No: A&L/NFSU/7thACResolution No._7(a)/199/2024 **Date: 22/7/2024**

Read:

(1) Section 19 of the NFSU Act, 2020;
(2) Meeting of the Board of Studies of the School of Cyber Security & Digital Forensics dated 29/05/2024;
(3) Academic Council Meeting dated 27/6/2024 - Resolution No: 7(a)

CIRCULAR

It is hereby informed to all concerned that the Academic Council in its meeting held on 27/6/2024, has resolved to approve the **Syllabi, Teaching and Examination Scheme of the Semester VII, VIII, IX and X of B. Tech. - M. Tech. Computer Science & Engineering (Cyber Security) to meet the requirements of the New Education Policy, 2020/Industry/Law, for the students admitted in the Academic Year 2021-22 and onwards and to be made effective from the Academic Year 2024-25 and onwards,** as per **Annexure-A** enclosed herewith.

Executive Registrar
NFSU, Gandhinagar

To:

- Campus Director – Gandhinagar / Delhi / Goa / Tripura / Dharwad / Guwahati / Bhopal / Uganda
- Director – Academics, Research and Consultancy
- Concerned Dean/Associate Dean

Copy to:

- Controller of Examinations, NFSU, Gandhinagar
- Dy. Registrar – Admin/Academic & Legal/Exam
- Programme Coordinator

C.f.w.c to: Hon'ble Vice Chancellor for kind information

Encl: Annexure A

List of Program Elective		
Sr. No.	**Subject Code**	**Subject Name**
	Semester V	
1	CTBTCSE SV P6 EL1	Big Data
2	CTBTCSE SV P6 EL2	Cloud Computing
	Semester VI	
1	CTBTCSE SVI P6 EL1	Computer Graphics
2	CTBTCSE SVI P6 EL2	Advance Web Development Technology
	Semester VII	
1	CTBTCSE SVII P6 EL1	Research Methodology Part -1
2	CTBTCSE SVII P6 EL2	Digital Forensics
3	CTBTCSE SVII P6 EL3	Android Development
4	CTBTCSE SVII P6 EL4	Physics of Semiconductor Devices
	Semester VIII	
1	CTBTCSE SVIII P5 EL1	Research Methodology Part – 2
2	CTBTCSE SVIII P5 EL2	Social Media Analytics
3	CTBTCSE SVIII P5 EL3	Internet of Things
4	CTBTCSE SVIII P5 EL4	Semiconductor Hardware Design & Security
	Semester IX	
	Program Elective 1	
1	CTMTCSE SIX P3 EL1	Introduction to PowerShell and Shell Scripting
2	CTMTCSE SIX P3 EL2	Advance Digital Forensics
3	CTMTCSE SIX P3 EL3	Risk Management and Contingency Planning
	Program Elective 2	
1	CTMTCSE SIX P4 EL1	Advanced Malware Analysis
1	CTMTCSE SIX P4 EL2	Internet of Things Security
2	CTMTCSE SIX P4 EL3	SCADA Security

Total Credits: 200 **L:** Lecture **T:** Tutorial **P:** Practical 1 C = 1 Hour of Lecture / Tutorial and 1 C = 2 Hours of Practical / Project. **TCH:** Total Credit Hours

Note: TA will be taken in two parts TA-1 and TA-2. TA-1 will be written examination of 00:45 Hour and TA-2 will be in form of assignments or workshops.

1342

Annexure -II

National Forensic Sciences University

An Institution of National Importance
(Ministry of Home Affairs, Government of India)
Sector – 9, Gandhinagar, Gujarat – 382007

School of Cyber Security & Digital Forensics

B.Tech. – M.Tech. Computer Science and Engineering
(Cyber Security)

Syllabus

(Semester – VII to X)

(D.D. Dave)

1343

SEMESTER – VII

7394

CTBTCSE SVII P1: Vulnerability Analysis & Web Application Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To learn the concept of web application technology.
2. Learn various aspects of web application security.
3. Learn to vulnerability assessment of web application security.
4. Exploitation of potential found vulnerability.
5. Learn industry standard techniques to exploit advanced vulnerability.

UNIT – I

Introduction to web technology and information Gathering

TCP, HTTP/S Protocol Basics, Encoding, Origin, Cookies, Sessions, Fingerprinting the web server, Subdomain's enumeration, finding virtual hosts, fingerprinting custom applications, Enumerating resources, Relevant information through misconfigurations, Google hacking.

UNIT – II

Web Application Security Vulnerability Terminology

Introduction to Vulnerability Assessment, Life cycle of Vulnerability Assessment, Vulnerability Scanners, Unknown Vulnerability, False Positive, CVE, CWE, Common Vulnerability Scoring System (CVSS), STRIDE, DREAD, Secure Source Code Review.

UNIT – III

Proxy and Interception

Burp Suite / OWASP Zed Attack Proxy (ZAP): Logging and monitoring, learning tools to spider a website, analyzing website content, Brute forcing unlinked files and directories via ZAP and ffuf, Web authentication mechanisms, Fuzzing with Burp Intruder, Username harvesting and password guessing, Burp sequencer, Session management and attacks, Authentication and authorization bypass.

J345

UNIT – IV

Attack Landscape - Web Application Security

OWASP 10 Ten – Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring, Cross Site Request Forgery, File Inclusion, Click Jacking, File Inclusion, File Upload, Insecure Captcha, SSRF/XSPA.

UNIT – V

Advanced Web Security Pen-Testing

Web Service concepts, REST concepts, SQL Injection - Vulnerable code, Sensitive data in GET, Weak Auth tokens & IDOR, Leaky APIs, Automated Scanning with FuzzAPI / Astra / other industry standard tools, Introduction to CMS and Docker containers security.

Reference Books

1. Web Application Security, A Beginner's Guide by Bryan Sullivan, Vincent Liu, McGraw-Hill Education Publication (2011).
2. Hands-On Bug Hunting for Penetration Testers A Practical Guide to Help Ethical Hackers Discover Web Application Security Flaws by Joseph Marshall, Packt Publication (2018).
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard, Marcus Pinto, 2nd Edition, Wiley Publication (2007).
4. The Penetration Tester's Guide to Web Applications by Serge Borso, Artech House Publication (2019).
5. Web Application Security Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman, O'Reilly Media Publication (2020)

1346

CTBTCSE SVII P2: Cyber Law, Policies and Compliance

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs					
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To learn the concept of security audit and compliance.
2. To understand and create IT security related organizational policy.
3. To learn risk assessment & business impact analysis.
4. To learn various globally accepted security standards.
5. To understand various Indian IT Act sections and amendments.

UNIT – I
Introduction to information system security compliance

The need for information system security compliance, What is IT security assessment?, what is IT security audit?, what is compliance? How does an audit differs from an assessment? Why are governance and compliance important? What if organization does not comply with compliance laws? What is the scope of an IT compliance audit?, what your organization do to be in compliance?, What are you auditing within the IT infrastructure?, Maintaining IT compliance.

UNIT – II
Planning and implementation of an IT Infrastructure Audit for compliance

Defining the scope for audit, Identifying critical requirements for the audit, assessing IT security, Obtaining Information, Documentation and Resources, Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure, Identifying and Testing Monitoring Requirements What Are Controls and Why Are They Important?, Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Setting the Stage for Control Implementation through Security Architecture Design, Implementing a Multitiered Governance and Control Framework in a Business.

UNIT – III
Conducting an IT Infrastructure Audit for Compliance

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions, Seven Domains of a Typical IT Infrastructure, Writing the IT

1347

Infrastructure Audit Report. Compliance within User Domain, Compliance law requirements and business drivers, Items Commonly Found in the User Domain, Compliance within the workstation domain, Compliance law requirements and business drivers, devices and components commonly found in the workstation domain, Maximizing C-I-A, Compliance within the LAN Domain, Compliance law requirements and business drivers, devices and components commonly found in the LAN domain, Maximizing C-I-A, Compliance within LAN and WAN Domain, Devices and Components Commonly Found in the Domain , Penetration Testing and Validating Configurations, Compliance within Remote Access and Application Domain, Devices and Components Commonly Found in the Domain, Application Server Vulnerability Management, Application Patch Management.

UNIT – IV
Risk Assessment and BCP, DR Planning

Introduction to Risk Analysis, Risk Identification, Risk Assessment, Risk Response and Mitigation, Risk Reporting, Introduction to Business Continuity Planning (BCP), Overview of BCP Life Cycle, Need for BCP, Identifying and Selecting Business Continuity Strategies, Introduction to Disaster Recovery (DR) planning, Identification of potential disaster status, DR Strategies, Plans for Business Resumption.

UNIT – V
Cyber Law and Auditing Standards/Frameworks

Indian IT ACT with Amendments, Adjudication under Indian IT ACT, Overview of Auditing Standards and Frameworks: ISO/IEC 27001/2, COBIT, HIPAA, GDPR PCIDSS and The Digital Personal Data Protection Act, 2023.

