POST GRADUATE DIPLOMA IN CYBER SECURITY AND LAW(PGDCSL)

PREAMBLE

Cyber-security is a niche subject of modern studies wherein this diploma is an advanced Penetration Testing & Information Security Program. The course provides intensive practical sessions to prepare an individual with uncompromising practical knowledge in a simplified and easily graspable manner.

SESSION DURATION

	SEMESTER 1	**SEMESTER 2**
Course	15 weeks	15 weeks
Project	4 weeks	8 weeks
Exams	1	1
Total Academic course duration - 42 weeks excluding examination		

COURSE CONTENT

Semester I	**Semester II**
● Fundamentals of Computer Security ● Networking Basics and Network Security ● Fundamentals of Web Designing and Web Application Security ● Cryptography ● Cloud Fundamentals and Cloud Security ● Project 1	● Mobile Eco System Security ● Internet of Things Security (IoT) ● Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques ● Cyber Laws and Forensics ● Information Security Compliance Management ● Project 2

EXAMINATION PATTERN: (40 Theory 40 Practical and 20 Internal Assessments)

EXAM: Diploma Certificate will be issued to participants only after clearing final examination of both the semesters conducted the end of the final semester. The span period of the course will be as per the University Policy.

EXAM DURATION: As per guidelines issued by University of Delhi.

DURATION OF COURSE: 1 year.

SPAN OF COURSE: 2 years.

DELIVERABLES: Each student will get:

- A toolkit containing tools as required in the curriculum
- Videos for referrals case studies and White papers
- Subject Wise E- Tutorials

The schedule of papers prescribed for two semesters shall be as follows:

Semester I

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Written Exam
1	Fundamentals of Computer Security	60 lectures	100	20	40	40
2	Networking Basics and Network Security	60 lectures	100	20	40	40
3	Fundamentals of Web Designing and Web Application Security	60 lectures	100	20	40	40
4	Cryptography	60 lectures	100	20	40	40
5	Cloud Fundamentals and Cloud Security	60 lectures	100	20	40	40
6	Project 1	4 weeks	100			

Semester II

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Written Exam
1	Mobile Eco System Security	60 lectures	100	20	40	40
2	Internet of Things Security	60 lectures	100	20	40	40
3	Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques	60 lectures	100	20	40	40
4	Cyber Law & Forensics	60 lectures	100	20	40	40
5	Information Security Compliance Management	60 lectures	100	20	40	40
6	Project 2 + Internship	8 weeks	100			

Note: Each lecture will be of 60 minutes duration.

SCHEME OF EXAMINATIONS

English shall be the medium of instruction and examination.

1. Examinations shall be conducted at the end of each Semester as per the Academic Calendar notified by the University of Delhi
2. The system of evaluation shall be as follows:
   2.1. Each paper will carry 100 marks, of which 20 marks shall be for internal assessment based on a combination of classroom participation, project work, seminar, term papers, tests, and attendance. The weightage given to each of these components in a combination shall be decided and announced at the beginning of the semester in consultation with the faculty of the concerned paper. The system so decided will be communicated by the Institute for Cyber Security and Laws.
   2.2. The remaining 80 marks in each paper shall be awarded on the basis of a practical and written examination of 40 marks each at the end of each semester.

PASS PERCENTAGE & PROMOTION CRITERIA

1. The minimum marks required to pass any paper in a semester shall be 50% in each paper and 50% in aggregate of a semester.
2. **Semester to Semester Promotion:** Students shall be required to fulfil the Part to Partpromotion criteria. Students shall be allowed to be promoted from semester I to semester II, provided s/he has passed at least 60 per cent of the papers in the course of the current semester including project.

DIVISION CRITERIA

Successful candidates will be classified on the basis of the combined results of Semester -I and Semester -II examinations as follows:

- Candidates securing **60% and above**: I Division
- Candidates securing **50% or more but less than 60%**: II Division

ATTENDANCE REQUIREMENT

Attendance in lectures, tutorials, seminars etc. arranged by the Centre for Cyber Security and Laws from time to time, is mandatory according to the Internal Assessment requirement as per University rules. The marks for attendance shall be awarded on the basis of existing norms as per the Internal Assessment Scheme of University of Delhi.

Semester - 1
Paper 101: Fundamentals of Computer Security

Marks: 100 **Lectures 60**

Objective: This course will be responsible to lay the foundation for creating comprehensive understanding in the field of cyber security. With a view that incumbents in this diploma course are from varied disciplines, this paper will set the level field for all the students to be able to come at par and move together as they must go deeper into hard-core cyber security topics during the course duration.

