Savitribai Phule Pune University
(Formerly University of Pune)

Department of Technology
Board of Studies Information Security (IS)
Curriculum Structure for M.Tech Program

Sr. No.	Subject Code	Subject Name	Credits	Teaching Scheme (Theory)	Teaching Scheme (Tut)
Semester (I)					
1	IS101	Fundamentals of Computer Networks	4	√	√
2	IS102	Fundamentals of Information Security	4	√	√
3	IS103	Foundation of Data Privacy	4	√	√
4	IS104	Building blocks of NOC & SOC	2	√	√
5	IS105	Lab Practice- 1	2		
6	ISSM1	Seminar – 1	2		
Semester (II)					
7	IS201	SIEM & Log Analytics	4	√	√
8	IS202	Vulnerability Analysis & System Hardening Methodologies	4	√	√
9	IS203	Network Defense Technologies	2	√	√
10	IS204	Network Security Design	2	√	√
11	IS205	Security of Operational Technologies	2	√	√
12	IS206	Lab Practice- 2	2		
13	ISSM2	Seminar – 2	2		
Semester (III)					
14	IS301	Cyber Threat & Risk Modeling	4	√	√
15	IS302	Fundamentals of Network Resiliency	2	√	√
16	IS303	Virus & Malware Research	2	√	√
17	ISIntProj	Interim Project	10		
Semester (IV)					
18	ISFinProj	Final Project	16		
		TOTAL CREDITS	70		

AUDIT COURSES				
Sr. No.	Subject Code	Subject Name	Credits	Semester
1	CYSA	Cyber Security	2	I
2	HRE101	Human Rights & Duties	1	I
3	HRE102/HRE103	Human Rights & Vulnerable Groups/Law Policy , Society & Enforcement mechanism	1	II

[IS101] Fundamentals of Computer Networks

Contents:

The OSI Model and the TCP/IP Protocol Suite, Underlying Technologies, Introduction to Network Layer, IP Addresses, Delivery and Forwarding of IP Packets, Internet Protocol Version 4 (IPv4) & Version 6 (IPv6),   Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Unicast Routing Protocols (RIP, OSPF and BGP), Multicasting and Multicast Routing Protocols,   Introduction to the Transport Layer, User Datagram Protocol (UDP), Transmission Control Protocol (TCP),   Introduction to the Application Layer, Host Configuration: DHCP, Domain Name System (DNS), Remote Login: TELNET and SSH, File Transfer: FTP and TFTP, World Wide Web and HTTP, Electronic Mail: SMTP, POP, IMAP and MIME,   Network Management: SNMP, Multimedia, IPSec & VPN tunnelling, VLAN, Network Address Translation & Port Address Translation

Books:

1.TCP/IP Protocol Suite E/4 , ISBN: 9780070706521, Author: Behrouz A. Forouzan, Tata McGraw-Hill
2.Data Communications & Networks, ISBN: 9780071077705, Authors: Achyut Godbole, Atul Kahate, Tata McGraw-Hill
3.Data Communications And Networking ISBN: 9781259064753 Authors Behrouz A. Forouzan, Tata McGraw-Hill

[IS102] Fundamentals of Information Security

Contents:

Understand and Apply Concepts of Confidentiality, Integrity, and Availability, Information Security, Evaluate and Apply Security Governance Principles, Alignment of Security Functions to Business Strategy, Goals, Mission, and Objectives, Vision, Mission, and Strategy Governance, Due Care, Determine Compliance Requirements, Legal Compliance, Jurisdiction, Legal Tradition, Legal Compliance Expectations, Understand Legal and Regulatory Issues That Pertain to Information Security in a Global Context, Cyber Crimes and Data Breaches, Privacy, Understand, Adhere to, and Promote Professional Ethics, Ethical Decision-Making, Established Standards of Ethical Conduct, Ethical Practices, Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines, Organizational Documents, Policy Development, Policy Review Process, Identify, Analyze, and Prioritize Business Continuity Requirements, Develop and Document Scope and Plan, Risk Assessment, Business Impact Analysis, Develop the Business Continuity Plan, Contribute to and Enforce Personnel Security Policies and Procedures, Key Control Principles, Candidate Screening and Hiring, Onboarding and Termination Processes, Vendor, Consultant, and Contractor Agreements and Controls, Privacy in the Workplace, Understand and Apply Risk Management Concepts, Risk, Risk Management Frameworks, Risk Assessment Methodologies, Understand and Apply Threat Modeling Concepts and Methodologies, Threat Modeling Concepts, Threat Modeling Methodologies, Apply Risk-Based Management Concepts to

