Course Specification

(Bachelor)

Course Title:	Penetration Testing and Vulnerability Analysis
Course Code:	IT465
Program:	BS IT
Department:	Information Technology
College:	College of Computer and Information Sciences
Institution:	Majmaah University
Version:	V2023
Last Revision Date:	9 May 2022

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: 3 (2 2 0)

2. Course type

A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☐Required		☒ Elective		

3. Level/year at which this course is offered: (Level 8)

4. Course general Description:

This course will focus on advanced security techniques often referred to as vulnerability analysis or network penetration testing (pen testing). Students will learn the methods, techniques, and tools to test the security of computer networks, infrastructure and applications. Topics include vulnerability analysis, methodologies, Ethical & Legal Issues, Passive & active Scanning Techniques, Malware & Viruses, Malicious Web-Based Code, Windows Hacking Techniques, Specific Attacks on Websites, SQL Script Injection, Vulnerability Scanning, Linux Hacking

5. Pre-requirements for this course (if any): **IT461**

6. Pre-requirements for this course (if any):

7. Course Main Objective(s):

To make the students to

1. Understand what pen testing is and how it's used
2. Understand Windows vulnerabilities
3. Recognize SQL injection and cross-site scripting attacks
4. Identify Linux vulnerabilities and password cracks
5. Apply general hacking technique and social engineering

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	30
2.	**Laboratory/Studio**	30
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify)**	
Total		60

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Understand general hacking technique and social engineering, Identify Linux vulnerabilities and password cracks	K1	Lecture, Lab exercises	Test, Assignments, Lab Assignments, Final and Mid exams
1.2	Identify and analyze the tools to scan and analyze malware and vulnerability in computers and network systems	S3	Lecture, Lab exercises	Test, Assignments, Lab Assignments, Final and Mid exams
...				
2.0	**Skills**			

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
2.1	Able to communicate with clarity and purpose when exchanging ideas, thoughts, opinions, knowledge, and data during written and verbal communication.	S3	Presentation, Lab viva	Assignments, Lab based Assignments, Lab Exam and Viva , Mini Project, Mid and Final Exam
2.2				
...				
3.0	**Values, autonomy, and responsibility**			
3.1	Recognize Penetration testing professional responsibilities and make vulnerability scanning reports in computing practice based on legal and ethical principles	V2	Lecture, Lab exercises	Test, Lab Assignments, Final and Mid exams
3.2				
...				

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction and Pen Test Methodologies, Vulnerability scans, Penetrationtests, Ethical and legal issues, fraud and related activities, important certifications	10
2.	Vulnerability Analysis, Assessment & Methodologies	10
3.	Passive & Active Scanning Tools & Techniques Netcraft, Shodan, Social media, Google searching, port scanning, wireshark	5
4.	Malware & Malicious Web-Based Code Type of viruses, Trojan horses, Rootkit, Simple script for virus creation	5
5.	Windows Hacking Techniques & tools Boot process, windows logs, registry, windows password hashing	5
6.	Web hacking Specific Attacks on Websites, SQL script injection	5
7.	Vulnerability Scanning & tools CVE, NIST, Packet capture, tcpdump, network scanners, Aircrack	5

8.	Linux Hacking, Shell commands, Linux firewall Linux passwords	**5**
9.	Linux hacking tricks, Boot hack and backspace hack	**10**
Total		**60**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment	Week 2, 4,8	10%
2.	Mid Term	Week 5	20%
3.	Lab based Assignments	Week 6,9	10%
4.	Final Exam	Week 11	40%
5.	Practical exam	Week 10	20%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	1. Penetration Testing Fundamentals: A Hands-On Guide toReliable Security Audits, by William EasttomPublisher: Pearson IT 2. Penetration testing A Hands-On Introduction to Hacking SanFrancisco by Georgia Weidman 3. Hands-On Penetration Testing on Windows: Unleash KaliLinux, PowerShell, and Windows debugging tools for security testing and analysis Paperback (July 30, 2018) by Phil Bramwel Packt Publishing
Supportive References	
Electronic Materials	1. https://lira.epac.to/DOCS-TECH/Hacking/Practical%20Malware%20Analysis.pdf https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classroom
Technology equipment (projector, smart board, software)	LCD Projector, Digital Forensics Lab
Other equipment (depending on the nature of the specialty)	

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Indirect (Students)	CLO Survey
Effectiveness of Students assessment	Direct (Instructor)	Quiz, Mid exam, Assignments, Exercises, Final Exam and Indirect Survey
Quality of learning resources	Convener, instructors, HOD	Regular follow ups
The extent to which CLOs have been achieved	Instructor, TA	Performance in the exam for a particular CLO(s)
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**IT COUNCIL**
REFERENCE NO.	
DATE	