GUJARAT TECHNOLOGICAL UNIVERSITY

Syllabus for Integrated Master of Computer Applications, 7th Semester
Subject Name: Cyber Security
Subject Code: 2678603

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 practical tips and tricks and to educate the students to learn how to avoid becoming victims of cybercrimes.
   - 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**

Sr No.	UNIT	Weightage %
1	**Introduction to Cyber security:** Cyberspace, the Internet, and the World Wide Web, The Beginning of the Internet and Cyberspace, Vulnerabilities of the Internet, Cyber security – Introduction and Importance. Overview of Cyberspace Intrusions, Threat Factors - The Evolution of Cybercrime, Threats to Cyber security by Criminals and Organized Crime – Cybercrimes, Fraud and Financial Crimes, Cyberbullying. An Evolving Threat: The Deep Web - The Surface Web, The Deep Web and Darknets, Payment: Cryptocurrency, Terrorist Presence on the Deep and Dark Web.	30%
2	**Attacker Techniques and Motivations :** Antiforensics - How and Why Attackers Use Proxies, Tunnelling Techniques, Fraud Techniques - Rogue Antivirus, Phishing, Smashing, Vishing, and Mobile Malicious Code, Click Fraud , Threat Infrastructure - Botnets, Fast-Flux , Advanced Fast-Flux Exploitation.	15%
3	**Exploitation and Malicious Code :** Techniques to Gain a Foothold – Shellcode, Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows, Format String Vulnerabilities, SQL Injection, Malicious PDF Files Race Conditions, Web Exploit Tools DoS Conditions, Brute Force and Dictionary Attacks, Misdirection, Reconnaissance, and Disruption Methods. Malicious Code - Self-Replicating Malicious Code, Evading Detection and Elevating Privileges, Stealing Information and Exploitation.	30%
4	**Digital Forensics with Open Source Tools:** Digital Forensics - Goals of Forensic Analysis, The Digital Forensics Process. Open Source Examination Platform : Open Source Examination Platform, Using Linux as the Host, Using Windows as the Host, Disk and File System Analysis - Media Analysis Concepts, The Sleuth Kit, Partitioning and Disk Layouts, Special Containers, Hashing, Carving, Forensic Imaging. Windows Systems and Artefacts - Windows File Systems, Registry, Event Logs, Prefetch Files, Shortcut Files and Windows Executable.	25%

5*	**Tools and Utilities: Using Basic Tools:** IFconfig/IPconfig, Whois, Nslookup, PING, Traceroute, Telnet, Secure Shell, Monitoring Tools and Software: Nagios, SolarWinds, Microsoft Network Monitor, Wireshark, Snort, Nmap, Nikto, OpenVAS, Metasploit, The Browser Exploitation Framework. * **This unit 5 is pertinent for practical only and question should not be asked in theory component.**	

4. Text Books:

- Cyberspace, cyber security, and cybercrime / Janine Kremling, California State University, San Bernardino, Amanda M. Sharp Parker, Campbell University. SAGE Publications, First Edition, ISBN 9781506347257
- Cyber Security Essentials - James Graham, Richard Howard, Ryan Olson CRC Press, ISBN - 13: 978-1-4398-5126-5.
- Digital Forensics with Open Source Tools - Cory Altheide, Harlan Carvey, ISBN: 978-1-59749-586-8, Elsevier, Syngress.
- Cybersecurity Essentials - Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short , ISBN: 978-1-119-36239-5. SYBEX

5. Reference Books:

- Dafydd Stuttard, The Web Application Hacker′s Handbook: Finding and Exploiting Security Flaws Paperback – Wiley, 2nd Edition,
- Wade Alcorn , Christian Frichot, Michele Orru, , The Browser Hacker's Handbook Book, WIley
- James Graham, Richar Howard,Ryan Olson, “Cyber Security Essentials”, CRC Press, Tailor and Francis Group, 2011
- Robert Jones, “Internet Forensics: Using Digital Evidence to Solve Computer Crime”,O’Reilly Media, October, 2005
- Chad Steel, “Windows Forensics: The field guide for conducting corporate computer investigations”, Wiley India Publications, December, 2006
- Nelson Phillips, Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.
- Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.
- 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#	Chapters
1	1	1 to 4, 8
2	2	2.1 to 2.3
3	2	3.1 to 3.2, 4.1 to 4.3
4	3	1, 2, 3,4
5	4	23.1, 23.2

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: Cyber pornography Involving a Juvenile Criminal
Mini-Case 2: Cyber defamation: 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:
    a) WHOIS Search
    b) Whois CLI Command
    c) Nslookup
    d) Host
    e) Ping
    f) Traceroute
    g) Netstat
    h) Tcpdump and Windump
2. Create a malicious program that is (Atleast one program):
    a) Virus
    b) Worm
    c) Trojan
    d) 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.
   Command Execution
    - SQL Injection
    - SQL Injection (Blind)
    - File Inclusion
    - File Upload
    - Insecure CAPTCHA
    - Brute Force
    - CSRF
    - Weak Session IDs
    - XSS (DOM)
    - XSS (Reflected)
    - XSS (Stored)
    - CSP Bypass
    - JavaScript

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 attack launching/vulnerability exploiting machine.
8. Create an intentionally vulnerable Linux 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 file using 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 (Phase 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.
    - Topic

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. or Perform forensic analysis through helix.	30%
	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