GUJARAT UNIVERSITY
DEPARTMENT OF BIOCHEMISTRY AND FORENSIC SCIENCE,
University School of Sciences,
Ahmedabad-380009

M.Sc Cyber Security & Forensics
(Year of introduction-2019)

In today's world, where information technology plays a pivotal role, businesses, organizations, and individuals are increasingly susceptible to various cyber threats, including ransomware, cyber warfare, cyber terrorism, cyberbullying, and hacking. To address this growing concern, Gujarat University is introducing a master's course in cybersecurity. This initiative aligns with the digital India movement and aims to cultivate highly skilled cybersecurity professionals.

Following the UGC norms and the introduction of the choice-based semester system, this program will equip students with the knowledge and skills needed to excel in various cybersecurity careers. Graduates will be well-prepared for roles such as Cyber Security Analyst, Network Security Engineer, Security Architect, Cyber Security Manager, Chief Information Security Officer (CISO), as well as positions within police forces and banks.

Syllabus
(Revised syllabus effective from June 2024)
M. Sc. Cyber Security & Forensics

1. There shall be Four papers each of four hours (3+1) duration and two practical each of Nine hours per week.
2. Each Course (Theory & Practical) shall carry 100 (Hundred) marks (Internal 30 marks and External 70 marks). External exam for each theory is of 3 hours and practical exam is of more than 6 hours per semester.
3. The major emphasis of this Course is to motivate students for improvement through regular internal assessment. They should be encouraged for self-study and seminar according to allotted times of the course per week.
4. Each theory paper is divided into four UNIT. Each UNIT – will have equal weightage of teaching and while setting question paper.
5. Question or its sub question including the options will be set from the same UNIT.
6. Practical batch will be consisting of maximum 10 students.
7. The elective papers will be offered as per availability of the expert faculty and feasibility of the department and schedule of teaching.

8. There shall be at least one study tour during the span of two years of P.G. study, pertaining to different central and state FSL, research laboratories and eminent institutions even outside Gujarat State. The study tour is highly essential for study various concepts, processes and technology pertaining to forensic science.

Design and Structure of M.Sc. Cyber Security & Forensic
PG Courses for Credit Based Semester system to be implemented from 2024-25

M.Sc. CYBER SECURITY & FORENSIC					
SEM 1					
Subject Code	**Subject**	**Total Marks**	*** Internal Marks**	**External Marks**	**Credit**
CSF 401	Fundamental of Information Security	100	30	70	4
CSF 402	Network Security	100	30	70	4
CSF 403	Advance Web Application Security	100	30	70	4
CSF 404	Advance Mobile Application Security	100	30	70	4
CSF 405 PR	Practical 1(CSF 401 & CSF 402)	100	30	70	4
CSF 406 PR	Practical 2(CSF 403 & CSF 404)	100	30	70	4
	Total	600	180	420	24

M.Sc. CYBER SECURITY & FORENSIC					
SEM 2					
Subject Code	**Subject**	**Total Marks**	**Internal Marks**	**External Marks**	**Credit**
CSF 407	Fundamental of MSF and Advance Cryptography	100	30	70	4
CSF 408	Cyber Forensic and Investigation	100	30	70	4
CSF 409	Cloud Security	100	30	70	4
CSF 410	Reverse Engineering and Malware Analysis	100	30	70	4
CSF 411 PR	Practical 1 (CSF 407 & CSF 408)	100	30	70	4
CSF 412 PR	Practical 2 (CSF 409 & CSF 410)	100	30	70	4
		600			24

M.Sc. CYBER SECURITY & FORENSIC					
SEM 3					
Subject Code	**Subject**	**Total Marks**	**Internal Marks**	**External Marks**	**Credit**
CSF 501	Security Monitoring	100	30	70	4
CSF 502 EA	ISMS - ISO				
CSF 502 EB	ISMS – PCI – DSS				
CSF 502 EC	ISMS - PIMS	100	30	70	4
CSF 503 EA	VAPT				
CSF 503 EB	Malware Analysis				
CSF 503 EC	SCADA & IOT	100	30	70	4
CSF 504 EA	SOC				
CSF 504 EB	Digital Forensic				
CSF 504 EC	Cloud Security	100	30	70	4
CSF 505 PR	Practical 1 (CSF 501 & CSF 502)	100	30	70	4
CSF 506 PR	Practical 2 (CSF 503 & CSF 504)	100	30	70	4
		600			24

