Uka Tarsadia University

B. Tech.

Semester VI

VULNERABILITY ASSESSMENT AND PENETRATION TESTING
CY5011

Effective from June-2023

Syllabus version: 1.00

Subject Code	Subject Title	Teaching Scheme			
		Hours		Credits	
		Theory	Practical	Theory	Practical
CY5011	Vulnerability Assessment and Penetration Testing	3	2	3	1

Subject Code	Subject Title	Theory Examination Marks		Practical Examination Marks	Total Marks
		Internal	External	CIE	
CY5011	Vulnerability Assessment and Penetration Testing	40	60	50	150

Objectives of the course:

- Understand BackTrack for penetration testing, target scoping, information gathering, and vulnerability assessment using advanced tools.
- Learn ethical hacking principles, recognize vulnerabilities like SQL injection and buffer overflows, and defend against various cyber threats.

Course outcomes:

Upon completion of the course, the student shall be able to,

CO1: Understand the basics the basic concepts of BackTrack and utilize BackTrack for penetration testing.

CO2: Excel in target scoping, information gathering, and vulnerability assessment, with proficiency in tools like the Social Engineering Toolkit and Common User Passwords Profiler.

CO3: Skilled in finding vulnerabilities and using advanced tools and learn how to elevate privileges by attacking passwords and using network tools.

CO4: Proficient in maintaining access through protocol tunneling and proxies and learn documentation and prepare reports, including verification, presentation, and post-testing procedures.

CO5: Understand ethical hacking, its terminology, and legal aspects, recognize different hacking technologies, and learn hacker classifications.

CO6: Identify vulnerabilities like SQL injection and buffer overflows, and defending against password hacks and wireless attacks.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction to BackTrack and Penetration Testing Methodologies:** Beginning with BackTrack– BackTrackpurpose, Getting BackTrack, Using BackTrack, Configuring network connection, UpdatingBackTrack, CustomizingBackTrack, Penetration testing methodologies – Typesof penetration testing, Vulnerability assessment versus penetration testing, Security testing methodologies, BackTrack testing methodology.	6
	Unit – II	
2	**Penetration Testers Armory:** Target scoping, Information gathering, Target discovery, Enumerating target, Vulnerability mapping, Social engineering – Modeling human psychology, Attack process, Attack methods, Social Engineering Toolkit (SET), Common User Passwords Profiler (CUPP).	8
	Unit – III	
3	**Target Exploitation:** Vulnerabilityresearch, Vulnerability and exploit repositories, Advanced exploitation toolkit. **Privilege Escalation:** Attackingthe password, Network sniffers, Network spoofing tools.	8
	Unit – IV	
4	**Maintaining Access**: Protocol tunneling, Proxy, End-to-end connection. **Documentation and Reporting:** Documentation and results verification,Types of reports, Presentation, Post testing procedures.	7
	Unit – V	
5	**Introduction to Ethical Hacking, Ethics, and Legality:** Ethical hacking terminology, Identifying different types of hacking Technologies, Understanding the different phases involved in ethical, What is hacktivism? Listing different types of hacker classes, Defining the skills required to become an ethical hacker, Describing the ways to conduct ethical hacking, Understanding the legal implications of hacking.	8
	Unit – VI	
6	**Web Application Security:** Hacking Web Servers, Web application vulnerabilities, Web based	8

	password cracking techniques, SQL injection, Buffer overflows, Wireless hacking.	

Sr. No.	Software Project Management(Practicals)	Hours
1	Install BackTrack, Set up network connectivity, Customize BackTrack and update BackTrack to ensure it has the latest security tools and patches.	2
2	Understand and apply different types of penetration testing methodologies including vulnerability assessment and security testing.	2
3	Perform information gathering and target discovery.	2
4	Understand human psychology, attack processes, and methods. Familiarize with tools like Social Engineering Toolkit (SET) and Common User Passwords Profiler (CUPP).	2
5	Collect information about the target environment, including IP addresses, open ports, services, and technologies in use.	2
6	Conduct vulnerability scans using tools to identify potential weaknesses and security vulnerabilities within the target systems/applications	2
7	Study techniques for identifying and exploiting vulnerabilities in web servers.	2
8	Attempt to exploit identified vulnerabilities to assess their severity and potential impact on the target systems.	2
9	Perform social engineering tests to evaluate the susceptibility of employees to phishing attacks, pretexting, or other manipulation techniques aimed at obtaining sensitive information.	2
10	Understand terminology related to ethical hacking and cybersecurity.	2
11	Understand the methodology and best practices for conducting ethical hacking.	2
12	Conduct thorough testing of web applications for vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.	2
13	Assess the security of wireless networks by conducting wireless penetration tests andidentify weaknesses in encryption, authentication, and access control mechanisms.	2
14	Understand common vulnerabilities present in web applications and how to exploit them	2
15	Utilize tools and techniques for cracking passwords used in web applications.	2

Text books:

1. Kimberly Graves, "CEH: Official Certified Ethical Hacker Review Guide", Wiley Publishing Inc. 2007.
2. TediHeriyanto, Shakeel Ali, "Backtrack 4: Assuring Security byPenetration Testing", Shroff/Packt Publishing.

Reference books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress.
2. Ronald L. Krutz and Russell Dean Vines, "The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking", Wiley.

Course objectives and Course outcomes mapping:

- Understand BackTrack for penetration testing, target scoping, information gathering, and vulnerability assessment using advanced tools: CO1,CO2, and CO3
- Learn ethical hacking principles, recognize vulnerabilities like SQL injection and buffer overflows, and defend against various cyber threats: CO4, CO5 and CO6

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction to BackTrack and Penetration Testing Methodologies	✓					
2	Penetration Testers Armory		✓				
3	Target Exploitation and Privilege Escalation			✓			
4	Maintaining Access, Documentation and Reporting				✓		
5	Introduction to Ethical Hacking, Ethics, and Legality					✓	
6	Web Application Security						✓

Programme outcomes:

PO 1: Engineering knowledge: An ability to apply knowledge of mathematics, science, and engineering.

PO 2: Problem analysis: An ability to identify, formulates, and solves engineering problems.

PO 3: Design/development of solutions: An ability to design a system, component, or process to meet desired needs within realistic constraints.

PO 4: Conduct investigations of complex problems: An ability to use the techniques, skills, and modern engineering tools necessary for solving engineering problems.

PO 5: Modern tool usage: The broad education and understanding of new engineering techniques necessary to solve engineering problems.

PO 6: The engineer and society: Achieve professional success with an understanding and appreciation of ethical behavior, social responsibility, and diversity, both as individuals and in team environments.

PO 7: Environment and sustainability: Articulate a comprehensive world view that integrates diverse approaches to sustainability.

PO 8: Ethics: Identify and demonstrate knowledge of ethical values in non-classroom activities, such as service learning, internships, and field work.

PO 9: Individual and team work: An ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO 10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give/receive clear instructions.

PO 11: Project management and finance: An ability to demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO 12: Life-long learning: A recognition of the need for, and an ability to engage in life-long learning.

Programme outcomes and Course outcomes mapping:

Programme Outcomes	Course Outcomes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1	✓	✓	✓	✓	✓	
PO2		✓	✓			
PO3	✓	✓		✓		
PO4			✓	✓		
PO5	✓	✓	✓	✓		
PO6					✓	✓

PO7				✓	✓	
PO8					✓	✓
PO9						
PO10	✓		✓			
PO11				✓	✓	
PO12						