21CYS06	VULNERABILITY AND PENETRATION TESTING	L	T	P	C
		3	0	0	3

Course Objectives

- To think and work like an ethical penetration tester, implementing a repeatable and maturemethodology that is tailored for each assessment.
- To successfully identify vulnerabilities, score their risk, and explain mitigations with a given target.
- To responsibly disclose findings in a professional report that can be used to recreate theexploit, explain the impact to the target, and prioritize each finding.

UNIT I	INTRODUCTION TO WEB APPLICATIONS SECURITY	9 HOURS

Introduction to web applications security, threats and OWASP principles, introduction to secure design, web server: introduction a secure setup of apache, firewalling a server Browser: general concepts, functionalities, browsers war, configuration (HTTP-cookies, contents, scripting etc. attack to browsers, and users tracking/profiling (third party cookies, super cookies, XSS, CSFR, Command Injection), browser security (add-ons, plugins, same-origin policy etc.) & secure browsing.

UNIT II	THREATS AND OWASP PRINCIPLES	9 HOURS

Attacks to privacy, (spyware & backdoors, browser, email etc.) Tracking techniques: (HTTP cookies, third party cookies, browser fingerprinting, CSP) Advanced browser configuration, anonymity and onion routing (Tor). Internet E-mail: Architecture and infrastructure, functions, agents and standards, MIME & PGP, phishing, spamming & spoofing, DKIM, SPF, introduction to email forensics.

UNIT III	INTRODUCTION TO SECURE DESIGN	9 HOURS

Introduction to ethical hacking: Terminology-Five stages of hacking –Vulnerability- Research- Legal implication of hacking Impact of hacking- Foot printing & Social engineering.

UNIT IV	WEBSERVER: INTRODUCTION OF A SECURE SETUP OF APACHE	9 HOURS

Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks. Scanning & Enumeration Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting Enumeration. System Hacking Password.

UNIT V	ATTACK ON BROWSERS, AND USERS TRACKING/PROFILING	9 HOURS

Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack – Countermeasures- Cracking techniques- Key loggers- Escalating privileges- Hiding Files-Steganography technologies- Countermeasures.

UNIT VI	CASE STUDIES	

Case studies for implementing vulnerability and penetration testing

TOTAL PERIODS: 45

Course Outcomes:

At the end of the course, Students can able to

- Enumerate target hosts, domains, exposures, and attack surface.
- Identify flaws and vulnerabilities in applications, websites, networks, systems, protocols, and configurations using both manual techniques and assistive tools.
- Reverse engineer compiled applications to discover exploitable weaknesses.
- Write new exploits to test various types of vulnerabilities on clients, against servers, and to escalate privileges.

Textbooks:

1. Whitaker, A., & Newman, D. P. (2005). Penetration Testing and Network Defense: Penetration Testing _1. Cisco Press.
2. Baloch, R. (2017). Ethical hacking and penetration testing guide. CRC Press.

Reference Books:

1. Maynor, D. (2011). Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Elsevier.
2. Guzman, A., & Gupta, A. (2017). IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. Packt Publishing Ltd.