M.Sc. CYBER SECURITY & FORENSIC					
SEM 4					
Subject Code	**Subject**	**Total Marks**	**Internal Marks**	**External Marks**	**Credit**
CSF 507	Internship	200	60	140	8
CSF 508	Final Dissertation/ Project	400	120	280	16
		600			24

* Internal Marks Composition - The internal marks for this course are determined by a combination of the following components:

Tests: Regular assessments to evaluate understanding of the course material.

Assignments: Homework and project work submitted throughout the course.

Attendance: Active participation and attendance in classes.

Presentations: Students will deliver presentations on assigned topics.

Seminars: Participation in seminars will be required, where students will engage in discussions and present their insights on various topics.

MSc Cyber Security and Forensics Semester I

Syllabus

CSF 401

Fundamentals of Information Security and SCADA & IoT

Unit: 1 Introduction to Cyber Security

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Linux/Mac Terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security.

Unit: 2 Python Basics

Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages.

Unit: 3 Encoding and SCADA & IoT

Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes and Binary Reedmuller codes. Structure, Properties, Usage, Unicode and Legacy Encodings. SCADA basic, IoT basics, system architecture, Industry set up, Machine-to-Machine (M2M) communication, Radio Frequency Identification, Wireless Sensor Network, Human Machine Interface, Supervisory (computer) system, Remote Terminal Units (RTUs), Programmable Logic Controller (PLCs), Communication infrastructure, A history of the Internet of Things, How sensor nodes collect and communicate information, Data management and process management, Networking the IoT.

Unit: 4 Web and Mobile App Architecture.

HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache – Computing the Overlay, Virtualisation, Server Configurations, Mobile Application Firewalls.

Practical List:

Practical 1: Introduction to Kali Linux, understanding and implementing of basic tools using Kali Linux.

Practical 2: Understanding and Implementing with DOS Prompt / Linux/Mac Terminal and Commands. Use of Specific commands for cyber security.

Practical 3: Understanding and using Search Engines like Maltego and Shodan

Practical 4: To search Industrial Control systems, IOT using Shodan.io

Practical 5: To perform information gathering on particular organization's IT asset, mapping their IT Landscape and finding open ports on all IT Assests using Shodan.

Practical 6: Setting up XAMPP Server & Hosting Websites on XAMPP Server

Practical 7: Understanding Server and System Hardening concepts and Implementing server configurations on Windows 2008,2012 and 2016 Servers and Linux Servers

Practical 8: To learn operators, string and regular expressions in python. Perform operation on dictionary, tuples using Python.

Practical 9: To implement OOP for python.

Practical 10: To learn file handling using python.

Practical 11: Working with SQLite using python.

CSF 402

Network Security

Unit 1: Fundamentals of Networking
Introduction to Computer Networking (History & Evolution), Types of networks (LAN, WAN), Types of Topologies, Basic Networking Terminologies: IP Address, NAT, Subnetting, DHCP Server, Ports, DNS, DNS Server, Router, Switch, Hub.
Network Models (OSI & TCP/IP)

Unit 2: Fundamentals of Network Security
Introduction to Network Security (Importance & Network Security Threats),
Role of Network Security in Modern Computing, CIA Triad
Different types of network layer attacks–Firewall, ACL, Packet Filtering, DMZ, Alerts and Audit Trails.
Risk assessment and management.

