Savitribai Phule Pune University
(Formerly University of Pune)

Department of Technology
Board of Studies Information Security (IS)
STRUCTURE OF ONE YEAR FULL TIME POST GRADUATE DIPLOMA IN
Advanced Network Security (PGD-ANS)

Semester I

Sr. No.	Course Code	Course Name	Teaching Scheme		Credits
			L	T	
1	ANS101	Systems and Network Security	3	1	4
2	ANS102	Cryptography Advanced	3	1	4
3	ANS103	Internet Technologies and Protocols	3	1	4
4	ANS104	Security Architecture	3	1	4
5	ANS105	Operating Systems Security	3	1	4
		Total Credits			**20**

Semester II

Sr. No.	Course Code	Course Name	Teaching Scheme		Credits
			L	T	
6	ANS201	Vulnerability Assessment and Penetration Testing	3	1	4
7	ANS202	Malware and Reverse Engineering	3	1	4
8	ANS203	Governance, Risk and Compliance	3	1	4
9	ANS204	Mobile Security	3	1	4
10	ANS205	Cyber Forensics	3	1	4
		Total Credits			**20**

Systems and Network Security

Introduction, Monitoring Key Files in the System, Security Objectives, Rootkits, Antivirus Software, Intrusion Detection, Full-packet capture devices, Out-of-Band Attack Vectors.
Design principles for secure systems, host based security, systems security, server security, authentication, authorization, access control, network layer security, TCP security issues; DDoS attacks; end-to-end security, link encryption, and secure network communication, IPSEC, network authentication, firewalls, intrusion detection and prevention.
Electronic User Authentication Principles, Password-Based Authentication, Token-Based Authentication, Biometric Authentication, Remote User Authentication, and Security Issues for User Authentication, Practical Applications and Case Studies.
Detection, Network Based detection of Intrusions, Preventing System Intrusions, Traditional Reconnaissance and Attacks, malicious software, Defense in depth, Guarding against network intrusions. Securing Cloud Computing systems, managing risks in cloud, SaaS, PaaS and IaaS, Achieving security in private cloud.
Unix and Linux Security, Basic security overview, achieving Unix security, Protecting User Account and Authentications, eliminating security weaknesses of Linux and Unix Operating Systems, Hardening Linux and Unix and Proactive Defense.
Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack
Internet Security, Defending against attacks on Internet, Internet Security Checklist, Security at transport & network layers, SSL, IPsec, Authentication header, encapsulating security payload protocol. Intranet Security, Wireless Network Security, Wired Network Protection, LAN Security.

Reference Books:

1. Network Security: The Complete Reference by Roberta Bragg, Mark Phodes –Ousley, Keith Strassberg Tata McGraw-Hill.
2. Network and System Security by John Vacca.

Cryptography Advanced

Intro to advanced Cryptography Security, Location of Symmetric Encryption Devices, Public-Key Cryptography and Message Authentication, Secure Hash Functions, HMAC, Integers & finite group theory, RSA and ElGamal ciphers, cyclic groups and the discrete log problem, Baby-step Giant-step and the Index Calculus probabilistic algorithms to compute discrete logs in cyclic groups, Naor – Reingold and Blum – Blum – Shub Random Number Generators, Fermat, Euler and Miller-Rabin primality tests, Pollard's and Quadratic Sieve factorization algorithms, transfer protocols and zero-knowledge proofs, Commutative rings, finite fields, rings of polynomials, and finding of the greatest common divisor in the ring of polynomial, Irreducible polynomials, Field extensions, elliptic curves the ElGamal cipher on elliptic curves, SHA-512 as well as various digital signatures, entity authentication and key management issues, Quantum cryptography

Reference Books:

1. Cryptanalysis of number theoretic Cyphers, Samuel S. Wagstaff Jr.
2. Cryptography and Network Security by William Stallings

Internet Technologies and Protocols

Internet Security Protocols and Standards, Secure Email and S/MIME, DomainKeys Identified Mail, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), HTTPSIPv4 and IPv6 Security, Internet Authentication Applications, Kerberos, X.509, Public-Key Infrastructure, Federated Identity Management, Protocols – http, https, ssl, tls, email protocols, snmp, ldap, routing protocols, Modbus, Vpn protocols, Ipv6, Soap, Dns, dhcp, arp

Reference Books:

1. Computer Networking with Internet Protocols and Technology by Stallings.

Security Architecture

Intro to security architecture, Objectives of Security - DiD, CIA, Developing security policy, Structured monitoring, Security planning for businesses, Implementing security (DLP, UTM), Virtualization, Tools for protocol disassembly, reassembly – wireshark / tcpdump / netcat, Netflow

Reference Books:

1. Information Security Architecture: An integrated Approach to Security in the organization by Jan Killmeyer.
2. Enterprise Security Architecture by Nicholas Sherwood

