GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering
Semester – III
Subject Code: 4735902
Subject Name: Incident Response and e-Discovery

Type of course: Cyber Security

Prerequisite:

- Information Security knowledge, Digital Forensics Concepts.

Rationale:

- This course will focus upon vulnerabilities identification methos within computer networks and the countermeasures that mitigate risks and damage.
- It covers prominent content on contingency planning and effective techniques that minimize downtime in an emergency, and ways to reduce losses in case of any cyber-attack.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	**UNIT-I: Introduction** Cyber Incident Detection and Response: Preparing for inevitable incident, Incident Response Goals, Need for Incident Response, Real world incidents and case studies, Incident Categorization, Low Level Incident, Middle Level Incident, High Level Incident, Incident Response Process, Pre-incident Preparation.	06	15
2	**UNIT-II:** Incident Detection and Characterization, Incident Handling, Disaster Recovery, Technologies and Impacts, Virtualization and Impacts, Estimated Cost of an Incident, Incident Reporting Organizations, Vulnerability Reports, Understanding Investigative Priorities.	06	15

3	**UNIT-III:** Discovering the scope of incident, Live Data Collection on different operating systems, Network Evidence Monitoring types and Data Analysis.	06	15
4	**UNIT-IV:** Cyber Incident Response and Recovery Implementation: Incident Detection and Plan Activation, Incident Response, Incident Response Recovery and Preventative Maintenance, Incident Response Forensics and eDiscovery, Incident Recovery: Preparation and Implementation, Business Continuity Planning and Implementation, Crisis Management and Human Factors.	06	15
5	**UNIT-V:** Vulnerability Discovery Methodologies, what is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing	06	15
6	**UNIT-VI:** Targets and Automation- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation	06	15
7	**UNIT-VII: Current Trends** Advanced Fuzzy Technologies- Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection, The topics on most recent Incident Response and Disaster Recovery developments.	04	10

Textbook:

1. Jason Luttgens, Matthew Pepe, and Kevin Mandia, Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education; 3rd Edition, (August 8, 2014). ISBN: 978-0071798686.
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni.

Reference Book:

1. Murdoch Don, 2016, “Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder”, CreateSpace Independent Publishing Platform, 2.2 Edition, ISBN: 978-1500734756
2. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Increase knowledge on potential defences and counter measures against common threat vectors/vulnerabilities.	UN
02	Gain experience using tools and common processes in performing analysis of compromised systems.	AN
03	Demonstrate how to exploit a program and different types of software exploitation techniques with the understanding of the exploit development process.	AP
04	Use their own exploits for vulnerable application to obtain current knowledge of events and tools/support kits in the subject area.	AP
05	Assess a critical evaluation and use of digital forensics technique to do incident response with an independent project.	EL

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

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform
- Coursera OOC: Cyber Incident Response Specialization (https://www.coursera.org/specializations/cyber-incident-response)

- Recently Published papers/articles in reputed journals