CTMTAIDS SII P2: Mobile Security and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the architecture of the mobile devices operating systems like Android.
2. To understand the security concepts of the mobile devices and its OS.
3. To learn the android application security testing and auditing.

UNIT –I

Introduction to Android, Android's Architecture, Android Run Time, Android Application Framework, Introduction to Android Application component, Sandboxing, Android application inter-process communication, Application permission, Android boot process, Android partitions, File systems.

UNIT – II

Configuration of lab using Santoku or Kali Linux or Mobexler or Android Studio or GenY motion, ADB commands, Configuration vulnerable application, Open GApps Project, need of ARM Translator, Mobile application security pen-testing strategy, Android application vulnerability exploitation : Insecure login, hard core issues, insecure data storage issue, input validation issues, access control issues, content provider leakage, path traversal Client-side injection attacks or other latest vulnerability or latest OWASP top 10 vulnerabilities.

UNIT – III

Reverse engineering using APK Tool, JADX, JD-GUI, Hex Dump, Dex Dump, Reversing and Auditing Android Apps: Android application teardown and secure source code review.

UNIT-IV

Security auditing using Drozer, MobSF (Mobile Security Framework): Static and Dynamic Analysis, Android application security vulnerability assessment using

QARK, Android dynamic instrumentation using Frida and Objection framework. Introduction to Xposed is a framework.

UNIT-V

Traffic Analysis for Android Devices, Android traffic interception, Ways to analyse Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception, other ways to intercept SSL traffic.

Reference Books

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov, No Starch Press Publication (2015).
2. Android Hacker's Handbook by Joshua J. Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A. Ridley, Collin Mulliner, Wiley Publication (2014).
3. Learning Pentesting for Android Devices by Aditya Gupta, Packt Publication (2014).
4. Android Apps Security Mitigate Hacking Attacks and Security Breaches by Sheran Gunasekera, Apress Publication (2020).
5. The Mobile Application Hacker's Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, Wiley Publication (2015).