GUJARAT TECHNOLOGICAL UNIVERSITY

Syllabus for Master of Computer Applications, 4th Semester
Subject Name: Cyber Security & Forensic (CSF)
Subject Code: 4649309

With effective from academic year 2018-19

1. Learning Objectives:

- To understand the major concepts of Cyber Security and Forensics and to create the awareness through simple practical tips and tricks and to educate the students to learn how to avoid becoming victims of cyber crime
- To understand the major concepts of Cyber Security and Forensics and to create the awareness through simple practical tips and tricks and to educate the students to learn how to avoid becoming victims of cyber-crimes.
- The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security.
- To gain experience of doing independent study and research in the field of cyber security and cyber forensics.

2. Prerequisites:

Basic fundamental knowledge of Networking, Web Application, Mobile Application and Relational Database Management System

3. Contents

Unit	Course Content	Weightage Percentage
Unit I	**UNIT- I: Introduction to Cybercrime:** Introduction, Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Newsgroup Spam/Crimes from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses , Software Piracy, Password Sniffing, Credit Card Frauds and Identity Theft. Cyber offenses: How Criminals Plan that attack, Categories of Cybercrime, How Criminals Plan the Attacks: Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector and Cloud Computing.	**15%**
Unit II	**Cybercrime: Mobile and Wireless Devices** Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era and Laptops.	**10%**
Unit III	**Tools and Methods Used in Cybercrime** Introduction, Proxy Servers and Anonymizers, Phishing, Password	**25%**

	Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft): Types of Identity Theft, Techniques of ID Theft, Identity Theft- Countermeasures, How to Protect your Online Identity.	
Unit IV	**Cybercrimes and Cybersecurity: The Legal Perspectives** Introduction, Why Do We Need Cyberlaws: The Indian Context, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act , Amendments to the Indian IT Act, Cybercrime and Punishment, Cyberlaw, Technology and Students: Indian Scenario.	**10%**
Unit V	**Understanding Computer Forensics** Introduction, Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence, Forensics Analysis of E-Mail : RFC282, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing and Antiforensics.	**25%**
Unit VI	**Forensics of Hand-Held Devices** Introduction, Hand-Held Devices and Digital Forensics, Toolkits for Hand-Held Device Forensics: EnCase, Device Seizure and PDA Seizure, Palm DD, Forensics Card Reader, Cell Seizure, MOBILedit!, ForensicSIM, Organizational Guidelines on Cell Phone Forensics: Hand- Held Forensics as the Specialty Domain in Crime Context .	**15%**

4. Text Book:

1) Nina Godbole, Sunit Belpure, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley, 2011

5. Reference Books:

1) Dafydd Stuttard , The Web Application Hacker′s Handbook: Finding and Exploiting Security Flaws Paperback – Wiley, 2nd Edition, .
2) Wade Alcorn , Christian Frichot, Michele Orru, , The Browser Hacker's Handbook Book, WIley

3) James Graham, Richar Howard,Ryan Olson, "Cyber Security Essentials", CRC Press, Tailor and Francis Group, 2011
4) Robert Jones, "Internet Forensics: Using Digital Evidence to Solve Computer Crime",
5) O'Reilly Media, October, 2005
6) Chad Steel, "Windows Forensics: The field guide for conducting corporate computer investigations", Wiley India Publications, December, 2006
7) Nelson Phillips, Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
8) Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
9) Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.

Practical/ Tools:

1) Mike Shema, Anti-Hacker Tool Kit (Indian Edition), Mc Graw Hill.
2) Christian Martorella , Learning Python Web Penetration Testing,PAKT
3) Vijay Kumar Velu , Mastering Kali Linux for Advanced Penetration Testing, PAKT, Book 2017
4) Nipun Jaswal, Mastering Metasploit,: Take your penetration testing and IT security skills to a whole new level with the secrets of Metasploit, 3rd Edition Paperback – Import, 28 May 2018 by
5) Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Web Penetration Testing with Kali Linux - PAKT, Third Edition February 2018

6. Chapter Wise Coverage from Text Book:

Unit	Book#	Topics
I	1	1.1 to 1.5, 2.1 to 2.8
II	1	3.1 to 3.12
III	1	4.1 to 4.12 , 5.1, 5.2, 5.3
IV	1	6.1, 6.3, 6.4, 6.5, 6.6, 6.8, 6.9, 6.10
V	1	7.1 to 7.14, 7.16, 7.17, 7.18, 7.19
VI	1	8.1, 8.3, 8.4, 8.8

Additional Topics:

Cybercrime: Illustrations, Examples and Mini-Cases, Scams
(Only for the referential context should not be asked in the examination)

Real-Life Examples:

Example 1: Official Website of Maharashtra Government Hacked
Example 2: E-Mail Spoofing Instances
Example 3: I Love You Melissa – Come Meet Me on the Internet
Example 4: Ring-Ring Telephone Ring: Chatting Sessions Turn Dangerous
Example 5: Young Lady's Privacy Impacted
Example 6: Indian Banks Lose Millions of Rupees
Example 7: "Justice" vs. "Justice": Software Developer Arrested for Launching Website Attacks
Example 8: Parliament Attack
Example9: Pune City Police Bust Nigerian Racket