Unit 3: Network Protocols
SSL/ TLS & SSH
Tunnelling Protocols
Authentication Header- IPSEC Protocol Suite & IKE
Kerberos
OAuth 2.0 & TACACS+
LDAP & RADIUS

Unit 4: Network Attacks & Security Protocols
IDS & IPS, VPN
Network Sniffing (Information gathering): Host Discovery, Port Scanning, Banner Grabbing/OS Fingerprinting
Network Scanning Report Generation
Denial of services attack.
Fake Authentication Attack, DNS Poisoning.
Dictionary Attack
MITM & Brute Force Attack

CSF 403

Advance Web Application Security

Unit 1: Introduction to Web Applications
Understanding web applications, how web applications work, client-server model, DNS, web application proxy, same-origin policies, core-origin policies, cookies, sessions, tokens, browser extensions, Google Hacking Database, web applications vs. cloud applications, future of web applications.

Unit 2: Web Application Security
Understanding OWASP, OWASP Top 10 vulnerabilities, How web security works, importance of web application security, web application security vs. network security, HTTP request-response, web application status codes, tools and installation: XAMPP, Burp-Suite, Burp-Suite configuration with browser, Zap-Proxy, Nuclei, use of GitHub, footprinting and enumeration tools, Wayback Machine, WP-Scan, Wappalyzer, Whatweb.net, NS-Lookup.

Unit 3: Web Application Vulnerabilities Assessment
Vulnerability assessment concepts, classification and assessment types, footprinting concepts, footprinting through search engines, footprinting through social networking sites, DNS footprinting, host discovery, enumeration concepts, website crawling, finding vulnerable parameters.

Unit 4: Web Application Attacks and Mitigation
SQL injections, SQL Map, cross-site scripting, types of cross-site scripting, advanced phishing attacks, broken access control, broken authentication session management, local file inclusion, remote file inclusion, session hijacking, clickjacking, OTP bypass, two-factor authentication bypass, cross-origin resource sharing, business logic flaws, cross-site request forgery, CAPTCHA bypass, insecure direct object references, mitigation steps.

PRACTICAL LIST-

1. To perform information gathering on web applications using whois, nsLookup, Netcraft, and domain tools.
2. To perform port scanning on web applications using NMAP.
3. To perform web server fingerprinting and subdomain enumeration using pentest tools and manual scripts.
4. To explore vulnerable URLs and web application vulnerabilities using Google Hacking Database and Shodan.
5. To perform vulnerability scanning using ZAP proxy.
6. To perform authentication bypass using SQL queries.
7. To perform union-based SQL injections on web applications (GET/SEARCH) to retrieve sensitive database information.
8. To perform union-based SQL injections on web applications (POST/SEARCH) to retrieve sensitive database information
9. To perform error-based SQL injection attacks.
10. To perform time-based SQL injections to retrieve sensitive database information.
11. To perform SQL injection attacks using sqlmap.
12. To perform cross-site scripting (XSS) attacks.

13. To perform command injection attacks.
14. To perform directory traversal attacks.
15. To exploit broken authentication and session management vulnerabilities.
16. To perform HTML injection attacks.
17. To understand and use Burp Suite's functionalities (Intruder, Repeater, Sequencer, Interceptor, Scanner).
18. To perform automated vulnerability scanning using Nessus.

CSF 404

Advance Mobile Application Security

Unit 1: Introduction to Android Applications and Mobile App Security
History of Android, Understanding Android Hardware and Software Architecture, Understanding Android Security Model, Understanding Android Permission Model for Application Security, Sandboxing, Codesigning, Encryption, Rooting Devices, Understanding APK Understanding Directories and Files on an APK.

Unit 2: Introduction to IOS & IPA Applications
History of iOS, Understanding iOS Hardware and Software Architecture, Understanding iOS Security Model, Understanding iOS Permission Model for Application Security, Sandboxing, Codesigning, Keychain and Encryption, Jailbreaking Devices, Understanding IPA, Understanding Directories and Files on an IPA.

Unit 3: Mobile Application Attacks 1
Setting up Mobile App Pentesting Environment, Interact with the Devices, Starting with Drozer, Understanding AndroidManifest.xml, Configuring, Burp and Traffic Interception, Traffic Interception Bypass, Weak Server Side Controls, Insecure Data Storage, Insufficient Transport Layer Protection, Unintended Data Leakage, Poor Authentication & Authorization.

