strategies - Types of IDS Alerts -IPS - IDPS Product Selection Considerations - IDS Counterparts
Secure VPN Configuration and Management: Understanding Virtual Private Network (VPN) - How VPN works? - Why to Establish VPN ? - VPN Components - VPN Concentrators - Types of VPN - VPN Categories - Selecting Appropriate VPN - VPN Core Functions-VPN Technologies - VPN Topologies - Common VPN Flaws - VPN Security - Quality Of Service and Performance in VPNs.

10+3 Hours
Total: 45+15 Hours

Reading Materials

1. ”CND Study Guide” by EC-Council, 2016

21CCS005 TCP/IP

4 0 0 4

Course Outcomes

1. Understand and analyze various network layer protocols
2. Differentiate sub netting and super netting
3. Implement flow control and error control mechanisms for TCP and UDP
4. Understand the various concepts of socket programming
5. Implement various applications using socket programming
6. Understand and analysis the use of IPv6

Unit I

Introduction to Computer Networks and Network Layer Protocols

Introduction to Layered Architecture (TCP/IP, OSI), Networking Devices, IP addressing, Sub-netting, Super-netting, VLSM, CIDR, Router IOS- Static and Default Routing-Interior Gateway Routing Protocols: RIPV1&V2, OSPF, EIGRP- Exterior Gateway Routing Protocol: BGP.

12+4 Hours

Unit II
Transport Layer Protocols

TCP & UDP datagram and its characteristics, RTP, Flow Control and Error Control Mechanisms, Silly Window Syndrome - Clark's and Nagle Algorithm – Congestion Control Mechanisms - Token Bucket and Leaky Bucket.

10+3 Hours

Unit III
Socket Programming

Introduction to socket programming- Concurrent Processing in Client-Server Software-Byte ordering and address conversion functions – Socket Interface -System calls used with sockets - Iterative server and concurrent server- Multiprotocol and Multi service server- TCP/UDP Client server programs – Thread Creation and Termination – TCP Echo Server using threads- Remote Procedure Call.

12+4 Hours

Unit IV
Next Generation Internet Protocol

Introduction to IPv6 – IPv6 Advanced Features –V4 and V6 header comparison –V6 Address types –Stateless auto configuration – IPv6 routing protocols – IPv4-V6 Tunneling and Translation Techniques.

11+4 Hours
Total: 45+15 Hours

Reading Materials

1. Douglas E. Comer ,"Internetworking with TCP/IP, Principles, Protocols, and Architecture", Addison- Wesley, 5th edition, Vol. 1, 2005.
2. Douglas E. Comer, David L. Stevens ,"Internetworking with TCP/IP Vol. III, Client-Server Programming and Applications", Addison-Wesley, 2nd edition, 2000.
3. Wendell Odom, "CCNP Route 642-902, CCIE", Official Certification Guide, Pearson Education, 2010.
4. Behrouz A. Forouzan, "Data Communications and Networking", McGraw-Hill, 5th edition, 2012.

21CCS006 Wireless Ad hoc Networks

4 0 0 4

Course outcomes

1. Understand fundamentals of wireless networks
2. Understand MAC protocols for Ad Hoc Wireless Networks
3. Explore different Routing and Transport protocols for Ad Hoc Wireless Networks
4. Understand the need for Quality of service and Energy Management in Ad Hoc Wireless Networks
5. Understand the issues and challenges in Wireless Network security
6. Understand architecture of wireless sensor networks

UNIT-I

Wireless Ad Hoc Networks: Introduction, Properties, applications, limitations, Issues in Ad Hoc Wireless Networks, Ad Hoc Wireless Internet.

MAC Protocols: Introduction, Issues in Designing a MAC protocol for Ad Hoc Wireless Networks, Design goals of a MAC Protocol for Ad Hoc Wireless Networks, Classifications of MAC Protocols, Contention - Based Protocols, Contention - Based Protocols with reservation Mechanisms, Contention – Based MAC Protocols with Scheduling Mechanisms

11+4 Hours

UNIT -II

Routing Protocols: Introduction, Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks, Classification of Routing Protocols, Proactive/ Table–Driven Routing Protocols, Reactive/ On–Demand Routing Protocols, Hybrid Routing Protocols, Hierarchical Routing Protocols, Power – Aware Routing Protocols.

Transport Layer: Introduction, Issues in Designing a Transport Layer Protocol for Ad Hoc Wireless Networks, Design Goals of a Transport Layer Protocol for Ad Hoc Wireless Networks, Classification of Transport Layer Solutions, TCP Over Ad Hoc Wireless Networks, Other Transport Layer Protocol for Ad Hoc Wireless Networks.

11+4 Hours

UNIT –III

Quality of Service: Introduction, Issues and Challenges in Providing QoS in Ad Hoc Wireless Networks, Classification of QoS Solutions, MAC Layer Solutions, Network Layer Solutions, QoS Frameworks for Ad Hoc Wireless Networks.

Energy Management: Introduction, Need for Energy Management in Ad Hoc Wireless Networks, Classification of Ad Hoc Wireless Networks, Battery Management Schemes, Transmission Power Management Schemes, System Power Management Schemes.

11+4 Hours

UNIT – IV

Security Protocols: Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management, Secure Routing in Ad Hoc Wireless Networks.

Wireless Sensor Networks: Introduction, Sensor Network Architecture, Data Dissemination, Data Gathering, Location Discovery, Quality of a Sensor Network, Evolving Standards, Other Issues.

