JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech. in CYBER FORENSICS & INFORMATION SECURITY / CYBER SECURITY
EFFECTIVE FROM ACADEMIC YEAR 2017- 18 ADMITTED BATCH

COURSE STRUCTURE AND SYLLABUS

I Semester

Category	Course Title	Int. marks	Ext. marks	L	T	P	C
PC-1	Secure Operating System	25	75	4	0	0	4
PC-2	Applied Cryptography	25	75	4	0	0	4
PC-3	Network and Wireless Security	25	75	4	0	0	4
PE-1	1. Database Security 2. Advanced Algorithms 3. Cloud Computing and Security 4. Information Systems Control And Audit	25	75	**3**	0	0	3
PE-2	1. Machine Learning 2. Web Security 3. Distributed Systems 4. Mobile Application Security	25	75	**3**	0	0	3
OE-1	***Open Elective – 1**	25	75	3	0	0	3
Laboratory I	Algorithms and Information Security Lab	25	75	0	0	3	2
Seminar I	Seminar-I	100	0	0	0	3	2
	Total	**275**	**525**	**21**	**0**	**6**	**25**

II Semester

Category	Course Title	Int. marks	Ext. marks	L	T	P	C
PC-4	IT Security-Threats and Vulnerability	25	75	4	0	0	4
PC-5	Ethical Hacking	25	75	4	0	0	4
PC-6	Computer Forensics	25	75	4	0	0	4
PE-3	1. Privacy and Security in Cyber Space 2. Cyber laws and Security Policies 3. Digital Watermarking and Steganography 4. Incident Response and Forensics	25	75	**3**	0	0	3
PE4	1. Software Security Engineering 2. IT Security Metrics 3. Intrusion Detection and Prevention Systems 4. Reverse Engineering and Malware Analysis	25	75	**3**	0	0	3
OE-2	***Open Elective – 2**	25	75	3	0	0	3
Laboratory II	Computer Forensics Tools and Ethical Hacking Lab	25	75	0	0	3	2
Seminar II	Seminar -II	100	0	0	0	3	2
	Total	**275**	**525**	**21**	**0**	**6**	**25**

III Semester

Course Title	Int. marks	Ext. marks	L	T	P	C
Technical Paper Writing	100	0	0	3	0	2
Comprehensive Viva-Voce	0	100	0	0	0	4
Project work Review II	100	0	0	0	22	8
Total	**200**	**100**	0	**3**	22	**14**

IV Semester

Course Title	Int. marks	Ext. marks	L	T	P	C
Project work Review III	100	0	0	0	24	8
Project Evaluation (Viva-Voce)	0	100	0	0	0	16
Total	**100**	**100**	**0**	**0**	**24**	**24**

***Open Elective subjects must be chosen from the list of open electives offered by OTHER departments.**

 # For Project review I, please refer 7.10 in R17 Academic Regulations.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics & Information Security/Cyber Security)

IT SECURITY – THREATS AND VULNERABILITY (PC – 4)

UNIT- 1

Information Security: Introduction, How Much of Our Daily Lives Relies on Computers, Security Truisms, Basic Security, Terminology, Cyber Ethics, The Perception of Security, Threat Model, Security Is a Multidisciplinary Topic, Security Role-Playing Characters

UNIT – II

Passwords under Attack: Introduction, Authentication Process, Password Threats, Strong Passwords, Password Management. **Email Security –** Introduction, Email Systems, Email Security and Privacy

UNIT- III

Malware The Dark Side of Software, What Is Malware?, How Do I Get Malware?, What Does Malware Do?, **Malware: Defense in Depth,** Introduction, Data Backup, Firewalls, Software Patches, Antivirus Software, User Education

Securely Surfing the World Wide Web: Introduction, Web Browser, "HTTP Secure", Web Browser History, **Online Shopping**, Consumer Decisions, Spyware and Key-Loggers, Wireless Sniffing, Scams and Phishing Websites, Misuse and Exposure of Information

