

Certification Scheme in Information Security

Course Structure for Level2

Certified System Security Professional

S.No	Code	Paper	Theory(Hours)	Practical(Hours)
1.	IS-C2-01	Cryptography and Network Security	60	60
2.	IS-C2-02	System and Device Security	60	60
3.	IS-C2-03	Mobile and Wireless Security	60	60
4.	IS-C2-04	Database and Web Application Security	60	60

Cryptography and Network Security

IS-C2-01

1. Introduction - 02 hours
2. Classical Encryption Techniques - 04 hours
3. Mathematics Fundamentals associated with cryptography - 06 hours
4. Symmetric ciphers - 08 hours
5. Asymmetric ciphers - 10 hours
6. Internet Security Protocols - 08 hours
7. User Authentication and Kerberos - 06 hours
8. Electronic Mail Security - 04 hours
9. IP Security - 06 hours
10. Firewalls and Virtual Private Networks (VPN) - 06 hours

Introduction - **02 hours**

Active attacks, passive attacks, confidentiality, integrity, availability, more repudiation, plain text, encryption algorithm, secret key, decryption algorithm, cryptanalysis, brute force attacks.

Classical Encryption Techniques - **04 hours**

Substitution Techniques, Transposition Techniques, Rotor machine, steganography key range and key size.

Mathematics Fundamentals associated with cryptography - **06 hours**

Groups, Rings, Fields, Prime numbers, Euclid's Algorithm, Modular Arithmetic and Discrete logarithms, Finite Fields, Poly nominal arithmetic. Fermat's Theorem Euler's Theorem, Chinese Remainder Testing for Primality Quadratic Residues, Legendr Symbol, Jacobi Symbol Hasse's Theorem, Quadratic Reciprocity Theorem, Masseyomura protocol, Inverse of a matrix.

Symmetric ciphers - **08 hours**

Block cipher principles, DES, Strength of DES, Differential and Linear crypt a analysis, Block cipher Design principles, International Data Encryption algorithm (IDEA), Steam cipher RC4, RC5, Blowfish, AES Evaluation criteria for AES, Triple DES, Traffic confidentiality key distribution, Random number generation

Asymmetric chippers - **10 hours**

Brief history, overview, RSA algorithm, Key management, Diffie-Hellman key exchange, Elliptic curve cryptography, Difference between Asymmetric and Symmetric ciphers. Authentication message, Authentication codes, Hash functions, Security of Hash functions and MAC, Hash Algorithm Whirlpool, HMAC, CMAC. Digital Signature, Authentication protocols, Digital signature standard, Public-key Infrastructure, Models of PKI, Digital certifications private key management.

Internet Security Protocols - **08 hours**

Introduction, secure socket layer, Transport Security Layer (TLS), Secure Hyper Text Transfer Protocol (SHTTP), Time Stamping Protocol (TSP), Secure Electronic Transaction (SET), SSL Versus SET, 3D Secure Protocol, Electronic Money.

User Authentication and Kerberos - **06 hours**

Introduction, Authentication Basics, Passwords, Authentication, Biometric Authentication, Kerberos, Key Distribution Centre (KDC), Security Handshake Default, Single Sign (SSO) Approached .

Electronic Mail Security - **04 hours**

Introduction, E-mail headers and Body Proxy SPTP, Pretty Good Privacy (PGP), S/MIME.

IP Security - **06 hours**

IP Security overview, IP Security Architecture, Authentication Header, Encapsulating Security payload (ESP), Combining Security Associations, Key Management .