the Supply Chain, Supply Chain Risks, Supply Chain Risk Management, Establish and Maintain a Security Awareness, Education, and Training Program,

Security Awareness Overview, Developing an Awareness Program,Training

Books:

1.(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide 8th Edition, ISBN-13: 978-1119475934 , Author: Mike Chapple, James Michael Stewart, Darril Gibson
2.The Official (ISC)2 Guide to the CISSP CBK Reference, 5th Edition, ISBN: 978-1-119-42334-8, Authors: John Warsinske, Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl, Mike Vasquez

[IS103] Foundation of Data Privacy

Contents:

Fundamental concepts of privacy and data protection, including:
- Common privacy principles and approaches.
- Global data protection models.
- Information security controls.
- Online privacy protections.

Privacy by Design - The 7 Foundational Principles

Motivations of data privacy, key terminologies related with data privacy, Classification of protection procedures, user's privacy in communication & information retrieval, Privacy models & disclosure risk measures

Privacy Regulations – India Data Privacy Act, GDPR, CCPA,

Books:

1. Foundations of Information Privacy and Data Protection by Peter P. Swire, CIPP/US, and Kenesa Ahmad, CIPP/US, Terry McQuay, CIPP/US ISBN0979590175 (ISBN13: 9780979590177)
2. Data Privacy: Foundations, New Developments and the Big Data Challenge ISBN331957356X (ISBN13: 9783319573564)
3. The Foundations of EU Data Protection Law ISBN0198718233 (ISBN13: 9780198718239)
4. The EU General Data Protection Regulation (GDPR), A Practical Guide ISBN331986291X (ISBN13: 9783319862910)
5. THE PERSONAL DATA PROTECTION BILL, 2019

[IS104] Building blocks of NOC & SOC

Contents:

NOC: The Basic Ingredients of Network Management, The Network Device, Management Agent, Management Information, MOs, MIBs, and Real Resources, Basic Management Ingredients—Revisited, The Management System, Management System and Manager Role, A Management System's Reason for Being, The Management Network, Networking for Management, The Pros and Cons of a Dedicated Management Network, The Management Support Organization: NOC, NOC, Who's There?, Managing the Management, Inside the Network Operations Center, Management Functions and Reference Models: Getting Organized, FCAPS: The ABCs of Management, Limitations of the FCAPS Categorization, OAM&P: The Other FCAPS,FAB and eTOM, How It All Relates and What It Means to You: Using Your Network Management ABCs

SOC: Review high-level issues, such as vulnerability and risk management, threat intelligence, digital investigation, and data collection/analysis, Understand the technical components of a modern SOC, Assess the current state of your SOC and identify areas of improvement, Plan SOC strategy, mission, functions, and services, Design and build out SOC infrastructure, from facilities and networks to systems, storage, and physical security, Collect and successfully analyze security data, Establish an effective vulnerability management practice, Organize incident response teams and measure their performance. Define an optimal governance and staffing model, Develop a practical SOC handbook that people can actually use, Prepare SOC to go live, with comprehensive transition plans, React quickly and collaboratively to security incidents, Implement best practice security operations, including continuous enhancement and improvement

Books:

1.Network Management Fundamentals, ISBN-13: 978-1-58705-280-4, Author: Alexander Clemm
2.Security Operations Center: Building, Operating, and Maintaining your SOC, ISBN-13: 978-0-13-405201-4, Authors: By Joseph Muniz, Gary McIntyre, Nadhem AlFardan.