UNIT - IV

Wireless Internet Security: Introduction, How Wireless Networks Work, Wireless Security Threats, Public Wi-Fi Security, Wireless Network Administration

Social Networking: Introduction, Choose Your Friends Wisely, Information Sharing, Malware and Phishing

UNIT - V

Social Engineering: Phishing for Suckers: Introduction, Social Engineering: Malware Distribution, Phishing, Detecting a Phishing URL, Application of Knowledge

Staying Safe Online: The Human Threat: Introduction, The Differences between Cyberspace and the Physical World, Consider the Context: Watch What You Say and How It Is Communicated, What You Do on the Internet Lasts Forever, Nothing Is Private, Now or in the Future, Can You Really Tell Who You Are Talking with?, Cameras and Photo Sharing, I Am a Good Person, That Would Never Happen to Me, Is There Anything I Can Do to Make the Internet a Safer Place for My Child?

TEXTBOOKS

1. Douglas Jacobson, Joseph Idziorek, “Computer Security Literacy: Staying Safe in a Digital World”, CRC Press

REFERENCES

1. Elementary Information Security, 2/e by Richard E Smith
2. Hacker Techniques, Tools, and Incident Handling, 2/e by Sean Philip Oriyano
3. Fundamentals of Information Systems Security, 3/e by David Kim & Michael G. Solomon
4. Internet Security: How to Defend Against Attackers on the Web, 2/e by Mike Harwood

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics & Information Security/Cyber Security)

ETHICAL HACKING (PC – 5)

Prerequisites:

- A course on "Operating Systems"
- A course on "Computer Networks"
- A course on "Network Security and Cryptography"

Course Objectives:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Course Outcomes:

- Gain the knowledge of the use and availability of tools to support an ethical hack
- Gain the knowledge of interpreting the results of a controlled attack
- Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
- Comprehend the dangers associated with penetration testing

UNIT - I

Introduction: Hacking Impacts, The Hacker

Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration

Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture

Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

UNIT - II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges

Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

UNIT - III

Preparing for a Hack: Technical Preparation, Managing the Engagement

Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

UNIT - IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase

Exploitation: Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT -V

Deliverable: The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation

Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

TEXT BOOK

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press

REFERENCE BOOKS

1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics & Information Security/Cyber Security)

COMPUTER FORENSICS (PC – 6)

Course Objectives:

- To understand the cyberspace.
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence.

UNIT - I :

Computer Forensics Fundamentals: Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps Taken by Computer Forensics Specialists, Who Can Use Computer Forensic Evidence?.**Types of Computer Forensics Technology :** Types of Military Computer Forensic Technology, Types of Law Enforcement Computer Forensic Technology, Types of Business Computer Forensics Technology.

UNIT- II :

Computer Forensics Evidence and Capture: Data Recovery: Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution, Case Histories. **Evidence Collection and Data Seizure:** Why Collect Evidence?, Collection Options, Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collecting and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody.

UNIT III: Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene, Computer Evidence Processing Steps, Legal Aspects of Collecting And Preserving Computer Forensic Evidence. **Computer Image Verification and Authentication :** Special Needs of Evidential Authentication, Practical Considerations, Practical Implementation.

UNIT IV: Computer Forensics Analysis: Discovery of Electronic Evidence: Electronic Document Discovery: A Powerful New Litigation Tool, **Identification of Data:** Timekeeping, Time Matters,Forensic Identification and Analysis of Technical Surveillance Devices. **Reconstructing Past Events**: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files. **Networks:** Network Forensics Scenario, A Technical Approach, Destruction of Email, Damaging Computer Evidence, International Principles Against Damaging of Computer Evidence, Tools Needed for Intrusion Response to the Destruction of Data, Incident Reporting and Contact Forms.

UNIT V: Current Computer Forensics Tools: Evaluating Computer Forensics Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating and Testing Forensics Software.