Firewalls and Virtual Private Networks (VPN) - **06 hours**

Firewalls, Firewall Design Principles, Virtual Private Network (VPN), Intrusion

SYSTEM AND DEVICE SECURITY

IS-C2-02

Lecture Hours: 60 Hours

Practical Hours: 60Hours

Outline of the Syllabus

Sr.no	Topic	Minimum no. of hours
Part I (Operating System Threat)		
1.	Program Security	2
2.	Fascination of Malicious Code Analysis	4
3.	Malicious Code Environment	4
4.	Classification of Infection Strategies	3
5.	Strategies of Computer Worm	3
Part II (Securing OS from Threats)		
6.	Antivirus Techniques	4
7.	Advanced Antivirus Techniques	6
8.	Case Studies	4
Part III (Device Security)		
9.	Introduction to Network Infrastructure Security	4
10.	Switch Security	2
11.	Router Security	4
12.	DNS Security	4
13.	ADSL Security	5
14.	Cable Modem Security	5
15.	Protecting Network Infrastructure- A new approach	6

Detailed Syllabus

Part-I (Operating System Threats)

- 1. Program Security** **02 hours**
Secure Program, Virus and other Malicious code, targeted malicious code,

Control against Program threats

2. **Fascination of Malicious Code Analysis** **04Hours**
Common pattern of virus research, antivirus defense development, terminology of malicious program, Computer malware naming scheme
3. **Malicious Code Environment** **04Hours**
Computer architecture dependency, CPU dependency, OS dependency, File system and file format dependency, Network protocol dependency
4. **Classification of Infection Strategies** **03Hours**
Boot Viruses, File infection techniques, In depth look at WIN32 Viruses
5. **Strategies of Computer Worm** **03Hours**
Generic structure of computer worms, Common worms code transfer and execution techniques

Part-II (Securing OS from threats)

6. **Antivirus Techniques** **04Hours**
Detection: Static Methods, Scanners, Static Heuristics, Integrity Checkers, Dynamic Methods, Behavior Monitors/Blockers, Emulation, Comparison of antivirus techniques
7. **Advanced antivirus techniques** **06Hours**
Retroviruses, Entry point obfuscation, Anti-Emulation (outlast, outsmart, overextent) Armoring (Anti-Debugging, Anti-bisassembly), Tunneling (Integrity checkers attacks), Avoidance, Deworming, defense (User, host, perimeter), capture and containment (Honey pots, Reverse Firewalls, Throtting), Automatic Counter measures
8. **Case Studies** **04Hours**
Linux/Unix Security Details, Trusted Operating Systems

Part-III (Device Security)

9. **Introduction to Network infrastructure security** **04Hours**
Internet infrastructure, key components in the internet infrastructure, internet infrastructure security
10. **Switch Security** **02Hours**
Introduction, How switches can be attacked

- 11. Router security** **04Hours**
Over view of Internet routing, External and internal attacks, RIP attacks and countermeasures, OSPF attacks and countermeasures, BGP Attacks and countermeasures
- 12. DNS Security** **04Hours**
Introduction, DHCP attacks, DNS attacks
- 13. ADSL Security** **05Hours**
Introduction, DSL family tree, ADSL, ADSL benefits, security threats, countermeasures, topologies with ADSL models, Topologies with ADSL routers, recommended topologies, using routers as a firewall, limitations, Features Risk, precautionary Measures.
- 14. Cable Modem security** **05Hours**
Working of cable Modem, Cable Modem security threats, different filtering techniques, DHCP server filter, Microsoft networking filter, Network isolation filter, static IP address filter, MAC address filter, comparing DSL and cable Modem security threats.
- 15. Protecting Network Infrastructure- A new Approach** **06Hours**
Analysis on security problems of network infrastructure, steps in hacking network infrastructure, Flat network design model and Masquerading, A new Model to protect network infrastructure.