[IS201] SIEM & Log Analytics

Contents:

SIEM Concepts:

Log Management, Syslog, Alerts, Flow Data, Vulnerability Assessment Data, Logging Solutions, Event Correlation, Event Normalization, Correlation Rules

The Anatomy of a SIEM

Source Device, Operating Systems, Appliances, Applications, Determining Needed Logs, Determining Needed SIEM Resources, Log Collection, Push Log Collection, Pull Log Collection, Prebuilt Log Collection,

Custom Log Collection, Mixed Environments, Parsing/Normalization of Logs, Rule Engine/Correlation Engine, Correlation Engine, Log Storage, Database, Flat Text File, Binary File, Monitoring

Books:

1.Security Information and Event Management (SIEM) Implementation, Authors: DAVI D R . MILLER, SHON HARRIS, ALLEN A. HARPER, STEPHEN VANDYKE, CHRIS BLASK, ISBN: 978-0-07-170108-2, McGraw Hill
2.Network Security Through Data Analysis, Author: Michael Collins, ISBN: 978-1-449-35790-0 O'Reilly Media, Inc
3.Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices, Author: Arun E Thomas, ISBN-13: 978-1533408501

[IS202] Vulnerability Analysis & System Hardening Methodologies

Contents:

OVERVIEW OF THE VAM METHODOLOGY, System object types, Attributes of System objects. Introduction to Software Security Assessment, SOFTWARE VULNERABILITY FUNDAMENTALS, Vulnerabilities, Security Policies, Security Expectations, The Necessity of Auditing, Auditing Versus Black Box Testing, Code Auditing and the Development Life Cycle, Classifying Vulnerabilities, Design Vulnerabilities, Implementation Vulnerabilities

Operational Vulnerabilities, Gray Areas, Common Threads, Input and Data Flow, Trust Relationships, Assumptions and Misplaced Trust, Interfaces, Environmental Attacks, Exceptional Conditions, DESIGN REVIEW, Software Design Fundamentals, Algorithms

Abstraction and Decomposition, Trust Relationships, Principles of Software Design, Fundamental Design Flaws, Enforcing Security Policy, Authentication, Authorization, Accountability, Confidentiality, Integrity, Availability, Threat Modeling, Information Collection, Application Architecture Modeling, Threat Identification, Documentation of Findings, Prioritizing the Implementation Review, OPERATIONAL REVIEW, Exposure, Attack Surface, Insecure Defaults, Access Control, Unnecessary Services, Secure Channels

Spoofing and Identification, Network Profiles, Web-Specific Considerations, HTTP Request Methods, Directory Indexing, File Handlers, Authentication, Default Site Installations, Overly Verbose Error Messages, Public-Facing Administrative Interfaces, Protective Measures, Development Measures, Host-Based Measures, Network-Based Measures, APPLICATION REVIEW PROCESS, Overview of the Application Review Process, Rationale, Process Outline

System Security Hardening: Linux & Windows Operating systems.

Books:

1.The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Authors: John McDonald (Author), Mark Down (Author), Justin Schuh (Author), ISBN-13: 978-0321444424, Addison Wesley
2.The Vulnerability Assessment & Mitigation Methodology, Authors: Philip S. Antón, Robert H. Anderson, Richard Mesic, Michael Scheiern,, ISBN 0-8330-3434-0
3.Mastering Linux Security and Hardening, Author: Donald A. Tevault, ISBN-13: 978-1788620307

[IS203] Network Defense Technologies

Contents:

Introduction to Network Security Solutions, Overview of Network Security Technologies, Firewalls, Network Firewalls, Network Address Translation (NAT), Stateful Firewalls, Deep Packet Inspection, Demilitarized Zones, Personal Firewalls, Virtual Private Networks (VPN), Technical Overview of IPsec, Phase 1, Phase 2, SSL VPNs, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS),Pattern Matching, Protocol Analysis, Heuristic-Based Analysis, Anomaly-Based Analysis, Anomaly Detection Systems, Authentication, Authorization, and Accounting (AAA) and Identity Management, RADIUS, TACACS+, Identity Management Concepts, Network Admission Control, NAC Appliance, NAC Framework, Routing Mechanisms as Security Tools, Data Center Security, Protecting the Data Center Against Denial of Service (DoS) Attacks and Worms, SYN Cookies in Firewalls and Load Balancers.