Reference Books

1. Auditing IT Infrastructures for Compliance By Martin M. Weiss, Michael G. Solomon, Jones & Bartlet Learning, 2015.
2. The Information Technology Act, 2000 Bare Act with Short Notes by Universal, 2020.
3. The IT Regulatory and Standards Compliance Handbook By Craig S. Wright, Syngress, 2015.
4. Information Technology Control and Audit 5th Edition By Angel R. Otero, 2019.
5. (Internal Audit and IT Audit Series) The Complete Guide to Cyber Security Risks and Controls By Anne Kohnke, Dan Shoemaker, Ken Sigler, 2016.

1348

6. PCI DSS An Integrated Data Security Standard Guide- APress By Jim Seaman, 2020.
7. AICPA - Guide_ SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy-Wiley, 2018.
8. The EU General Data Protection Regulation (GDPR) A Practical Guide By Paul Voigt and Axel von dem Bussche, 2017.
9. PCI DSS, SAQ Instructions and Guidelines (Available online).
10. Business Continuity and Disaster Recovery for Infosec Managers.
11. Bob Hayes, Kathleen Kotwica, "Business Continuity 2nd Edition", Elsevier Pub. 2013.
12. The Indian Evidence Act, 1872 Bare Act with Short Notes by Universal, 2020.
13. ISO-IEC 27002-2013 standard.
14. COBIT 5 for assurance, ISACA.
15. HIPPA compliance guide, HHS.
16. Cyber Law - The Indian Perspective by Pawan Duggal.
17. Risk Management COBIT 5, ISACA.
18. Governance, risk, and compliance by Microsoft, 2019.
19. IT Act Bill 2000 and Amendments.

1349

CTBTCSE SVII P3: Artificial Intelligence

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand the concept of Machine Learning, analyze the data patterns and modelling for applying the learning algorithms
2. To understand, compare and evaluate the performance of various basic Machine Learning algorithms.
3. To create models to understand applications of Machine Learning.
4. To learn the neural network concept.
5. Apply the Machine Learning concepts in real life problems and Cyber Security.

UNIT-I

Introduction

Introduction: What is AI? : The AI Problems, The Underlying Assumption, What Is An AI Techniques, what is machine learning, History of machine learning, Mathematics for AI/ML: Vectors, Matrices; Introduction to Anaconda, Working with NumPy, Pandas and Matplotlib.

UNIT-II

Machine Learning (ML): Supervised Learning

Introduction: Defining Machine Learning, Applications of ML, Issues and Challenges in ML, Types of ML. Data Preprocessing: Data Cleaning, Dimensionality Reduction Technique : Feature Selection, Normalization, Training, Testing & Validation Sets; Supervised Learning: Prediction, Classification; Different Models of Supervised Learning: Linear and Logistic Regression, Decision Trees, Learning Decision Trees, K-nearest Neighbors; Measuring Performance: Accuracy and Loss, Underfitting & Overfitting, Regularization, Evaluation metrics: accuracy, precision, recall, Confusion metric and F1 score.

1350

UNIT-III

Unsupervised Learning

Introduction to Clustering, K-means Clustering, Hierarchical clustering, Agglomerative Hierarchical Clustering, Dimensionality reduction techniques (PCA, SVD), Gaussian Mixture Models, Model Evaluation and Performance Optimization: Hyperparameter tuning,

UNIT-IV

Artificial Neural Network

Understanding Biological Brain, Defining Artificial Neural Network (ANN), Applications of ANN, Types: Single-layer & Multi-layer ANNs. Algorithms: Perceptron Learning algorithm, Defining & Building a Perceptron, Feed Forward, Back propagation, Activation & Loss Functions, Compiling & Evaluating a Model.

UNIT-V

Applications of AI/ML

Introduction to Role of ML in Cyber Security, Malware Detection & Classification, Anomaly Detection, Definition and concept of Deepfake, Historical background and evolution, Motivations behind the development of Deepfake technology, Definition of ethics and its importance in AI development and deployment, Overview of ethical principles relevant to AI, such as fairness, transparency, accountability, and privacy, Pen testing using ML, ML based intrusion detection other application of AI/ML.

Reference Books

1. T. Hastie, R. Tibshirani, and J. Friedman. The Elements of Statistical Learning. Springer 2011.
2. Kevin P. Murphy. Machine Learning: A Probabilistic Perspective, MIT Press 2012.
3. Christopher M. Bishop. Pattern Recognition and Machine Learning, Springer 2007.
4. S. Haykin. Neural networks and learning machines. Pearson 2008.
5. Pattern Classification, 2nd Ed., Richard Duda, Peter Hart, David Stork, John Wiley Sons, 2001.
6. Machine Learning with Python for Everyone, Mark Fenner, Pearson
7. Tom Mitchell, Machine Learning, TMH
8. Ethem Alpaydin, Introduction to Machine Learning, PHI

1351

CTBTCSE SVII P4: Information and Network Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
2	0	0	2	2	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand the concept of encryption, Public key cryptography, message authentication and hash functions.
2. To learn about the essentials of network security.
3. To understand the basics of network vulnerability assessment and penetration testing methodology.
4. To understand the important network communication protocols.
5. To understand the basics of wireless network protocols and its security concepts.

Unit - I

Introduction to Security

Introduction to Security: need for security, principle of security, security approaches. Confidentiality, Integrity, and Availability. Encryption Techniques: plaintext, cipher text, substitution & transposition techniques, encryption & decryption, key range & size. Symmetric and Asymmetric encryption. Public Key Cryptography and Message Authentication: Public key cryptographic principles, digital signatures, key management, hash function and message digest.

Unit - II

Basics of Networking

ISO/OSI, TCP-IP, Networking devices: Host, Hub, Bridge, Switch, Router and its functioning, Perimeter devices: IDS, IPS, Firewall and its functioning. NOC, SOC, SIEM, Servers: DNS, DHCP, Proxy, Mail and Application servers. Threat, vulnerability, attack surface, attack vector, exploit. Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.

Unit - III

Penetration Testing

Penetration testing life cycle: Scope, SOW, Reconnaissance, target enumeration, vulnerability identification, assessment, exploitation, and reporting. Information

1352

gathering, Scanning: active and passive, ICMP (Ping), OS and server fingerprinting, scanning tools and port status, TCP and UDP scan. SNMP services enumeration, and countermeasures. Routing devices enumeration and countermeasures. Advanced enumeration: Password cracking, sniffing password hashes and password protection. Vulnerability exploitation, Buffer overflow, vulnerability assessment tools, source code assessment tools, application assessment tools, system assessment tools, exploit tools.

Unit - IV

Wireless Network Security

802.11 Protocols, WAP and inherent security issues, promiscuous and monitor mode, Sniffing wireless packets, management, control, and data frames, WLAN authentication and encryption, WEP, WPA and WPA 2. WLAN authentication and security flaws. WLAN based attacks and countermeasures. WLAN Pen testing tools.

Unit - V

Network Forensics

Digital evidence, Network based digital evidence, Network Forensic investigation methodology, Sources of network-based evidence, Evidence acquisition, Network traffic capture and analysis.

References Books

1. Stamp Mark, Information Security: Principles and Practice. Second Edition, Published by John Wiley & Sons, 2011.
2. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
3. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
4. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, 2010 2.
5. Michael Gregg, Build Your Own Security Lab: A Field Guide for Networking Testing.
6. Sherri Davidoff and Jonathan Ham, Network Forensics Tracking Hackers through Cyberspace.
7. Mastering Wireless Penetration Testing for Highly Secured Environments by Aaron Johns

CTBTCSE SVII P5: PROJECT - 1

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
Th	Tu	Pr	C	TCH	Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
0	0	5	5	10	25	00:45	50	01:30	-	-	100	3:00	200

Project 1 is based on the Research and development-oriented problems of practical and theoretical interest. Evaluation will be done at the end of the semester based on periodic presentations/student seminars/written reports and evaluation of the developed system.

1354

CTBTCSE SVII P6 EL1: RESEARCH METHODOLOGY PART-1

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
2	0	0	2	2	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand basic concepts of research and its methodologies.
2. To identify appropriate research topics.
3. To understand the research designing and problem forming ability.
4. To define and select appropriate research problem and parameters.
5. To learn how to prepare a research documentation and report.

Unit - I

Research Methodology Introduction

Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research

Unit - II

Literature Survey and Defining the Research Problem

Literature survey, Review concepts and theories, identifying the limitation of different approaches. What is a Research Problem?, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem.

Unit - III

Research Design

Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs

1355

Unit - IV

Methods of Data Collection

Collection of Primary Data, Observation Method, Interview Method, Collection of Data through Questionnaires, Collection of Data through Schedules, Difference between Questionnaires and Schedules, Some Other Methods of Data Collection, Collection of Secondary Data, Selection of Appropriate Method for Data Collection.

Unit - V

Technical Report Writing and Presentation

Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation

References Books

1. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
2. C. R. Kothari, "Research Methodology: Methods and Techniques", New Age International Publisher.
3. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students"
4. Shanti Bhushan Mishra and Shashi Alok, "Handbook of Research Methodology: A Compendium for Scholars & Researchers", EDUCREATION PUBLISHING.