IS-C2-03: Mobile and Wireless Network Security

Lecture Hours: 60 Hours

Practical Hours: 60Hours

Outline of the Syllabus

Sr.no	Topic	Minimum no. Of hours
--------------	--------------	-----------------------------

Part I (Wireless Technology)

- | | | |
|----|--|---|
| 1. | Wireless Fundamentals | 2 |
| 2. | Wireless Network Logical Architecture | 4 |
| 3. | Wireless Network Physical Architecture | 4 |
| 4. | Wireless LAN Standard | 4 |

Part II (Security for Mobility)

- | | | |
|-----|---|---|
| 5. | PKI in Mobile Systems | 2 |
| 6. | Personal PKI | 2 |
| 7. | Smartcard as a Mobile Security Device | 2 |
| 8. | Secure Mobile Tokens-The Future | 2 |
| 9. | Universal Mobile Telecommunications System(UMTS) Security | 2 |
| 10. | Securing Network Access in Future Mobile System | 6 |
| 11. | Security Issues in a MobileIPV6 Network | 2 |
| 12. | Mobile Code Issues | 4 |
| 13. | Secure Mobile Commerce | 2 |

Part III (Wireless Network Security)

- | | | |
|-----|--|---|
| 14. | Security in Traditional Wireless Network | 2 |
| 15. | Wireless LAN Security | 2 |
| 16. | Security in Wireless Ad-hoc Network | 2 |
| 17. | Implementing Basic Wireless Security | 2 |
| 18. | Implementing Advanced Wireless Security | 2 |

Part IV (Other Wireless Technology)

19. Home Network Security	2
20. Wireless Embedded System Security	2
21. RFID Security	2
22. Security Issues in Single Hop Wireless Networks	2
23. Security Issues in Multi Hop Wireless Networks	4

Detailed Syllabus

Part-I (Wireless Technology)

- 1. Wireless Fundamentals** **2Hours**
Wireless Medium: Radio Propagation Effects, Exposed Terminal Problem, Bandwidth, Wireless Networking Basics: WLAN, working of WLAN, Current WLAN Standard
- 2. Wireless Networking Logical Architecture** **4Hours**
OSI Network Model, Network Layer Technologies, Data Link Layer Technologies, Operating System Consideration
- 3. Wireless Network Physical Architecture** **4Hours**
Wired Network Topologies, Wireless Network Topologies, Wireless LAN Devices, Wireless PAN Devices, Wireless MAN Devices
- 4. Wireless LAN Standard** **4Hours**
THE 802.11 WLAN Standards, 802.11 MAC Layer, 802.11 PHY Layer, 802.11 Enhancements, other WLAN Standard

Part-II (Security for Mobility)

- 5. PKI in Mobile Systems** **2Hours**
PKI overview, PKI in current Mobile Systems, PKI in Future Mobile System
- 6. Personal PKI** **2Hours**
Issues in Personal PKI, Personal PKI requirement, Personal CAs, Device Initialization, Proof of possession, Revocation in Personal PKIs
- 7. Smartcard as a Mobile Security Device** **2Hours**
Storage cards and Processor cards, Standardization data objects and commands, Smartcards and biometrics
- 8. Secure Mobile Tokens-The Future** **2Hours**
Security Modules, Current use of Security Modules, Security Module Technology, Current use of secure mobile tokens, Personal Security tokens

9. Universal Mobile Telecommunication System Security 2 Hours

Building a GSM Security, UMTS access security, Network Security, IP Multimedia Subsystem Security

10. Securing Network Access in Future Mobile System 6Hours

Outline of Security Architecture, Design alternatives for authentication and establishment of Security association, IP Layer Security, Link Layer Security, Network Security options

11. Security Issues in a Mobile IPV6 Network 2Hours

Introduction to Mobile IP, MobileIPV6 Security Mechanisms, AAA (authorization, authentication and accounting) requirements for Mobile IP

12. Mobile Code Issues 4Hours

Agent and Multi-agent Systems, Security Implication, Security Measures for Mobile Agents, Security Issues for Downloaded code in Mobile phones

13. Secure Mobile Commerce 2Hours

M-Commerce and its security challenges, Security of the radio interface, Security of m-commerce

Part-III (Wireless Network Security)

