IS-433 & 433L Security Assessment & Evaluation / Laboratory			
Credit Hours	2-1-3	**Prerequisites**	IS241

Course Learning Outcomes:

S No	CLO	Domain	Taxonomy Level	PLO
1.	Explain the basic principles and techniques of how attackers can enter computer systems.	Cognitive	1	1
2.	Analyses of data breaches and audits of information technology security	Cognitive	4	2
3.	Evaluate the strengths and weaknesses of various information technology solutions in terms of data security	Cognitive	6	3
4.	Put acquired knowledge into practice by performing ethical penetration tests and hide the intrusion	Psychomotor	4	5

Course Content:

Underlying principles and techniques associated with the cyber security practice known as penetration testing or ethical hacking. This course covers entire penetration testing process including Penetration Testing Planning and Scoping, reconnaissance and foot printing, Basic Usage of Linux and its services, Information Gathering, Port Scanning, Buffer Overflow Exploitation, Client Side Exploitation, Post Exploitation, Wireless Hacking, Password Attacks, spoofing and sniffing at system and network level, Man in the Middle Attacks, Vulnerability Assessment, Messing with Ports, Web Application Hacking, Port Scanning and Writing a Penetration Testing Report. Social Engineering Attacks, Web Security and Vulnerabilities, Denial of Service attack and mitigation, Top Ten OWASP vulnerabilities and their mitigation, Buffer Overflow Attacks, Defense and Mitigation. The course will provide the fundamental information associated with each of the methods employed and insecurities identified. In all cases, remedial techniques will be explored, the students will develop an excellent understanding of current cyber security issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam
Reference Materials:
1. Patrick Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking, 2nd Edition 2013 2. Raymond Deep, Hacking With Kali Linux: Advanced Guide on Ethical Hacking and Penetration Testing with Kali. 2019 3. Michael T. Simpson, NichollisAntil. Hands-On Ethical Hacking and Network Defense, 3rd Edition 2016 In addition there will be lecture notes and selected articles.

IS433L Security Assessment & Evaluation Laboratory Experiments
Reconnaissance and Scanning: NMap, ZenMap, Maltego
Sniffing and Spoofing: Driftnet, Ettercap, Bettercap, MACChanger, IP Spoofing, Email Spoofing
System Exploitation: Armitage
Social Engineering Attacks: SE Toolkit
System Exploitation: Metasploit Framework, Veil
Exploit Development: Payload Obfuscation, Encoding, Randomization
Post Exploitation: Backdoor factory, Intercept, Powersploit
Wireless Hacking/Cracking: WEP, WPA, WPA2, Krack
Web Exploitation: Burpsuite, SQLMap, Beef
Mobile Exploitation: Metasploit, Android payload development

IS382 Security Engineering Management					
Credit Hours:	3-0-3	**Prerequisites**	IS201		
Course Learning Outcomes:					
S No	**CLO**		**Domain**	**Taxonomy Level**	**PLO**
1.	Comprehend complex and unpredictable contexts to select security engineering		Cognitive	2	1

	management controls for an organization			
2.	Analysis of complex, incomplete or contradictory evidence/data and argue for a scheme of risk management appropriate for an organization	Cognitive	4	2
3.	Develop original and creative critical responses to the task of developing an appropriate security engineering management system/Physical Security and Safety.	Cognitive	5	3

Course Content:

Information Security Management System (ISMS) Implementation, Industry Standard bodie (NIST), Industry Standards (International Organization for Standardization (ISO) and th International Electrotechnical Commission (ISO/IEC), BSI), Organization Security Levels Organization Security Structure, Risk analysis and assessment, Information Assurance an Protection Mechanisms, Business Continuity Planning /Disaster Recovery Planning, Introduction t Incident Handling, Project Management and Initiation, Business Impact Analysis (BIA), Recover Strategies, Plan Development and Implementation, Testing, Maintenance, Awareness and Training IT Governance COBIT. Details of ISO standards for Security & Resilience (223xx series), Networ Security (18028) and Systems Security Engineering (21827) and NIST framework for Cybe Physical Systems (SP 1500-201). The OSHA Act, Standards, and Liability, OSHA WISHA Inspections, Violations, Citations, Appeals, Fire and Emergency Egress, Confined Spaces, Accider and Incident Investigation, Root Cause Analysis, Accident Prevention.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trir and Yang-Im Lee, 2014
2. Information Security Management Handbook, 6th Edition by Harold F. Tipton and Micki Krause

In addition there will be lecture notes and selected articles.