Books:

1.Guide to Network Defence and Countermeasures, Author: Randy Weaver, Dawn Weaver, Dean Farwood, ISBN-13: 978-1133727941
2.End-to-End Network Security: Defense-in-Depth, Author: Omar Santos, ISBN-13: 978-0-13-279844-0, Cisco Press

[IS204] Network Security Design

Contents:

I. NETWORK SECURITY FOUNDATIONS.
1. Network Security Axioms.
Network Security Is a System. Business Priorities Must Come First. Network Security Promotes Good Network Design. Everything Is a Target. Everything Is a Weapon. Strive for Operational Simplicity. Good Network Security Is Predictable. Avoid Security Through Obscurity. Confidentiality and Security Are Not the Same.
2. Security Policy and Operations Life Cycle.
Security System Development and Operations Overview.
3. Secure Networking Threats.

Books:

1.Network Security Architectures Author: Sean Convery, ISBN-13: 978-1-58705-115-9, Cisco Press

2.Designing Network Security (paperback) (2nd Edition), Author: Merike Kaeo, ISBN: 9781587142499

[IS205] Security in Operational technology

Contents:

Overview of Industrial Control Systems, ICS Risk Management & Assessment, ICS Security Architecture, Applying Security Controls to ICS, ICS Security Program Development & Deployment.

Elements of IoT, Things in the Internet of Things, Intelligent decision making, Sensors and actuators, Embedded systems , Communications, Security considerations, Challenge of defining horizontal baseline security measures, Architecture, Asset taxonomy, Threats and risk analysis, Security incidents, Threat taxonomy, Examples of IoT cyber security attack scenarios, Critical attack scenarios, Attack scenario 1: IoT administration system compromise, Attack scenario 2: Value manipulation in IoT devices, Attack scenario 3: Botnet / Commands injection, Security measures and good practices, Security measures and good practices, Policies, Security by design, Privacy by design, Asset Management, Risk and Threat Identification and Assessment, Organizational, People and Process measures, End-of-life support, Proven solutions, Management of security vulnerabilities and/or incidents, Human Resources Security Training and Awareness, Third-Party relationships, Technical Measures, Hardware security, Trust and Integrity Management, Strong default security and privacy, Data protection and compliance, System safety and reliability, Secure Software / Firmware updates, Authentication, Authorization, Access Control - Physical and Environmental security, Cryptography, Secure and trusted communications , Secure Interfaces and network services, Secure input and output handling, Logging , Monitoring and Auditing

Books:
1.Guide to Industrial Control Systems, (ICS) Security, ISBN-10 : 1469954826, ISBN-13 : 978-1469954820
2.Baseline Security Recommendations for IoT, Author: ENISA, ISBN: 978-92-9204-236-3
3.Practical Internet of Things Security, Author: Brian Russell, Drew Van Duren, ISBN: 9781785889639

[IS301] Cyber Threat & Risk Modeling

Content:

Cyber Threat Modelling

Strategies for Threat Modeling, Threat detection: STRIDE. Threat Tree, Attack Trees, Attack Libraries, Privacy Tools, Managing and Addressing Threats, Defensive Tactics and Technologies, Trade-Offs When

Addressing Threats, Validating That Threats Are Addressed, Threat Modeling Tools, Threat Modeling in Technologies and Tricky Areas, Requirements Cookbook, Web and Cloud Threats, Accounts and Identity, Human Factors and Usability, Threats to Cryptosystems

Cyber Risk Modelling

Mathematical models for cybersecurity risk management, adversarial risk analysis, The Cybersecurity and Cyber Insurance Landscape, Risk Management Models for Cyber Insurance, A Case Study in Cybersecurity Resource Allocation and Cyber Insurance

Books:

1. Threat Modeling: Designing for Security by Adam Shostack
ISBN: 978-1-118-80999-0
2. Security Risk Models for Cyber Insurance, Edited By David Rios Insua, Caroline Baylon, Jose Vila
   ISBN-10 : 0367339498, ISBN-13 : 978-0367339494
3. Cyber-Risk Management
Authors: Refsdal, Atle, Solhaug, Bjørnar, Stolen, Ketil
4. Cyber-Risk Informatics by Mehmet Sahinoglu Released May 2016
   Publisher(s): Wiley ISBN: 9781119087519

[IS302] Fundamentals of Network Resiliency

Contents:

Fundamentals of IP Resilient Networks, Revisiting IP, TCP, and UDP, Internet Protocol, Transmission Control Protocol, TCP Three-Way Handshake, TCP Sliding Window, User Datagram Protocol, Device-Level Resiliency, Online Insertion and Removal (OIR), Single Line Card Reload, High System Availability, Route Processor Redundancy, Route Processor Redundancy Plus, Stateful Switchover, Nonstop Forwarding, Impact of Different Switching Paths, Process Switching, Protecting the Control Plane and Data Plane, Establishing a Resiliency Strategy, Redundancy Strategy, Logical Resiliency, Physical Resiliency, Scaling Strategy, Key Principles for Designing Resilient Networks, Resilient Border Gateway Protocol (BGP) Design, Using Network Address Translation (NAT), Enhanced NAT Resiliency, NAT with Route Map, Static Mapping with Hot Standby Routing Protocol (HSRP) Support, Stateful NAT, Limiting NAT Entries, Multihoming with NAT, Effects of NAT on Network and Applications, Data Center Environmental Considerations, Cabling, Tagging,

Documentation, Discipline, Rack Space, Server Size, Power, Next-Generation Server Architecture, Data Center Network Considerations, Security, Server Performance, Fault-Tolerant Server Features, Multifaceted Server, Data Center Network Architecture, Access Layer Design, NIC Teaming, Clustering, Architecture Scaling Consideration, Data Center Network Security, Layer 2 Security, Private VLANs (PVLANs), VLAN Access Control List (VACL), Port Security, Dynamic ARP Inspection, Layer 3 Security,

Switch Forwarding Architecture, Control Plane Policing, DHCP Server Protection, Service Optimization, Server Load Balancing, Global Site Selector, Understanding DNS Resolution, Using GSS, Web Cache Communication Protocol (WCCP), Integrated Service Modules

Books:

1.	Building Resilient IP Networks, Author: Kok-Keong Lee, Fung Lim, Beng-Hui Ong, Cisco Press, ISBN-13: 978-1-58705-215-6

[IS303] Virus & Malware Research

Content:

Strategies of the Attacker:
Malicious code analysis, malicious code environments, infection strategies, Computer virus generator kits, basic self-protection strategies, exploits, vulnerabilities, buffer overflow attacks, strategies for computer worm, payload-based strategies
Strategies of the Defender:
Antivirus defense techniques, memory scanning & disinfection, worm blocking techniques & HIDS, Network level defense,

The Goals of Malware Analysis, Malware Analysis Techniques, Basic Static Analysis, Basic Dynamic Analysis, Advanced Static Analysis, Advanced Dynamic Analysis, Types of Malwares, General Rules for Malware Analysis, Basic Analysis, Basic Static Techniques, Antivirus Scanning: A Useful First Step Hashing: A Fingerprint for Malware, Finding Strings, Packed and Obfuscated Malware, Packing Files Detecting Packers with PEiD, Portable Executable File Format, Linked Libraries and Functions Static, Runtime, and Dynamic Linking, Exploring Dynamically Linked Functions with Dependency Walker Imported Functions, Exported Functions, Static Analysis in Practice, Potential Keylogger.exe: An Unpacked Executable, PackedProgram.exe: A Dead End, The PE File Headers and Sections, Examining PE Files with PEview, Viewing the Resource Section with Resource Hacker Using Other PE File Tools PE Header Summary

Books

1.	Art of Computer Virus Research and Defense, by Peter Szor
	ISBN-13: 978-0321304544/ ISBN-10: 9780321304544
2.	Practical Malware Analysis by Michael Sikorski, Andrew Honig Released February 2012
	Publisher(s): No Starch Press ISBN: 9781593272906