11+4 Hours

Total: 45 Hours

Reading material

1. Ad Hoc Wireless Networks: Architectures and Protocols - C. Siva Ram Murthy and B.S.Manoj, 2004, PHI.
2. Wireless Ad- hoc and Sensor Networks: Protocols, Performance and Control - Jagannathan Sarangapani, CRC Press

21CCS007 Fundamentals of Computer Science & Engineering

4 0 0 4

Course Outcomes

1. Select and use an appropriate data structure and algorithm to solve a given problem.
2. Build an understanding of the fundamental concepts of computer networking.
3. Master the basic concepts and understand the applications of database systems.
4. Basic ability to analyze algorithms and to determine algorithm correctness and time efficiency class.
5. Describe, contrast and compare different structures for operating systems.
6. Analyze the processor scheduling techniques and use the appropriate one for a given application.

Unit I

Data Structures and Computer Networks

Topics in Data Structures: Stack Queues, Linked List, Heap, BST, AVL Trees, B+ Tree, and Abstract Data Types using Python and C Language.
Topics in Computer Networks: OSI Model and each layer working, properties and related protocols in security areas

11+4 Hours

Unit II
Data Base Management Systems

Topics in Data Base Management Systems: Entity–Relationship model (E-R model) – E-R Diagrams,Functional Dependencies – Non-loss Decomposition, First, Second, Third Normal Forms,Dependency Preservation – Boyce/Codd Normal Form- Multi-Valued Dependencies and FourthNormal Form – Join Dependencies and Fifth Normal Form, Two Phase Commit, ACID Property, TwoPhase Locking –Intent Locking – Deadlock- Serializability, Magnetic Disks – RAID – Tertiarystorage – File Organization

12+3 Hours

Unit III
Algorithms

Topics in Algorithms: Algorithm Development, Complexity analysis, Sorting, Searching, BFS, DFS,Minimum Spanning Tree, Prim's and Kruskal'; s algorithms, Greedy algorithms – Divide and conquer– Dynamic Programming – backtracking– algorithm analysis

11+4 Hours

Unit IV
Operating System

Topics in Operating System: Overview of operating systems, functionalities and characteristics of OS,concept of a process, operations on processes, process states, concurrent processes, process controlblock, process context, Job and processor scheduling, scheduling algorithms, Deadlock: prevention,detection, avoidance, banker's algorithm, Memory organization and management, storage allocationAndroid OS, iOS, Linux OS file structure and security features

11+4 Hours
Total: 45+15 Hours

Reading Materials

1. Fundamentals of Data Structures in C,Horowitz, Sahni and Anderson Freed,2nd Edition ,Universities Press.
2. Operating System Concepts- Abraham Silberchatz, Peter B. Galvin, Greg Gagne 7th Edition, John Wiley.
3. Computer Networking and Internet, Fred Halsll, Lingana Gouda Kulkarni, 5th Edition, Pearson Education.
4. Database System Concepts, Silberschatz, Korth, McGraw hill, 5th Edition.

21CCS008 Fundamentals of Wireless Sensor Networks

4 0 0 4

Course outcomes

1. Understand architecture of wireless sensors.
2. Uunderstand fundamental concepts of physical layer for WSN.
3. Master the basic concepts and understand the data link layer and MAC protocols.
4. Uunderstand fundamental concepts of transport layer for WSN.
5. Describe, contrast and compare different applications of WSN.
6. Analyze the various topology control methods of WSN.

UNIT I

Wireless Sensor Networks: Introduction, Node and Network Architectures- Wireless Sensor Device Architecture, and Network Architectures. Application Domains and Examples, Challenges and the Need for Energy Saving Mechanisms. **The Physical Layer**: Wireless Propagation Models, Energy Dissipation Model, Error Models, Sensing Models.

13+4 Hours

UNIT II

The Data Link Layer: The Medium Access Control Sub-layer-Common MAC Protocols, MAC Protocols for WSNs. The Logical Link Control Sub-layer-Error Control, Performance Analysis of LLC Protocols, and Energy Analysis of LLC Protocols. The Network Layer: Routing Protocols for WSNs.

12+4 Hours

UNIT III

The Transport Layer:

Transport Layer Functions, Wireless Sensor Network Applications- Single Packet–Low Reliability Applications, Single Packet–High Reliability Applications, Multiple Packet–Low Reliability Applications, and Multiple Packet–High Reliability Applications. Congestion Control in Wireless Sensor Networks, The Use of TCP and UDP in Wireless Sensor Networks.

10+4 Hours

UNIT IV

Topology Control:

Motivations for Topology Control - Energy Conservation, Collision Avoidance, and Increased Network Capacity. Challenges in Topology Control, Design Guidelines, Definition of Topology Control, Topology Control and the Communications Protocol Stack, Topology Control Taxonomy and Road Map.

10+3Hours

Total: 45+15 Hours

Reading material:

1. Miguel A. Labrador, and Pedro M. Wightman, “Topology control in Wireless Sensor Networks with a companion simulation tool for teaching and research”, Springer 2007.
2. Kazem Sohraby, Daniel Minoli and Taieb Znati, “Wireless Sensor Networks Technology, Protocols, and Applications“, John Wiley & Sons, 2007.
3. Holger Karl and Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks”, John Wiley & Sons, Ltd, 2005.
4. K. Akkaya and M. Younis, “A survey of routing protocols in wireless sensor networks”, Elsevier Ad Hoc Network Journal, Vol. 3, no. 3, pp. 325--349
5. Philip Levis, “ TinyOS Programming” 3.Anna Ha´c, “Wireless Sensor Network Designs”, John Wiley & Sons Ltd,

21CCS009 Network Intrusion and Incidence Response

4 0 0 4

Course outcomes

1. Identify Different wireless technologies.
2. Implement Different attacks on wireless medium
3. Analyze Network Traffic Monitoring
4. Identify Different Packet sniffing techniques
5. Apply Risk management
6. Identify Data Backup and recovery methods

Unit I

Wireless Network Defense

Wireless Terminologies - Wireless Networks - Wireless Standard - Wireless Topologies - Typical Use of Wireless Networks - Components of Wireless Network - WEP (Wired Equivalent Privacy) Encryption - WPA (Wi-Fi Protected Access) Encryption - WPA2 Encryption - WEP vs. WPA vs. WPA2 - Wi-Fi Authentication Method - Wi-Fi Authentication Process Using a Centralized Authentication Server - Wireless Network Threats - Bluetooth Threats - Wireless Network Security - Wi-Fi Discovery Tools - Locating Rogue Access points - Protecting from Denial-of-Service Attacks: Interference - Assessing Wireless Network Security - Wi-Fi Security Auditing Tool: AirMagnetWi-Fi Analyzer - WPA Security Assessment Tool - Wi-Fi Vulnerability Scanning Tools - Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS) - WIPS Tool - Configuring Security on Wireless Routers - Additional Wireless Network Security Guidelines.

12+4 Hours

Unit II

Network Traffic Monitoring and Analysis

Network Traffic Monitoring and Analysis(Introductions - Network Monitoring: Positioning your Machine at Appropriate Location - Network Traffic Signatures - Packet Sniffer: Wireshark - Detecting OS Fingerprinting Attempts - Detecting PING Sweep Attempt - Detecting ARP Sweep/ ARP Scan Attempt - Detecting TCP Scan Attempt - Detecting SYN/FIN DDOS Attempt - Detecting UDP Scan Attempt - Detecting Password Cracking Attempts - Detecting FTP Password Cracking Attempts - Detecting Sniffing (MITM) Attempts - Detecting the Mac Flooding Attempt - Detecting the ARP Poisoning Attempt - Additional Packet Sniffing Tools - Network Monitoring and Analysis - Bandwidth Monitoring.

11+4 Hours

Unit III

Network Risk & Vulnerability Management, Data Backup and Recovery

Network Risk & Vulnerability Management: What is Risk? - Risk Levels - Risk Matrix - Key Risk Indicators (KRI) - Risk Management Phase - Enterprise Network Risk Management - Vulnerability Management

Data Backup and Recovery: Introduction to Data Backup - RAID (Redundant Array Of Independent Disks) Technology - Storage Area Network (SAN) - Network Attached Storage (NAS) - Selecting Appropriate Backup Method - Choosing the Right Location for Backup - Backup Types - Conducting Recovery Drill Test

11+4 Hours

Unit IV

Data Recovery, Network Incident Response and Management

Data Recovery: Windows Data Recovery Tool - RAID Data Recovery Services - SAN Data Recovery Software - NAS Data Recovery Services.

Network Incident Response and Management: Incident Handling and Response - Incident Response Team Members: Roles and Responsibilities - First Responder - Incident Handling and Response Process - Overview of IH& R Process Flow.

11+3 Hours
Total: 45+15 Hour

Reading Materials

1. “CND Study Guide” by EC-Council, 2016

21CCS102 Cryptography and Network Security Laboratory

0 0 3 1.5

Course Outcomes

1. Understand and implement DES algorithm.
2. Analyze the DES algorithm to break it.
3. Understand the concepts of public key encryption and implement RSA.
4. Analyze the concepts of number theory and its applications in cryptography.
5. Implement encryption and decryption with openssl.
6. Understand the basic concepts of IP tables in Linux.

The following programs should be implemented preferably on platform Windows/Unix using C language (for 1-5) and other standard utilities available with UNIX systems (for 6-15) :-

1. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer) in C
2. Write a program to break the above DES coding
3. Implement Linear Congruential Algorithm to generate 5 pseudo- random numbers in C
4. Implement Rabin-Miller Primality Testing Algorithm in C
5. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C
6. a)Implement RSA algorithm for encryption and decryption in C
7. b) In an RSA System, the public key of a given user is e=31,n=3599.
8. Write a program to find private key of the User.
9. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.
10. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
11. Configure a firewall to block the following for 5 minutes and verify the correctness of this system using the configured parameters: (a) Two neighborhood IP addresses on your LAN (b) All ICMP requests (c) All TCP SYN Packets
12. Configure S/MIME and show email-authentication.
13. Implement encryption and decryption with openssl.
14. Implement Using IP TABLES on Linux and setting the filtering rules.
15. Implementation of proxy based security protocols in C or C++ withfeatures like Confidentiality, integrity and authentication.
16. Working with Sniffers for monitoring network communication (Ethereal)
17. Using IP TABLES on Linux and setting the filtering rules

21CCS201 Principles of Secure Coding

0 0 3 1.5

Course outcomes

1. Illustrate Importance of secure coding
2. Identify Different security violations while coding
3. Implement Secure coding in C++
4. Implement Secure coding in JAVA
5. Implement Secure database coding
6. Analyze Software security engineering

Unit I

Introduction and Secure Coding in C

Need for secure systems- Proactive security development process- Security principles to live by and threat modeling, Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – BufferOverflow based vulnerabilities

11+4 Hours

Unit II

Secure Coding in C++ And JAVA

Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double – free vulnerabilities –Integer security- Mitigation strategies Java security principles and secure coding practices Java Security Platform, Sandbox, JVM, Class loading, Bytecode verifier, Security Manager, security policies, and Java Security Framework Best practices and standards and guidelines for secure file input/output and serialization Java input validation techniques, validation errors, and best practices

11+4 Hours

Unit III

Data Base and Web Specific Input Issues

Quoting the Input – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies: Java Authentication and Authorization Service (JAAS), its architecture, Pluggable Authentication Module (PAM) Framework, and access permissions through Java Security Model&Secure Java concurrency and session management that includes Java Memory Model, Java Thread Implementation methods, secure coding practices, and guidelines for handling threads, race conditions, and deadlocks.