TEXT BOOKS:

1. “Computer Forensics : Computer Crime Scene Investigation”, JOHN R. VACCA, Firewall Media.
2. “Guide to Computer Forensics and Investigations” 4e, Nelson, Phillips Enfinger, Steuart, Cengage Learning.

REFERENCES:

1. “Computer Forensics and Cyber Crime”, Marjie T Britz, Pearson Education.
2. “Computer Forensics”, David Cowen, Mc Graw Hill.
3. Brian Carrier , "File System Forensic Analysis" , Addison Wesley, 2005
4. Dan Farmer & Wietse Venema ,"Forensic Discovery", Addison Wesley, 2005
5. Eoghan Casey , —Digital Evidence and Computer Crime —, Edition 3, Academic Press, 2011
6. Chris Pogue, Cory Altheide, Todd Haverkos ,Unix and Linux Forensic Analysis DVD ToolKit, Syngress Inc. , 2008
7. Harlan Carvey ,Windows Forensic Analysis DVD Toolkit, Edition 2, Syngress Inc. , 2009
8. Harlan Carvey ,Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry , Syngress Inc, Feb 2011
9. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2009
10. Gonzales/ Woods/ Eddins, Digital Image Processing using MATLAB, 2nd edition, Gatesmark Publishing, ISBN 9780982085400
11. N.Efford, Digital Image Processing, Addison Wesley 2000, ISBN 0-201-59623-7
12. M Sonka, V Hlavac and R Boyle, Image Processing, Analysis and Machine Vision, PWS
13. 1999, ISBN 0-534-95393-
14. Pratt. W.K., Digital Image Processing, John Wiley and Sons, New York, 1978

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

PRIVACY AND SECURITY IN CYBER SPACE (PE - III)

Course Objectives:

- To understand the computer security fundamentals
- To understand the integrity policies
- To understand system, user, program security issues

UNIT - I :

An Overview of Computer Security: The Basic Components, Threats, Policy and Mechanism, Assumptions and Trust, Assurance, Operational Issues, Human Issues. Security Policies: Security Policies, Types of Security Policies, The Role of Trust, Types of Access Control, Example: Academic Computer Security Policy, General University Policy, Electronic Mail Policy, Confidentiality Policies: Goals of Confidentiality Policies, The Bell-LaPadula Model, Informal Description, Example: The Data General B2 UNIX System.

UNIT - II

Integrity Policies: Goals, Biba Integrity Model, Clark-Wilson Integrity Model, The Model, Comparison with the Requirements, Comparison with Other Models, Hybrid Policies: Chinese Wall Model, Bell-LaPadula and Chinese Wall Models, Clark-Wilson and Chinese Wall Models, Clinical Information Systems Security Policy, Bell-LaPadula and Clark-Wilson Models, Originator Controlled Access Control, Role-Based Access Control.

UNIT - III :

Design Principles: Overview, Design Principles, Principle of Least Privilege, Principle of Fail-Safe Defaults, Principle of Economy of Mechanism, Principle of Complete Mediation, Principle of Open Design, Principle of Separation of Privilege, Principle of Least Common Mechanism, Principle of Psychological Acceptability.

UNIT - III :

System Security: Introduction, Policy: The Web Server System in the DMZ, The Development System, Networks: The Web Server System in the DMZ, The Development System, Users: The Web Server System in the DMZ, The Development System, Authentication: The Web Server System in the DMZ, Development Network System.

UNIT - IV :

User Security: Policy, Access: Passwords, The Login Procedure, Trusted Hosts, Leaving the System, Files and Devices: Files, File Permissions on Creation, Group Access, File Deletion, Devices, Writable Devices, Smart Terminals, Monitors and Window Systems, Processes: Copying and Moving Files, Accidentally Overwriting Files, Encryption, Cryptographic Keys, and Passwords, Start-up Settings, Limiting Privileges, Malicious Logic.

