**Subject Code: 01CY0203**

**Subject Name: Web Application and Penetration Testing**

**MTech. Year – 1 (Semester – 2)**

**Objective:** The purpose is to understand Web basics and its application with methodologies and techniques used for penetrating a machine using tools.

**Credits Earned:** 4 Credits

**Course Outcomes:** After completion of this course, student will be able to

* Understand web basics and web applications
* Recognize the techniques of Web hacking
* To identify security vulnerabilities and weaknesses in the target applications
* To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
* Apply fundamental principles of problem solving in software engineering.

**Pre-requisite of course:** Network Security

**Teaching and Examination Scheme**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Teaching Scheme (Hours) | | | Credits | Theory Marks | | | Tutorial/ Practical Marks | | Total Marks |
| Theory | Tutorial | Practical | ESE (E) | Mid Sem (M) | Internal (I) | Viva (V) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents:**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | Overview of the web for penetration tester’s perspective, Understanding the concept of servers and clients, Web architectures, OWASP, Different types of vulnerabilities, Defining a web application test scope and process, Types of penetration testing. | 6 |
| 2 | Discovering the infrastructure within the application, Identifying the machines and operating systems, SSL configuration and weaknesses, learning tools to spider a website, Automate web request, Brute forcing. | 7 |
| 3 | Web app vulnerabilities and manual verification techniques. Interception proxies, Zed Attack Proxy, Burp Suite. | 8 |
| 4 | Information leakage and directory browsing, Username harvesting, Command injection, SQL injection, Blind SQL injection, Local file inclusion, Remote file inclusion. | 10 |
| 5 | Cross Site Scripting, Cross Site request forgery, Session flaws, Logic attacks, exploiting applications to steal cookies, Exploring methods to zombify browsers, Metasploit for web penetration, Sqlmap tool. | 9 |
|  | **Total Hours** | **40** |

**References:**

1. Hacking Exposed Web Applications, 3rd edition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Rich Bowen, Ken Coar, “Apache Cookbook”, O’Reilly
4. Open Web Application Security Project. A Guide to Building Secure Web Applications and Web Services. http://www.owasp.org/index.php/Category:OWASP\_Guide\_Project

**Suggested Theory distribution:**

The suggested theory distribution as per Bloom’s taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Distribution of Theory for course delivery and evaluation | | | |  |
| Remember | Understand | Apply | Analyze | Evaluate | Create |
| 5% | 10% | 15% | 30% | 20% | 30% |

**Suggested List of Experiments:**

**Instructional Method:**

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory