

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Critical Infrastructure Practical
Course Code:	2ET2070209P
Pre-requisite Course:	Fundamentals Of Cyber Security

Course Objectives:

Elements of Criminal Procedure Code related to forensic science and Law.

1. Identify the key research questions in the area of cyber-security of critical infrastructure
2. Apply research methods which includes survey, experiments, and articulation of research problems in this area, and methods for finding solutions to selected problems
3. Present in written and/or verbal form key findings in the specific subject area of the course from contemporary research papers.
4. Read and analyze research papers from journals and conferences in the specific subject area of the course.

Teaching and Examination Scheme:

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	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.	8
	Study of packet sniffer tools like wireshark, ethereal, tcpdump etc. Use the tools to do the following 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show that packets can be traced based on different filters.	
	Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.	
2	Detect ARP spoofing using open source tool ARPWATCH.	8
	Use the Nessus tool to scan the network for vulnerabilities.	

	Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram.	
3	Installation of rootkits and study about the variety of options.	8
	Perform an Experiment to Sniff Traffic using ARP Poisoning.	
4	Demonstrate intrusion detection system using any tool (snort or any other s/w).	8
	Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.	

Reference Books:

1. Industrial Cybersecurity: Efficiently secure critical infrastructure systems Paperback – Import, 18 October 2017 by Pascal Ackerman (Author)
2. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare Hardcover – 16 April 2015 by Thomas A. Johnson
3. Cyber Security of Critical Infrastructures Hardcover – Import, 24 December 2021 by Leandros Maglaras (Editor), Ioanna Kantzavelou (Editor), Mohamed Amine Ferrag (Editor)

Course Outcomes:

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

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	To cover the fundamentals and mathematical models in digital image and video processing.	Understanding (2)
COL2	To develop time and frequency domain techniques for image enhancement.	Understanding (2)
COL3	To expose the students to current technologies and issues in image and video processing.	Applying (3)
COL4	To develop image and video processing applications in practice.	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
CL1	H	M	M		M											
CL2	H	M			M							L				

CL3	H	M	M		M											
CL4	M	M	M		M							L				

H: High, M: Medium, L: Low