1356

CTBTCSE SVII P6 EL2: Digital Forensics

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs					
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand what is Digital Forensics and what are the various branches of Digital Forensics.
2. To learn the process of recovering, analyzing, and preserving computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
3. To understand the Filesystems and its architecture.
4. Designing procedures at a suspected crime scene which can help in ensuring that the digital evidence obtained is not corrupted.
5. Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate the integrity.

UNIT – I

Digital Forensics and Electronic Evidence

Digital Forensics: Definition, Process, Locard's Principle of Exchange, Branches of Digital Forensics, Overview of the Various Branches, Handling Digital Crime Scene, Important Documents and Electronic Evidences. Introduction to Evidence Acquisition: Identification, Acquisition, Labeling and Packaging, Transportation, Chain-of-Custody, Importance of Documentation and Preservation.

UNIT – II

Acquisition and Data Recovery

Acquisition Process: Write-Blockers, Imaging Techniques, Evidence Integrity, Standard Operating Procedures for Acquisitions and Preservation of Evidences.
Introduction to Data Recovery and Carving: Importance of Data Recovery in Forensic Investigation, Carving Methods, Difference between Data Recovery and Carving

1357

UNIT – III

File System Analysis

Understanding and Analyzing FAT and NTFS File Systems, Understanding and Analyzing EXT File System, Understanding and Analyzing HFS and HFS+ File System, Understanding APFS. Mobile Device based OS, Other File Systems

UNIT – IV

Understanding Forensics Artefacts

Windows Registry Analysis: Understanding Windows Registry, Analyzing Windows Registry, Finding Important Artefacts Related to User Activities, User/Application Configurations and Preferences; Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations; Installed Applications and Others from Windows Registry. Forensic Artefacts: Browser Artefacts, Network Related Artefacts. Case Studies related to Digital Forensics, Understanding Anti-forensic techniques, Steganography.

UNIT – V

Log Analysis

Log Analysis: Windows Event and Log Analysis: Introduction to Windows Events, Understanding Windows Events (Evt and Evtx Files). Analyzing Logs of Third-party Applications. Linux & Mac OS: Understanding Various Logs, Analyzing Important Logs to Find Important Artefacts Related to User Activities, User/Application Configurations and Preferences; Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations; Installed Applications.

Reference Books

1. Practical Guide to Computer Forensics Investigations, A (Pearson IT Cybersecurity Curriculum (ITCC)) 1st Edition by Darren R. Hayes
2. Learn Computer Forensics: A beginner's guide to searching, analysing, and securing digital evidence 1st Edition by William Oettinger
3. Investigating Windows Systems 1st Edition by Harlan Carvey
4. Windows Forensics Cookbook by Oleg Skulkin, Scar de Courcier
5. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition by Harlan Carvey (Author)
6. Practical Linux Forensics: A Guide for Digital Investigators by Bruce Nikkel

1358

7. Linux Forensics Kindle Edition by Philip Polstra
8. Computer Systems_ Digital Design, Fundamentals of Computer Architecture and Assembly Language
9. Digital Forensics with Open Source Tools 1st Edition by Cory Altheide, Harlan Carvey
10. Operating System Concepts 10th Edition by Abraham Silberschatz, Greg Gagne, Peter B. Galvin
11. Operating Systems: Internals and Design Principles, 9/e by WILLIAM STALLINGS
12. Linux Bible 10th Edition by Christopher Negus
13. Linux Pocket Guide: Essential Commands 3rd Edition by Daniel J. Barrett

1359

CTBTCSE SVII P6 EL3: Android Development

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand Kotlin and Android.
2. To understand basic User Interface in android
3. To translate the real-life situations in android programming form and solve them by storing data on database.
4. To translate the real-life situations in android programming form and solve them by providing concepts of Maps, Location, UI-UX and test and detect that it is optimized applications.
5. To understand the real-life situation in android programming and solve it using concepts of Audio, Video, Camera, Telephony and make it live for the other people.

UNIT-I

Introduction to Kotlin and Android

Basics of Kotlin, Operations and Priorities, Decision Making, Loop Control, Data Structures(Collections), Functions, Object Oriented Programming: Inheritance, abstract, interface, super and this, visibility modifiers, Introduction to Android Components, Android Architecture, ANDROID SDK Features, Basics of an ANDROID application, introduction to manifest.

UNIT-II

Introduction to User Interface and Development features of Android

Android Application lifecycle, Android activities, fragments, Intents, Explicit and Implicit Intent, Introduction to Development Features, Widgets: Button, TextView, ImageView, ProgressBar, ListView, EditText, Calendar, DateTime etc, Working with Intent, Toast, Dialogs, Adapters, View, ViewGroups, externalizing resources

UNIT-III

File, Preferences, Database and Content Provider

Creating, saving and retrieving shares preferences, Including static files as resources, working with the file system, Introducing ANDROID databases, Content

7360

values and cursors, Working with SQLite databases, Creating content providers, Using content providers, Native ANDROID Content providers

UNIT-IV

Enhancing User Experience, Maps and Location Based Services, Jetpack Compose

Menus and dialogs, drawable and gradients, Using location-based services, Selecting a location provider, Finding your current location, and Material Design, Introduction to Jetpack Compose, Introduction of recycle view and card view. Basics of Android Secure Coding

UNIT-V

Audio, Video, Camera, Telephony & SMS, and Monetizing the applications

Playing audio and video, manipulating raw audio, using camera to take pictures, recording video, adding media to media store, Hardware support for telephony, using telephony, introducing SMS and MMS, Signing and publishing applications, introduction to monetizing applications

Reference Books

1. Modern Android 13 Development Cookbook, Madona S. Wambua, Packt Publishing, ISBN: 9781803233215, 2023
2. Jetpack Compose 1. 3 Essentials, By Neil Smyth · 2023, Payload Media, ISBN 9781951442644
3. Android Internals, By Jonathan Levin · 2021, Publisher: Technologeeks, ISBN: 9780991055586
4. Head First Android Development, By Dawn Griffiths, David Griffiths · 2021, O'Reilly Media, ISBN: 9781492076476
5. Google Associate Android Developer Exam Practice Questions & Dumps, By Pascal Books · 2021, Amazon Digital Services LLC - KDP Print US, ISBN: 9798511754970
6. Android Programming with Kotlin for Beginners By John Horton, Packt Publishing, 2019
7. Android Application Development with Kotlin, by Hardik Trivedi (Author), BPB Publishing, 2020, ISBN: 978-9389423501
8. Pro Android with Kotlin Developing Modern Mobile Apps with Kotlin and Jetpack,By Peter Spath 2022, Apress, ISBN 9781484287446
9. Mastering Android Studio: A Beginner's Guide, Sufyan bin Uzayr, CRC Press, 2022, ISBN: 9781000537703

1361

10. Kotlin for Android Development - Creating Efficient and Elegant Apps By Daniel Melehi 2023, Publisher:Amazon Digital Services LLC - Kdp ISBN: 9798393937867
11. Android Programming The Big Nerd Ranch Guide, By Bryan Sills, Brian Gardner, Kristin Marsicano, Chris Stewart, Publisher: Addison Wesley Professional, 2022, ISBN: 9780137645541

1362

CTBTCSE SVII P6 EL4: Physics of Semiconductor Devices

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs					
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To impart the basic concepts & Functional understanding of semiconductor devices
2. Foundations of device modelling & Engineering.
3. To understand concepts of common use for converting a physical parameter into an electrical quantity.
4. Learning of p-n junction and contact potentials.
5. To learn Field Effect Transistors like, MOSFET, MOS capacitor

Unit-I
Semiconductor

Semiconductors: Energy Band and Charge Carriers: Energy bands in semiconductors, Types of semiconductors, Charge carriers, Intrinsic and extrinsic materials. Carrier concentration: Fermi Level, Electron and hole concentration equilibrium, Temperature dependence of carrier concentration, Compensation, and charge neutrality.

Unit-II
Transport Characteristics

Conductivity and mobility, Effect of temperature, Doping and high electric field, carrier generation, Carrier lifetime, diffusion length, Direct and indirect recombination and trapping, Diffusion of carriers, Einstein relation, Continuity equation, Carrier injection, Diffusion length. Haynes-Shockley experiment.

Unit-III
Junction

p-n junction and contact potential, Fermi levels, Space charge, Reverse and Forward bias, Zener and Avalanche breakdown. Capacitance of p-n junction, Schottky barriers; Schottky barrier height, C-V characteristics, current flow across Schottky barrier: thermionic emission, Rectifying contact and Ohmic contact.

Unit-IV

Bi-polar Junction Transistors

Fundamentals of BJT operation. Minority carrier distribution, Solution of diffusion equation in base region, Terminal current, Current transfer ratio, Ebers-Moll equations, Charge control analysis. BJT switching: Cut off, Saturation, Switching cycle.

Unit -V

Field Effect Transistors

MOSFET, Operation, MOS capacitor, Debye screening length, Effect of real surfaces; Work function difference, Interface charge, Threshold voltage and its control, MOS C-V analysis and time dependent capacitance. Output and transfer characteristics of MOSFET.

Reference Books:

1. Streetman, B. and Banerjee, S., Solid State Electronics, Prentice Hall India, (2006).
2. Tyagi, M.S., Introduction to semiconductor materials and devices, John Wiley, (2000).
3. Mishra, Umesh K. and Singh, Jaspreet, Semiconductor Device Physics and Design, Springer, (2008).
4. Semiconductor physics and Devices, Third edition (Tata-Mcgraw Hill), by Donald Neamen.

1364

CTBTCSE SVII L1: Vulnerability Analysis & Web Application Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1365

CTBTCSE SVII L2: Artificial Intelligence Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1366

CTBTCSE SVII L3: Information and Network Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1367

CTBTCSE SVII L4 EL1: Research Methodology Part-1 Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

7368

CTBTCSE SVII L4 EL2: Digital Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1369

CTBTCSE SVII L4 EL3: Android Development Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1370

CTBTCSE SVII L4 EL4: Physics of Semiconductor Devices Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1371

SEMESTER – VIII

1372

CTBTCSE SVIII P1: Mobile Phone Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. Understanding the Architecture of the Mobile Devices Operating Systems like Android.
2. Understanding the security concepts of the Mobile Devices and its OS.
3. Learning reverse engineering of android applications.
4. Learning Traffic Interception of android for penetration testing.
5. Learning the Android Application Security Testing and Auditing.

Unit –I

Introduction Android Security

Introduction to Android, Android's Architecture, Android Run Time, Android Application Framework, Introduction to Android Application component, Sandboxing, Android application inter-process communication, Application permission, Android boot process, Android partitions, File systems.

Unit – II

Android Application Pen-Testing

Configuration of lab using Santoku or Kali Linux or Mobexler or Android Studio or GenY motion, ADB commands, Configuration vulnerable application, Open GApps Project, need of ARM Translator, Mobile application security pen-testing strategy, Android application vulnerability exploitation : Insecure login, hard core issues, insecure data storage issue, input validation issues, access control issues, content provider leakage, path traversal Client-side injection attacks or other latest vulnerability or latest OWASP top 10 vulnerabilities.

1373

Unit – III

Reverse Engineering and Secure Source Code Review

Reverse engineering using APKTool, JADX, JD-GUI, Hex Dump, Dex Dump, Reversing and Auditing Android Apps: Android application teardown and secure source code review.

Unit-IV

Android Application Security Auditing and Pen-Testing

Security auditing using Drozer, MobSF (Mobile Security Framework): Static and Dynamic Analysis, Android application security vulnerability assessment using QARK, Android dynamic instrumentation using Frida and Objection framework. Introduction to Xposed is a framework.

Unit-V

Request Interception and traffic analysis

Traffic Analysis for Android Devices, Android traffic interception, Ways to analyse Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception, Other ways to intercept SSL traffic.

Reference Books

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov, No Starch Press Publication (2015).
2. Android Hacker's Handbook by Joshua J. Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A. Ridley, Collin Mulliner, Wiley Publication (2014).
3. Learning Pentesting for Android Devices by Aditya Gupta, Packt Publication (2014).
4. Android Apps Security Mitigate Hacking Attacks and Security Breaches by Sheran Gunasekera, Apress Publication (2020).
5. The Mobile Application Hacker's Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, Wiley Publication (2015).

2374

CTBTCSE SVIII P2: Malware Analysis

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. To understand about malware and its types.
2. To understand the internals of windows OS.
3. To learn details of PE file and its structure.
4. To learn various tools related to malware analysis.
5. To learn hands-on exercise of basic static and dynamic analysis techniques.

UNIT – I
Windows System Architecture, Process, Jobs and Threads

Overview of Windows system architecture: Windows Portability on Hardware, Symmetric Multiprocessing, Virtualization based security architecture, Environment subsystems and subsystem Dlls, Windows executive, Device drivers, System Process; Creation of a process: Process Internals, Protected Process, Flow of CreateProcess, Terminating Process, Image Loader, DLL name resolution and redirection, API sets; Jobs: Various types of Jobs, Windows Containers; Introduction to Threads and its internals.

UNIT – II
Windows Portable Executable (PE) File Internals

General Concept, PE Structure; PE Headers: MS-DOS Stub, Signature, COFF and optional header; Section Table, Other content of PE file: relocation, symbol, strings and certificate; Various Special Sections of PE File, Archive (Library) File Format, Import Library Format, Calcuating Authenticode PE Image Hash.

UNIT – III
Malware

What is Malware, Various Types of Malwares and its History: Virus, Worm, Trojan, Botnet, Spyware, Rootkits, Adware, Logic Bomb, Time Bomb, Ransomware, Multi-faceted/Polymorphic Malwares, Advanced Persistent Threats; The Goals of malware

1375

analysis, Various Malware Analysis Techniques and its Pros & Cons: Basis Static, Basic Dynamic, Advanced Static, Advanced Dynamic.

UNIT – IV
Basic Static Analysis

Static Analysis: Hashing, Finding Strings, Decoding Obfuscated Strings Using FLOSS, PE Files Headers and Sections, PE View, Linked Libraries and Functions, Dependency Walker, CFF Explorer, Resource Hacker, Malware signature and Clam AV Virus Signature, YARA Signatures.

UNIT – V
Basic Dynamic Analysis

Dynamic Analysis: Lab Set-up with virtual machine, Sandboxes: advantages and disadvantages, set-up of sandbox for analysis, Running and Monitoring a Malware, Understanding and practical of various dynamic analysis tools: Process Monitor, Process Explorer, RegShot, faking a network, Using Wireshark for Packet Analysis.

Reference Books

1. Windows Internals Part-1: System architecture, processes, threads, memory management, and more by Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, and David A. Solomon, Microsoft Press, (2017).
2. Microsoft Portable Executable and Common Object File Format Specification (Rev. 11), Microsoft Corporation, June (2017).
3. Practical malware analysis: the hands-on guide to dissecting malicious software by Michael Sikorski and Andrew Honig, No starch press, (2012).
4. History of malware by Nikola Milošević, arXiv preprint arXiv:1302.5392 (2013).
5. Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyse and Investigate Windows Malware by Monappa K A (2018).
6. Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks by Alexey Kleymenov, Amr Thabet (2019).
7. Malware Analysis Cookbook: Tools and Techniques for Fighting Malicious Code by Matthew Richard, Blake Hartstein, Michael Hale Ligh, Steven Adair (2010).

1376

CTBTCSE SVIII P3: Incident Response Management and Threat Hunting

Teaching Scheme					EvaluationScheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
02	00	00	02	02	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand cyber incident response and its components.
2. To learn known frameworks and tools for incident response.
3. To get general knowledge of planning for incident response readiness and managing the operational aspects of the incident response team.
4. To understand fundamental of Threat Intelligence
5. To learn various Threat Intelligence Techniques

UNIT–I

Introduction to Incident Response Management

Data Classification, Events & Incidents, Overview of incident response management: What is incident response?, Incident response lifecycle, Incident types and classifications, Incident Identification - Precursors & Indicators, Incident response team roles and responsibilities, Responsibilities of the SOC Team, Incident response tools and technologies.

UNIT–II

Incident Detection and Analysis

Common attack vectors, Techniques for incident detection, Log analysis and correlation, Network traffic analysis, Endpoint monitoring and analysis, Incident response frameworks and standards: NIST Computer Security Incident Handling Guide, SANS incident response process, NIST Guide to Integrating Forensic Techniques into Incident Response, Emerging and future cyber threats.

UNIT–III

Incident Response and Mitigation

Incident triage and prioritization, Triage – concept and procedures, Principles of first response, Containment and eradication strategies, Evidence preservation

1377

and chain of custody, Incident documentation and reporting, Legal and regulatory considerations in incident response, Incident communication and coordination, Post Incident Steps.

UNIT–IV

Threat Hunting Fundamentals

Introduction to threat hunting: Exploring the different types of threat actors, Proactive vs. reactive threat hunting; Roles & Responsibilities of Threat Hunters, Introduction to Threat intelligence, Six Phases of the Threat Intelligence Lifecycle: Direction; Collection; Processing; Analysis; Dissemination, Threat hunting methodologies and frameworks, Threat hunting tools and platforms.

UNIT–V

Advanced Threat Hunting Techniques

Behavioural analysis and anomaly detection, Endpoint detection and response (EDR) solutions, Threat hunting for cloud environments, Analytical Frameworks: The Lockheed Martin Cyber Kill Chain; The Diamond Model; The MITRE ATT&CK Framework, Threat hunting case studies and practical exercises

Reference Books

1. Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia
2. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
3. Incident Handling and Response: A Holistic approach for an efficient security incident management by Jithin Aby Alex
4. Blue Team Handbook: Incident Response Edition by Don Murdoch
5. Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques by Vinny Troia
6. Critical Incident Management: A Complete Response Guide, Second Edition by John McNall, Thomas T. Gillespie, Vincent F. Faggiano.
7. Incident Management for Operations by Chris Hawley, Rob Schnepp and Ron Vidal.
8. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence, Dr. Christopher Ahlberg, CyberEdge Press.

1378

CTBTCSE SVIII P4: PROJECT - 2

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
Th	Tu	Pr	C	TCH	Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
4	0	2	6	8	25	00:45	50	01:30	-	-	100	3:00	200

Project 2 is based on the Research and development-oriented problems of practical and theoretical interest and may be continuation of Project-1. Evaluation will be done at the end of the semester based on periodic presentations/student seminars/written reports and evaluation of the developed system.

1379

CTBTCSE SVIII P5 EL1: RESEARCH METHODOLOGY PART-2

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
Th	Tu	Pr	C	TCH	Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
2	0	0	2	2	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand advance concepts of research and its methodologies.
2. To identify appropriate research topics, problem and parameters.
3. To evaluate the proposed work and compare it with the existing work.
4. To learn how to prepare a project proposal to undertake a project or a grant.
5. To learn how to write a research report and thesis based on the research.

Unit - I

Data Modelling and Simulation

Processing Operations, Some Problems in Processing, Elements/Types of Analysis, Statistics in Research, Measures of Central Tendency, Measures of Dispersion, Measures of Asymmetry (Skewness), Measures of Relationship, Simple Regression Analysis, Multiple Correlation and Regression, Partial Correlation, Need for Sampling, Some Fundamental Definitions, Important Sampling Distributions, Central Limit Theorem, Sampling Theory, Sandler's A-test, Concept of Standard Error, Estimation, Estimating the Population Mean, Estimating Population Proportion, Sample Size and its Determination.

Unit - II

Testing of Hypotheses

What is a Hypothesis?, Basic Concepts Concerning Testing of Hypotheses, Procedure for Hypothesis Testing, Flow Diagram for Hypothesis Testing, Measuring the Power of a Hypothesis Test, Tests of Hypotheses, Important Parametric Tests, Hypothesis Testing of Means, Hypothesis Testing for Differences between Means, Hypothesis Testing for Comparing Two Related Samples, Hypothesis Testing of Proportions, Hypothesis Testing for Difference between Proportions, Chi-square Test

1380

Unit - III

Thesis Writing, Project Proposal Writing

Types of research report: Dissertation and thesis, research paper, review article, short communication, conference presentation, meeting report etc. Practice on Research writing tool such as Latex. Structure and organization of research reports: Title, abstract, key words, introduction, methodology, results, discussion, conclusion, acknowledgement, references, footnotes, tables and illustrations. Use of reference managing softwares (such asMENDELEY, ENDNOTE). Impact factor, rating, indexing and citation of journals, Project cost management, Funding agencies and research grants.

Unit - IV

Research Ethics

Research ethics, responsibility and accountability of the researchers, ethical consideration during animal experimentation including CPCSEA guidelines, Plagiarism and use of plagiarism detection software's.

Unit - V

Intellectual Property

Patents, Designs, Trade and Copyright, Process of Patenting and Development: Technological research innovation, patenting, development., International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT. Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications

References Books

1. S. K. Yadav, "Research and Publication Ethics", Springer International Publishing.
2. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
3. C. R. Kothari, "Research Methodology: Methods and Techniques", New Age International Publisher.
4. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students"
5. Shanti Bhushan Mishra and Shashi Alok, "Handbook of Research Methodology: A Compendium for Scholars & Researchers", EDUCREATION PUBLISHING.

1387

CTBTCSE SVIII P5 EL2: SOCIAL MEDIA ANALYTICS

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
2	0	0	2	2	25	00:45	50	01.30	100	03:00	-	-	200

Objectives

1. Learning social media and social network based online data investigations and analysis.
2. Analysing data collected with all online source intelligence like content of posts, comments, and messages for evidence of criminal activity or other relevant information.
3. Determining the activity and usage patterns of Social media and Social network content.
4. Collecting and preserving digital evidence in a forensically sound manner to be used in legal proceedings.
5. Identifying and tracking the spread of misinformation, propaganda, and other malicious content.

UNIT – I
Fundamentals of social media and social network

Emerging Trends in social media and social network, Fundamentals of social media and social network, Cyber psychology, Crimes associated with social media and social network, OPSEC fundamentals, Introduction to Application Programming Interfaces (APIs), Graph theory and its components

UNIT – II
Social Media and Social Network Legal Aspects

Social media and social network ethics, Security and privacy in social media and social network, Legal aspects of social media and social network investigation, Investigation abroad (MLAT, LoR and CrPC notices), Latest acts and laws for intermediaries and service providers, Role of service provider in social media and social network investigations, Legal aspects of breached data collection, Report writing

UNIT – III
Information Gathering from Online Resources

Web fundamentals, Search engines, Intelligence gathering, Web archive, Proxy and VPN, ASINT, online multimedia and document metadata analysis, Deep web and Darkweb investigation, Image analysis and reverse image searches, Fake news

detection and verification, Introduction to Deepfake technique, Deep learning concepts

UNIT – IV
Social media and Social network Investigations

Social media and social network data collection and analysis, Micro formats, Username search, Email search, Breach data and leaked data sources, Basics of Darkweb and Deepweb, Geolocation based investigations, Sentiment analysis, Domain and IP search, IP tracking and tracing, Forensic analysis of social network data from various smart devices and cloud storage, Case studies

UNIT – V
Advance ASINT

Practical OSINT using web services and API, OSINT VMs, Social media and social network data analysis and linkage visualization, Threat intelligence and malware intelligence, Deleted websites analysis, Website owner information, Videos uploaded by location, Newspaper archives & scans, Social content by location, GEOINT, Historical satellite imagery, Duplicate copies of photos, public government records, practical data visualization tools and technology, Introduction to cryptocurrency and its forensic case studies.

Reference Books

1. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, Nihad A Hassan, Rami Hijazi.
2. Social Network Analysis: Methods and Applications by Katherine Faust and Stanley Wasserman.
3. Deep Dive: Exploring the Real-world Value of Open Source Intelligence, Rae L. Baker.
4. Social network analysis, John Scott.
5. OSINT Techniques, By Michael Bazzell.
6. Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency, Andy Greenberg.
7. Social Network Analysis by David Knoke and Song Yang.
8. Advances in Social Network Analysis: Research in the Social and Behavioural Sciences by Joseph Galaskiewicz, Stanley Wasserman.
9. Understanding Social Networks: Theories, Concepts, and Findings by Charles Kadushin.
10. Open Source Intelligence Investigation: From Strategy to Implementation (Advanced Sciences and Technologies for Security Applications), Babak Akhgar, P. Saskia Bayerl, Fraser Sampson.

11. Dark Web Investigation (Security Informatics and Law Enforcement), by Babak Akhgar , Marco Gercke , Stefanos Vrochidis , Helen Gibson.
12. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence, Nick Furneaux.

1384

CTBTCSE SVIII P5 EL3: Internet of Things

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				Semester End Examination (SEE)		University Exams (LPW)		Total
					TA-1 & TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Marks	Marks	Hrs	Marks	Hrs.	
02	00	00	02	02	25	00:45	50	25	100	03:00	--	--	200

Objectives

1. To understand the basic concept and architecture of IoT.
2. To learn remote control of devices and equipment using IoT.
3. To understand the IoT communication and messaging protocols.
4. To understand the IoT enabling technologies & Cloud computing.
5. To learn development of IoT applications.

UNIT – I

Introduction to IoT

Definition & Characteristics of IoT; Evolution of IoT; Physical Design of IoT – IoT Components; Logical Design of IoT; IoT Levels and Deployment Techniques; IoT Applications & Domains; IoT Enabling Technologies; Challenges in IoT.

UNIT – II

Sensors, Actuators & Microcontrollers used in IoT

Types of sensors and actuators; Interfacing of sensors and actuators with microcontrollers like Arduino, ESP 8266, ESP 32 & Raspberry Pi; Arduino & Raspberry Pi: Architecture, Programming and Application Developments.

UNIT – III

IoT Communication Protocols

IoT Communication: device-to-device, device-to-gateway, gateway-to-data center, or gateway-to-cloud communication, as well as communication between data centers; Protocol Stack for IoT; Brief about IoT Communication Protocols: MQTT, AMQP, CoAP, DDS, TCP, UDP, IP, 6LoWPAN Transport protocols, RFID, & HTTP communication protocols, Bluetooth and BLE, LoRa and LoRaWAN, LPWAN , LWM2M, Zigbee, Z-wave, NFC, 5G.

1385

UNIT – IV

IoT Data Management & Cloud Computing

Introduction to Edge, Fog & Cloud computing; Service Models: IaaS, PaaS, SaaS; Cloud Deployment Models: Public, Private, Hybrid cloud; Security and Privacy in Cloud-based IoT; Case Study: Cloud-based IoT Architecture.

UNIT – V

IoT Applications, Case Studies & Emerging Trends

Generic IoT Application Architecture; Case Studies: Smart Home Automation, Industrial IoT (IIoT), Agriculture and Environmental Monitoring, Healthcare and Wearable Devices, Smart Cities and Urban Infrastructure, Transportation and Vehicle Telematics, Energy Management and Smart Grid, Retail and Supply Chain Management; Emerging Trends in IoT: AI & IoT Integration, Block chain for IoT, Quantum computing & IoT, 5G & IoT.