Mini-Cases:
- Mini-Case 1: Cyberpornography Involving a Juvenile Criminal
- Mini-Case 2: Cyberdefamation: A Young Couple Impacted
- Mini-Case 12: Internet Used for Murdering
- Mini-Case 13: Social Networking Victim – The MySpace Suicide Case
- Mini-Case 16: NASSCOM vs. Ajay Sood and Others

Online Scams:
- Scam No. 1 – Foreign Country Visit Bait
- Scam No. 2 – Romance Scam
- Scam No. 3 – Lottery Scam
- Scam No. 4 – Bomb Scams
- Scam No. 5 – Charity Scams
- Scam No. 6 – Fake Job Offer Scam

Financial Crimes in Cyber Domain:
- Financial Crime 1: Banking Related Frauds
- Financial Crime 2: Credit Card Related Frauds

7. Accomplishment:

After learning the course the students should be able to: student should understand cyber-attack, types of cybercrimes, cyber laws and also how to protect them self and ultimately society from such attacks

Practical List

Part I - Commands

1. Study of following network emulators:
   i) WHOIS Search
   ii) Whois CLI Command
   iii) Nslookup
   iv) Host
   v) Ping
   vi) Traceroute
   vii) Netstat
   viii) Tcpdump and Windump
2. Create a malicious program that is (Atleast one program):
   i) Virus
   ii) Worm
   iii) Trojan
   iv) Dropper
3. TCP / UDP connectivity using Netcat
4. TCP scanning using NMAP.
5. Port scanning using NMAP.
6. TCP / UDP connectivity using Netcat.

Part II - Exploits

7. Exploit Web application Security using DVWA (Manual).
   Command Execution
   - SQL Injection
   - File Inclusion
   - XSS /CSIRF
   - Brute Force

8. Exploit Web application Security using DVWA
   Automated SQL injection with SqlMap .

Part III - Forensics

9. Perform a forensic analysis through autopsy sleuth kit.
10. Perform forensic analysis through helix.
11. Study of Forensic Tools (Study any TWO)
    - Password Clearing
    - File Recovery
    - Data Hiding Techniques
    - Steganography
    - CheckSum
    - Hiren's BootCD

Note: Above list is a suggestive, you may selective from Internet

Part IV: Desirable (add on knowledge)

1. Network vulnerability using OpenVAS.
2. Perform image acquisition of the first partition carry out a dead analysis on image.
3. Study "omni peek "and perform live network analysis to capture packets.
4. Perform forensic data recovery through (Icare) a disk drill.
5. Perform forensic hash analysis and integrity check of evidence through FCIV and windiff.
6. Securely deleting file permanently (use tool like File shradder).
7. Install Kali-Linux on a PC for using it as an attacklaunching/vulnerability exploiting machine.
8. Create an intentionally vulnerableLinux Machine using MetaSploitable2 on another machine.
9. Perform Scanning/Reconnaissance testing on above mentioned machine in 5) using the machine mentioned in 4) using tools like NMAPand OpenVAS.
10. Study and Use MetaSploit Framework (already bundled with Kali Linux) present in machine to exploit vulnerabilities in the target vulnerable machine mentioned in5) using both command line and Armitage GUI utility.
11. Verify the integrity of a downloaded .tar.gz fileusing the shasum command. Eg. Hadoop Installation files can be taken as an example.Visit Hadoop Downloads Homepage:http://hadoop.apache.org/releases.html

Evaluation Parameters:

- Group Size : (2-3 Persons)
- Evaluation of the projects would be done considering Report (Pahse I,II and III). The main parameter of assessment would be the ability of the students to understand Cyber Security and Forensic concepts and process
- Though the project and domain specific knowledge would be not be assessed for, the evaluation would predominantly depend on the students' ability to explain, modify or execute security testing.
- Though the project would be evaluated for the entire team, the examiner should emphasize on the contribution of each team member in the project
- Documentation
    - Outcome: Report (Document) Minimum Pages : 50 Pages
    - The documentation should also include description related to Tools and methodologies used in.
    - Topics

I - Basics	a) Study, run and document (Part I)	20%
II - Exploit	Select an application and Exploit Web application Security using DVWA (Manual and Automate) Document work done	30%
III _ Forensic	A) Perform a forensic analysis through autopsy sleuth kit.	30%

	or Perform forensic analysis through helix.	
	B) Study and document any two Forensic Tools (refer List Part 3 #11)	
IV - VIVA	VIVA	20%

- Following **is expected to be demonstrated**
  - Understanding of Basic Commands, Threats working
  - The execution of the Security Tools

Note: Some of the practicals form the above practical list may have seemingly similar definitions. For better learning and good practice, it is advised that students do maximum number of practicals. In the practical examination, the definition asked need not have the same wordings as given in the practical list. However, the definitions asked in the exams will be similar to the ones given in the practical list.