GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Engineering
Level: PG
Branch: Applied Instrumentation
Subject Code : ME02067111
Subject Name : Industrial Cyber Security

WEF Academic Year:	2024-25
Semester:	2
Category of the Course:	Professional Elective Course

Prerequisite :	None
Rationale :	In this digital age, the information and data are immense and need to be secured. The cybercrimes have increased as attackers see it as gaining big rewards. There is a need to examine the cyber-attack patterns and provide security measures for them and also need to learn the cyber laws formed to effectively act upon cybercrimes.

Course Outcome :

After Completion of the Course, Student will able to :

No	Course Outcomes	RBT Level*
01	Understanding Industrial Control Systems and Their Vulnerabilities	**RM**
02	Develop the ability to use both passive and active network discovery techniques to map and assess the infrastructure of industrial networks	**UN**
03	Development of Cyber security Risk Management Strategies for ICS	**AP**
04	Skillful Use of Metasploit for Cyber-attack Simulations	**EL**
05	Implementing Zero Trust Security Models in ICS/OT Networks	**CR**

***RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Teaching and ExaminationScheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Course Content:

Sr. No.	Course Content	No. of Hours	% of Weightage
1	**Industrial Control Systems Overview:** Describe basic industrial control systems, Ladder Logic Exercises, Discuss cyber risks to industrial control systems, Discuss a process control exploit	6	13
2	**Network Discovery and Mapping:** Employ Passive Discovery, Passive Discovery Exercises, Employ Active Discovery, Active Discovery Exercises	7	15
3	Network Defense, Detection and Analysis, Develop the requirements to manage cyber security risk, Grass Marlin Exercise, Develop safeguards to ensure delivery of critical infrastructure services, Firewall Exercise, Identify a cyber security event, Network Monitoring Exercises, Execute activities taken during and after a cyber security event, Network Forensics Exercises, Recognize current trends	8	18
4	The Exploitation Process using Metasploit, Discuss the three main stages of an attack, Describe Metasploit, Use the Metasploit Framework, Customizations to Metasploit and Kali Exercise	8	18
5	Network Attacks and Exploits, Discuss basic web hacking techniques, Describe password security, Discuss basic wireless hacking techniques, Basic Web Hacking Exercise	8	18
6	Zero Trust in ICS/OT, Define Zero Trust, Discuss the Zero Trust Maturity Model (ZTMM), Describe how Zero Trust principles can be applied to an ICS/OT Network	8	18
	Total	**45**	**100**

Reference Book :

1."Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems" by Eric D. Knapp and Raj Samani

2. "The Industrial Cyber security Professional: Securing Critical Infrastructure Systems" by Eric D. Knapp and Kevin Stine

3. "Network Security for Industrial Control Systems" by Edward R. Marsic and John J. F. McDermott.

Suggested Course Practical List :

1. Program a basic industrial control system (ICS) using Ladder Logic to automate a real-world process
2. Perform passive network discovery to map the structure and topology of an industrial network without directly interacting with the systems.
3. Conduct active network discovery to identify live hosts, services, and potential vulnerabilities in an industrial control system's network.
4. Configure a firewall to restrict access to critical infrastructure, implementing rules based on industrial cyber security policies.
5. Use Metasploit to simulate an exploit in an industrial control system, identify vulnerabilities, and assess the system's resilience.
6. Perform basic web application security testing on an industrial system's web interface, such as exploiting common web vulnerabilities
7. Assess password security in industrial control systems by using password cracking techniques
8. Conduct a wireless network assessment and attempt to exploit weaknesses in an ICS/OT wireless communication system.
9. Analyze network traffic logs to identify a cyber security event or breach in an industrial control system network and execute a proper incident response plan.
10. Set up and configure Zero Trust security policies for an industrial control system, enforcing strict identity and access management controls.

List of Laboratory/Learning Resources Required:

1. NPTEL
2. Virtual Laboratory (vlab.co.in)

* * * * * * *