Reference Books

1. Internet of Things_ A Hands-On Approach by Arshdeep Bahga, Vijay Madisetti - Universities Press (India) Private Limited, 2015.
2. Practical Internet of Things Security, by Brian Russell and Drew Van Duren, 2016.
3. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, by Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, 1st Edition, Academic Press, 2014.
4. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017.
5. 21 IoT Experiments, Yashavant Kanetkar, Shrirang Korde, BPB.
6. IoT Based Projects, Rajesh Singh at el, BPB.
7. Internet of Things with ARDUINO and BOLT, Ashwin Pajankar, BPB.

1386

CTBTCSE SVIII P5 EL4: Semiconductor Hardware Design & Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				Semester End Examination (SEE)		University Exams (LPW)		Total
					TA-1 & TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Marks	Marks	Hrs	Marks	Hrs.	
02	00	00	02	02	25	00:45	50	25	100	03:00	--	--	200

Objectives:

1. To Understand Synchronous Design Methodology.
2. To develop an ability to perform basic experiments related to FPGA and VHDL
3. To develop an ability to design CMOS Circuit, logic families.
4. To understand the different attacks possible on hardware.
5. Understanding of hardware security scenarios.

UNIT- 1

CMOS VLSI Basics

System on chip (SOC) Architecture basics. Logic families, CMOS logic, Electrical behavior of CMOS circuits, CMOS steady state electrical behavior, CMOS dynamic electrical behavior, CMOS Input and Output structures, CMOS logic families, CMOS/TTL interfacing, Timing Hazards, Quine-McCluskey Method of finding Minimal SOP and POS Expressions.

UNIT-II

Synchronous Design

Bistable elements, Latches and Flip-Flops, Clocked Synchronous State-machine Analysis, Clocked Synchronous State- machine Design, Designing State Machines using State Diagrams, State-machine Synthesis using Transition Lists. Shift Registers and counters, Iterative versus Sequential Circuits.

UNIT-III

FPGA/Memories

Field Programmable Gate Arrays, Memories: Classification of Memories, Static/Dynamic memories/cells, Flash memories. Introduction to ASICS, Types o Asics, Field Programmable Arrays (FPGA's), Case studies, economics of Asics, ASIC Technologies and comparative analysis, ASIC cell Libraries.

7387

UNIT -IV

Hardware and Side Channel Attacks

Hardware Attacks: Hardware Trojans, Trojans in FPGA, trust benchmarks, countermeasures against hardware Trojans, design of hardware Trojan attack. Side Channel Attacks: Background, Power Analysis Attacks, Electromagnetic Side-Channel Attacks, Fault Injection Attacks, Timing Attacks, Covert channels, experimental design of side channel attacks.

UNIT-V

Hardware Security & Design Implementation

Hardware Security Primitives: Physical Unclonable Function (PUFs), True Random Number Generator hardware, Primitive Designs with Emerging Nanodevices, experimental design, Pre-silicon Security and Trust Assessment for SoCs, Post-silicon Security and Trust Assessment for ICs, design for security. Hardware Description Language & Design Implementation: Implementing the combinational & Sequential design with Verilog.

Reference Books:

1. Digital Design: Principles & Practices-John F. Wakerly (4th edition, Prentice Hall).
2. Digital Design with an Introduction to the Verilog HDL, VHDL, and SystemVerilog, Sixth Edition, By Michael D. Ciletti and M. Morris Mano, Pearson.
3. Basic VLSI Design by Douglas A. Pucknell, PHI.
4. Application Specific Integrated Circuits by Sebastian & Smith (Addison Wesley/Pearson Education).
5. CMOS Digital Integrated Circuits Analysis & Design by Kang and Yusuf Leblebici.

1388

CTBTCSE SVIII L1: Mobile Phone Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

7389

CTBTCSE SVIII L2: Malware Analysis Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

CTBTCSE SVIII L3: Incident Response Management and Threat Hunting Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

CTBTCSE SVIII L4 EL1: Research Methodology Part-2 Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
0	0	1	1	02	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1392

CTBTCSE SVIII L4 EL2: Social Media Analytics Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1393

CTBTCSE SVIII L4 EL3: Internet of Things Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1394

CTBTCSE SVIII L4 EL4: Semiconductor Hardware Design & Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1395

SEMESTER – IX

1396

CTMTCSE SIX P1: Blockchain Technology and Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To learn Crypto-currency and hashing.
2. To understand the concept of Blockchain.
3. To learn various Use-Cases of Blockchain.
4. To understand fundamentals of Blockchain Security.
5. To learn various Blockchain Security Techniques.

UNIT–I

Introduction to Cryptography and Cryptocurrencies

Introduction, Cryptography, Hash Function, Hash Pointers and One-Way Functions, Data Structures, Digital Signatures – ECDSA, Memory Hard Algorithm, Zero Knowledge Proof, Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Memory Hard Algorithm – Hashcash Implementation, Direct Acyclic Graph, Introduction to Quantum Computing and How it will break existing methods

UNIT-II

Blockchain

Introduction, Advantages over Conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain Application, Soft & Hard Fork, Private and Public Blockchain

UNIT–III

Distributed Consensus

Nakamoto Consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy Utilization, Alternate Smart Contract Construction

7397

UNIT–IV

Cryptocurrency

History, Distributed Ledger, Bitcoin Protocols – Mining Strategy and Rewards, Ethereum Construction, Gas Limit, DAO, Smart Contract, GHOST, Vulnerabilities, Attacks, Sidechain, Name coin, Case Study related to – Naïve Blockchain Construction, Play with Go-Ethereum, Toy Application using Blockchain

UNIT-V

Cryptocurrency Regulation

Stakeholders, Roots of Bitcoin, Legal Aspects-Cryptocurrency Exchange, Black Market and Global Economy, Applications: Internet of Things, Medical Record Management System, Domain Name Service and Future of Blockchain, Case study related to Mining Puzzles

Reference Books

1. Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton University Press, 2016 by Arvind Marayan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder.
2. Bitcoin and Blockchain Security by Elli Androulaki and Ghassan Karame
3. Blockchain Cybersecurity, Trust and Privacy by Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo
4. Blockchain for Cyber Security and Privacy: Architectures, Challenges and Applications by Mamoun Alazab, Yassine Maleh, Mohammad Shojafar, Imed Romdhani
5. The Truth Machine: The Blockchain and the Future of Everything by Michael Casey and Paul Vigna
6. Blockchain for Distributed Systems Security by Laurent L. Njilla, Charles Kamhoua and Sachin Shetty
7. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
8. The Age of Cryptocurrency by Paul Vigna and Michael Casey
9. The Basics of Bitcoins and Blockchains by Antony Lewis
10. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

1398

CTMTCSE SIX P2: MAJOR PROJECT - 1

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
-	-	-	8	-	25	00:45	50	01:30	-	-	100	3:00	200

Major Project 1 is based on the Research and development-oriented problems of practical and theoretical interest. Evaluation will be done at the end of the semester based on periodic presentations/student seminars/written reports and evaluation of the developed system (if applicable).

1399

CTMTCSE SIX P3 EL1: Introduction to PowerShell and Shell Scripting

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. To understand the basics of shell scripting and its role in automating tasks.
2. To learn foundational concepts and commands of shell scripting
3. To learn to perform defensive security operations with shell scripting
4. To develop proficiency in PowerShell scripting for efficient data management and advanced cmdlet usage.
5. To learn advanced PowerShell scripting techniques

UNIT – I
Introduction to Shell Scripting

What Is "The Shell", Understanding the File System Tree and its Navigation, Exploring the System, Manipulating Files and Directories, Manipulating Files and Directories, I/O Redirection, Expansion, Permissions, Job Control, Configuration and The Environment, Introduction To vi, Customizing the Prompt

UNIT – II
Advance Shell Scripting

Package Management, Storage Media, Networking, Searching for Files, Archiving and Backup, Regular Expressions, Text Processing, Formatting Output, Printing, Compiling Programs. Writing Shell Scripts: Starting A Project, Top-Down Design, Flow Control: Branching With if, Reading Keyboard Input, Flow Control: Looping With while / until & for, Troubleshooting, Strings and Numbers, Arrays

UNIT – III
Defensive Security Operations with bash

Data collection: commands(cut, file, head, reg, wevtutil), Gathering Linux Log files Gathering, Windows Log files Gathering System Information, Gathering the Windows Registry, Data Processing: Processing delimited files, Processing XML,

1400

Processing JSON, Data analysis : Web Server Access Log Familiarization, Displaying Data in a Histogram, Finding Uniqueness in Data, Identifying Anomalies in Data, Network Monitoring, Filesystem monitoring, Script Obfuscation

UNIT – IV
Introduction to PowerShell Scripting

Overview PowerShell, Environment Setup, PowerShell Integrated Script Environment (ISE), Working with PowerShell scripts, cmdlets, files and folders, dates and timers, file I/O, Advanced Cmdlets, PowerShell Scripting: special variables, operators, looping, conditions, array, hash tables, regex, blackets, alias, WMIC & PowerShell. PowerShell providers and drives, $Args variable, param statement, Passing data by value and by reference

UNIT – V
Advance PowerShell Scripting

PowerShell Advanced Functions, Using PowerShell remoting capabilities: emoting concepts Invoking remote commands, processing output, Objects in Windows PowerShell: Error handling concepts, terminating and non- terminating errors, Handling errors using $?, $Error and $lastExitCode variables, Error Record object anatomy, Working with textual files : Saving information into textual and csv files, Reading information from textual and csv files, Example implementation of error handling code.

