Maulana Abul Kalam Azad University of Technology, West Bengal
(Formerly known as West Bengal University of Technology)
Syllabus of B.Sc. in Cyber Security
Effective from academic session 2023-2024

SEMESTER 5

Cyber Systems & Cyber Threat and Modelling

Credits- 3L+ 2P

Course Code – FYCYS 501 (Theory) , FYCYS 591 (Practical)

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome
1.	Apply threat models by discussing strategies and structuredapproaches to threat modelling.
2.	Apply different processes(such as finding, spoofing, tampering etc.) to the threats.
3.	Make use of different techniques for managing and addressing thethreats.
4.	Explain and Identify different threat modelling tools.
5.	Evaluate different threats to cryptosystems.
6.	Appraise different intrusion and detection techniques.

Maulana Abul Kalam Azad University of Technology, West Bengal
(Formerly known as West Bengal University of Technology)
Syllabus of B.Sc. in Cyber Security
Effective from academic session 2023-2024

Theory

Module Number	Headline	Total Hours	%age of questions	Blooms Level
M1	Dive In and Threat Model	12	25	3,4,5
M2	Finding Threats	12	30	3,4,5
M3	Managing and Addressing Threats	12	30	3,4,5
M4	Threat Modelling Tools	12	15	3,4,5
		48	**100**	

Practical

Module No	Headline	Total Hours	%age of questions	Blooms Level
M5	Threats to Cryptosystems	28	60	3,4,5
M6	Intrusion and detection techniques	28	40	3,4,5
		56	**100**	

Module-1: Dive in and Threat Model, learning to Threat Model. Strategies for Threat Modelling, Brainstorming Your Threats, Structured Approaches to Threat Modelling, Models of Software,

Module-2: Finding Threats, STRIDE, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats. Attack Trees, Working withAttack Trees, Representing a Tree, Real Attack Trees. Attack Libraries, Properties of Attack Libraries.

Module-3 Managing and Addressing Threats, Processing and Managing Threats, Starting the Threat Modelling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specific Elements of Threat Modelling. Defensive Tactics and Technologies, Tactics and Technologies for Mitigating Threats, Addressing Threats with Patterns, Mitigating PrivacyThreats.

Module-4 Threat Modelling Tools, Generally Useful Tools, Open-Source Tools, Commercial Tools. Web and Cloud Threats, Web Threats, Cloud Tenant Threats, Cloud Provider Threats, Mobile Threats.

Module-5 Threats to Cryptosystems, Cryptographic Primitives, Classic Threat Actors, Attacks against Cryptosystems, building with Crypto, Things to Remember about Crypto Experimental Approaches, looking in the Seams, Operational Threat Models, Threats toThreat Modelling Approaches, How to Experiment.

Module 6: Intrusion and detection techniques, Programming Bugs and Malicious code, E- commerce Security, web browser security, Mini Project.

Suggested Readings:

1. Adam Shostack, “Threat Modelling: Designing for Security Designing for Security” Wileypublication, Edition, 2008.
2. Frank Swiderski, Window Snyder “Threat Modelling (Microsoft Professional)” MicrosoftPress, Edition,2008.

Vulnerability Analysis, Penetration Testing, and Incident Handling
Credits- 3L+2P
Course Code – FYCYS 502 (Theory), FYCYS 592 (Practical)

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome
1.	Apply details of vulnerability.
2.	Make use of and penetration testing overview.
3.	Examine the details of cyber security incident management.
4.	Test for ethical hacking.
5.	Test for and evaluate vulnerability assessment tool.
6.	Determine and design different hacking techniques.

Theory

Module No	Headline	Total Hours	%age of questions	Blooms Level
M1	Vulnerability	12	25	3,4, 5
M2	Introduction to Penetration Testing, Penetration Testing Overview	12	25	3,4, 5

M3	Cyber Security Incident Management	12	25	3,4, 5
M4	Ethical Hacking	12	25	3,4, 5
		48	**100**	

Practical

Module No	**Headline**	**Total Hours**	**%age of questions**	**Blooms Level**
M5	Working of Vulnerability Assessment Tool	28	50	3,4,5
M6	Hacking Techniques	28	50	3,4,5
		56	**100**	

Vulnerability Analysis, Penetration Testing, and Incident Handling

Module 1: Vulnerability - Introduction, Overview of Security threats and Vulnerability, Benefits, Methodology, Vulnerability and Threats, Malware: Viruses, Worms, Trojan horses, Security Vulnerabilities Types of attacks on Confidentiality, Integrity and Availability, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application vulnerability, Security Counter Measures, Intrusion Detection, Antivirus Software Intrusion Detection, Antivirus Software, vulnerability to security risks, Failure to Restrict URL, Remote Code Execution, tools use for vulnerability checking.