14. Security in Traditional Wireless Networks 2 Hours

Security in First Generation TWNs, Security in Second Generation TWNs, Security in 2.5 Generation TWNs, Security in 3G TWNs

15. Wireless LAN Security 2 Hours

Key Establishment, Anonymity, Authentication, Confidentiality, Data Integrity and Loopholes in 802.11

16. Security in Wireless Ad-hoc Network 2 Hours

Bluetooth: Basics, Security Modes, Key Establishment, Authentication, Confidentiality, Integrity Protection, Enhancements

17. Implementing Basic Wireless Security 2 Hours

Enabling Security Features on a Linksys WAP 11802.11b Access, Filtering by MAC Address, Enabling Security Features on a Linksys WRT54G 802.11b/g, Configuring Security Features on Wireless Clients

18. Implementing Advanced Wireless Security 2 Hours

Implementing WiFi Protected Access (WPA), Implementing a Wireless Gateway with Reef Edge, Implementing a VPN on a Linksys WRV54G VPN Broadband

Part-IV (Other Wireless Technology)

19. Home Network Security

2 Hours

Basics of Wireless Security, Basics of Wireless Security Measures, Additional Hotspot Security Measures

20. Wireless Embedded System Security

2 Hours

Wireless Technologies, Bluetooth, ZigBee, Wireless Technologies and the Future

21. RFID Security

2 Hours

Introduction, RFID Radio Basics, RFID Architecture, Threat and Target Identification, Management of RFID Security

22. Security Issues in Single Hop Wireless Networks

2 Hours

Cellular Network Security , Access Control and Roaming Issues, Mobile IP Security, Pervasive Computing Security

23. Security Issues in Multihop Wireless Networks

4 Hours

Mobile Adhoc Network Security, Trust Management and Routing Issues, Wireless Sensor Network Security, Key Management, Sybil Attacks and Location Privacy, Vehicular Network Applications and Security, Wireless Metropolitan Area Networks(e.g. 802.11b)

Database and Web Applications Security
IS-C2-04

Database Security

30 hours

11.	Integrity	-	06 hours
12.	Access Control	-	08 hours
13.	Database Auditing	-	06 hours
14.	Network Access and Requirements	-	06 hours
15.	Operating System	-	02 hours

Web Applications Security

30 hours

16.	Fundamental of Web Application Security	-	02 hours
17.	Core Defense Mechanisms	-	02 hours
18.	Web Application Technologies	-	03 hours
19.	Client-side Exploit Frame Work	-	03 hours
20.	Bypassing Client-side Controls	-	02 hours
21.	Web Based Malware	-	02 hours
22.	Securing Authentication	-	03 hours
23.	Securing Session Management	-	02 hours
24.	Securing Access Controls	-	02 hours
25.	Securing Application Architecture	-	03 hours
26.	Web Server and Web Application Testing with Back Track	-	03 hours
27.	Securing Web Based Services	-	05 hours

Database Security

1. Integrity - 06 hours

Software Integrity

Current DBMS Version, DBMS Software/Object Modification, Unused Database Software/Components

Database Software Development

Shared Production/Development Systems

Ad Hoc Queries

Multiple Services Host Systems

Data Integrity

Database File Integrity, Database Software Baseline, Database File Backup and Recovery

2. Access Control - 08 hours

Database Account Controls

Authentication

Password Guidelines, Certificate Guidelines

Database Accounts

Administrative Database Accounts, Application Object Ownership/Schema Account, Default Application Accounts, Application Non-interactive/Automated Processing Accounts, N-Tier Application Connection Accounts, Application User Database Accounts

Database Authorizations

Database Object Access, Database Roles, Application Developer Roles, Application Administrator Roles, Application User Database Roles

Protection of Sensitive Data

Protection of Stored Applications

Protection of Database Files

3. Database Auditing - 06 hours

Precautions to Auditing

Audit Data Requirements

Minimum Required Audit Operations, DBA Auditing, Required Audit Operations on Audit Data

