KAMARAJ COLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institution - AFFILIATED TO ANNA UNIVERSITY, CHENNAI)

S.P.G.Chidambara Nadar - C.Nagammal Campus

S.P.G.C. Nagar, K.Vellakulam – 625 701 (Near VIRUDHUNAGAR).

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

Syllabus

Course Code	Course Name	L	T	P	C
Value Added Course	**Foundations of Ethical Hacking and Cyber Security**	**15**	**0**	**30**	**2**

Course Objectives

The course enables the students to:

- Understand the fundamentals of cybersecurity, ethical hacking, Linux operating system, and information security principles.
- Develop practical skills in Linux, networking fundamentals, and network reconnaissance using Nmap.
- Apply secure email communication techniques using GnuPG and digital signatures for protecting data confidentiality and authenticity.
- Analyze web application communication and security mechanisms using Burp Suite.
- Perform basic web vulnerability assessment using industry-standard tools and recommend suitable security mitigation techniques following ethical cybersecurity practices.

UNIT I – Introduction to Ethical Hacking and Linux Fundamentals (9)

Theory: Introduction to cybersecurity, cyber threats and attacks, ethical hacking concepts, phases of ethical hacking, types of hackers, information security principles (CIA Triad), introduction to Linux operating system, Linux file system, Linux command-line interface, file and directory management, user management, and file permissions.

Laboratory: Installation and configuration of Oracle VirtualBox and Kali Linux. Practice of Linux commands including file and directory operations, file editing, searching, compression, user management, file permissions, process management, and package installation.

Activity: Linux Command Challenge – Students perform practical tasks using Linux commands such as creating directory structures, managing files and permissions, locating files, monitoring running processes, and troubleshooting basic Linux operations.

UNIT II – Networking Fundamentals and Network Scanning using Nmap (9)

Theory: Fundamentals of computer networking, network components, OSI and TCP/IP models, IP addressing, DNS, HTTP and HTTPS protocols, introduction to network security, concepts of Denial-of-Service (DoS) attacks, network reconnaissance, Nmap architecture, host discovery, port scanning techniques, service and version detection, operating system detection, and interpretation of scan results.

Laboratory: Installation and configuration of Nmap. Performing host discovery, TCP and UDP port scanning, service and version detection, operating system detection, and basic network mapping on authorized laboratory systems.

Activity: Students perform network scanning using Nmap on an authorized laboratory network, identify active hosts and open ports, interpret scan results, and prepare a network reconnaissance report. A faculty demonstration illustrates the concept of a DoS attack and discusses preventive measures.

UNIT III – Secure Email Communication using GnuPG (9)

Theory: Fundamentals of email security, common email threats including phishing, spoofing, spam and malicious attachments, introduction to GnuPG (GNU Privacy Guard), public and private keys, key generation, encryption and decryption of files, email encryption, digital signatures, signature verification, key management, and secure communication best practices.

Laboratory: Installation and configuration of GnuPG (GPG), generation of public and private key pairs, encryption and decryption of files, creation and verification of digital signatures, secure file sharing, encryption and signing of emails, and verification of received encrypted and digitally signed emails.

Activity: Students exchange encrypted and digitally signed files and emails using GnuPG, verify authenticity and integrity, and prepare a report explaining the process of secure email communication and the advantages of digital signatures.

UNIT IV – Web Application Security using Burp Suite (9)

Theory: Introduction to web applications, client-server architecture, HTTP and HTTPS fundamentals, request-response model, authentication mechanisms, session management, cookies, security headers, input validation, secure coding principles, and overview of the OWASP Top 10 web application security risks.

Laboratory: Installation and configuration of Burp Suite Community Edition, configuring Burp Suite as an intercepting proxy, capturing and inspecting HTTP requests and responses, analyzing authentication mechanisms, session management, cookies, and HTTP security headers.

Activity: Students analyze the communication between a web browser and a web server using Burp Suite, identify authentication and session information, inspect cookies and security headers, and prepare a brief analysis report.

UNIT V – Web Vulnerability Assessment (9)

Theory: Concepts of SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), secure coding practices, input validation, vulnerability assessment methodology, vulnerability reporting, and mitigation techniques.

Laboratory: Installation and exploration of OWASP Juice Shop, identification of common web application vulnerabilities using Burp Suite, testing input validation, documenting identified vulnerabilities, and recommending appropriate mitigation strategies.

Activity: Students work in teams to perform a basic security assessment of an authorized vulnerable web application (OWASP Juice Shop). Each team identifies common vulnerabilities, prepares a vulnerability assessment report, recommends suitable mitigation measures, and presents their observations.

Software Requirements:

- Oracle VirtualBox
- Kali Linux
- Nmap
- GnuPG (GNU Privacy Guard)
- Thunderbird (or any email client supporting OpenPGP)
- Burp Suite Community Edition
- OWASP Juice Shop
- Metasploitable 2

Course Outcomes

Upon successful completion of the course, students will be able to:

CO1: Explain cybersecurity concepts, ethical hacking methodology, Linux fundamentals, and information security principles.

CO2: Apply Linux commands and networking concepts to perform network discovery and reconnaissance using Nmap.

CO3: Demonstrate secure file and email communication using GnuPG, generate and verify digital signatures, and apply secure communication practices.

CO4: Analyze HTTP communication, authentication mechanisms, cookies, sessions, and web application security using Burp Suite.

CO5: Identify common web application vulnerabilities, prepare vulnerability assessment reports, and recommend suitable mitigation techniques using ethical security practices.

CO-PO Mapping and SDG Mapping

CO - PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	H	M	-	-	M	-	-	H	-	-	-	H	M
CO2	H	H	M	M	H	-	-	M	-	-	-	H	H
CO3	H	M	M	M	H	-	-	H	-	M	-	H	H
CO4	H	H	M	H	H	-	-	H	-	M	-	H	H
CO5	H	H	H	H	H	M	M	H	M	H	M	H	H

SDG Mapping

CO's	SDG mapping with CO's	
CO1	SDG 04 - Quality Education	-
CO2	SDG 04 - Quality Education	SDG 09 - Industry, Innovation, and Infrastructure
CO3	SDG 04 - Quality Education	SDG 16 – Peace, Justice and Strong Institutions
CO4	SDG 04 - Quality Education	SDG 16 – Peace, Justice and Strong Institutions
CO5	SDG 04 - Quality Education	SDG 16 – Peace, Justice and Strong Institutions, SDG 17-Partnerships for the Goals