UNIT - V:

Program Security: Introduction, Common Security-Related Programming Problems, Improper Choice of Initial Protection Domain, Improper Isolation of Implementation Detail, Improper Change, Improper Naming, Improper Deallocation or Deletion, Improper Validation, Improper Indivisibility, Improper Sequencing, Improper Choice of Operand or Operation, Testing, Maintenance, and Operation.

TEXT BOOK:

1. "Introduction to Computer Security", Matt Bishop, Sathyanarayana S. Venkatramanayya, Pearson Education.

REFERENCES:

1. "Computer Security", Dieter Gollmann, Wiley India.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech- I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

CYBER LAWS AND SECURITY POLICIES (PE - III)

Course Objectives:

- To understand the computer security issues
- To make secure system planning, policies

UNIT- I

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT-II

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

UNIT-III

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT- IV

Information security: fundamentals-Employee responsibilities- information classification-
Information handling- Tools of information security- Information processing-secure program administration.

UNIT-V

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

TEXT BOOK:

1. Debby Russell and Sr. G. T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.

REFERENCES:

1. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
2. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
3. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
4. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
5. James Graham, "Cyber Security Essentials" Averbach Publication T & F Group.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

DIGITAL WATERMARKING AND STEGANOGRAPHY (PE - III)

Course Objectives:

- To learn about the watermarking models and message coding
- To learn about watermark security and authentication.
- To learn about stegnography. Perceptual models

UNIT - I

INTRODUCTION: Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems.
WATERMARKING MODELS & MESSAGE CODING: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

UNIT- II

WATERMARKING WITH SIDE INFORMATION & ANALYZING ERRORS: Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

UNIT - III

PERCEPTUAL MODELS: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients

UNIT - IV

WATERMARK SECURITY & AUTHENTICATION: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

UNIT - V

STEGANOGRAPHY: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

REFERENCES:

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Margan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, “Digital Watermarking”, Margan Kaufmann Publishers, New York, 2003.
3. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Contest Protection”, Artech House, London, 2003.
4. Juergen Seits, “Digital Watermarking for Digital Media”, IDEA Group Publisher, New York, 2005.
5. Peter Wayner, “Disappearing Cryptography – Information Hiding: Steganography & Watermarking”, Morgan Kaufmann Publishers, New York, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech- I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

INCIDENT RESPONSE AND FORENSICS (PE - III)

Course Objectives:

- To know the real world incidents
- To make a pre incident preparation
- To understand about incident detection and characterization

UNIT - I:

Real-World Incidents: What Constitutes an Incident?, What Is Incident Response?, Where We Are Now, Why Should You Care About Incident Response?, Concept of the Attack Lifecycle, IR Management Handbook: What Is a Computer Security Incident?, What Are the Goals of Incident Response?, Who Is Involved in the IR Process?, The Incident Response Process: Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information, Reporting.

UNIT - II:

Pre-Incident Preparation: Preparing the Organization for Incident Response, Identifying Risk, Policies That Promote a Successful IR, Working with Outsourced IT, Thoughts on Global Infrastructure Issues, Educating Users on Host-Based Security, Preparing the IR Team, Preparing the Infrastructure for Incident Response, Computing Device Configuration, Network Configuration.

UNIT - III:

Incident Detection and Characterization: Collecting Initial Facts, Checklists, Maintenance of Case Notes, Building an Attack Timeline, Understanding Investigative Priorities, What Are Elements of Proof?, Setting Expectations with Management, Initial Development of Leads, Defining Leads of Value, Acting on Leads, Turning Leads into Indicators, The Lifecycle of Indicator Generation, Resolving Internal Leads, Resolving External Leads.

UNIT - IV:

Data Collection: Live Data Collection, When to Perform a Live Response, Selecting a Live Response Tool, What to Collect, Live Data Collection on Microsoft Windows Systems, Prebuilt Toolkits, Do It Yourself, Memory Collection, Live Data Collection on Unix-Based Systems, Live Response Toolkits, Memory Collection.