Unit I: Computers and Cyber Security

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Linux/Mac Terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT, Smartphone Operating systems, introduction to compliances ,Globalization and border less world.

Unit II: Python Scripting and PHP Basics

Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages.

Unit III: Cyber Laws

Need for Cyber Regulations; Scope and Significance of Cyber laws : Information Technology Act 2000; Network and Network Security, Access and Unauthorised Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Unit IV: Encoding

Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes and Binary Reedmuller codes.

Unit V: Web Application Architecture

HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache, Virtualisation, Server Configurations, Web Application Firewalls..

Suggested Readings:

1. Langtangen, H.P. (2012). *Python Scripting for Computational Science* (4th Ed.). Springer
2. Behrouz A. Forouzan (2004). *Data communication and Networking*. Tata McGraw-Hill.
3. Kurose, James F. & Ross, Keith W. (2003). *Computer Networking: A Top-Down Approach Featuring the Internet* (3rd Ed.). Pearson Education.
4. Shklar, L. & Rosen, R. (2009). *Web Application Architecture: Principles, Protocols and Practices* (2nd Ed.). John Wiley & Sons.
5. Craig, B. (2012). *Cyber Law: The Law of the Internet and Information Technology*. Pearson.
6. Sharma J. P. & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt Ltd.
7. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.
8. Forbes, A. (2015). *The Joy of PHP: A Beginner's Guide to Programming Interactive Web Applications with PHP and mySQL* (4th Ed.). Plum Island Publishing LLC.
9. Shema, M. (2012). *Hacking Web Apps: Detecting and Preventing Web Application Security Problems.*
10. Peterson. W.W, (1972), *Error Correcting Codes,* MIT Press
11. Hill. R, (1980), *A First Course in Coding Theory,* Oxford University Press.
12. Macwilliams F J and Sloane N J A, (2013), *Theory of Error Correcting Codes*, North Holland Elsevier Science Ltd

Semester - 1
Paper 102: Network Basics and Network Security

Marks: 100 **Lectures 60**

Objective: This course aims at teaching students about the fundamentals and distinctions of network building along with setup of present day networks in complex environments. The networks today are vulnerable to various attacks and the course aims at acquainting students with the techniques used by hackers for network attacks and also the techniques adopted in order to guard the entire infrastructure against varied attacks.

Unit I: Introduction to Network Security

Types of networks, IP Address, NAT , IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers , Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS,IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).

Unit II: Virtual Private Networks

VPN and its types –Tunneling Protocols – Tunnel and Transport Mode –Authentication Header-Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation(GRE). Implementation of VPNs.

Unit III: Network Attacks Part 1

Network Sniffing, Wireshark, packet analysis, display and capture filters, ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta,Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting,

Unit IV: Network Attacks Part 2

Network Exploitation OS Detection in network, nmap, open ports, filtered ports, service detection, metasploit framework, interface of metasploit framework, network vulnerability assessment, Evade anti viruses and firewalls, metasploit scripting, exploits, vulnerabilities,

payloads, custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploits delivery. End Point Security.

Unit V: Wireless Attacks

Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP , WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

Suggested Readings:

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security, Private communication in public world* (2nd Ed.). PHI
2. Monte, M. (2015). *Network Attacks and Exploitation: A Framework*. Wiley.
3. Perez, Andre. (2014). *Network Security*. Wiley.
4. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (5th Ed.). Prentice Hall

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1

Paper 103: Fundamentals of Web Designing and Web Application Security

Marks: 100 **Lectures 60**

Objective: Moving from networks the most important component any technology stack is the software which is positioned at the top of infrastructure. We will start with the necessities of how software applications are built, where students will understand and build their applications to have the real world feel on how the internet stack is working, along with showing them real loopholes while coding himself so that they understand the real world attacks which are possible on applications, and simulate them so that they can themselves come to conclusions and understand the best practices involved in application security.

Unit I: Web Designing and Penetration Testing Process

Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis.

PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering

HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit III: Web Application Attacks Part I: SQL Injections & Cross Site Scripting

SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation. Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation.

Unit IV: Web Application Attacks Part II

Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

Practical: This paper will have 30 lectures for the practical work.

Suggested Readings:

1. Shema, M. & Adam. (2010). *Seven deadliest web application attacks*. Amsterdam: Syngress Media.

2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed). Indianapolis, IN: Wiley, John & Sons.

3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). *Web application obfuscation*. Amsterdam: Syngress Media,U.S.

