**Sona College of Technology (Autonomous), Salem – 636 005**
**Department of Computer Science and Engineering**
**Advanced Diploma in CYBER SECURITY**
**CURRICULUM & SYLLABI**
**Academic year – 2021-22**

**I Year / I Semester**

| S. No. | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | | Data Communication and Networking | 3 | 0 | 0 | 3 |
| 2. | | Introduction to Programming ('C' & Java) | 3 | 0 | 0 | 3 |
| 3. | | Principles of Cyber Security | 3 | 0 | 0 | 3 |
| 4. | | Networking Lab | 0 | 0 | 2 | 1 |
| | | | | | **Total Credits** | 10 |

**I Year / II Semester**

| S. No. | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | | Cyber Laws and Standards | 3 | 0 | 0 | 3 |
| 2. | | GRC management in Cyber Security | 3 | 0 | 0 | 3 |
| 3. | | Vulnerability assessment of IT infrastructure | 3 | 0 | 0 | 3 |
| 4. | | Vulnerability Testing Lab | 0 | 0 | 2 | 1 |
| | | | | | **Total Credits** | 10 |

**II Year / III Semester**

| S. No. | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | | Web technologies & Introduction to internet security | 3 | 0 | 0 | 3 |
| 2. | | Introduction to Cryptography and network security | 3 | 0 | 0 | 3 |
| 3. | | Ethical Hacking & Popular hacking cases | 3 | 0 | 0 | 3 |
| 4. | | Penetration testing Lab | 0 | 0 | 2 | 1 |
| | | | | | **Total Credits** | 10 |

**II Year / IV Semester**

| S. No. | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | | Introduction to Cyber Forensics | 3 | 0 | 0 | 3 |
| 2. | | Introduction to Security operations & incidents | 3 | 0 | 0 | 3 |
| 3. | | Programming full stack web portal | 0 | 1 | 2 | 2 |
| 4. | | Project (Creation of Vulnerable site & exploiting it) | 0 | 1 | 2 | 2 |
| | | | | | **Total Credits** | 10 |

## DATA COMMUNICATION AND NETWORKING

**UNIT I INTRODUCTION TO DATA COMMUNICATION 9**

Data Communications: Components-Data Representation-Data flow Networks-Network criteria-Physical structure-Network types-Internet history- Protocol layering – OSI model- TCP/IP protocol suite

**UNIT II PHYSICAL LAYER 9**

Data and Signals-Periodic analogue signals-Digital signals-Transmission impairments-Performance-Transmission media – Switching: Circuit switching-Packet switching

**UNIT II APPLICATION LAYER AND TRANSPORT LAYER 9**

Application Layer Functionality and Protocols- Introduction, making provision for applications and services- Application layer protocols and services- OSI Transport Layer- The TCP protocol – communicating with reliability, Managing TCP sessions-The UDP protocol communicating with low overheads.

**UNIT III DATA LINK LAYER 9**

Introduction-Link layer addressing- Error detection and correction – Medium Access Control – Wired LANs: Ethernet – Wireless LANs: WiFi-Bluetooth-Connecting Devices and Virtual LANs

**UNIT IV NETWORK LAYER AND TRANSPORT LAYER 9**

Network Layer services – Addressing : IPv4-ICMPv4-IPv6-ICMPv6-Subnetting-Unicast Routing Basics: RIP-OSPF-BGP

Transport Layer – Introduction-Transport layer protocols: TCP-UDP.

**UNIT V APPLICATION LAYER 9**

Application layer services – World Wide Web and HTTP – FTP – Electronic Mail – Secure Shell (SSH) – Domain Name System (DNS)- Introduction to network management basics – Cryptography and Network security – Internet security : IPSec – SSL / TLS – Email security: PGP-S/MIME-Firewalls

**Total: 45 Hours**

**Books for References:**

1. Behrouz Forouzan, “Data Communications and Networking”, Edition 5, Tata McGraw-Hill.2012.
2. Andrews S. Tanenbaum, David J Wetherall, “Computer Networks”, Edition 5, Pearson Education, 2012.
3. William Stallings, “Data & Computer Communications”, PHI, Edition 6, 2012.
4. Jerry Fitzgerald, Alan Dennis, “Business Data Communications & Networking” , John Wiley & Sons Inc, 2010.

