

 SANKALCHAND PATEL UNIVERSITY ॥ अथातो ज्ञानजिज्ञासा ॥	Faculty of Engineering and Technology Master of Technology (Semester I / First year) In Effect from Academic Year 2023-24
--	--

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	IOT security and Forensics Practical
Course Code:	2ET2070104P
Pre-requisite Course:	The main objective of this practical session is that students will get the exposure to various IOT security and forensic tools.

Course Objectives:

The objective of this course is to learn and develop a comprehensive understanding of IoT systems and unique security challenges.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

Course Contents:

Unit	Details	Contact Hours
1	a. Research how to securely authenticate and authorize IoT devices on a network. b. Use these frameworks to assess the security of IoT devices and networks. c. Conduct penetration testing on IoT devices to identify vulnerabilities. d. Explore and compare existing IoT security testing frameworks (e.g., OWASP IoT Top Ten).	8
2	a. Study of Computer Forensics and different tools used for forensic b. Develop a practical demonstration of secure device registration and access control investigation using protocols like MQTT, OAuth, or X.509 certificates. c. Analyze IoT malware samples to understand their behavior and propagation methods. e. Study security challenges and solutions in edge computing environments, where IoT devices often operate.	4
3	a. Using Ghostnet tool hide a message into a picture or any image file. b. Using kgbkey logger tool record or generate an document what a user working on system c. Using pinpoint metaviewr tool extract a metadata from system or from image file. d. Using Bulk Extractor tool extract information from windows file system.	8
4	a. Backup the images file from RAM using Helix3pro tool and show the analysis. b. Using Santoku operating system shows how attackers opened various Firefox URL"s and pdf document JavaScript files and show the analysis. c. Using exiftool (-k) generate the any picture hardware and software. d. Using deft_6.1 tool recover the attacker browsing data from any computer	8

Reference Books:

1. Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom" by Lars Daniel and Larry E. Daniel
2. Digital Forensics with Kali Linux" by Shiva V. N Parasram
3. Handbook of Digital Forensics and Investigation" edited by Eoghan Casey

Course Outcomes:

At the end of the course, students will be able to:

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Students should be able to explain the components and architecture of IoT systems, including sensors, actuators, edge devices, gateways, and cloud platforms.	Understanding (2)
CO2	Students should be proficient in implementing and configuring secure communication protocols (e.g., MQTT, CoAP, HTTPS) to protect data transmission between IoT devices and servers.	Understanding (2)
CO3	Encourage students to stay updated on current research and emerging trends in IoT forensics to adapt to evolving technology.	Applying (3)
CO4	Students should understand and apply security best practices in IoT design, deployment, and maintenance to prevent future forensic challenges.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3	PS O4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				

H: High, M: Medium, L: Low