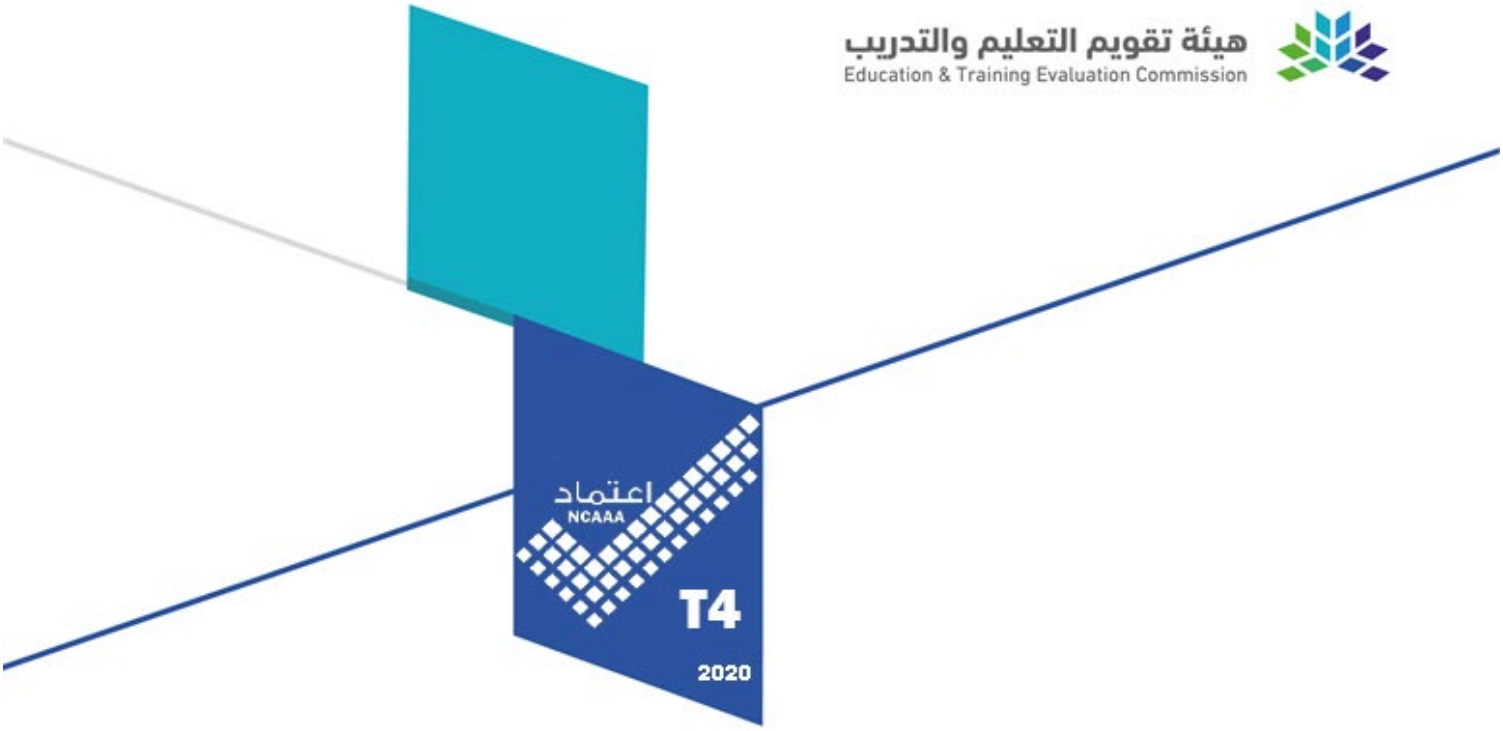

Course Specifications

Course Title:	Penetration Testing and Vulnerability Analysis
Course Code:	**IT 466**
Program:	**BS IT**
Department:	**Information Technology**
College:	**College of Computer and Information Sciences**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☐ Elective ☐
3. Level/year at which this course is offered: Level 10
4. Pre-requisites for this course (if any)**: IT461**
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	44	100
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	33
2	**Laboratory/Studio**	11
3	**Tutorial**	
4	**Others** (specify)	
	Total	44

B. Course Objectives and Learning Outcomes

1. Course 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

2. Course Main Objective

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

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	SO(4) Recognize Penetration testing professional responsibilities and make vulnerability scanning reports in computing practice based on legal and ethical principles	K1
1.2		
1.3		
1...		
2	**Skills :**	
2.1	SO(6)Identify and analyze the tools to scan and analyze malware and vulnerability in computers and network systems	S1
2.2		
2.3		
2...		
3	**Values:**	
3.1	SO(1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions	
3.2	SO(3) Communicate effectively in a variety of professional contexts	
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Introduction and Pen Test Methodologies, Vulnerability scans, Penetration tests, Ethical and legal issues, fraud and related activities, important certifications	6
2	Vulnerability Analysis, Assessment & Methodologies	4
3	Passive & Active Scanning Tools & Techniques Netcraft, Shodan, Social media, Google searching, port scanning, wireshark	6
4	Malware & Malicious Web-Based Code Type of viruses, Trojan horses, Rootkit, Simple script for virus creation	6
5	Windows Hacking Techniques & tools Boot process, windows logs, registry, windows password hashing	4
6	Web hacking Specific Attacks on Websites, SQL script injection	6
7	Vulnerability Scanning & tools CVE, NIST, Packet capture, tcpdump, network scanners, Aircrack	4
8	Linux Hacking, Shell commands, Linux firewall Linux passwords	4
9	Linux hacking tricks, Boot hack and backspace hack	4
Total		44

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	CLO-5 Apply general hacking technique and social engineering	Lecture	Direct-Quiz, Mid Term Exam, Final Exam,
2.0	**Skills**		
2.1	Identify Linux vulnerabilities and password cracks	Lecture, lab demo	Lab Assignments, CLO Survey
3.0	**Values**		
3.1	CLO-1 Understand what pen testing is and how it's used	Lecture	Quiz, Mid Term Exam, Practical exam
3.2	CLO-2. Recognize SQL injection and cross-site scripting attacks	Lecture, Tool demo	Assignment, Practical exam
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Test 1	Week 3	10%
2	Mid Term	Week 8	20%
3	Test 2	Week 9	10%
5	Practical exam	Week 10	20%
6	Final Exam	Week 11	40%
7			
8			

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

Every faculty will be assigned 10 students in the corresponding department for academic advising. Students can meet the faculty during advising hours or whenever the faculty is in the office.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	1. Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, by William EasttomPublisher: Pearson IT 2. Penetration testing A Hands-On Introduction to Hacking San Francisco by Georgia Weidman

	3. Hands-On Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows debugging tools for security testing and analysis Paperback (July 30, 2018) by Phil Bramwel Packt Publishing
Essential References Materials	
Electronic Materials	1. https://lira.epac.to/DOCS-TECH/Hacking/Practical%20Malware%20Analysis.pdf 2. https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom
Technology Resources (AV, data show, Smart Board, software, etc.)	LCD Projector, Digital Forensics Lab
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Test-1, Test-2Final Examination, Mid term exam, and Practical exam	Faculty	Direct
Survey	Students	Indirect

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	