# INTRODUCTION TO JAVA PROGRAMMING

**UNIT I JAVA BASICS** **9**

Review of Object oriented concepts, History of Java, Java buzzwords, JVM architecture, Data types, Variables, Scope and life time of variables, arrays, operators, control statements, type conversion and casting, simple java program, constructors, methods, Static block, Static Data, Static Method

**UNIT II INHERITANCE AND POLYMORPHISM** **9**

Basic concepts, Types of inheritance, Member access rules, Usage of this and Super key word, Method Overloading, Method overriding, Abstract classes, Usage of final keyword. Packages and interfaces: Defining package, Access protection, importing packages, Defining and Implementing interfaces, and Extending interfaces.

**UNIT III EXCEPTION HANDLING AND THREADS** **9**

Exception types, Usage of Try, Catch, Throw, Throws and Finally keywords, Built-in Exceptions, Creating own Exception classes. Multi threading: Concepts of Thread, Thread life cycle, creating threads using Thread class and Runnable interface, Synchronization, Thread priorities, Inter Thread communication.

**UNIT IV – IO STREAMS** **9**

I / O STREAMS: Concepts of streams, Stream classes- Byte and Character stream, Reading console Input and Writing Console output, File Handling.

**UNIT V INTRODUCTION TO SOCKET PROGRAMMING** **9**

Looking up Internet Addresses – Retrieving Data with URLs – Sockets for Clients – Sockets for Servers – UDP Datagram Sockets – Java Mail API – The URLConnection class – Protocol Handlers – Content Handlers – Secure Sockets

**Total: 45 Hours**

**TEXT BOOKS:**

1. Herbert schildt (2010), The complete reference, 7th edition, Tata Mc graw Hill, New Delhi

**REFERENCE BOOKS:**

1. Head First Java, O'rielly publications

2. T. Budd (2009), An Introduction to Object Oriented Programming, 3rd edition, PearsonEducation, India.

3. J. Nino, F. A. Hosch (2002), An Introduction to programming and OO design using Java, John Wiley & sons, New Jersey.

4. Y. Daniel Liang (2010), Introduction to Java programming, 7th edition, Pearson education, India

5. Java Network Programming, O'Reilly publications, 2nd edition

# PRINCIPLES OF CYBER SECURITY

**UNIT I INTRODUCTION TO SECURITY TRENDS 9**

The Computer Security Problem - Targets and Attacks - Approaches to Computer Security - Ethics - Basic Security Terminology - Security Models

**UNIT II OPERATIONAL AND ORGANIZATIONAL SECURITY 9**

Policies, Procedures, Standards, and Guidelines - Security Awareness and Training - Interoperability Agreements - The Security Perimeter - Physical Security - Environmental Issues - Wireless - Electromagnetic Eavesdropping - People—A Security Problem - People as a Security Tool

**UNIT III CRYPTOGRAPHY 9**

Cryptography in Practice - Historical Perspectives - Algorithms - Hashing Functions - Symmetric Encryption - Asymmetric Encryption - Quantum Cryptography- Cryptography Algorithm Use

**UNIT IV AUTHENTICATION AND REMOTE ACCESS 9**

User, Group, and Role Management - Password Policies - Single Sign-On - Security Controls and Permissions - Preventing Data Loss or Theft - The Remote Access Process - Remote Access Methods

**UNIT V INTRUSION DETECTION SYSTEMS 9**

History of Intrusion Detection Systems - IDS Overview - Network-Based IDSs - Host-Based IDSs- Intrusion Prevention Systems - Honeypots and Honeynets - Tools

TEXT BOOKS

1 W.A.Coklin, G.White, Principles of Computer Security: Fourth Edition, McGrawHill, 2016
2 William Stallings, Cryptography and Network Security Principles and Practices, Seventh Edition,Pearson

REFERENCE BOOKS

Achyut S. Godbole, Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing, Tata McGraw-Hill Education, 2013 E BOOKS