UNIT - V:

Forensic Duplication: Forensic Image Formats, Complete Disk Image, Partition Image, Logical Image, Image Integrity, Traditional Duplication, Hardware Write Blockers, Image Creation Tools, Live System Duplication, Duplication of Enterprise Assets, Duplication of Virtual Machines.

TEXT BOOK:

1. " Incident Response and Computer Forensics", Kevin Mandia, Mathew Pepe, Jason Luttgens, 3rd Edition, McGraw-Hill Osborne Media, 2014.

REFERENCES:

1. "Handbook Computer Crime Investigation's Forensic Tools and Technology", Eoghan Casey, Academic Press.
2. "A Step-by-Step Guide to Computer Attacks and Effective Defenses", Skoudis. E., Perlman. R. Counter Hack, Prentice Hall Professional Technical Reference.
3. "Disk Detective: Secret You Must Know to Recover Information From a Computer", Norbert Zaenglein, Paladin Press.

4. “Guide to computer forensics and investigations”, Bill Nelson, Amelia Philips and Christopher Steuart, Cengage Learning.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

SOFTWARE SECURITY ENGINEERING (PE - IV)

Course Objectives:

- Students will demonstrate knowledge of the distinction between critical and non-critical systems.
- Students will demonstrate the ability to manage a project including planning, scheduling and risk assessment/management.
- Students will author a software requirements document.
- Students will demonstrate an understanding of the proper contents of a software requirements document.
- Students will author a formal specification for a software system.
- Students will demonstrate an understanding of distributed system architectures and application architectures.
- Students will demonstrate an understanding of the differences between real-time and non-real time systems.
- Students will demonstrate proficiency in rapid software development techniques.
- Students will be able to identify specific components of a software design that can be targeted for reuse.
- Students will demonstrate proficiency in software development cost estimation.
- Students will author a software testing plan.

UNIT – I

Security a software Issue: introduction, the problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of Detecting Software Security

What Makes Software Secure: Properties of Secure Software, Influencing the security properties of software, Asserting and specifying the desired security properties?

UNIT – II

Requirements Engineering for secure software: Introduction, the SQUARE process Model, Requirements elicitation and prioritization

UNIT – III

Secure Software Architecture and Design: Introduction, software security practices for architecture and design: architectural risk analysis, software security knowledge for architecture and design: security principles, security guidelines and attack patterns

Secure coding and Testing: Code analysis, Software Security testing, Security testing considerations throughput the SDLC

UNIT – IV

Security and Complexity: System Assembly Challenges: introduction, security failures, functional and attacker perspectives for security analysis, system complexity drivers and security

UNIT – V

Governance and Managing for More Secure Software: Governance and security, Adopting an enterprise software security framework, How much security is enough?, Security and project management, Maturity of Practice

TEXT BOOK:

1. Software Security Engineering: Julia H. Allen, Pearson Education

REFERNCE BOOKS:

1. Developing Secure Software: Jason Grembi, Cengage Learning
2. Software Security : Richard Sinn, Cengage Learning

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

IT SECURITY METRICS (PE - IV)

Course Objectives:

- To understand about the data and security metrics and measurements of the data
- To know about the security operations, cost and values

UNIT- I:

What Is a **Security Metric?** Metric and Measurement, Security Metrics Today, The Dissatisfying State of Security Metrics, Reassessing Our Ideas About Security Metrics. **Designing Effective Security Metrics:** Choosing Good Metrics, GQM for Better Security Metrics, More Security Uses for GQM, Summary.

UNIT- II:

Understanding Data: What are Data? Data Sources for Security Metrics; We Have Metrics and Data -Now what, Summary, Case Study 1. **The Security Process Management** Framework: Managing Security as a Business Process, the SPM Framework, Before You Begin SPM, Summary. **The Analyzing Security Metrics Data:** The Most Important Step, Analysis Tools and Techniques, Summary. **Designing the Security Measurement Project:** Before the Project Begins, Phase One: Build a Project Plan and Assemble the Team, Phase two: Gather the Metrics Data, phase Three: Analyze the Metrics Data and Build Conclusions, phase Four: Present Results, Phase Five: Reuse the Results, Project Management Tools, Summary.