12+4 Hours

Unit IV

Software Security Engineering

Requirements engineering for secure software: Misuse and abuse cases- SQUARE process model- Software security practices and knowledge for architecture and design &Secure Software Development Lifecycle, threat modelling, software security frameworks, and secure software architectures.

11+3 Hours

Total: 45+15 Hours

Reading Materials

1. Michael Howard , David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition, 2003.
2. Robert C.Seacord, “ Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security Engineering : A guide for Project Managers”, Addison-Wesley Professional, 2008.

21CCS202 Cybernet Security

4 0 0 4

Course Outcomes

1. Explain the fundamental concepts of Cyber security
2. Demonstrate the web security and different attacks
3. Identify different network scanning and security measures
4. List out different types of Intrusion detection.
5. Model different types of Intrusion prevention systems
6. Outline different cyber crimes, IT laws and acts.

Unit I

Introduction to Cyber Security

What is Cyber Security, its need, cyber-threats, Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage), Career Growth, Statistics, Inferences, Need for a Comprehensive Cyber Security Policy, Classification of Cyber Crimes,kinds of cyber crimes, Reasons for Cyber Crimes, Cyber Security Tools : Nmap, Metasploit, wireshark, tcpdump, snort.
Cyber security awareness, social engineering, cyber stalking

11+7 Hours

Unit II

Web security

Same origin Policy, Cross Origin Resource Sharing, DDOS, SQL Injection, XSS, Homograph, Generating and storing session tokens.

Networking Scanning & Security Measures:

Packet Sniffing and spoofing, Network scanning types, port scanning & its tools, and Network Architecture

Security Measures : IPtables(firewalls) , Webservers (Nmap & Metasploit for securing webservers), Cyber Threats and Attacks (Malware, DOS, MITM, Social engineering attacks, Spoofing, Phishing)
Cross-Site Request Forgery (XSRF/CSRF), spear phishing.

11+8 Hours

Unit III

Intrusion Detection System: Intruders, Intrusion Detection, Analysis Approaches, Network-Based IDS, Host-Based IDS, signature based IDS, anomaly based IDS, advantages and disadvantages of NIDS and HIDS

Intrusion Detection Tools, snort architecture, snort rules, case studies of intrusion detection systems,Intrusion detection exchange format. Honeypots, different types of honeypots, benefits and dangers of honeypots
firewall vs IDS, Physical IDS, honeynet

11+8 Hours

Unit IV

Cyber Laws and Digital Forensics

Digital Forensics: Introduction to Digital Forensics, historical background of digital forensics, Forensic Software, and Hardware, need for computer forensics science, special tools and techniques digital forensic life cycle, challenges in digital forensic. **Law Perspective:** Introduction to the Legal Perspectives of Cybercrimes and Cybersecurity, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Cybercrime Scenario in India, Digital Signatures and the Indian IT Act.

12 + 7 Hours

Reading Material

1. Wenliang Du, Computer & Internet Security: A Hands-on Approach, (2019)
2. William Stallings, Lawrie Brown, Computer Security Principle sand Practice Third Edition,2015
3. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Wiley India Pvt. Ltd, 2011.
4. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi

21CCS203 Secure Coding Laboratory

0 0 3 1.5

Course Outcomes

1. Identify String Manipulation Errors and vulnerabilities
2. Identify Different validation techniques
3. Implement SQL and XSS attacks
4. Apply Secure Java concurrency and session management
5. Implement java concurrency and session management
6. Identify secure coding practices

The following are the experiments:

1. String manipulation errors
2. String Vulnerabilities and exploits
3. Mitigation strategies in pointer based vulnerabilities
4. Buffer Overflow based vulnerabilities
5. Integer security- Mitigation strategies
6. secure file input/output and serialization
7. Java input validation techniques, validation errors
8. Building SQL statements securely
9. XSS related attacks and remedies
10. Secure Java concurrency and session management that includes Java Memory Model, Java Thread Implementation methods
11. Secure coding practices, and guidelines for handling threads, race conditions, and deadlocks

References

1. Michael Howard , David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition,2003.
2. Robert C.Seacord, “ Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security sEngineering: A guide for Project Managers”, Addison-Wesley Professional, 2008.

21CCS204 Cybernet Security Laboratory

0 0 3 1.5

Course Outcomes

1. Understand and implement network related LINUX commands.
2. Analyze the network statistics through network scanning tools.
3. Understand and implement various attacks.
4. Analyze the concepts of firewalls.
5. Implement intrusion detection rules.
6. Understand the basic concepts of security policies.

The following programs should be implemented preferably on platform Windows/Unix/LINUX and other standard security tools available with LINUX :-

1. Study the use of network reconnaissance tools like WHOIS, dig, ping, hping, traceroute, nslookup to gather information about networks and domain registrars.
2. Study of packet sniffer tools like tcpdump , wireshark etc.
3. Perform port scanning using Nmap
4. Penetration Testing and Exploiting with Metasploit, Armitage and msfconsole
5. Simulate DOS and DDOS attacks using various tools.
6. Study of SQLMap to explore SQL Injection attacks
7. Use iptables in linux to create firewalls..
8. Use Snort as packet sniffer and write your own IDS rules
9. Write a security policy for password protection
10. Case Study on Indian IT ACT 2000

21CCS010 Ethical Hacking and counter Measures-2

4 0 0 4

Course Outcomes

1. Identify Session Hijacking Concepts
2. Analyze Hacking web servers
3. Analyze Hacking web applications
4. Implement SQL Injections
5. Analyze Hacking wireless networks
6. Apply Evading IDS, firewalls and honeypots

Unit -I
Session Hijacking and Hacking Webservers

Session Hijacking: Session Hijacking Concepts – Application Level Session Hijacking – Network level Session Hijacking – Session Hijacking Tools – Countermeasures – Penetration Testing.
Hacking Webservers: Webserver Concepts – Webserver Attacks – Attack Methodology – Webserver Attack Tools – Countermeasures – Patch Management – Webserver Security Tools – Webserver Pen Testing.