E BOOKS

https://www.newhorizons.com/promotions/cybersecurity

# NETWORKING LAB

## LIST OF PROGRAMS:

1. To detect Errors using Vertical Redundancy Check (VRC).
2. To detect Errors using Longitudinal Redundancy Check (LRC).
3. To detect Errors using Cyclic Redundancy Check (CRC).
4. Socket programming to implement Asynchronous Communication.
5. Socket programming to implement Isochronous Communication.
6. To implement Stop & Wait Protocol.
7. To implement Sliding Window Protocol.
8. To implement the Shortest Path Routing using Dijkstra algorithm.
9. Socket Programming to Perform file transfer from Server to the Client.
10. To implement Remote Procedure call under Client / Server Environment.
11. Code simulating PING and TRACEROUTE commands
12. Implementing of Subnetting

## CYBER LAWS AND STANDARDS

**UNIT I INTRODUCTION** **9**

Introduction to cyber space -UNCITRAL Model Law - Information Technology Act, 2000 with recent
amendments - Jurisdictional issues - Digital signatures - regulation of - certifying authorities – Cyber Regulation Appellate Tribunal – Human Rights Issues.

**UNIT II ONLINE CONTRACTS** **9**

Formation of online contracts - E banking transactions, online payment options, online advertising - Electronic and digital signatures - Taxation issues in cyber space- indirect tax, tax evasion, double tax, international tax, permanent establishment - Protection of trade secrets and deceptive trade practices.

**UNIT III CYBER CRIMES** **9**

Understanding cybercrimes - Identifying Theft and Frauds - Types of crimes in the internet: Against person, against property, against government - Digital evidence- investigation and adjudication of cybercrimes in India- cyber arbitration, cyber conflict investigation- cyber Terrorism.

**UNIT IV INTELLECTUAL PROPERTY RIGHTS (IPR) AND CYBER SPACE** **9**

Copyright issues in the internet- protection of computer software, caching, international regime- OSS, DMCA, Data Protection Directive - Trademark issues in the internet – Domain Name Registration, Domain Name Registration, Domain Name Dispute, ICANN, UDRP policy, linking, framing, tagging - Database issues in the internet.

**UNIT V THE INDIAN EVIDENCE ACT OF 1872 V. IT ACT, 2000** **9**

Status of Electronic Records as Evidence, Proof and Management of Electronic Records; Relevancy, Admissibility and Probative Value of E-Evidence, Proving Digital Signatures, Proof of Electronic Agreements, Proving Electronic Messages.

CASE STUDY- PROTECTION OF CYBER CONSUMERS IN INDIA:

Are Cyber Consumers Covered Under the Consumer Protection Act? Goods and Services, Consumer Complaint, Defect in Goods and Deficiency in Services, Restrictive and Unfair Trade Practices, Instances of Unfair Trade Practices, Reliefs Under CPA, Beware Consumers, Consumer Foras, Jurisdiction and Implications on cyber Consumers in India, Applicability of CPA to Manufacturers, Distributors, Retailers and Service Providers Based in Foreign Lands Whose Goods are Sold or Services Provided to a Consumer in India.

**Books for References:**

1. Karnika Seth, " Computers, Internet and New Technology Laws" ,Cyber Lawyer and Expert and is The Managing Partner of Seth Associates, Edition 2012.
2. S.K.Verma, Raman mittal , "Legal dimensions of cyber space" ,Indian Law Institute, New Delhi Indian Institute,2004.
3. Law Relating to Computers Internet & E-commerce – "A Guide to Cyber laws & the Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws", 2012.
4. Jeff Kosseff , "Cyber security Law", Wiley Publications, 2017.
5. Ian. J. Lyod , "Information technology law" , Information Technology Act 2000, its amendment and IT Rules, 2014.
6.Yee fen Lim , "Cyber space law commentaries and Materials", second edition, Galexia Consulting Pvt Ltd, Australia.

## RISK MANAGEMENT IN CYBER SECURITY

**UNIT I INTRODUCTIONTO CYBERSECURITY 9**

The Security Environment: Threats, vulnerabilities, and consequences - Advanced persistent threats - The state of security today. Principles of Cybersecurity: The interrelated components of the computing environment - Cybersecurity models - Variations on a theme: computer security, information security, and information assurance. Cybersecurity Management Concepts: Management models, roles, and functions. Enterprise Roles and Structures: Information security roles and positions.

**UNIT II STRATEGIC PLANNING AND SECURITY PLANS 9**

Strategy and Strategic Planning: Strategy - Strategic planning and security strategy - The information security lifecycle - Architecting the enterprise. Security Plans and Policies: Levels of planning - Planning misalignment - The System Security Plan (SSP)- Policy development and implementation. Security Standards and Controls: Security standards and controls - Certification and accreditation (C&A).

