COURSE DESCRIPTION FORM: CS-4061: Ethical Hacking Concepts and Practices

COURSE DESCRIPTION FORM

INSTITUTION   FAST School of Computing, National University of Computer and Emerging Sciences, Islamabad

PROGRAM TO BE EVALUATED   BS-CS – **Fall 2021**

Course Description

Course Code	CS-4061
Course Title	Ethical Hacking Concepts and Practices
Credit Hours	3
Prerequisites by Course(s) and Topics	
Grading Policy	Absolute grading
Policy about missed assessment items in the course	Retake of missed assessment items (other than midterm/ final exam) will not be held. For a missed midterm/ final exam, an exam retake/ pretake application along with necessary evidence are required to be submitted to the department secretary. The examination assessment and retake committee decides the exam retake/ pretake cases.
Course Plagiarism Policy	Plagiarism in project or midterm/ final exam may result in F grade in the course. Plagiarism in an assignment will result in zero marks in the whole assignments category.
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	*60% Theory 40% Practical* Assessment Items

Assessment Item	Number	Weight (%)
Assignments	4	15
Quizzes	4	10
Mid Term Exam	1	25
Project	1	10
Final Exam	1	40

Course Instructors	Mr. Zeeshan Qaiser
Lab Instructors (if any)	
Course Coordinator	Mr. Zeeshan Qaiser
URL (if any)	
Current Catalog Description	The course aims to familiarize the students with ethical hacking concepts using hands-on approach and techniques. The course focuses on using different operating system to test the vulnerabilities in the system, network and applications. This course also focuses on

getting familiarization of hacker's mindset i.e. exploit the system in a test case in order to avoid any potential breach in real. The course will be covering all the ethical hacking modules including information gathering, scanning, exploitation, covering tracks and reporting. The course also covers sub modules including OWASP top 10 vulnerabilities, Metasploit, man in the middle. All the topics are covered using hands-on approach. The students (group of 2-3) will be given a practical task in which students will be performing all the steps they learnt to test a scenario and later on will present in the last 3 classes of the semester.

Textbook (or **Laboratory Manual** for Laboratory Courses)	James Broad, Andrew Bindner, "Penetration Testing with Kali Linux" 1st Edition, Elsevier.
Reference Material	Certified Ethical Hacking Guide" Version 9 or 10

Course Learning Outcomes

A. Course Learning Outcomes (CLOs)

After completion of the course, the students shall be able to:

1. Define concepts of ethical hacking and terminologies
2. Setup the machines and can configure the testing and vulnerable environments
3. Test System, network, web and mobile platform by applying all ethical hacking steps.
4. Make professional reports of all the assessment and penetration testing

B. Program Learning Outcomes

1. Computing Knowledge	Apply knowledge of mathematics, natural sciences, computing fundamentals, and a computing specialization to the solution of complex computing problems.	✔
2. Problem Analysis	Identify, formulate, research literature, and analyze complex computing problems, reaching substantiated conclusions using first principles of mathematics, natural sciences, and computing sciences.	✔
3. Design/ Develop Solutions	Design solutions for complex computing problems and design systems, components, and processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal, and environmental considerations.	
4. Investigation & Experimentation	Conduct investigation of complex computing problems using research based knowledge and research based methods.	✔
5. Modern Tool Usage	Create, select, and apply appropriate techniques, resources and modern computing tools, including prediction and modelling for complex computing problems.	✔
6. Society Responsibility	Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal, and cultural issues relevant to context of complex	✔

	computing problems.	
7. Environment and Sustainability	Understand and evaluate sustainability and impact of professional computing work in the solution of complex computing problems.	
8. Ethics	Apply ethical principles and commit to professional ethics and responsibilities and norms of computing practice.	✔
9. Individual and Team Work	Function effectively as an individual, and as a member or leader in diverse teams and in multi-disciplinary settings.	✔
10. Communication	Communicate effectively on complex computing activities with the computing community and with society at large.	✔
11. Project Management and Finance	Demonstrate knowledge and understanding of management principles and economic decision making and apply these to one's own work as a member or a team.	✔
12. Life Long Learning	Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological changes.	✔

