COURSE TITLE	**MASTERING KALI LINUX**
COURSE CODE	**01CC0404**
COURSE CREDITS	**4**

Objective:

1 The objective of this course is to provide students with a strong foundation in Kali Linux, covering its history, architecture, installation, and command-line operations to ensure confident system navigation and management. It aims to develop proficiency in essential Linux tasks such as file handling, user/group management, package installation, and basic networking. Students will also gain hands-on experience with a wide array of Kali Linux tools for information gathering, network reconnaissance, vulnerability analysis, and penetration testing of web and wireless networks. Additionally, the course focuses on building practical skills in exploiting system vulnerabilities and conducting real-world security assessments in safe environments. Basic shell scripting will also be introduced to help students automate and enhance their penetration testing workflows.

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

1 Install and configure Kali Linux in different environments

2 Perform basic Linux operations like file navigation, user management, and package handling.

3 Execute penetration testing tools for information gathering and vulnerability scanning.

4 Analyze network reconnaissance techniques and web application testing methodologies.

5 Evaluate shell scripting for automation in penetration testing.

Pre-requisite of course:1. Basic Knowledge of Coding 2. Basic Knowledge of Database Management 3. Basic Knowledge of Networking 4. Basic Knowledge if OS

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Kali Linux** Overview of Kali Linux, History and evolution of Kali Linux, Installation and setup of Kali Linux, Understanding Kali Linux architecture, Introduction to command-line interface (CLI) in Kali Linux	12
2	**Basic Operations and Tools in Kali Linux** File system navigation and management, User and group management, Package management with apt, Basic network configuration and troubleshooting, Introduction to Kali Linux tools for information gathering and reconnaissance	12

Contents : Unit	Topics	Contact Hours
3	**Advanced Operations and Penetration Testing with Kali Linux** Advanced file system operations and permissions, Networking tools and utilities in Kali Linux, Exploitation and vulnerability assessment using Kali Linux tools, Wireless penetration testing with Kali Linux, Web application penetration testing with Kali Linux tools	12
4	**Information Gathering and Network Reconnaissance** Information Gathering Methodology, Network Enumeration Techniques (DNS reconnaissance, subnet scanning, network discovery tools), Whois and Fingerprinting Techniques, Social Engineering Concepts, Footprinting Web Applications	12
5	**Introduction to Shell Scripting and Kali Linux** Overview of Shell Scripting, Introduction to Kali Linux,, Understanding the Linux command line interface, Basics of shell scripting (variables, loops, conditionals),, Writing and executing simple shell scripts,, Introduction to basic Linux commands used in shell scripting	12
Total Hours		**60**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** To understand and identify common vulnerabilities in web applications by exploring specific CVEs and testing them in a controlled environment, Tools Required: DVWA (Damn Vulnerable Web Application) OWASP ZAP (Zed Attack Proxy)	2
2	**Practical 2** To analyze the current threat landscape by researching recent web application security incidents and understanding the methods used by attackers, Tools Required: Internet access Access to CVE databases (e.g., MITRE CVE, NVD) Security news websites (e.g., Krebs on Security, The Hacker News)	2
3	**Practical 3** To perform advanced reconnaissance on a target web application to gather detailed information that can be used in further penetration testing phases., Tools Required: Nmap theHarvester Metasploit	2
4	**Practical 4** Tools Required:, Burp Suite, Browser Developer Tools (e.g., Chrome DevTools), A vulnerable web application (e.g., OWASP Juice Shop)	2
5	**Practical 5** Tools Required:, Burp Suite, A vulnerable web application (e.g., DVWA, OWASP Juice Shop)	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
6	**Practical 6** Tools Required:, Burp Suite, A vulnerable web application (e.g., OWASP Juice Shop)	2
7	**Practical 7** Tools Required, A web development environment (e.g., Visual Studio Code, Node.js, Express.js), OWASP ZAP	2
8	**Practical 8** Tools Required:, Internet access for research, CVE databases (e.g., MITRE CVE, NVD)	2
9	**Practical 9** Tools Required:, Incident response plan template, A mock web application	2
10	**Practical 10** Tools Required:, Sqlmap, Nmap	2
11	**Practical 11** Objective: Simulate brute force attacks to test authentication resilience, Tools: Hydra, Burp Suite Intruder, DVWA	2
12	**Practical 12** Objective: Analyze cookie flags, token handling, and session vulnerabilities., Tools: Burp Suite, Chrome DevTools, OWASP Juice Shop	2
13	**Practical 13** Objective: Test privilege escalation and broken access controls., Tools: Burp Suite, DVWA, OWASP Juice Shop	2
14	**Practical 14** Objective: Identify and exploit deserialization flaws leading to RCE., Tools: Burp Suite, OWASP WebGoat	2
15	**Practical 15** Objective: Identify server misconfigurations and path traversal issues., Tools: Nmap, Dirb, Burp Suite, DVWA	2
Total Hours		**30**

Textbook :

1 Exploit Database, Vijay Kumar Velu, Packt Publishing, 2017

References:

1 Kali Rolling Release, Kali Rolling Release, Glen D. Singh, Packt Publishing, 2022

Suggested Theory Distribution:

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

Distribution of Theory for course delivery

Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
10.00	10.00	50.00	15.00	15.00	0.00

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.

Supplementary Resources:

1. "TryHackMe" – https://tryhackme.com.
2. "Hack The Box (HTB Academy) "– https://academy.hackthebox.com
3. "Cybrary "– https://www.cybrary.it
4. "OWASP Top 10" – https://owasp.org/www-project-top-ten/

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)