4. Sullivan, Bryan (2012). *Web Application Security, A Beginner's Guide*. McGraw- Hill Education.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 104: Cryptography

Marks: 100 **Lectures 60**

Objective: After infrastructure and software, the communication in between multiple devices using applications and securing them become most important, cryptography is the mechanism using which we hide the information in public eye site from anybody and is something which is used very popularly almost anything across the internet. So we start with fundamentals of what is cryptography and how cryptography algorithms work and then come to real world scenarios on how currently our data processed on the internet is secured from the eyes of an intruder. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

Unit I: - Classical Ciphers

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher.
Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit II: Secret Key Cryptography

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography and Bitcoins

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.
Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit IV: Message authentication code and Hash Functions

Message authentication code Authentication functions, Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

Suggested Readings:

1. Delfs, H. & Knebl, H. (2001). *Introduction to Cryptography: Principles and Applications*. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). *The Handbook of Applied Cryptography*. CRC Press.

4. Schneier, B. (1995). *Applied cryptography, Protocols, algorithms and source code in C* (2nd ed.). New York: John Wiley & Sons.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 105: Cloud Fundamentals and Cloud Security

Marks: 100 **Lectures 60**

Objective: The purpose of the course is to make students understand and comprehend the revolutionizing concept of CLOUD in the cyber world with a view to enable them with achieving cloud security. It also aims at developing expertise amongst students with the cloud architecture as well as the security concerns for organizations planning a move towards Cloud or planning to enhance their cloud security.

Unit I: Introduction to Cloud Computing
Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vsprivateclouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit II: Cloud Application Architecture
Technologies and the processes required when deploying web services; Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.

Unit III: Cloud Services Management
Reliability, availability and security of services deployed from the cloud.
Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Unit IV: Cloud Application Development
Service creation environments to develop cloud based applications. Development environments for service development; Amazon, Azure, Google App.Applicability of laws to data stored outside the nation's boundary.

Unit V: Cloud IT Model
Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO)

Suggested Readings:

1. Rittinghouse, J.W. & Ransome, J.F. (2010). *Cloud Computing: Implementation, Management, and Security*. CRC Press.

2. Rountree, D. & Castrillo, I. (2013). *The Basics Of Cloud Computing: Understanding The Fundamentals Of Cloud Computing In Theory And Practice*. Syngress, Elsevier

3. Stallings (2016). *Cryptography & Network Security*. Paperback.

4. Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges*. CRC Press

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 106: Project - 1

Marks: 100 Duration: 4 Weeks

Rules for the Project:

- The students would develop their project individually and get the topic approved by the head/ director of the centre. For the purpose of approval, they have to submit their project titles and proposals with the name of internal or external guides to the head/ director of the centre within forty five days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal, is required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject.

- The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover they have to submit the progress reports with the final project report at the time of external examination.

- The external examiners appointed by the head/ director of the Institute shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and out of 40 on the basis of Project Report. The internal guide shall award out of 40 Marks.

Semester 2
Paper 201: Mobile Eco- System Security

Marks: 100 **Lectures 60**

Objective: At time when companies are looking at not only a mobile first approach but a mobile only approach, the cell phone revolution has hit both the enterprise and the consumer market in a massive way. Its entire eco system needs to be very carefully understood , and the various attacks which can be possible at each stage needs to be carefully, practically performed in order to understanding how to protect the entire mobility ecosystem, which is going to be one of the most important pillars of transforming an organisation into a digital organisation.

Unit I: Introduction to Mobile Eco-System Security
Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile Eco-System Technology
Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery

Unit III: Mobile Eco-System Networks
Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS , Web Technologies - server-side and client side web applications

Unit IV: Management
Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools

Unit V: Scenario Testing
Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS

Suggested Readings:

1. Fried, S. (2010). *Mobile device security: A comprehensive guide to securing your information in a moving world*. Boca Raton, FL: Auerbach Publications.
2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed.). Indianapolis, IN: Wiley, John & Sons.
3. Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile application security*. New York: McGraw-Hill Companies.

Semester 2
Paper 202: Internet of Things Security (IoT)

Marks: 100 **Lectures 60**

Objective: The human race is going to go through a major transformation in the next ten years thanks to the internet of thing , when such a transformation happens, where internet and technology are going to touch possibly every aspect of our life , the security of the same would be of highest importance , here we will dwell with most popular IoT devices available in the market at present and their security concerns along with potential hacks that can be performed on such devices and to ensure its security according to best global practices.

Unit I: Introduction
Requirement and Basic Properties in Internet of Things, Primary challenges in security maintenance, Confidentiality, Integrity, Availability, Non-Repudiation.

Unit II: Architecture of Internet of Things
Device - device, Device - Cloud, Device - Gateway, Gateway - Cloud, Cloud – Backend - Applications

Unit III: Security Classification and Access Control
Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity

Unit IV: Attacks and Implementation of Internet of Things
Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices

Unit V: Security Protocols and Management
Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management

Suggested Readings:

1. Russell, B. (2016). *Practical Internet of Things Security***.** Packt Publishing Limited
2. FeiHu (2016). *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations***.** CRC Press
3. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley
4. Pfister, C. (2011). *Getting Started with the Internet of Things*. Shroff Publisher.

Semester 2

Paper 203: Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques

Marks: 100 **Lectures 60**

Objective: What Internet of things would be to consumers, SCADA and Industrial control systems would be to enterprises, the heavy machinery that we have been thinking of its intelligent management is going to be completely taken over by the technology. Although it looks like a great boon however if take over, we have seen in the past some of the national critical infrastructures of some very developed countries being compromised and the damages happening which are irreversible hence it becomes most important to understand the cyber risks that such technologies posses and to give the education of the best practices followed for securing such technologies.

Unit I: Introduction

Network Segmentation and Segregation , Boundary Protection, Firewalls , Logically Separated Control Network , Network Segregation, Recommended Defence-in-Depth Architecture, General Firewall Policies for ICS , Recommended Firewall Rules for Specific Services , Network Address Translation (NAT), Specific ICS Firewall Issues , Unidirectional Gateways , Single Points of Failure , Redundancy and Fault Tolerance , Preventing Man-in-the-Middle Attacks , Authentication and Authorization , Monitoring, Logging, and Auditing, Monitoring, Logging, and Auditing , Response, and System Recovery

Unit II: Network Segregation

Dual-Homed Computer/Dual Network Interface Cards (NIC) , Firewall between Corporate Network and Control Network , Firewall and Router between Corporate Network and Control Network , Firewall with DMZ between Corporate Network and Control Network , Paired Firewalls between Corporate Network and Control Network , Network Segregation Summary

Unit III: Recommended Firewall Rules for Specific Services

Domain Name System (DNS) , Hypertext Transfer Protocol (HTTP) ,FTP and Trivial File Transfer Protocol (TFTP) ,Telnet ,Dynamic Host Configuration Protocol (DHCP) , Secure Shell (SSH) ,Simple Object Access Protocol (SOAP) , Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) ,Distributed Component Object Model (DCOM),SCADA and Industrial Protocols: DNP3 Protocol. Smart Grid Security.

Unit IV Information Hiding Techniques

Introduction to Steganography, Watermarking. Differences between Watermarking and Steganography, A Brief History. Digital Steganography, Applications of Steganography, Covert Communication, Techniques of steganography(for Text and Image) . Steganographic Software: S-Tools, StegoDos, EzStego, Jsteg-Jpeg.

Unit V : Digital Water Marking

Classification in Digital Watermarking, Classification Based on Characteristics: Blind versus Nonblind, Perceptible versus Imperceptible, Private versus Public, Robust versus Fragile, Spatial Domain-Based versus Frequency Domain-Based. Classification Based on Applications: Copyright Protection Watermarks, Data Authentication Watermarks, Fingerprint Watermarks, Copy Control Watermarks, Device Control Watermarks. Watermarking Techniques for Visible and Invisible Watermarks. Watermarking tools: uMark, TSR Watermark. Steganalysis

Suggested Readings

1. Macaulay, T. & Singer, B. (2016). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL: CRC Press.

2. Langner, R. (2011). *Robust control system networks: How to achieve reliable control after Stuxnet*. New York: Momentum Press.

3. Knapp, E.D. & Langill, J.T. (2011). Industrial network security: Securing critical infrastructure networks for smart grid, SCADA , and other industrial control systems. Waltham, MA: Syngress Media, U.S.

4. Katzenbeisser, S. & Fabien A P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Petitcolas, Artech House.

5. Cox, I., Miller, M., Bloom, J., Fridrich, J. & Kalker, T. (2007). *Digital Watermarking and Steganography* (2nd Ed.). Elsevier.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester 2
Paper 204: Cyber Law and Forensic Evidence

Marks: 100 **Lectures 60**

Objective: The paper aims to create the basic clarity and understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. The paper would address and emphasise on the activities leading to infringement of individual or organisational privacy. Further, the paper intends to create highly sensitised professionals who can be responsible for handling the cyber security issues pertaining to varied domains and dealing in forensics diligently.