**UNIT III RISK MANAGEMENT 9**

Risk Management: Principles of risk - Types of risk - Risk strategies - The Risk Management Framework (RMF). Physical Security and Environmental Events: Physical and environmental threats - Physical and environmental controls. Contingency Planning: Developing a contingency plan - Understanding the different types of contingency plan - Responding to events.

**UNIT IV SECURITY AWARENESS 9**

Security Education, Training, and Awareness: Human factors in security - Developing and implementing a security training plan - Cross-domain training (IT and other security domains). The future of cyber security: Key future uncertainties - Possible future scenarios - How to apply what you've learned.

**UNIT V CASE STUDY 9**

Case Study on Pune Citibank MphasiS Call Center Fraud – The Bank NSP Case – UTI Bank hooked in a phishing attack – Mumbai Police can now nail web offenders – Orkut: The new danger.

Total: 45 Hours

**Books for References:**

1. Rhodes-Ousley, Mark. "Information Security: The Complete Reference, Second Edition, Information Security Management: Concepts and Practice", New York, McGraw-Hill, 2013.
2. Whitman, Michael E. and Herbert J. Mattord, " Roadmap to Information Security for IT and Infosec Managers", Boston, MA: Course Technology, 2011.
3. Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security", Course Technology, Cengage Learning, Fourth Edition, Nov, 2014.

## VULNERABILITY ASSESSMENT OF IT INFRASTRUCTURE

**UNIT I Fundamental** **9**

Defining vulnerability, exploit, threat and risk-Creating a vulnerability report-Conducting an initial scan-Common Vulnerabilities and Exposure (CVE) list, **Scanning and exploits:** Vulnerability detection methods-Types of scanners-Port scanning and OS fingerprinting-Enumerating targets to test information leakage-Types of exploits: worm, spyware, backdoor, rootkits, Denial of Service (DoS)-Deploying exploit frameworks

**UNIT II** Analyzing Vulnerabilities and Exploits 12

**Uncovering infrastructure vulnerabilities:** Uncovering switch weaknesses-Vulnerabilities in infrastructure support servers-Network management tool attacks,**Attacks against analyzers and IDS:** Identifying Snort IDS bypass attacks-Corrupting memory and causing Denial of Service, **Exposing server vulnerabilities:** Scanning servers: assessing vulnerabilities on your network-Uploading rogue scripts and file inclusion-Catching input validation errors-Performing buffer overflow attacks-SQL injection-Cross–Site Scripting (XSS) and cookie theft,**Revealing desktop vulnerabilities:** Scanning for desktop vulnerabilities-Client buffer overflows-Silent downloading: spyware and adware-Identifying design errors

**UNIT III** Configuring Scanners and Generating Reports 8

**Implementing scanner operations and configuration:** Choosing credentials, ports and dangerous tests-Preventing false negatives-Creating custom vulnerability tests-Customizing Nessus scans-Handling false positives, **Creating and interpreting reports:**Filtering and customizing reports-Interpreting complex reports-Contrasting the results of different scanners

**UNIT IV** Assessing Risks in a Changing Environment 8

**Researching alert information:** Using the National Vulnerability Database (NVD) to find relevant vulnerability and patch information-Evaluating and investigating security alerts and advisories-Employing the Common Vulnerability Scoring System (CVSS), **Identifying factors that affect risk:** Evaluating the impact of a successful attack-Determining vulnerability frequency-Calculating vulnerability severity-Weighing important risk factors-Performing a risk assessment

**UNIT V** Managing Vulnerabilities 8

**The vulnerability management cycle:** Standardizing scanning with Open Vulnerability Assessment Language (OVAL)-Patch and configuration management-Analyzing the vulnerability management process, **Vulnerability controversies:** Rewards for vulnerability discovery-Markets for bugs and exploits-Challenge programs

Total: 45 Hours

# Vulnerability Testing Lab

1. Perform protocol analysis using packet captures and analysis data using a sniffer (e.g. Wireshark)
2. Investigate and uncover network devices, operating systems, ports, and services (e.g. Nmap)
3. Discover network security issues using an intrusion detection tool (e.g. Snort)
4. Implement and leverage penetration testing suite of applications (e.g. Metasploit)

FIREWALL AND INTERNET SECURITY

UNIT I FIREWALLS AND SECURITY MECHANISM 9

Introduction – Types of Firewalls – Packet filters – Application gate ways – Limitations of firewalls -Internet Security - Email security – PGP - S/MIME - IP security – Overview – IP Security Architecture- Web security - SSL, TLS, SET.

