Course Code	Course Name	Credits
CSDLO7031	**Advanced System Security and Digital Forensics**	**4**

Course Objectives:

1. To understand cyber attacks and defence strategies.
2. To understand underlying principles of access control mechanisms.
3. To explore software vulnerabilities, attacks and protection mechanisms of wireless networks and protocols, mobile devices and web applications.
4. To develop and mitigate security management and policies.
5. To understand and explore techniques used in digital forensics.

Course Outcomes: At the end of the course learner will able to

1. Understand cyber attacks and apply access control policies and control mechanisms.
2. Identify malicious code and targeted malicious code.
3. Detect and counter threats to web applications.
4. Understand the vulnerabilities of Wi-Fi networks and explore different measures to secure wireless protocols, WLAN and VPN networks.
5. Understand the ethical and legal issues associated with cyber crimes and be able to mitigate impact of crimes with suitable policies.
6. Use different forensic tools to acquire and duplicate data from compromised systems and analyse the same.

Prerequisite: Cryptography and System Security

Module No.	Unit No.	Detailed Content	Hrs.
1	**Introduction & Access Control**		08
	1.1	Cyber-attacks, Vulnerabilities, Defence Strategies and Techniques, Authentication Methods and Protocols, Defence in Depth Strategies.	
	1.2	Access Control Policies: DAC, MAC, Multi-level Security Models: Biba Model, Bell La Padula Model, Single Sign on, Federated Identity Management.	
2	**Program & OS Security**		08
	2.1	Malicious and Non-Malicious programming errors, Targeted Malicious codes: Salami Attack, Linearization Attack, Covert Channel, Control against Program threats.	
	2.2	Operating System Security: Memory and Address protection, File Protection Mechanism, User Authentication.	
	2.3	Linux and Windows: Vulnerabilities, File System Security.	
3	**Web Application Security**		12
		OWASP, Web Security Considerations, User Authentication and Session	

		Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, Web Service Security, OAuth 2.0	
4	**Wireless Security**		08
		Wi-Fi Security, WEP, WPA, WPA-2, Mobile Device Security- Security Threats, Device Security, GSM and UMTS Security, IEEE 802.11/802.11i Wireless LAN Security, VPN Security.	
5	**Legal and Ethical issues**		06
	5.1	Cybercrime and its types, Intellectual property, Privacy, Ethical issues.	
	5.2	Protecting Programs and Data, Information and the Law, Rights of Employees and Employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security, case studies of ethics.	
6	**Digital Forensics**		10
		Introduction to Digital Forensics, Acquiring Volatile Data from Windows and Unix systems, Forensic Duplication Techniques, Analysis of forensic images using open source tools like Autopsy and SIFT, Investigating logs from Unix and windows systems, Investigating Windows Registry.	

Text Books:

1. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
2. Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education
3. Network Security and Cryptography, Bernard Menezes, Cengage Learning
4. Network Security Bible, Eric Cole, Second Edition, Wiley

Reference Books:

1. Computer Security, Dieter Gollman, Third Edition, Wiley
2. Digital Forensics by Nilakshi Jain & Kalbande, Wiley.
3. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley.
4. Cyber Security. Nina Godbole, Sunit Belapure, Wiley.

Digital references:

1. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Assessment:

Internal Assessment:

Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.

Theory Examination:

1. Question paper will comprise of total six question.
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

==========

Laboratory/ Experimental Work

 # The Experiments for this course are required to be performed and to be evaluated in CSL704: Computational Lab-1.

Lab Outcome:

Learner will able to

1. Analyze static code and program vulnerabilities using open source tools.
2. Explore and analyze network vulnerabilities using open source tools.
3. Explore and analyze different security tools to detect web application and browser vulnerabilities.
4. Explore and analyze different tools to secure wireless networks and routers, and mobile devices and perform penetration testing, and analyze its impact.
5. Understand and implement AAA using RADIUS and TACACS.
6. Explore various forensics tools in Kali Linux and use them to acquire, duplicate and analyze data and recover deleted data.

Sr. No	Description
1	Static code analysis using open source tools like RATS, Flawfinder etc.
3	Vulnerability scanning using Nessus, Nikto (Kali Linux)
4	Explore web-application vulnerabilities using open source tools like Wapiti, browser exploitation framework (BeEf), etc.
5	Detect SQL injection vulnerabilities in a website database using SQLMap
6	Performing a penetration testing using Metasploit (Kali Linux)
7	Exploring Router and VLAN security, setting up access lists using Cisco Packet tracer(student edition)
8	Exploring VPN security using Cisco Packet tracer(student edition)
9	Exploring Authentication and access control using RADIUS, TACACS and TACACS+
10	Install and use a security app on an Android mobile (e.g. Droidcrypt)
11	Explore forensics tools in Kali Linux for acquiring, analyzing and duplicating data: dd, dcfldd, foremost, scalpel, debugfs, wireshark, tcptrace, tcpflow
12	Analysis of forensic images using open source tools like Autopsy, SIFT, FKT Imager
13	Use of steganographic tools like OpenStego, to detect data hiding or unauthorized file copying

14.	Use Password cracking using tools like John the Ripper/Cain and Abel/ Ophcrack to detect weak passwords.

Reference Books:

1. Build your own Security Lab, Michael Gregg, Wiley India
2. CCNA Security, Study Guide, Tim Boyles, Sybex.
3. Web Application Hacker's Handbook, Dafydd Stuttard, Marcus Pinto, Wiley India
4. Network Infrastructure Security, Randy Waver, Dawn Weaver, Cengage Learning.
5. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley.

Digital References:

http://www.opentechinfo.com/learn-use-kali-linux/