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law
The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit II: Regulatory Framework of Information and Technology Act 2000
Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal.(Rules announced under the Act)

Unit III: **Offences and Penalties**
Offences under the Information and Technology Act 2000, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed).Limitations of Cyber Law.

Unit IV: Fundamentals of Cyber Forensics
Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery

Unit V: Data Recovery Tools, Data Recovery Procedures and Ethics
Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files,

Introduction to Encase Forensic Edition, Forensic Toolkit etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Unit VI: Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems , Hashcat. Work on open Source, Commercial tools and Cyber range.

Suggested readings

1. Craig, B. *Cyber Law: The Law of the Internet and Information Technology.* Pearson Education

2. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.

3. Lindsay, D. (2007). *International domain name law: ICANN and the UDRP*. Oxford: Hart Publishing.

4. Sharma J. P, & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt. Ltd.

5. Duggal, P. *Cyber Laws*. (2016) Universal Law Publishing.

6. Kamath, N. (2004). *Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.)*. Delhi: Universal Law Publishing Co.

7. Stephenson, P.R. & Gilbert, K. *Investigating computer- related crime a handbook for corporate investigators*. Boca Raton, FL: Taylor & Francis.

8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

Latest Editions of the Suggested Readings along with discussion material by the Faculty.

Semester 2
Paper 205: Information Security Compliance Management

Marks: 100 **Lectures 60**

Objective: In view of providingtechnical superiority essentially be complimented with the appropriate compliance advancement to maintain hygiene from the point of view of cyber security.Complianceshaveincreasinglycoming up not in just financial or aviation space but also in conventional industries like manufacturing, real estate among others and hence its of tremendous importance for a cyber-security professional to have comprehensive knowledge of the most important compliances and the modus operandi from people, process and technology to get through a compliance check.

Unit I: Introduction to Information Security Management System (ISMS) - ISO/IEC 27001
Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information security,ISO/IEC 27001 certification process,Information Security Management System (ISMS), detailed presentation of the clauses 4 to 8 of ISO/IEC 27001

Unit II: Planning and Initiating an ISO/IEC 27001 audit
Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting

Unit III: Conducting an ISO/IEC 27001 audit
Communication during the audit, Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities

Unit IV: Concluding and ensuring the follow-up of an ISO/IEC 27001 audit
Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans, ISO/IEC 27001 Surveillance audit, internal audit management program

Unit V: PCI DSS, HIPPA
Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from

Malicious Software, Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption

Unit VI Intellectual Property Rights

Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.

Suggested Readings:

1. Godbole, N. *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley

2. Calder, A. (2009*). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide* (2nd Ed.). Van Haren Publishing

3. Humphreys, E. (2007). *Implementing the ISO / IEC 27001 Information Security Management System Standard*. Artech House Publishers.

4. Watkins, S. G. (2013). *An Introduction to Information Security and ISO 27001: A Pocket Guide*. IT Governance Publishing.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Paper 206: Project - 2

Marks: 100 **Duration: 8 Weeks**

Rules for the Project:

- The students would develop their project individually and get the topic approved by the head/ director of the centre. For the purpose of approval, they have to submit their project titles and proposals with the name of internal or external guides to the head/ director of the centre within twenty one days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal, is required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject.

- The students have to report to the guide for at least five times during the project lifespan with the progress report duly signed by the internal guide. Moreover they have to submit the progress reports with the final project report at the time of external examination.

- The external examiners appointed by the head/ director of the Institute shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and out of 40 on the basis of Project Report. The internal guide shall award out of 40 Marks.

University of Delhi

Institute for Cyber Security and Law

Admission criteria

Qualifying examination for the purpose of Admission to the Post Graduate Diploma in Cyber Security and Law shall be graduates or above in Science (Physics & Chemistry), Information Technology, Mathematics, Engineering in Technology (Computer science/ Electronics/Electronics and Communication, Information Technology), BCA, MCA, M.Tech or any other degree equivalent thereto. The admissions shall be based on the merit drawn from the marks obtained in graduation and personal interview. The admission process shall be following:

STAGE I: The merit list, for admission shall be determined on the basis of marks obtained (CGPA equivalent thereto) by the candidate in graduation or in the degree applicable as qualifying examination.

STAGE II: The candidates shall be called for Personal Interview on the basis of merit drawn as prescribed in stage I.

Stage III: A combined merit on the basis of 85% from Stage I and 15 % from Stage II shall be drawn. Admissions shall be based in the order of combined merit.

Note: Candidates appearing in the final year examination of Bachelor's degree are eligible to apply. If selected, candidates will be eligible for admission only when they submit the result meeting the minimum eligibility criteria at the time of final admission, as per University Rules.