Audit Data Backup

Audit Data Reviews

Audit Data Access

Database Monitoring

4. Network Access and Requirements - 06 hours

Protection of Database Identification Parameters

Network Connections to the Database

Remote Administrative Database Access, Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), Web Server or Middle-Tier Connections to Databases, Database Session Inactivity Time Out

Database Replication

Database Links

- 5. Operating System - 02 hours**
- Database File Access
 - Local Database Accounts
 - Database Administration Accounts
 - Database OS Groups

Web Applications Security

- 6. Fundamental of Web Application Security - 02 hours**

The core security problem, Key problem factors, immature security awareness, Deceptive Simplicity, Resource and Time constraints, Overextended Technologies, The new security perimeter, The future of Web Application Security.

- 7. Core Defense Mechanisms - 02 hours**

Handling user Access, Handling user input, boundary validation, multistep validation and canonicalization, handling errors, Maintaining Audit logs, Altering Administrators, Reacting to attacks, Managing the application.

- 8. Web Application Technologies - 03 hours**

The HTTP Protocol, HTTP Headers, Cookies, Status codes, Web Functionality, Server-side Functionality, Client-side Functionality, State and Sessions, Encoding scheme (URL Encoding, Unicode Encoding, HTML Encoding, Base 64 Encoding, Hex Encoding).

- 9. Client-side Exploit Frame Work - 03 hours**

Attack API, BeEF (Installing, configuring and controlling), CAL 9000, overview of XSS-proxy, using XSS-proxy.

- 10. Bypassing Client-side Controls - 02 hours**

Transmitting Data via the client, Capturing user Data: HTML forms, Capturing user Data: Thick-client components, ActiveX Controls, Shockwave Flash objects, handling client-side data securely.

- 11. Web Based Malware - 02 hours**

Attacks on Web, Hacking into Web sites, Index Hijacking, DNS poisoning, Malware and the Web, Parsing and Emulating HTML, Browser vulnerabilities, Testing HTTP.

12. Securing Authentication - 03 hours

Authentication Technologies, Design Flows in Authentication Mechanisms, Implementing Flows in Authentication, Securing Authentication, Strong credentials, handle credentials secretively, validate credentials properly, Prevent information leakage, prevent Brute-Force Attacks, log, monitor and notify.

13. Securing Session Management - 02 hours

Weakness in Session Token Generation, Weakness in Session Token Handling, Securing Session Management, Generate strong Tokens, log, Monitor and Alert.

14. Securing Access Controls - 02 hours

Common vulnerabilities, Attacking Access controls, Securing Access Controls, A multi-layered Privilege Model.

15. Securing Application Architecture - 03 hours

Tiered Architecture, Attacking tiered Architecture, Securing Tiered Architecture, Virtual Hosting, Shared Application services, Attacking shared Environments, Securing Shared Environment, Secure Customer Access, Segregate customer Functionality, Segregate components in a shared Application.

16. Web Server and Web Application Testing with Back Track - 03 hours

Introduction, Web Server Testing, CGI and Default Pages Testing, Web Application Testing, Core technologies, Open Source Tools, Scanning Tools, Assessment Tools, Exploitation Tools.

17. Securing Web Based Services - 05 hours

Web Server Lockdown, Handling Directory and Data Structures, Eliminating Scripting vulnerabilities, Logging Activity, Stopping Browser Exploits, SSL and HTTP/S, Instant Messaging, Web Based Vulnerabilities, Making Browsers and E-mail client more secure, FTP Security, Directory Services and LDAP Security, Web Application Assessments, Source Code and Binary Analysis, Application threat modeling and Architectural Analysis, Web Services and Active X Analysis, Compliance Assessments for Visa CISP, Mastercard SDP, GLBA, SOX, Web Server Security, Operating system specific Security, Permissions and Scripting, HTAccess prevention measures, Cross Site scripting, Cross Site request forgery, User Authentication Session management.