12+4 Hours

Unit-II
Hacking Web Applications and SQL Injection

Hacking Web Applications: Web App Concepts – Web App Threats – Hacking Methodology – Web Application Hacking Tools – Countermeasures – Security Tools – Web App Pen Testing.
SQL Injection: SQL Injection Concepts – Types of SQL Injection – SQL Injection Methodology – SQL Injection Tools – Evasion Techniques – Countermeasures.

11+4 Hours

Unit -III
Hacking Wireless Networks and Hacking Mobile Platforms

Hacking Wireless Networks: Wireless Concepts – Wireless Encryption – Wireless Threats – Wireless Hacking methodology – Wireless Hacking Tools – Bluetooth Hacking – Countermeasures - Wireless Security Tools – Wi-Fi Pen Testing.
Hacking Mobile Platforms: Mobile Platform Attack vectors – Hacking Android OS – Hacking iOS – Hacking Windows Phone OS – Hacking BlackBerry – Mobile Device Management – Mobile Security Guidelines and Tools – Mobile Pen Testing.

(11+4 Hours)

Unit-IV
Evading IDS, Firewalls, and Honeypots and Cloud Computing

Evading IDS, Firewalls, and Honeypots: IDS, Firewall and Honeypot Concepts – IDS, Firewall and Honeypot Solutions – Evading IDS – Evading Firewalls – IDS/Firewall Evading Tools – Detecting Honeypots – IDS/Firewall Evasion Countermeasures – Penetration Testing.
Cloud Computing: Introduction to Cloud Computing – Cloud Computing Threats – Cloud Computing Attacks – Cloud Security – Cloud Security tools –Cloud Penetration Testing.

11+3 Hours
Total: 45+15 Hours

Reading Materials

1. "CEH Study Guide" by EC-Council, 2016.

21CCS011 Computer Hacking and Forensic Investigator – 2

4 0 0 4

Course Outcomes

1. Identify different information collection methods.
2. Identify Data Acquisition and Duplication Concepts
3. Implementation of Recovering Deleted Files and Deleted Partitions
4. Implement Forensics Investigation
5. Implement Different Forensics Investigation using Access Data FTK
6. Identify Application Password Crackers

Unit -I

Windows Forensics, Data Acquisition and Duplication

Windows Forensics: Collecting Volatile Information -Collecting Non-volatile Information - Windows Memory Analysis - Windows Registry Analysis - Cache, Cookie, and History Analysis - MD5 Calculation - Windows File Analysis - Metadata Investigation - Text Based Logs - Other Audit Events - Forensic Analysis of Event Logs - Windows Password Issues - Forensic Tools.

Data Acquisition and Duplication: Data Acquisition and Duplication Concepts - Data Acquisition Types - Disk Acquisition Tool Requirements - Validation Methods - RAID Data Acquisition - Acquisition Best Practices - Data Acquisition Software Tools - Data Acquisition Hardware Tools.

12+4 Hours

Unit-II

Recovering Deleted Files and Deleted Partitions

Recovering Deleted Files and Deleted Partitions: Recovering the Deleted Files - Deleting Files - What Happens When a File is Deleted in Windows? - Recycle Bin in Windows - File Recovery in MAC OS X - File Recovery in Linux - File Recovery Tools for Windows - File Recovery Tools for MAC - File Recovery Tools for Linux - Recovering the Deleted Partitions - Partition Recovery Tools.

Forensics Investigation using Access Data FTK: Overview and Installation of FTK - Overview of Forensic Toolkit (FTK) - Features of FTK - Software Requirement - Configuration Option - Database Installation - FTK Application Installation - FTK Case Manager User Interface - FTK Examiner User Interface - Starting with FTK - FTK Interface Tabs - Working with Reports.

12+4 Hours

Unit-III

Forensics Investigation Using EnCase, Steganography and Image File Forensics

Forensics Investigation Using EnCase: Overview of EnCase Forensic - EnCase Forensic Features - EnCase Forensic Platform - EnCase Forensic Modules - Installing EnCase Forensic - EnCase Interface - Case Management - Working with Evidence - Source Processor - Analyzing and Searching Files - Viewing File Content - Bookmarking Items – Reporting.

Steganography and Image File Forensics: Steganography - What is Steganography? - How Steganography Works - Legal Use of Steganography - Unethical Use of Steganography - Steganography Techniques – Steganalysis - Image Files - Data Compression - Locating and Recovering Image Files - Image File Forensics Tools.

12+4 Hours

Unit- IV
Application Password Crackers

Password Cracking Concepts - Password – Terminology - Password Types -Password Cracker -How Does a Password Cracker Work? - How Hash Passwords are Stored in Windows SAM - Types of Password Attacks - Classification of Cracking Software - Systems Software vs. Applications Software - System Software Password Cracking - Application Software Password Cracking - Password Cracking Tools.

9+3 Hours

Total: 45+15 Hours

Reading Materials

1. ”CHFI Study Guide” by EC-Council, 2016.

21CCS012 Incident Handler-2

4 0 0 4

Course Outcomes

1. Identify Handling Malicious Code Incidents
2. Identify Handling Insider Threats
3. Implement Forensic Analysis and Incident Response
4. Implement Incident Reporting
5. Implement Incident Recovery
6. Identify Security Policies and Laws

Unit - I

Handling Malicious Code Incidents& Handling Insider Threats

Count of Malware Samples – Virus – Worms - Trojans and Spywares - Incident Handling Preparation - Incident Prevention - Detection of Malicious Code - Containment Strategy - Evidence Gathering and Handling - Eradication and Recovery – Recommendations - Antivirus Systems.
Insider Threats - Anatomy of an Insider Attack - Insider Risk Matrix - Insider Threats Detection - Insider Threats Response - Insider's Incident Response Plan - Guidelines for Detecting and Preventing Insider Threats - Employee Monitoring Tools.