Reference Books

1. The linux command line: A Complete introduction by William E. Shotts Jr.
2. Cyber security Ops with bash: Attack, Defend, and Analyze from the Command Line by Paul Troncone and Carl Albing, O'reilly
3. Mastering PowerShell Scripting - Fourth Edition: Automate and manage your environment using PowerShell by Chris Dent

1401

CTMTCSE SIX P3 EL2: Advance Digital Forensics

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand architecture and working of Memory.
2. To Learn about Various Artefacts of Memory.
3. To Understand Windows and Linux Memory Analysis.
4. To Understand various Anti-Forensics Techniques.
5. To get Acquainted with the Emerging Domains of Computer Forensics.

UNIT – I

Introduction to Memory Forensics

Introduction to Primary Storage, Understanding Random Access Memory (RAM) and It's Working, Memory Management, Hibernation. Direct Memory Access (DMA). Address Space, Registers, Segmentation, Paging, Address Translation, Physical Address Extension, Virtual Memory, Demand Paging, Shared Memory, Stacks and Heaps, Privilege Separation, System Calls. Important Artefacts in Memory, Challenges involved in Memory Forensics, Live v/s Dead Forensics.

UNIT – II

Windows Memory Forensics

Acquiring RAM Dump from Windows Machines, Analyzing Windows RAM dump using Open-Source Tools. Understanding Windows Objects and Pool Allocation. Analyzing Processes, Handles, DLLs, Registry, Event Logs, Network Communications Disk Artefacts and Other Important Artefacts. Understanding Event Reconstruction and Timeline, Introduction to Analysis of Memory to Investigate Windows Malware

UNIT – III

Linux Memory Forensics

Understanding ELF Files, Shared Library, Global Offset Table, Procedure Linkage Table, Linux Address Translation. Acquiring RAM Dump from Linux Machines, Analyzing Linux RAM dump using Open-Source Tools. Analyzing Processes, Command-line Arguments, Handles, Bash History, Network Communications, Disk / Filesystem Artefacts and Other Important Artefacts. Understanding Event

14 02

Reconstruction and Timeline. Introduction to Analysis of Memory to Investigate Linux Malware

UNIT – IV

Handling Anti-Forensic Techniques

Introduction to Cryptography, Encryption Types, Handling Encrypted Evidences, Introduction to Steganography, Handling Stego Content, Detecting Log and Timestamp Manipulations, Analyzing Anonymous Browsers and Communications, Investigating Pluggable Devices and Applications, Detecting Wiping Tools, Identifying Important Artefacts to Support use of Anti-Forensic Techniques / Tools.

UNIT – V

Emerging Domains of Computer Forensics

Introduction to Chip-Off and JTAG. Investigating Containers and Virtual Machines Investigating Cryptocurrencies and Dark web Related Cases using Computer Forensics. Using Artificial Intelligence based Solutions for Effective Forensic Investigation of Computers. Other Emerging Challenges and Domains Related to Computer Forensics.

Reference Books

1. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, et al.
2. The little handbook of Windows Memory Analysis: Just some thoughts about Memory, Forensics and Volatility! by Andrea Fortuna
3. Introduction to Modern Cryptography: Third Edition by Jonathan Katz and Yehuda Lindell
4. Applied Cryptography: Protocols, Algorithms and Source Code in C 20th Edition by Bruce Schneider
5. Codes, Ciphers, Steganography & Secret Messages by Sunil Tanna
6. Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition by Frank Y. Shih
7. Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments 1st Edition by Diane Barrett and Greg Kipper
8. Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defense 1st Edition by Nihad Ahmad Hassan, Rami Hijazi
9. Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols 1st Edition by Michael T. Raggo and Chet Hosmer

1403

CTMTCSE SIX P3 EL3: Risk Management and Contingency Planning

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs					
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand risk management fundamentals
2. To learn risk assessment techniques and apply security controls and services.
3. To develop skills in risk mitigation, evaluation, and reporting.
4. To learn threat management and security architecture
5. To develop proficiency in contingency planning and business continuity strategies.

Unit I

Introduction to Risk Management

Security evolution, Risk management to information security, Goals of risk management, Architecting a security program, Qualitative and quantitative analysis, Risk management life cycle, Vulnerability assessment VS Risk assessment

Unit II

Risk Assessment and Analysis Techniques

Risk profiling: Risk sensitivity measurements, Risk impact categorization, Formulating a risk, Qualitative Risk Measures, Risk assessment, Security controls and services: Security control principals, Assurance models, Access control models

Unit III

Risk Mitigation and Reporting

Risk Evaluation, Risk Mitigation planning, Policy Exceptions and Risk Acceptance, Risk management artifacts, Writing Audit response, Risk assessment techniques : Operational assessments, Project based assessments, Third-party assessments

Unit IV

Building and Running a Risk Management Program

Threat and Vulnerability Management: Threat identification, Advisories and Testing, Workflow, FAIR Approach, Security Risk Reviews: Assessing the state of

1404

compliance, Implementing a process, Process optimization, NIST Approach, Risk in the Development Lifecycle, Security Architecture

Unit V

Contingency Planning

Introduction to contingency planning, Contingency planning and continuity of operations, Information system contingency planning, Development of information system for contingency plan, Introduction to Business Continuity Planning (BCP), Overview of BCP Life Cycle, Need for BCP, Identifying and Selecting Business Continuity Strategies, Introduction to Disaster Recovery (DR) planning, Identification of potential disaster status, DR Strategies, Plans for Business Resumption.

References Books:

1. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up" by Evan Wheeler, SYNGRESS Elsevier
2. FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security By Stephen D. Gantz, Daniel R. Philpott, SYNGRESS, Elsevire
3. (Internal Audit and IT Audit Series) The Complete Guide to Cyber-Security Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler, 2016
4. Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman, Oxford University Press
5. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N. K. McCarthy

1405

CTMTCSE SIX P4 EL1: Advanced Malware Analysis

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To understand the x86 assembly and its importance in malware analysis.
2. To understand the process of reverse engineering and anti-reverse engineering.
3. To learn the practical of malware debugging and its memory forensics.
4. To learn common windows APIs used by various malwares.
5. To understand malware analysis for android and linux platform.

UNIT – I
Reverse Engineering

Introduction to x86 Assembly, x86 Architecture, CPU Registers, Stack, Assembly Instructions; IDA Pro with its working and features for malware analysis, Recognizing C code construction in assembly; Analyzing Malicious Windows Programs: The windows API, Windows Registry, follow executing malware; Debugging: Various levels of debugging, Using Debugger with Breakpoints, modify execution; OllyDBG: Working and Features for malware analysis; Kernel Debugging with WinDBG: Setup and working with WinDBG.

UNIT – II
Advanced Malware Analysis

Malware Behaviour: Understanding various types of malware with their use of windows internals, Covert Malware: Process Injection, Process Replacement, Hook Injection, Detours; Data Encoding: Simple Cipher, Analysis of encryption and encoding methods with tools, Decoding methods; Malware-Focused Network Signatures: Indication of malicious activity, Safely investigate an attacker online, Use of snort to create signature/rule.

UNIT – III
Anti-Reverse Engineering Techniques

Anti-Disassembly: Understanding Anti-Disassembly, Types of disassembly, Various techniques of disassembly; Anti-Debugging: Various methods of debugger detection, Identify debugger behaviour; Anti-Virtual Machine Techniques: VMWare artefacts, Vulnerable instructions, Anti-VM x86 instructions; Packers and Unpacking: Packer

Anatomy, Types of packers, Well-known packers, Identification of packed programs, Automated Packing, Manual packing.

UNIT – IV
Malware Forensics

Volatile Data examination from Windows and Linux System: Understanding process, threads, ports, handles etc. Identifying services and drivers, determining scheduled tasks, Discovering and extracting malware and Associated Artifacts from windows and Linux system.

UNIT – V
Linux & Android Malware Analysis

Types of Linux Malware, Understanding ELF file structure, system calls, Common behaviour of linux malware: delivery and persistence of malware; Static and Dynamic analysis; Android Architecture, Android Internals, Types of Android Malware, Reverse Engineering of APK, Static Analysis with Permission, API Calls, Broadcast Receiver, Intents, Behavioral Analysis, Working with Sandbox and Emulator.

Reference Books:

1. Practical malware analysis: the hands-on guide to dissecting malicious software by Michael Sikorski and Andrew Honig, No starch press, (2012).
2. History of malware by Nikola Milošević, arXiv preprint arXiv:1302.5392 (2013).
3. Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyse and Investigate Windows Malware by Monappa K A (2018).
4. Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks by Alexey Kleymenov, Amr Thabet (2019).
5. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware by Abhijit Mohanta and Anoop Saldanha (2020).
6. Malware Analysis Cookbook: Tools and Techniques for Fighting Malicious Code by Matthew Richard, Blake Hartstein, Michael Hale Ligh, Steven Adair (2010).