UNIT- III:

Measurements **Security Operations:** Sample Metrics for Security Operations, Sample Measurement Project for Security Operations, Summary. **Measuring Compliance and Conformance:** The Challenges of Measuring Compliance, Sample Measurement Projects for Compliance and Conformance, Summary.

UNIT- IV:

Measuring Security Cost and Value: Sample Measurement Projects for Compliance and Conformance, The Importance of Data to Measuring Cost and Value, Summary. **Measuring People, Organizations, and Culture:** Sample Measurement Projects for People, Organizations, and Culture, Summary.

UNIT -V:

The Security Improvement Program: Moving from Projects to Programs, Managing Security Measurement with a Security, Requirements for a SIP, Measuring the SIP. Summary. **Learning Security: Different Contexts for Security Process Management:** Organizational Learning, Three Learning Styles for IT Security Metrics, Final Thoughts, Summary.

TEXT BOOKS:

1. IT Security Metrics, Lance Hayden, Tata Mcgraw-Hill.
2. Security Metrics, Caroline Wong, Tata Mcgraw-Hill.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech - I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

INTRUSION DETECTION AND PREVENTION SYSTEMS (PE - IV)

Course Objectives:

- To understand about the intruders.
- To know the intrusion detection and prevention policies

UNIT- I

INTRODUCTION: Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection

THEORETICAL FOUNDATIONS OF DETECTION: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

UNIT- II

ARCHITECTURE AND IMPLEMENTATION: Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture

UNIT- III

JUSTIFYING INTRUSION DETECTION: Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI)

UNIT- IV

APPLICATIONS AND TOOLS: Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security

UNIT- V

LEGAL ISSUES AND ORGANIZATIONS STANDARDS: Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

REFERENCES:

1. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
2. Carl Enrolf, Eugene Schultz, Jim Mellander, “Intrusion detection and Prevention”, McGraw Hill, 2004
3. Paul E. Proctor, “The Practical Intrusion Detection Handbook “,Prentice Hall , 2001.
4. Ankit Fadia and Mnu Zacharia, “Intrusiion Alert”, Vikas Publishing house Pvt., Ltd, 2007.
5. Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, Pearson Education, 2006.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech- I Year – II Semester (Cyber Forensics /Cyber Security & Information Security

REVERSE ENGINEERING AND MALWARE ANALYSIS (PE - IV)

UNIT - I:
BASIC ANALYSIS: Basic Static Techniques, Malware Analysis in Virtual, Machines, Basic Dynamic Analysis

UNIT - II:
ADVANCED STATIC ANALYSIS: A Crash Course in x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly
Analyzing Malicious Windows Programs

UNIT - III:
ADVANCED DYNAMIC ANALYSIS: Debugging, vi Brief Contents, Olly Dbg, Kernel Debugging with WinDbg

UNIT - IV:
MALWARE FUNCTIONALITY: Malware Behavior, Covert Malware Launching, Data Encoding, Malware-Focused Network Signatures

UNIT 5:
ANTI-REVERSE-ENGINEERING: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking

TEXTBOOKS:

1. Michael Sikorski and Andrew Honig, “Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software”, No Starch Press,2012.