Module 2: Introduction to Penetration Testing, Penetration Testing Overview: What is Penetration Testing? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance, Discovery, Analysing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, and Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing. White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing, Conclusion.

Module 3: Cyber security Incident Management: The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist, Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post- Incident Activity, Handling an Incident: Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sourcesof Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization & Incident Notification, Post-Incident Activity: Lessons Learned, Using Collected Incident Data, EvidenceRetention.

Module 4: Ethical Hacking, Penetration Testing, Vulnerability Assessment and Penetration Testing, SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Security Counter Measures, Overview of digitalforensics,

Module 5: Working of Vulnerability Assessment Tool, Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration, – vulnerability analysis, Planning and Discovery Knowledge Check, Attack and Reporting.

Module 6: Hacking Techniques, Penetration Testing Tools, Tools use in Incident Response, Incident Response Knowledge.

Suggested Readings:

1. Mastering Modern Web Penetration Testing by Prakhar Prasad, October 2016PacktPublishing.
2. Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran,Cameron Buchanan,2015 Packt Publishing.

SEMESTER 6

Cyber Forensics

Credits-5

Course Code – FYCYS 601

Course Objective:

It enables the students to make use of the knowledge in the field of Computer forensics & Cyber Crime. After completion of the course the students will be able toapply investigation tools and techniques, analysis of data to identify evidence, Technical Aspects & Legal Aspects related to cybercrime.

Sl. No.	Course Summary
1.	Examine and Discuss Cyber Forensic Science.
2.	Make use of Cyber Crime Scene Analysis.
3.	Take part in Evidence Management & Presentation.
4.	Discuss Computer Forensics.
5.	Assess details about Mobile Forensics.
6.	Evaluate recent trends in mobile forensics techniques and methods.

Module Number	Content	Total Hours	%age of questions	Blooms Level
1	Introduction of Cyber Forensic Science.	12	20	3, 4, 5
2	Cyber Crime Scene Analysis	10	20	3, 4, 5
3	Evidence Management & Presentation	12	20	3, 4, 5
4	Computer Forensics	12	25	3, 4, 5
5	System and Network Security	7	10	3, 4, 5

6	Recent trends in mobile forensics techniques And methods	7	5	3, 4, 5
	Total	60	100	
	Tutorial	16		

Cyber Forensics

Module 1: Cyber Forensics Science:

Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics

as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber- forensics

Module 2: Cyber Crime Scene Analysis:

Discuss the various court orders etc., methods to search and seizure electronic evidence,

retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

Module 3: Evidence Management & Presentation:

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would looklike, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

Module 4: Computer Forensics:

Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data

Module 5: Mobile Forensics:

Mobile forensics techniques, mobile forensics tools. Legal Aspects of Cyber Forensics: IT Act

2000, amendment of IT Act 2008.

Module 6: Recent trends in mobile forensic technique and methods:

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

Suggested Reading:

- 1. John Sammons, The Basics of Digital Forensics, Elsevier Model Curriculum of Engineering &Technology PG Courses [Volume-I]
- 2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Malware Analysis

Credit –5

Course Code – FYCYS 602

Course Objective:

This course provides all the necessary insights about the modern malware and anti-malwarelandscape. Participants will be able to evaluate about current malware functioning and howit infects companies' IT infrastructures through their weakest points, exploiting these weaknesses after infection.

Sl. No.	Course Summary
1.	Make use of Fundamentals of Malware Analysis (MA).
2.	Discuss about Malware Forensics.
3.	Examine Malware and Kernel Debugging.
4.	Explain Memory Forensics and Volatility.
5.	Make use of Researching and Mapping Source Domains/IPs.
6.	Assess Case Study(e.g. Finding Artifacts in Process Memory etc.