C. Mapping of CLOs on PLOs
(CLO: Course Learning Outcome, PLOs: Program Learning Outcomes)

		PLOs											
		1	2	3	4	5	6	7	8	9	10	11	12
CLOs	1	✔					✔		✔		✔	✔	✔
	2		✔	✔		✔				✔			✔
	3	✔	✔		✔	✔						✔	
	4	✔	✔	✔		✔			✔	✔	✔		

Topics covered in the course with number of lectures on each topic
(assume 15 weeks of instruction and 1.5 hour lecture duration)

Topics to be covered:

List of Topics	No. of Weeks	Contact Hours	CLO(s)
Introduction and basic terminologies regarding ethical hacking	1	3	1
Stages of Ethical Hacking, Hacker Classes, Vulnerability Research, Legal Implications of Hacking, Linux environment setup, Scope of Penetration Testing, documentation techniques of penetration testing,	1	3	2

	Linux basics, Introduction to foot printing, Information gathering methodology, DNS Enumeration, Whois and ARIN Lookups, Introduction to Social Engineering, Common type of social engineering attacks, Scanning phase, Vulnerability Assessment, Nessus, OpenVas, dirbuster, OwaspZap	2	6	3,4
	Nmap, NSE and Zenmap, Setup vulnerable server, DOS attacks, Malware threats, Network and OS threats, Metasploit, Armitage	3	9	3
	Hacking OS and Wireless network, MITM, sniffing, wireshark, network miner, session hijacking	2	6	2,3
	OWASP Top 10 vulnerabilities, web application testing using burp suite, hacking a web server, Maintaining Access, Clearing logs	3	9	1,2,3
	Hacking mobile platforms, Reporting, Review	2	6	3,4
	Project Presentations	1	3	1,2,3,4
	Total	15	45	

Laboratory Projects/Experiments Done in the Course	
Programming Assignments Done in the Course	

Class Time Spent (in percentage)	Theory (%)	Problem Analysis (%)	Solution Design (%)	Social and Ethical Issues (%)
	50	25	20	5

Oral and Written Communications	Every student is required to submit at least __4___ written reports of typically _5_____ pages and to make __1___ oral presentation of typically ____15___ minutes' duration.

COURSE CONTENTS

Weeks	Contents/ Topics	Courseware Events (Lab/ Case Study/ Quiz/ Assignment/ Project/ Presentation/ Research Report/ Term Paper etc.)	Comments (if any)
Week-01	Introduction and basic terminologies regarding ethical hacking		
Week-02	Stages of Ethical Hacking, Hacker Classes, Vulnerability Research, Legal Implications of Hacking, Linux environment setup, ethical hacking vs penetration testing, Scope of Penetration Testing. Black box white box, grey box Testing.		
Week-03	Phases of ethical hacking, Linux basics, Introduction to foot printing, Information gathering methodology, DNS Enumeration, Whois and ARIN Lookups, shodan, DNS enum, Wpscan, Dirbuster, Introduction to Social Engineering, Common type of social engineering attacks, phishing, vishing, smishing, pretexting, baiting, tailgating, piggybacking, Quid Pro Quo. Tools: Gophish	Assignment 1, Quiz 1	
Week-04	Setup vulnerable server, Scanning phase, Vulnerability Assessment, Nessus, Nikto, OpenVas, OwaspZap , FING		
Week-05	Open port, closed port, Filtered port, Nmap, NSE and Zenmap,	Assignment 2	
Week-06	DOS attacks, Hping Tool, Malware threats, Network and OS threats, HAK 5 Kit	Quiz 2	
Week-07	Usage of Metasploit, meterpreter, payload generation and exploit, Armitage. Project Discussion		
Week-08	Hacking OS and Wireless network, Routersploit	Assignment 3	
Week-09	MITM, sniffing, Wireshark, network miner, session hijacking	Quiz 3	
Week-10	OWASP Top 10 vulnerabilities version 2013 and 2017		
Week-11	Web application testing using, SQLmap, XSSER, burp suite	Assignment 4	
Week-12	Hacking a web server, Maintaining Access, Clearing logs	Quiz 4	
Week-13	Hacking mobile platforms, payload generation and encoding. Setting up L3mon and msfvenom		
Week-14	Making a professional report, Review, Introduction to Bug Bounty		
Week-15	Project Presentation		