Operating Systems Security

Mandatory access control, trusted computing, security models, security kernel, covert channel, distributed computing, cloud computing, Windows and Linux; Web Security, App Security; hardening OS; Assurance and Trust, Building Secure and Trusted Systems, Building Security In or Adding Security Later, DAC & MAC. Introduction to Operating System Security, System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/UNIX Security, Windows Security, Virtualization Security, Designing Trusted Operating Systems, What Is a Trusted System? Security Policies & Models of Security, Trusted Operating System Design, Assurance in Trusted Operating Systems , Security in Operating Systems, Cloud Computing, Cloud Security Risks and Countermeasures, Data Protection in the Cloud, Cloud Security as a Service, Protection in General-Purpose Operating Systems, Protected Objects and Methods of Protection, Memory and Address Protection, Control of Access to General Objects, File Protection Mechanisms, User Authentication, Linux's Security Model, The Linux DAC in Depth: Filesystem Security, Linux Vulnerabilities, Linux System Hardening, Application Security, Mandatory Access Controls, Windows Security Architecture, Windows Vulnerabilities, Windows Security Defenses, Browser Defenses, Cryptographic Services, Common Criteria, Mobile OS (Android & iOS; both Unix derivative)

Reference Books:

Operating System Security by Trent Jaegar, Ravi Sandhu

Vulnerability Assessment and Penetration Testing

Vulnerability analysis & Penetration testing, Vulnerability Classification, Frameworks, Offensive and defensive measures – OS, DB, Network (wired & wireless), Web Apps (owasp top 10, sans 25), Web Server, Infrastructure (Mail, AD, database, proxy, erp), Web client side, Thick clients – web / nonweb, Mobile – android, ios, windows, (owasp mobile top 10), Firewalls, IDS /IPS, Routers, Vulnerability, threat, exploit, Malware, Payload, Fuzz testing, Critical infrastructure

Reference Books:

1. Penetration Testing by Georgia Weidman
2. Mobile Application Penetration Testing by Vijay Kumar Velu
   Kali Linux Web Penetration Testing Cookbook by Gilberto Najera-Gutierrez

Malware and Reverse Engineering

Reverse engineering, File System, Registry, Process, Memory and Networking, File Format- Portable Executable (PE), Debuggers- OllyDbg, IDA Pro, Monitoring Tools, Reverse Engineering Tools, Malware Categories, Malware Analysis

Reference Books:

1. Practical Malware Analysis- Hands on Guide to Dissecting Malicious Software by Michael Sikorski
2. Android Malware Analysis by Ken Dunham

Cyber Forensics

Introduction to Cyber Forensics, Introduction to Cyber Crime Investigation, Imaging, Data Acquisition, Types of Evidence, Types of Cases, Storage Devices, File systems, Windows forensics, Linux forensics, Network analysis – Local area, network devices, hardware forensics, mobile forensics, steganography

Reference Books:

1. macintosh-forensic-analysis-os-26_SANS
2. facebook_forensics-finalized_fbiic.gov
3. Investigations Involving the Internet and Computer Networks, by National Institute of Justice, U.S. Department of Justice

Governance, Risk and Compliance

Security Policy, enforcement; Security standards, ISO 27001 standard, ISMS and PDCA. Aproach; ISO 27013 changes; Security controls, implementation; patch control issues, measurement of controls; automated approaches; security auditing; Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy, IT Security Management, Organizational Context and Security Policy, Security Risk Assessment, Detailed Security Risk Analysis, IT Security Management Implementation, Security Controls or Safeguards, IT Security Plan, Implementation of Controls, Monitoring Risks, Security Policies & their goal, The Role of Trust, Confidentiality Policies (Bell-LaPadula Model), Integrity Policies (Biba & Clark-Wilson), Hybrid Policies (Chinese wall model), Other Formal Models for Computer Security, The Concept of Trusted Systems, Application of Multilevel Security, Trusted Computing and the Trusted Platform Module, Common Criteria for Information Technology Security Evaluation, Assurance and Evaluation, Security Auditing Architecture, The Security

Audit Trail, Implementing the Logging Function, Audit Trail Analysis, Example: An Integrated Approach, The Economics of Cyber security , Making a Business Case, Quantifying Security, Modeling Cybersecurity

Reference Books:

1. NIST Special Publication 800-39 Managing Information Security Risk
2. Managing Information Security Risk_nistspecialpublication800-39
3. Guide for Conducting Risk Assessments_nistspecialpublication800-30r1

Mobile Security

Android vulnerability and security, iOS vulnerability and security, Windows vulnerability and security, Mobile application security, mobile communication security, mobile infrastructure, architecture and security

Reference Books:

1. Android Forensics by Andrew Hoog
2. Mobile Security and Privacy by Man Ho Au and Kim-Kwang Raymond Choo