Savitribai Phule Pune University(Formerly University of Pune)

Department of Technology

Board of Studies Information Security (IS)

STRUCTURE OF ONE YEAR FULL TIME

P.G. Diploma in Advanced Cyber Security (PGD-ACS)

Intake: 60

Eligibility Criteria: Graduation in any Stream

Sr. No.	Subject Code	Subject Name	Credits	Teaching Scheme (Theory)	Teaching Scheme (Tut)
Semester (I)					
1	PGDACSC1	Fundamentals of Computer Networks	4	√	√
2	PGDACSC2	Fundamentals of Information Security	4	√	√
3	PGDACC3	Foundation of Data Privacy	4	√	√
4	PGDACSC4	Building blocks of NOC & SOC	2	√	√
5	PGDACSLP1	Lab Practice- 1	2		√
6	PGDACSS1	Seminar – 1	2		√
7	PGDACSRM	Research Methodology	4		
Semester (II)					
8	PGDACSC5	SIEM & Log Analytics	4	√	√
9	PGDACSC6	Vulnerability Analysis & System Hardening Methodologies	4	√	√
10	PGDACSC7	Network Defense Technologies	2	√	√
11	PGDACSC8	Network Security Design	2	√	√
12	PGDACSC9	Security of Operational Technologies	2	√	√
13	PGDACSLP2	Lab Practice- 2	2		√
14	PGDACSMiniProj	Mini Project	6		√
		TOTAL CREDITS	44		

PGDACSC1

Fundamentals of Computer Networks

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 tothe 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

References:

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, TataMcGraw-Hill
3.Data Communications And Networking ISBN: 9781259064753 Authors Behrouz A. Forouzan, TataMcGraw-Hill

PGDACSC2

Fundamentals of Information Security

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 SecurityAwareness, Education, and Training Program, Security Awareness Overview, Developing an Awareness Program, Training

References:

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

PGDACSC3

Foundation of Data Privacy

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

References:

1. Foundations of Information Privacy and Data Protection by Peter P. Swire, CIPP/US, and KenesaAhmad, 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

PGDACSC4

Building blocks of NOC & SOC

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 forBeing, 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

References:

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.

PGDACSC5

SIEM & Log Analytics

SIEM Concepts: Log Management, Syslog, Alerts, Flow Data, Vulnerability Assessment Data, Logging Solutions, EventCorrelation, 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/CorrelationEngine, Correlation Engine, Log Storage, Database, Flat Text File, Binary File, Monitoring

References:

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'ReillyMedia, Inc
3. Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices, Author: Arun EThomas, ISBN-13: 978-1533408501

PGDACSC6

Vulnerability Analysis & System HardeningMethodologies

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 BlackBox 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, DESIGNREVIEW, Software Design Fundamentals, Algorithms

Abstraction and Decomposition, Trust Relationships, Principles of Software Design, Fundamental DesignFlaws, 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.

References:

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

PGDACSC7

Network Defense Technologies

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, AnomalyDetection 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.

References:

1. Guide to Network Defence and Countermeasures, Author: Randy Weaver, Dawn Weaver, DeanFarwood, 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

PGDACSC8

Network Security Design

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. GoodNetwork Security Is Predictable. Avoid Security Through Obscurity. Confidentiality and Security Are Notthe Same.
2. Security Policy and Operations Life Cycle.
Security System Development and Operations Overview.

3. Secure Networking Threats.

The Attack Process. Attacker Types. Vulnerability Types. Attack Results. Attack Taxonomy.

4. Network Security Technologies.

The Difficulties of Secure Networking. Security Technologies. Emerging Security Technologies.

II. DESIGNING SECURE NETWORKS.

5. Device Hardening.

Components of a Hardening Strategy. Network Devices. Host Operating Systems. Applications.Appliance-Based Network Services. Rogue Device Detection.

6. General Design Considerations.

Physical Security Issues. Layer 2 Security Considerations. IP Addressing Design Considerations. ICMP Design Considerations. Routing Considerations. Transport Protocol Design Considerations. DoS DesignConsiderations.

7. Network Security Platform Options and Best Deployment Practices.

Network Security Platform Options. Network Security Device Best Practices.

8. Common Application Design Considerations.

E-Mail. DNS. HTTP/HTTPS. FTP. Instant Messaging. Application Evaluation.

9. Identity Design Considerations.

Basic Foundation Identity Concepts. Types of Identity. Factors in Identity. Role of Identity in SecureNetworking. Identity Technology Guidelines. Identity Deployment Recommendations.

10. IPsec VPN Design Considerations.

VPN Basics. Types of IPsec VPNs. IPsec Modes of Operation and Security Options. Topology Considerations. Design Considerations. Site-to-Site Deployment Examples. IPsec Outsourcing.

11. Supporting-Technology Design Considerations. Content. Load Balancing.

Wireless LANs. IP Telephony.

12. Designing Your Security System.

Network Design Refresher. Security System Concepts. Impact of Network Security on the Entire Design.Ten Steps to Designing Your Security System. Summary. Applied Knowledge Questions.

III. SECURE NETWORK DESIGNS.

13. Edge Security Design.

What Is the Edge? Expected Threats. Threat Mitigation. Identity Considerations. Network Design Considerations. Small Network Edge Security Design. Medium Network Edge Security Design. High-EndResilient Edge Security Design. Provisions for E-Commerce and Extranet Design.

14. Campus Security Design.

What Is the Campus? Campus Trust Model. Expected Threats. Threat Mitigation. Identity Considerations.Network Design Considerations. Small Network Campus Security Design. Medium Network Campus Security Design. High-End Resilient Campus Security Design.

15. Teleworker Security Design.

Defining the Teleworker Environment. Expected Threats. Threat Mitigation. Identity Considerations.Network Design Considerations. Software-Based Teleworker Design. Hardware-Based Teleworker Design. Design Evaluations.

References:

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

PGDACSC9

Security in Operational technology

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 baselinesecurity 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

References:

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