11+4 Hours

Unit-II
Forensic Analysis and Incident Response

Computer Forensics - Objectives of Forensics Analysis - Role of Forensics Analysis in Incident Response - Forensic Readiness - Forensic Readiness And Business Continuity - Types of Computer Forensics - Computer Forensic Investigator - People Involved in Computer Forensics - Computer Forensics Process - Digital Evidence - Characteristics of Digital Evidence - Collecting Electronic Evidence - Challenging Aspects of Digital Evidence - Forensic Policy - Forensics in the Information System Life Cycle - Forensic Analysis Guidelines - Forensics Analysis Tools.

11+4 Hours

Unit-III
Incident Reporting

Incident Reporting - Why to Report an Incident - Why Organizations do not Report Computer Crimes - Whom to Report an Incident - How to Report an Incident - Details to be Reported - Preliminary Information Security Incident Reporting Form - CERT Incident Reference Numbers - Contact Information - Summary of Hosts Involved- Description of the Activity-Log Extracts Showing the Activity-Time Zone - Federal Agency Incident Categories - Organizations to Report Computer Incident- Incident Reporting Guidelines - Sample Incident Reporting Form - Sample Post Incident Report Form.

11+3 Hours

Unit- IV
Incident Recovery&Module 11: Security Policies and Laws

Incident Recovery - Principles of Incident Recovery - Incident Recovery Steps - Contingency/Continuity of Operations Planning - Business Continuity Planning - Incident Recovery Plan - Incident Recovery Planning Process. Security Policy - Key Elements of Security Policy - Goals of a Security Policy - Characteristics of a Security Policy - Design of Security Policy - Implementing Security Policies - Acceptable Use Policy (AUP) - Access Control Policy-Asset Control Policy - Audit Trail Policy - Logging Policy - Documentation Policy - Evidence Collection

Policy - Evidence Preservation Policy - Information Security Policy - National Information Assurance Certification & Accreditation Process (NIACAP) Policy - Physical Security Policy - Physical Security Guidelines - Personnel Security Policies & Guidance - Law and Incident Handling - Laws and Acts - Intellectual Property Laws.

12+4 Hours
Total: 45+15 Hours

Reading Materials

1. "ECIH Study Guide" by EC-Council, 2016.

21CCS013 Penetration Testing and Vulnerability Assessment

4 0 0 4

Course Outcomes

1. Apply Five stages of hacking
2. Analyze Different type of Information gathering methodologies
3. Implement Social Engineering attacks
4. Analyze network scanning techniques
5. Analyze Password cracking techniques and its countermeasures
6. Identify Sniffing techniques and its countermeasures

Unit I

Introduction to Hacking

Important Terminologies - What Is a Penetration Test? - Vulnerability Assessments versus Penetration Test - Penetration Testing Methodologies – Categories of Penetration Test - Categories of Penetration Test - Types of Penetration Tests - Report Writing – Guidance.

9+3 Hours

Unit II

Information Gathering Techniques

Active Information Gathering - Passive Information Gathering - Sources of Information Gathering - Neo Trace - Cheops-ng - Intercepting a Response – WhatWeb – Netcraft – Example – TIP regarding Filetype – Xcode Exploit Scanner – Interacting with DNS Servers – Nslookup – SMTP Enumeration – Intelligence Gathering Using Shodan.

9+3 Hours

Unit III

Target Enumeration and Port Scanning Techniques

Host Discovery - Scanning for Open Ports and Services - Types of Port Scanning - Understanding the TCP Three- Way Handshake - TCP Flags - Port Status Types - TCP SYN Scan - TCP Connect Scan - NULL, FIN, and XMAS Scans - NULL Scan - FIN Scan - XMAS Scan - TCP ACK Scan – Responses - UDP Port Scan - Anonymous Scan Types - IDLE Scan - Scanning for a Vulnerable Host - Performing an IDLE Scan with NMAP - TCP FTP Bounce Scan - Service Version Detection - OS Fingerprinting – POF

14+5 Hours

Unit IV

Vulnerability Assessment

Pros and Cons of a Vulnerability Scanner - Vulnerability Assessment with Nmap - Updating the Database - Scanning MS08 _ 067 _ netapi - Testing SCADA Environments with Nmap - Nessus Vulnerability Scanner - Installing Nessus on BackTrack - Adding a User - Creating a New Policy - Nessus Integration with Metasploit- Importing Nessus to Metasploit – Resource - Vulnerability Data Resources - Exploit Databases

13+4Hours
Total: 45+15 Hours

Reading Materials

1. Rafay Balpch, “Ethical Hacking And Penetration Testing Guide”, CRC Press, Taylor & Francis Group, 2015.

21CCS014 Practical Vulnerability Management

4 0 0 4

Course outcomes

1. Understand vulnerability fundamentals
2. Identify vulnerability targets
3. Implement different exploitation methods
4. Implement windows kernel debugging & exploitation methods
5. Implement windows heap overflows and cross-site exploitation methods
6. Understand android and iOS exploitation methods

UNIT I

Vulnerability discovery:

Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing. **Targets and Automation**- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation.

12+4 Hours

UNIT II

Advanced Linux Exploitation-Linux heap management, constructs, and environment, Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists, Defeating Linux exploit mitigation controls, Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls.

12+4 Hours

UNIT III

Windows Kernel Debugging and Exploitation- Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques. **Windows Heap Overflows and Client-Side Exploitation-** Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls.

12+4 Hours

UNIT IV

Android Exploitation- Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis. **iOS exploitation-**Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation.