UNIT II PROGRAM SECURITY 9

Secure programs – Non-malicious Program Errors – Viruses – Targeted Malicious code – Controls against Program Threat – Control of Access to General Objects – User Authentication – Good Coding Practices – Open Web Application Security Project Top 10 Flaws – Common Weakness Enumeration Top 25 Most Dangerous Software Errors.

UNIT III OPERATING SYSTEM SECURITY 9

Protected objects and methods of protection- Memory address protection- Control of access to general objects- File protection mechanism-Authentication: Authentication basics- Password-Challengeresponse- Biometrics.

UNIT IV SECURITY IN DATABASES 9

Security requirements of database systems – Reliability and Integrity in databases – Two Phase Update– Redundancy/Internal Consistency – Recovery – Concurrency/Consistency – Monitors – Sensitive Data– Types of disclosures – Inference.

UNIT V SECURITY IN NETWORKS AND CASE STUDY 9

Threats in networks – Encryption – Virtual Private Networks – PKI – SSH – SSL – IPSec –Content Integrity – Access Controls – Wireless Security – Honeypots – Traffic Flow Security – Firewalls – Intrusion Detection Systems – Secure e-mail.

Total: 45 Hours

**Books for References:**


1. Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, Pearson Education, 2007.

2. Matt Bishop, “Computer Security: Art and Science”, Pearson Education, 2003.

3. William Stallings, “Cryptography and Network Security: Principles and Practices”, Fifth Edition, Prentice Hall, 2010.

4. Michael Howard, David LeBlanc, John Viega, “24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them”, First Edition, Mc Graw Hill Osborne Media, 2009.

5. Kaufman, Perlman, Speciner, “Network Security”, Prentice Hall, 2nd Edition, 2003.

6. Eric Maiwald, “Network Security: A Beginner’s Guide”, TMH, 1999.

7. Macro Pistoia, Java Network Security, Pearson Education, 2nd Edition, 1999.

8. Whitman, Mattord, Principles of Information Security, Thomson, 2nd Edition, 2005.

INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY

**UNIT I INTRODUCTION TO CRYPTOGRAPHY 9**

Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model- Classical Cryptography: Dimensions of Cryptography, Classical Cryptographic Techniques.

**UNIT II BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY 9**

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES). Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie-Hellman Key exchange-Elliptic curve cryptosystem.

**UNIT III HASH FUNCTIONS AND DIGITAL SIGNATURE 9**

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD4&MD5 Message Digest Algorithm – SHA – HMAC – CMAC – Digital signature and authentication protocols – DSS – EIgamal – Schnorr signature.

**UNIT IV SECURITY PRACTICE AND SYSTEM SECURITY 9**

Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions.

**UNIT V E-MAIL SECURITY AND CASE STUDY 9**

E-mail Security: Security Services for E-mail-attacks possible through E-mail – Establishing keys privacy- Authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME- Internet Key Exchange Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtua Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

Total: 45 Hours

**Books for References:**

1. William Stallings, “Cryptography and Network Security: Principles and Practices”, 6th Edition, Pearson Education Ltd, 2016.
2. Bart Preneel, Christof Paar, Jan Pelzl, “Understanding Cryptography”, Springer-Verlag Berlin Heidelberg, 2010.
3. Atul Kahate, “Cryptography and Network Security”, Mc Graw Hill, 3rd Edition, 2011.
4. Behrouz A.Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security”, 5. Tata McGraw Hill Second Edition, 2010.
6. Wenbo Mao, “ Modern Cryptography: Theory and Practice”, Prentice Hall PTR, 1st Edition, 2003.
7. Douglas R. Stinson , “Cryptography: Theory and Practice”, CRC press, 3rd Edition, 2005.

ETHICAL HACKING

**UNIT I INTRODUCTION TO ETHICAL HACKING 9**

Security Fundamental - Security Testing - Hacker and Cracker – Descriptions - Test Plans- keeping it legal - Ethical and Legality-Technical Foundations of Hacking: The Attacker's Process - The Ethical Hacker's Process- Security and the Stack.