REFERENCES:

1. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley, 2005.
2. Dang, Gazet, Bachaalany, “Practical Reverse Engineering”, Wiley, 2014.
3. Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition, Jones & Bartlett, 2012.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech- I Year – II Semester (Cyber Forensics /Cyber Security & Information Security)

ETHICAL HACKING LAB
PART-I

ETHICAL HACKING LAB (Indicative list of experiments)

1. Using Active and Passive Techniques for scanning Networks, Enumeration, sniffing to Enumerate Network Hosts.
2. Conducting Active and Passive Footprinting and Reconnaissance against Target.
3. Using Armitage to Attack the Network.
4. Using Metasploit to Attack a Remote System - Scanning Networks, Enumeration, Sniffers, Evading IDS, Firewalls, and Honeypots.
5. Using Malware – Dark Comet for System Hacking, Trojans and Backdoors, Viruses and Worms.
6. Using the SHARK Remote Administration Tool for System Hacking, Trojans and Backdoors, Viruses and Worms.
7. Attacking a System- Using the SYSTEM account – System Hacking, Intrusion Detection – Evading IDS, Firewalls, and Honeypots.
8. Web-Based Hacking Servers and Applications for exploitation with IPv6 – System Hacking, Denial of Service, SQL Injection – Hacking Webservers, Hacking Web Applications, SQL Injection, LaunchingaBuffer Overflow – System Hacking, Buffer Overflow.
9. Cryptography - Breaking Windows Passwords –System Hacking, Using John the Ripper to Crack Linux Passwords – System Hacking, Using Certificates to Encrypt Email–Cryptography.

COMPUTER FORENSICS TOOLS LAB
PART-I

To perform the following tasks for the lab, Internet facility and open source tools should be provided.

1. Use a Web search engine, such as Google or Yahoo!, and search for companies specializing in computer forensics. Select three and write a two-to three-page paper comparing what each company does.(Project 1-1)
2. Search the Internet for articles on computer crime prosecutions. Find at least two. Write one to two pages summarizing the two articles and identify key features of the decisions you find in your search. (Project 1-5)
3. Use a Web search engine, search for various computer forensics tools.
4. Preparing and processing of investigations. Try to examine and identify the evidences from the drives. (Project 2-1)
5. Extracting of files that have been deleted.((Project 2-4)
6. Illustrate any Data acquisition method and validate. Use an open source data acquisition tool.
7. You're investigating an internal policy violation when you find an e-mail about a serious assault for which a police report needs to be filed. What should you do? Write a two-page paper specifying who in your company you need to talk to first and what evidence must be turned over to the police.(Project 5-2)
8. Create a file on a USB drive and calculate its hash value like FTK Imager. Change the file and calculate the hash value again to compare the files.(Project 5-4)
9. Compare two files created in Microsoft Office to determine whether the files are different at the hexadecimal level. Keep a log of what you find. (Project 6-1)
10. Illustrate the analysis of forensic data.
11. Illustrate the validating of forensic data.
12. Locate and extract Image (JPEG) files with altered extensions.(Project 10-1)
13. Examine or Investigate an E-mail message.

TEXT BOOK:

1. “Computer Forensics and Investigations”, Nelson, Phillips Enfinger, Steuart, Cengage Learning.

REFERENCES:

1. Brian Carrier , "File System Forensic Analysis" , Addison Wesley, 2005
2. Dan Farmer & Wietse Venema ,"Forensic Discovery", Addison Wesley, 2005
3. Eoghan Casey , —Digital Evidence and Computer Crime —, Edition 3, Academic Press, 2011
4. Chris Pogue, Cory Altheide, Todd Haverkos ,Unix and Linux Forensic Analysis DVD ToolKit, Syngress Inc. , 2008
5. Harlan Carvey ,Windows Forensic Analysis DVD Toolkit, Edition 2, Syngress Inc. , 2009
6. Harlan Carvey ,Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry , Syngress Inc, Feb 2011
7. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2009
8. Gonzales/ Woods/ Eddins, Digital Image Processing using MATLAB, 2nd edition, Gatesmark Publishing, ISBN 9780982085400
9. N.Efford, Digital Image Processing, Addison Wesley 2000, ISBN 0-201-59623-7
10. M Sonka, V Hlavac and R Boyle, Image Processing, Analysis and Machine Vision, PWS
11. 1999, ISBN 0-534-95393-
12. Pratt.W.K., Digital Image Processing, John Wiley and Sons, New York, 1978