1407

CTMTCSE SIX P4 EL2: Internet of Things Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				Semester End Examination (SEE)		University Exams (LPW)		
					TA-1 & TA-2		MSE		Marks	Hrs	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Marks					
03	00	00	03	03	25	00:45	50	25	100	03:00	--	--	200

Objectives

1. To understand the fundamental concepts of Internet of Things (IoT) security.
2. To explore the challenges and threats associated with IoT security.
3. To learn about different security mechanisms, various tools and techniques used for IoT Security.
4. To learn Vulnerability Assessment & Penetration Testing of IoT devices.
5. To understand standards and guidelines along with best practices and future scope of research for IoT security.

UNIT – I
Introduction to IoT Security

Overview of IoT Security: Importance, requirements & issues of IoT Security; IoT Security architecture; IoT Security threats & challenges; Algorithms used for implementing IoT Security; Privacy and Data Protection in IoT.

UNIT – II
Securing IoT Devices, IoT Networks and IoT Architecture

IoT Security classifications; IoT communication patterns; Event & Data Processing; IoT Attack Vectors & Vulnerabilities; Threat Modeling in IoT; Advanced IoT threats: Devices, Networks, Infrastructure; IoT Cloud Security Architecture; Trust and Trust models for IoT; IoT Device Authentication and Authorization; Secure Bootstrapping and Provisioning; Secure Firmware and Software Updates; IoT Device Integrity and Tamper Resistance; Network Security for IoT: Firewalls, Intrusion Detection Systems (IDS), Virtual Private Networks (VPNs), etc.; IoT Malware and Botnets; Case Study.

Unit – III
IoT Communication Security

Data Encryption algorithms; Secure Communication Protocols: SSL/TLS, DTLS, IPSec; Secure MQTT, CoAP, and HTTP Protocols.

1408

UNIT – IV
IoT Security Assessment and Testing

IoT Pen testing Approaches; Understanding OWASP Top 10 for IoT; Vulnerability Assessment and Penetration Testing for IoT; Security Auditing and Compliance in IoT; Risk Management in IoT Security; Incident Response and Handling in IoT; Ethical and Legal Aspects of IoT Security

UNIT – V
IoT Security Standards, IoT Forensics & Future Trends

IoT Security Standards; IoT Security Best Practice Solution; Introduction to IoT Forensics; Tools & Techniques used in IoT Forensics; Forensic Investigation of IoT devices & components; Case Studies; Security of Industrial IoT (IIoT) Systems; Artificial Intelligence (AI) in IoT Security; Block chain for IoT Security; Privacy-Preserving Techniques in IoT; Quantum Computing and IoT Security.

Reference Books

1. Internet of Things_ A Hands-On Approach by Arshdeep Bahga, Vijay Madisetti - Universities Press (India) Private Limited (2015)
2. A Beginner's Guide to Internet of Things Security-Attacks, Applications, Authentication, and Fundamentals - by B. B. Gupta (Author), Aakanksha Tiwari (Author) - CRC Press (2020).
3. IoT Penetration Testing Cookbook_ Identify vulnerabilities and secure your smart devices – by Aaron Guzman, Aditya Gupta - Packt Publishing (2017)
4. Practical IoT Hacking_ The Definitive Guide to Attacking the Internet of Things by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods - No Starch Press (2021)
5. Practical Internet of Things Security, by Brian Russell and Drew Van Duren, 2016.
6. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, by Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, 1st Edition, Academic Press, 2014.
7. Securing the Internet of Things, by Shancang Li and Li Da Xu, Elsevier, 2017
8. Digital Forensic Investigation of Internet of Thing Devices, Reza Montasari, Hamid Jahankhani, Richard Hill, Simon Parkinson, Springer; 1st ed. 2021 edition

1409

CTMTCSE SIX P4 EL3: SCADA Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				Semester End Examination (SEE)		University Exams (LPW)		Total
					TA-1 & TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Marks	Marks	Hrs	Marks	Hrs.	
03	00	00	03	03	25	00:45	50	25	100	03:00	--	--	200

Objectives

1. To understand the concept of ICS/SCADA and Critical Infrastructure.
2. To learn the difference between IT and OT.
3. To learn various protocols of ICS/SCADA and programming of PLC.
4. To understand the vulnerabilities of OT verticals.
5. To learn various security standards of ICS/SCADA.

UNIT - I

Introduction to SCADA system

History of Critical Infrastructure Directives, SCADA System Evolution, Definitions, and Basic Architecture, SCADA System Architecture, Components of SCADA, SCADA Applications, SCADA System Security Issues Overview, SCADA System Desirable Properties, Employment of SCADA Systems (Petroleum Refining, Nuclear Power Generation, Conventional Electric Power Generation, Petroleum Wellhead Pump Control, Water Purification System, Crane Control, SCADA in the Corporation, Chemical Plant, Benzene Production, Embedded Systems).

UNIT - II

Evolution of SCADA Protocols

Evolution of SCADA Protocols, Background Technologies of the SCADA Protocols (Overview of the OSI Model, Overview of the TCP/IP Model), SCADA Protocols, The Security Implications of the SCADA Protocols, Firewalls, Packet-Filtering Firewalls, Stateful Inspection Firewalls, Proxy Firewalls, Demilitarized Zone, Single Firewall DMZ, Dual Firewall DMZ, General Firewall Rules for Different Services, Virtual Private Networks.

UNIT - III

ICS Hacking (Penetration Testing) Strategies

The Purpose of a Penetration Test, Black Box, White Box, Gray Box, Special Considerations: ICS Penetration Testing Is Not IT Penetration Testing, Setting Up a Lab, Sampling "Like", Configured Systems,Virtualization, Equipment, Rules of Engagement, Using Risk Scenarios, ICS Penetration-Testing Strategies: Reconnaissance ("Footprinting"), External Testing, Pivoting, Thinking Outside of the Network: Asymmetric and Alternative Attack Vectors, Internal Testing: On the ICS Network, Hacking ICS Protocols.

UNIT - IV

Hacking ICS Devices and Applications

Exploiting Vulnerabilities in Software: Buffer Overflows, Integer Bugs, Pointer Manipulation, Exploiting Format Strings, Directory Traversal, DLL Hijacking, Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Exploiting Hard-Coded Values, Brute-Force, ICS Malware case-studies.

UNIT – V

Security Standards, Risk and Mitigation

Common ICS Cybersecurity Standards: NIST System Protection Profile for Industrial Control Systems (SPP ICS), ISA/IEC 62443 (formerly ISA-99), etc. Special ICS Risk Factors: CIA Triad, Defense-in-Depth, Safety, General ICS Risk Mitigation Considerations: ICS Network Considerations, ICS Host-Based Considerations, ICS Physical Access Considerations. Exploits, Threats, and Vulnerabilities: Eliminating Exploits, Eliminating Threats, Eliminating Vulnerabilities, Additional ICS Risk Mitigation Considerations: System Integration Issues, Compliance vs. Security, Insurance, Honeypots, The Risk Mitigation Process: Integrating the Risk Assessment Steps, Integrating the Risk Scenarios, performing a Cost-Benefit Analysis, Establishing the Risk Mitigation Strategy.

Reference Books:

1. An Architecture for SCADA Network Forensics, Tim Kilpatrick M.S., Jesus Gonzalez Ph.D., Rodrigo Chandia Ph.D., Mauricio Papa, SujeetShenoi
2. Handbook of SCADA/Control Systems Security, Robert Radvanovsky, Jacob Brodsky.
3. Ronald L. Krutz, "Securing SCADA Systems",Wiley Publication, Inc.
4. Clint Bodungen, Kyle Wilhoit, Aaron Shbeeb, Stephen Hilt, Bryan Singer, "Hacking Exposed: Industrial Control Systems", Tata McGraw Hill

CTMTCSE SIX L1: Blockchain Technology and Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1412

CTMTCSE SIX L2 EL1: Introduction To Powershell and Shell Scripting Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1413

CTMTCSE SIX L2 EL2: Advance Digital Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

I414

CTMTCSE SIX L2 EL3: Risk Management And Contingency Planning Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course.

1415

CTMTCSE SIX L3 EL1: Advanced Malware Analysis Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1476

CTMTCSE SIX L3 EL2: Internet of Things Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
Th	Tu	Pr	C	TCH	TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
					Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-	-	-	-	100	3:00	100

Experiments to support the associated theory course

1477

CTMTCSE SIX L3 EL3: SCADA Security Laboratory

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
0	0	1	1	2	-	-	-		-	-	100	3:00	100

Experiments to support the associated theory course

1418

SEMESTER – X

1419-A

CTMTCSE SX P1 - Industrial Training / Internship & Major Project-2

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
					Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs.	Marks	Hrs.	
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.					
-	-	-	20	-	25	00:45	50	01:30	-	-	100	3:00	200

In continuation of Major Project 1 at the end of the semester the students are expected to submit a final report and there will be a viva (or other forms of evaluation) based on the periodic presentations/student seminars/written reports and evaluation of the developed system (if applicable).