9+3Hours

Total: 45+15 Hours

Reading material

1. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

21CCS015 Intrusion Detection and Prevention

4 0 0 4

Course outcomes

1. Understand intrusion, threat and attack .
2. Analyze the network protocols and intrusion prevention techniques.
3. Understand and implement various intrusion detection tools.
4. Analyze the concepts of snort.
5. Implement intrusion detection rules in snort.
6. Understand the basic concepts of architecture models.

UNIT I

History of Intrusion:

Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources. **Prevention:** Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis , techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

14+4 Hours

UNIT II

Intrusion detection tool:Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes

12+3 Hours

UNIT III

Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL.

10+3 Hours

UNIT IV

Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

9+4 Hours

Total 45+15 Hours

Reading material

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003.
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
3. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.
4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002.
5. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". 6th Edition, KhannaPublihsers, 2012.

21CCS016 Cloud Architecture and Security

4 0 0 4

Course outcomes:

1. Interpret the architecture and infrastructure models of cloud computing, strengths, and limitations of cloud computing.
2. Understand the virtualization concepts of machines and data centers.
3. Infer the design concepts of cloud ready applications
4. Compare different cloud centre's implementation
5. Understand the concepts of cloud scaling and disaster recovery
6. Analyze the performance, scalability, and availability of the underlying cloud technologies and software

Unit I

Characterization of Distributed Systems:

Introduction, Examples of Distributed Systems, Resource Sharing and the Web, Challenges. System Models: Introduction, Architectural Models- Software Layers, System Architecture, Variations, Interface and Objects, Design Requirements for Distributed Architectures, Fundamental Models- Interaction Model, Failure Model, Security Model.
Beyond the Syllabus: Communication between Distributed Objects- Object Model, Distributed Object Modal.

12 +4 Hours

Unit II

Introduction to Cloud Computing

Overview of Computing Paradigm: Recent Trends in Computing, Evolution of Cloud Computing. Introduction to Cloud Computing: Cloud Computing (NIST Model), Properties, Characteristics & Disadvantages, Role of Open Standards. Cloud Computing Architecture: Cloud Computing Stack, Service Models (XaaS), Deployment Models. Infrastructure as a Service (IaaS): Introduction to IaaS, Resource Virtualization. Platform as a Service (PaaS): Introduction to PaaS, Cloud Platform and Management. Software as a Service (SaaS): Introduction to SaaS, Web services, Web 2.0, Web OS.
Beyond the Syllabus: Companies in the Cloud Today, Amazon Web Servies, Google services, IBM Cloud, Windows Azure, Tata Cloud, Salesforce.com

13+4 Hours

Unit III

Virtualization & Design

Virtualization, Virtual machine, Implementation Levels of Virtualization, Virtualization Structures/Tools and Mechanisms, Virtualization of CPU, Memory, and I/O Devices, Virtual Clusters and Resource Management, Data centre, Virtualization for Data-Centre Automation. Service Levels for Cloud Applications Ready for the cloud: Web Application Design, Machine Image Design, Privacy Design, Database Management.
Beyond the Syllabus: various hypervisors like VMware, KVM, oracle VM,

10+4 Hours

Unit IV

Cloud Service Providers

EMC, EMC IT, Captiva Cloud Toolkit, Google, Cloud Platform, Cloud Storage, Google Cloud Connect, Google Cloud Print, Google App Engine, Amazon Web Services, Amazon Elastic Compute Cloud, Amazon Simple Storage Service, Amazon Simple Queue, service, Microsoft, Windows Azure, Microsoft Assessment and Planning Toolkit, SharePoint, IBM, Cloud Models, IBM Smart Cloud, SAP Labs, SAP HANA Cloud Platform, Virtualization Services Provided by SAP, Sales force, Sales Cloud.
Service Cloud: Knowledge as a Service, Rack space, VMware, Manjra soft, Aneka Platform

10+3 Hours
Total: 45+15 Hours

Reading Material:

1. George Coulouris, Jean Dollimore, Tim Kindberg, "Distributed Systems- Concepts and Design", Fourth Edition, Pearson Publication
2. Cloud Computing Bible, Barrie Sosinsky, Wiley-India, 2010

3. Cloud Computing: Principles and Paradigms, Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, Wile, 2011
4. Cloud Computing: Principles, Systems and Applications, Editors: Nikos Antonopoulos, Lee Gillam, Springer, 2012
5. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, Wiley-India, 2010

21CCS017 Protocols and Architectures for Wireless Sensor Networks

4 0 0 4

Course outcomes

1. Select and use an appropriate wireless sensors to solve a given problem.
2. Understand fundamental concepts of medium access control protocols for WSN.
3. Master the basic concepts and understand the routing and data gathering protocols.
4. Understand fundamental concepts of operating systems for WSN.
5. Describe, contrast and compare different structures of WSN operating systems.
6. Analyze the various applications of WSN.

UNIT I

Characteristics Of WSN: Characteristic requirements for WSN - Challenges for WSNs – WSN vs Adhoc Networks - Sensor node architecture – Commercially available sensor nodes –Imote, IRIS, Mica Mote, EYES nodes, BTnodes, TelosB, Sunspot -Physical layer and transceiver design considerations in WSNs, Energy usage profile, Choice of modulation scheme, Dynamic modulation scaling, Antenna considerations. **Medium Access Control Protocols:** Fundamentals of MAC protocols - Low duty cycle protocols and wakeup concepts - Contentionbased protocols - Schedule-based protocols - SMAC - BMAC - Traffic-adaptive medium access protocol (TRAMA) - The IEEE 802.15.4 MAC protocol.

