GUJARAT TECHNOLOGICAL UNIVERSITY

CYBER SECURITY (59)
CYBER FORENSIC AND INCIDENT RESPONSE
SUBJECT CODE: 2715904
SEMESTER: I

Type of course: Core

Prerequisite: None

Rationale: Online theft has increased in years. During an investigation of a computer security incident, the untrained system administrator, law enforcement officer, or computer security expert may accidentally destroy valuable evidence or fail to discover critical clues of unlawful or unauthorized activity. Organization has to develop an incident response capability that successfully protects its assets.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	Introduction to the Incident Response Process What Is a Computer Security Incident? ,What Are the Goals of Incident Response? ,Who Is Involved in the Incident Response Process?, Incident Response Methodology, Pre-Incident Preparation, Detection of Incidents, Initial Response, Formulate a Response Strategy, Investigate the Incident, Reporting, Resolution .	**3**	10
2	Preparing for Incident Response Overview of Pre-incident Preparation , Identifying Risk , Preparing Individual Hosts, Preparing a Network, Establishing Appropriate Policies and Procedures, creating a response toolkit Establishing an Incident Response Team	**3**	5
3	After Detection of an Incident Overview of the Initial Response Phase, Establishing an Incident Notification Procedure ,Recording the Details after Initial Detection, Incident Declaration, Assembling the CSIRT , Performing Traditional Investigative Steps , Conducting Interviews, Formulating a Response Strategy	**4**	10

4	Live Data Collection from Windows Systems and Unix Systems Creating a Response Toolkit, Storing Information Obtained during the Initial Response, Obtaining Volatile Data, Performing an In-Depth Live Response, Is Forensic Duplication Necessary?	**4**	5
5	Forensic Duplication Forensic Duplicates As Admissible Evidence, Forensic Duplication Tool	**4**	10
	Requirements, Creating a Forensic Duplicate of a Hard Drive, Creating a Qualified Forensic Duplicate of a Hard Drive		
6	Collecting Network-based Evidence What Is Network-based Evidence?, What are the goals of network monitoring?, Types of Network Monitoring, Setting Up a Network Monitoring System, Performing a Trap-and-Trace Using tcpdump for Full-Content Monitoring, Collecting Network-based Log Files	**05**	5
7	Evidence Handling What Is Evidence?, The Challenges of Evidence Handling, Overview of Evidence-Handling Procedures	**03**	5
8	Computer System Storage Fundamentals Hard Drives and Interfaces, Preparation of Hard Drive Media, Introduction to File Systems and Storage Layers	**2**	5
9	Data Analysis Techniques Preparation for Forensic Analysis, Restoring a Forensic Duplicate, Preparing a Forensic Duplication for Analysis In Linux, Reviewing Image Files with Forensic Suites, Converting a Qualified Forensic Duplicate to a Forensic Duplicate, Recovering Deleted Files on Windows Systems, Recovering Unallocated Space, Free Space, and Slack Space Generating File Lists, Preparing a Drive for String Searches	**4**	5
10	Investigating Windows Systems Where Evidence Resides on Windows Systems, Conducting a Windows Investigation, File Auditing and Theft of Information, Handling the Departing Employee	**3**	5
11	Investigating Unix Systems An Overview of the Steps in a Unix Investigation, Reviewing Pertinent Logs, Performing Keyword Searches, Reviewing Relevant Files, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships, Detecting Trojan Loadable Kernel Modules	**3**	5
12	Analyzing Network Traffic Finding Network-Based Evidence, Generating Session Data with tcptrace, Reassembling Sessions Using tcpflow, Reassembling Sessions Using Ethereal, Refining tcpdump Filters	**5**	10
13	Investigating Hacker Tools What Are the Goals of Tool Analysis?, How Files Are Compiled Static Analysis of a Hacker Tool, Dynamic Analysis of a Hacker Tool	**3**	5
14	Investigating Routers Obtaining Volatile Data Prior to Powering Down, Finding the Proof, Using Routers as Response Tools	**2**	5
15	Writing Computer Forensic Reports What Is a Computer Forensics Report?, Report Writing Guidelines, A Template for Computer Forensic Reports	**2**	10

Reference Books:

1) Incident response and computer forensics, Kevin Mandia,Chris Prosise and Matt Pepe, McGraw-Hill/Osborne
2) Guide to Computer Forensics and Investigations, Bill Nelson Amelia Phillips, Christopher Steuart, Cengage Learning

Course Outcome:

After learning the course the students should be able to:

1) Investigate theft of digital data.
2) Find footprints and generate alerts for online investigation.
3) Write incidence response report.

List of Experiments:

1. Write a program to create checksum.
2. Implement tools - Netcat, Cryptcat
3. Implement tools - lsof and netstat and analyze the importance of tools during initial response?
4. Write a program to capture session data.
5. Write a program to perform forensic analysis of a Windows system and a Unix system.
6. Implement Snort.
7. Implement Wireshark.
8. Use a tool to acquire USB drive.
9. Write a program to find Digital hash.
10. Compare two files created through text editor to determine whether the files are different at the hexadecimal level. Create a log file. How to locate date and time in the metadata of a file?
11. Write a program to perform bit-shifting on a file. Also write a program to restore the file.

Design based Problems (DP)/Open Ended Problem:

1) Develop new utility that can be used for forensic backups. Design the guidelines to validate this tool before it can be added to cyber forensic toolset.

Major Equipment:

Computer systems having following minimum technical configurations
Processor:i3 or i5 or higher
RAM : minimum 4 GB
HDD : 1 TB
LAN of All computer Systems
Internet and wifi connectivity
Licence Window/Linux operating system
Open Source Network tools Snort, wireshark, Etheral, Netcat, NMAP, CyptCat,WireShark **List of Open Source Software/learning website:**

1) https://www.edx.org/course/computer-forensics-ritx-cyber502x 2) https://cyberforensics.tech.purdue.edu

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website.