Module Number	Content	Total Hours	%age of questions	BloomsLevel
1	Fundamentals of MalwareAnalysis (MA)	15	25	3,4,5
2	Malware Forensics	10	15	3,4,5
3	Malware and KernelDebugging	10	20	3,4,5
4	Memory Forensics andVolatility	10	20	3,4,5
5	Researching and MappingSource Domains/IPs	7	10	3,4,5
6	Case Study	8	10	3,4,5
		60	100	
	Tutorial	16		

Malware Analysis

Module 1: Fundamentals of Malware Analysis :

Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM)

Methodology,Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats,Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu,

Zeltser’sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOGfor Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware,Python , Other Analysis Tools

Module 2: Malware Forensics:

Using TSK for Network and Host Discoveries, Using Microsoft Offline API to RegistryDiscoveries, Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu- gins:, Bypassing Poison Ivy’s Locked Files, Bypassing Conficker’s File System ACL Restrictions,Detecting Rogue PKI Certificates

Module 3: Malware and Kernel Debugging:

Opening and Attaching to Processes, Configuration of JIT Debugger for Shell code Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging aVMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X).

Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts, Kernel Debugging with IDA Pro.

Module 4: Memory Forensics and Volatility:

Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.

Module 5: Researching and Mapping Source Domains/IPs:

Using WHOIS to Research Domains, DNS Hostname Resolution, Querying Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps

Module 6: Case Study:

Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind andYARA

Suggested Reading:

1. Michael Sikorski, Andrew Honig “Practical Malware Analysis: The Hands-On Guide toDissecting Malicious Software” publisher Williampollo

Advanced Computer Network & Security

Credits- 2T +2P

Course Code – FYCYS603 (Theory), FYCYS 693 (Practical)

Course Objective: The course is designed to provide an elaborate idea about the Computer networking in advance level and threats identification and prevention modelling of operatingsystems.

Sl. No.	Course Outcome
1.	Apply Computer Network Fundamental
2.	Analyze Network devices, IEEE protocols
3.	Analyze different techniques encoding, switching, and congestion control.
4.	Assess advance communication protocols.
5.	Plan and Discuss introduction and Security Threats
6.	Test for network security.

Theory

Module Number	Headline	Total Hours	%age of questions	Blooms Level
M1	Computer Network Fundamental	10	20	3,4,5
M2	Network devices, IEEE protocols	14	30	3,4,5
M3	Encoding, switching, congestion control	14	30	3,4,5
M4	Advance communicationprotocols	10	20	3,4,5
		48	100	

Practical

Module Number	Headline	Total Hours	%age of questions	Blooms Level
M5	IntroductionandSecurity Threats	28	40	3,4,5
M6	Network security	28	60	3,4,5
		56	100	

Module-1: Computer Network Fundamental

Data Communication, Analog-Digital Signals. TCP/IP and OSI Model, Client, Server and Peers, Client/Server architecture, Wired & Wireless transmission, Guided-Unguided Media, Bus, Star, Ring, Mesh, Hybrid, LAN, MAN, WAN, Simplex, Half duplex and Full duplex, Asynchronousand Synchronous Transmission, Parallel and Serial Transmission, Base band and Broadband transmission.

Module-2: Network devices, IEEE protocols

Different networking devices, IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11, FDDI, DQDEB, ATM, Physical Addressing, Logical Addressing, Port Addresses, IPV4, IPV6, Classfull-Classless Addressing, Subnetting and Masking, NAT, DHCP, BOOTP, ARP, RARP, ICMP

Module-3: Encoding, switching, congestion control

Different Encoding Techniques, FDM, TDM, Circuit Switching, Packet Switching, Message Switching. Routing, Routing Protocols: Distance Vector, Link State, Congestion Control: LeakyBucket and Token Bucket Algorithm, ISDN

Module-4: Advance communication protocols

TCP, UDP, Firewalls, Proxy Router, DNS, FTP, TFTP, SMTP, TELNET, NFS, WWW, E-mail, HTTPS,

Cable Network, Telephone Network

Module-5: Introduction and Security Threats

Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare, Confidentiality, Integrity, Availability, Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware: Viruses, Logic bombs.

Module 6: Network security

Centralized or decentralized infrastructure, private key protection, Trust Models: Hierarchical, peer to peer, hybrid, Firewalls: working, design principles, trusted systems, Kerberos, Securitytopologies, IP security: overview, architecture, IPSec configurations, IPSec security, Email security : security of email transmission, malicious code, spam, mail encryption.

Suggested Readings:

1. B. Fourauzan, “Data Communications and Networking”, 4th Edition, Tata McGraw-Hill
2. Tanenbaum, Computer Networks, 3rd Edition, PHI, New Delhi
3. D. Comer, “Computer Networks and Internet”, 2nd Edition, Pearson Education
4. Data and Communication by W. Stallings
5. An integrated approach to Computer Networks by Bhavneet Sidhu, Khanna Publishing H