**UNIT II FOOTPRINTING AND SCANNING 9**

Information Gathering - Determining the NetworkRange - Identifying Active Machines- Finding Open Ports and Access Points - OS Fingerprinting Services - Mapping the Network Attack Surface -Enumeration and System Hacking : Enumeration - System Hacking.

**UNIT III MALWARE THREATS AND SESSION HIJACKING 9**

Viruses and Worms- Trojans - Covert Communication - Keystroke Logging and Spyware – Malware Counter Measures- Sniffers - Session Hijacking - Denial of Service - Distributed Denial of Service.

**UNIT IV WEB SERVER HACKING AND ATTACKS 9**

Web Server Hacking - Web Application Hacking - Database Hacking - Wireless Technologies – Mobile Security and Attacks: Wireless Technologies - Mobile Device Operation and Security – Wireless LANs.

**UNIT V CASE STUDY 9**

Intrusion Detection Systems - Firewalls - Honeypots - Physical Security - Social Engineering – Case Studies: Intrusion detection Real Secure Tripwire Dragon Snort ,Packet sniffing Leave the sniffer running, Passwords in procedures & documents.

Total: 45 Hours

Books for References:

1. Michael Gregg,"Certified Ethical Hacker", Version 10, Third Edition, Pearson IT Certification, 2019.
2. Roger Grimes ,"Hacking the Hacker" , 1st Edition, Wiley, 2017.
3. Ankit Fadia, " The Unofficial Guide to Ethical Hacking", Laxmi Publications, 2ns Edition, 2006.

PENETRATION TESTING LAB

1. Perform reconnaissance about the target system
2. Scan the target system using NMAP tool
3. Perform OS fingerprinting and version scanning
4. Inject client-side attacks using Metasploit framework
5. Exploit the network services using Meterpreter sessions of the Metasploit framework
6. Perform DNS attacks with Bloodhound
7. Password Cracking with John the Ripper and Hashcat
8. PowerShell for Pen Testers

## INTRODUCTION TO CYBER FORENSICS

**UNIT I UNDERSTANDING THE THREAT FROM CYBER CRIME** **9**

Introduction Cyber Threat – Definition of Cyber Crime – Classification – Current Threats and Trends – Diversity of Cyber Crime – Cyber Hate Crimes – Cyber Terrorism.

**UNIT II RESPONDING TO CYBER CRIME** **9**

Cyber Strategy – National Security Strategy – Cyber Security Strategy – Organized Crime Strategy –Cyber Crime Strategy - Policy Cyber Crime – International Response – National Cyber Security Structure – Strategic Policy Requirements – Police and Crime Commissioners.

**UNIT III INVESTIGATING CYBER CRIME** **9**

Preventing Cyber Crime – Password Protection – Get Safe Online – Cyber Security Guidance for Business - Cyber Crime Investigation Skills – Criminal Investigation – Code of Ethics – Evidence – Hi-Tech Investigations – Capturing and Analyzing Digital Evidence.

**UNIT IV DIGITAL FORENSICS** **9**

Introduction to Digital Forensics - Forensic Software and Hardware - Analysis and Advanced Tools - Forensic Technology and Practices - Forensic Ballistics and Photography - Face, Iris and Fingerprint Recognition - Audio Video Analysis - Windows System Forensics - Linux System Forensics - Network Forensics.

**UNIT V: CASE STUDY** **9**

Latest Study Topics on Cyber Crime and Investigations - Recent Cyber Crime Cases – Recent Digital Forensics Cases – Bridging the Gaps in Cyber Crime Investigations between the cyber security stake holders.

Total: 45 Hours

TEXT BOOKS

Thomas Halt, Adam M. Bossler and Kathryn C.Seigfried Spellar, ―Cybercrime and Digital Forensics: An Introduction‖, Routledge Taylor and Francis Group 2017.

REFERENCE BOOKS

Bernadette H Schell, Clemens Martin, ―Cybercrime‖, ABC – CLIO Inc, California, 2004

E BOOKS

https://books.google.co.in/books/about/Cybercrime_and_Digital_Forensics.html?id=7SA6DwAAQBAJ&redir_esc=y