13+4 Hours

UNIT II

Routing And Data Gathering Protocols:

Routing Challenges and Design Issues in Wireless Sensor Networks, Flooding and gossiping – Data centric Routing – SPIN – Directed Diffusion – Energy aware routing - Gradient-based routing - Rumor Routing – COUGAR – ACQUIRE – Hierarchical Routing - LEACH, PEGASIS –Location Based Routing – GF, GAF, GEAR, GPSR – Real Time routing Protocols – TEEN,

APTEEN, SPEED, RAP - Data aggregation - data aggregation operations - Aggregate Queries in Sensor Networks - Aggregation Techniques – TAG, Tiny DB.

12+4 Hours

UNIT III

Embedded Operating Systems:

Operating Systems for Wireless Sensor Networks – Introduction - Operating System Design Issues - Examples of Operating Systems – TinyOS – Mate – MagnetOS – MANTIS - OSPM -EYES OS – SenOS – EMERALDS – PicOS – Introduction to Tiny OS – NesC – Interfaces and Modules- Configurations and Wiring - Generic Components - Programming in Tiny OS using

NesC, Emulator TOSSIM.

10+4 Hours

UNIT IV

Applications Of WSN:

WSN Applications - Home Control - Building Automation - Industrial Automation - Medical Applications - Reconfigurable Sensor Networks -Highway Monitoring - Military Applications - Civil and Environmental Engineering Applications - Wildfire Instrumentation - Habitat Monitoring - Nanoscopic Sensor Applications – Case Study: IEEE 802.15.4 LR-WPANs Standard - Target detection and tracking - Contour/edge detection -Field sampling.

10+3Hours

Total: 45+15 Hours

Reading material:

1. Kazem Sohraby, Daniel Minoli and Taieb Znati, " Wireless Sensor Networks Technology, Protocols, and Applications", John Wiley & Sons, 2007.
2. Holger Karl and Andreas Willig, "Protocols and Architectures for Wireless Sensor Networks", John Wiley & Sons, Ltd, 2005.
3. K. Akkaya and M. Younis, "A survey of routing protocols in wireless sensor networks", Elsevier Ad Hoc Network Journal, Vol. 3, no. 3, pp. 325--349
4. Philip Levis, " TinyOS Programming" 3.Anna Ha´c, "Wireless Sensor Network Designs", John Wiley & Sons Ltd.

21CCS018 Fundamentals of 5G Mobile Networks

4 0 0 4

Course outcomes

1. Understand basics of 5G networks
2. Understand small cells, spectrum allocation methods
3. Understand 5G Internet
4. Learn next generation wireless networks
5. Analyze mobile cloud
6. Understand cognitive radio for 5G wireless networks

UNIT I

5G: Introduction: Historical Trend of Wireless Communications, Evolution of LTE Technology to Beyond 4G, 5G Roadmap, Ten pillors of 5G, Evolution of Existing RATs, Hyperdense Small- Cell Deployment Self- Organising Network, Machine Type Communication, Developing Millimetre- Wave RATs, Redesigning Backhaul Links, Energy Efficiency, Allocation of New Spectrum for 5G, Spectrum Sharing, RAN Virtualisation.

13+4 Hours

UNIT II

The 5G Internet: Introduction, Internet of Things and Context- Awareness, Networking Reconfiguration and Virtualisation Support, Mobility, Quality of service control, Emerging Approach for Resource Over- Provisioning. **Small Cells for 5G Mobile Networks:** What are Small Cells, Capacity Limits and Achievable Gains with Densification, Mobile Data Demand.

11+4 Hours

UNIT III

Cooperation for Next Generation Wireless Networks: Cooperative Diversity and Relaying Strategies- Cooperation and Network Coding, and Cooperative ARQ MAC Protocols. PHY Layer Impact on MAC Protocol Analysis, **Mobile Clouds**: The Mobile Cloud, Mobile Cloud Enablers, Network Coding.

11+4 Hours

UNIT IV

Cognitive Radio for 5G Wireless Networks:

Overview of Cognitive Radio Technology in 5G Wireless, Spectrum Optimisation using Cognitive Radio, Relevant Spectrum Optimisation Literature in 5G, Cognitive Radio and Carrier Aggregation, Energy- Efficient Cognitive Radio Technology, Key Requirements and Challenges for 5G Cognitive Terminals.

10+3 Hours

Total 45+15 Hours

Reading material

1. Jonathan Rodriguez, “Fundamentals of 5G Mobile Networks”, Willy 2015.

21AT0001RESEARCH METHODOLOGY and IPR

0 0 0 0

Course Outcomes

1. Understand the various aspects of a research problem
2. Explain the importance of scope and objective of a research problem.
3. Analyze the various components of the format of a good research Proposal.
4. Identify the various concepts of IPR and patenting.
5. Interpret the various scopes of patent rights
6. Outline the various new developments in IPR

UNIT I

RESEARCH PROBLEM AND SCOPE FOR SOLUTION

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

UNIT II

FORMAT

Effective literature studies approaches, analysis, Plagiarism, Research ethics. Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT III

PROCESS AND DEVELOPMENT

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, patenting under PCT.

UNIT IV

PATENT RIGHTS and IPR

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

Textbook (s)

1. Goddard, Wayne, and Stuart Melville. Research methodology: An introduction. Juta and Company Ltd, 2004.
2. Kumar, Ranjit. Research methodology: A step-by-step guide for beginners. Sage, 2018.

Reference (s)

1. Halbert, “Resist ing Intellectual Property”, Taylor & Francis Ltd ,2007.
2. Mayall, “Industrial Design”, McGraw Hill, 1992.
3. Niebel, “Product Design”, McGraw Hill, 1974.
4. Asimov, “Introduction to Design”, Prent ice Hall, 1962.
5. Robert P. Merges, Peter S. Menell, Mark A. Lemley, “Intellectual Property in New Technological Age”, 2016.
6. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008