**CTMSDFIS S1 P3: Incident Response Management**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Teaching Scheme** | | | | | **Evaluation Scheme** | | | | | | | | |
| **Th** | **Tu** | **Pr** | **C** | **TCH** | **Theory** | | | | | | **Practical** | | **Tot al** |
| **Internal Exams** | | | | **University Exams** | | **University Exams (LPW)** | |
| **TA-1/TA-2** | | **MSE** | | **Marks** | **Hrs** | **Marks** | **Hrs** |
| **Marks** | **Hrs** | **Marks** | **Hrs** |
| 03 | 00 | 00 | 03 | 03 | 25 | 00:45 | 50 | 01:30 | 100 | 03:00 | - | - | 200 |

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

**Objectives**

1. To understand concept of Incident Response Management
2. To learn various Incident Response Management Techniques
3. To understand fundamental of Digital Forensics
4. To learn various Digital Forensics Techniques

**UNIT–I**

**Introduction to Incident Response**

Cyber Incident Statistics, Computer Security Incident, Information Warfare, Key Concepts of Information Security, Types of Computer Security Incidents, Examples of Computer Security Incidents, How to Identify an Incident, Need for Incident Response, Goals and Purpose of Incident Response, Signs of an Incident, Incident Categories

**UNIT–II**

**Incident Management**

Incident Prioritization, Use of Disaster Recovery Technologies, Impact of Virtualization on Incident Response and Handling, Estimating Cost of an Incident, Incident Reporting, Incident Reporting Organizations, Vulnerability Resources, Incident Management, Incident Response Team Roles, Incident Response Team Responsibilities, Dependencies.

**UNIT – III**

**Incident Handling**

Incident Handling Process, Real-time log capture and analysis, Botnet identification and counteraction, Enterprise Solutions for Incident Response and Recovery, Timeline Analysis, Malware Handling: Safety; Documentation; Distribution, Report Writing: Reporting Standards; Report Style and formatting; Report Content, Quality Assurance.

**UNIT–IV  
Data Collection**

When to perform a live response, selecting a live response tool, what to collect, collection best practices, live data collection on Microsoft windows systems, Live data collection on Unix-based systems, understanding network monitoring, Types of network monitoring, setting up a network monitoring system, network data analysis, collect logs generated from network events.

**UNIT–V  
Data Analysis**

Analysis methodology: Define Objectives; Where the data is stored? Outline an approach; select methods; evaluate results, investigating windows systems: NTFS and file system analysis; Prefetch; Event Logs; Scheduled tasks; the windows registry, investigating applications: What is application data; where is application data stored; general investigation methods; web browsers; email clients; instant message clients, Analysis of application data

**Reference Books**

1. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
2. Incident Handling and Response: A Holistic approach for an efficient security incident management by Jithin Aby Alex
3. Blue Team Handbook: Incident Response Edition by Don Murdoch
4. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N. K. McCarthy
5. Critical Incident Management: A Complete Response Guide, Second Edition by John McNall, Thomas T. Gillespie, Vincent F. Faggiano
6. Applied Incident Response by Steve Anson
7. Security Operations Centre – SIEM Use Cases and Cyber Threat Intelligence by Arun E Thomas
8. Incident Response & Computer Forensics by Jason T. Luttgens, Kevin Mandia and Matthew Pepe
9. Incident Management for Operations by Chris Hawley, Rob Schnepp and Ron Vidal
10. Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Modern Cyber Threats, 2nd Edition by Gerard Johansen