

Advanced Cyber Security Lab		Semester	5
Course Code	BCYL504	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		
Course objectives: ● To learn concepts of web application pen testing ● To identify and exploit vulnerabilities ● To understand the OWASP top 10 vulnerabilities and other common web security threats ● To learn concept of digital forensics			
Sl.NO	Experiments		
1	Password Cracking Objective: To understand password vulnerabilities and the importance of strong passwords Tools: Hashcat, John the Ripper		
2	Cross-Site Scripting (XSS) Objective: To learn about XSS attacks and how to mitigate them Tools: DVWA		
3	Insecure Direct Object References (IDOR) Objective: To identify and exploit IDOR vulnerabilities Tools: Burp Suite, DVWA, custom web application		
4	File Upload Vulnerabilities Objective: To understand the risks associated with file uploads Tools: DVWA, Burp Suite, a vulnerable web application		
5	Command Injection Objective: To learn how command injection attacks work Tools: DVWA, Burp Suite, custom vulnerable web application		
6	Man-in-the-Middle (MITM) Attack Objective: To understand how MITM attacks intercept and manipulate network traffic. Tools: Ettercap, Wireshark		
7	Privilege Escalation Objective: To learn techniques to escalate privileges on a compromised system Tools: Metasploit, Linux/Windows VMs with known vulnerabilities		
8	Buffer Overflow Exploitation Objective: To understand how buffer overflow vulnerabilities can be exploited Tools: Immunity Debugger, Metasploit, vulnerable application (e.g., VulnServer)		
9	XML External Entity (XXE) Injection Objective: To learn about XXE vulnerabilities and how to exploit them Tools: Burp Suite, a vulnerable XML-based application		
10	Session Hijacking and Fixation Objective: To learn how session hijacking and fixation attacks work Tools: DVWA, Burp Suite, browser developer tools		
11	Digital Forensics Objective: To learn the basics of digital forensics and evidence collection Tools: Autopsy, FTK Imager		
12	Acquisition of Mobile Data Objective: To learn the methods for acquiring data from mobile devices		

	Tools: ADB (Android Debug Bridge)
Course outcomes (Course Skill Set): At the end of the course the student will be able to: ● Design the experiment for the given problem using cyber-security tools. ● Develop the solution for the given real world cyber-security problem. ● Analyze the results and produce substantial written documentation.	
Assessment Details (both CIE and SEE) The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together Continuous Internal Evaluation (CIE): CIE marks for the practical course are 50 Marks. The split-up of CIE marks for record/ journal and test are in the ratio 60:40. ● Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session. ● Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks. ● Total marks scored by the students are scaled down to 30 marks (60% of maximum marks). ● Weightage to be given for neatness and submission of record/write-up on time. ● Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus. ● In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce. ● The suitable rubrics can be designed to evaluate each student's performance and learning ability. ● The marks scored shall be scaled down to 20 marks (40% of the maximum marks). The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.	

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.
- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

Suggested Learning Resources:

- <https://www.youtube.com/@CryptoCat>
- <http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf>
- <https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/>
- <https://blackhawkk.medium.com/cross-site-scripting-xss-dvwa-damn-vulnerable-web-applications-36808bff37b3>
- <https://medium.com/@eudorina67/dvwa-file-upload-vulnerabilities-40104b54d488>
- <https://www.youtube.com/@HackerSploit>
- <https://www.youtube.com/@NetworkChuck>
- <https://www.youtube.com/@davidbombal>
- Book: Web Penetration Testing with Kali Linux – Explore the Methods and Tools of Ethical Hacking with Kali Linux by Gilberto Najera-Gutierrez, Juned Ahmed Ansari – 2018, Third Edition, Packt Publishing
https://terrorgum.com/tfox/books/webpenetrationtestingwithkalilinux_ebook.pdf
- Book: Practical Web Penetration Testing – Secure Web Applications using Burp Suite, Nmap, Metasploit, and more by Gus Khawaja – 2018, Packt Publishing

<https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Practical%20Web%20Penetration%20Testing.pdf>

- Book: Ethical Hacking with Kali Linux – Learn Fast how to Hack like a Pro by Hugo Hoffman, 2020
<https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Ethical%20Hacking%20With%20Kali%20Linux%20Learn%20Fast%20How%20To%20Hack.pdf>