Unit 4: Mobile Application Attacks 2
Broken Cryptography, Client Side Injections, Security Decisions via Untrusted Input, Improper Session Handling, Lack of Binary Protection, Exploiting Debuggable Applications, Developer Backdoor, Location spoofing to download location restricted apps, Configuring Live Device for Penetration Testing, Mitigation Approach for all Vulnerabilities.

List of Practical

Practical 01: DIVA APP Installation
Practical 02: Genny motion setup
Practical 03: Performing static Analysis of Mobile Application using MOBSF
Practical 04: Reverse Engineering App
Practical 05: Insecure logging
Practical 06: Insecure Data Storage (PART 1) in DIVA:
Practical 07: Insecure Data Storage (PART 2) in DIVA:
Practical 08: Insecure Data Storage(PART 3) in DIVA:
Practical 09: Insecure Communication.
Practical 10: Input Validation:- Test the mobile app for input validation vulnerabilities, such as SQL injection, command injection, or insecure deserialization.
Practical 11: Authentication Bypass:- Attempt to bypass or circumvent the authentication mechanisms of a mobile app to gain unauthorized access or perform privileged actions.
Practical 12: Hard Coding Issue:- Perform a code review of the mobile app to identify potential security vulnerabilities introduced by insecure coding practices, such as buffer overflows, unvalidated inputs, or insecure data handling.
Practical 13: Jailbreak/Root Detection:- Assess the effectiveness of a mobile app's jailbreak or root detection mechanisms and explore ways to bypass or circumvent these protections.

Practical 14: Perform Jailbreaking on iOS Devices.
Practical 15: Perform a method to send Malicious Payload to the victims Device and check whether you can take over the control the victim's phone.
Practical 16: Perform Man-in-the-Middle attack by intercepting the Wireless parameter of Device on wireless network.
Practical 17: Perform social engineering Attack method and send the malicious link and SMS tricks which contains Malicious web page.

MSc Cyber Security and Forensics Semester II

Syllabus

CSF 407

Fundamental of MSF and Advance Cryptography

Unit I- Fundamentals of Metasploit framework

Metasploit History, Metasploit Architecture, Hardware Prerequisites, Metasploitable, Ubuntu 7.0, Msfconsole, Metasploit Exploits, Metasploit Payloads, Keylogging, Persistent Meterpreter Service, Meterpreter Backdoor Service, PHP Meterpreter Backdooring EXE Files

Unit II- Classical Ciphers:

Caesar Cipher, Vigenere Cipher, Rail-fence Cipher, Row Transposition Cipher, Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation, Secret Key Cryptography, Data Encryption Standard-Symmetric Ciphers (Stream Cipher & Block cipher), Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family, Public Key Cryptography, Principles of public key cryptosystems, The RSA algorithm, Key management, Diffie-Hellman Key exchange

Unit III- Bitcoins& Blockchain:

Bitcoin introduction, Working, Blockchain, Blockchain operation with bitcoins, Bitcoin glossary, Bitcoin wallets, Setup for Bitcoin payments, Bitcoin mining

Unit IV- Message authentication code and Hash Functions:

Message Authentication Code, Authentication functions, Hash Functions, Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital Signature Standard), Digital Certificate and Public Key Infrastructure

Practical List-

Practical 01: Metasploit Architecture basic

Practical 02: Set up metasploitable

Practical 03: Set up Ubuntu 7.04 or Windows 7

Practical 04: Exploit metasploitable through telnet

Practical 05: Find the FTP version of metasploittable

Practical 06: Find the SSH version of metasploittable

Practical 07: Implement Ceaser Cipher Encryption in python

Practical 08: Implement Ceaser cipher Decryption in python

Practical 09: Implement Playfair Cipher Encryption and Decryption on Paper

Practical 10: Implement Rolling Cipher Encryption-Decryption in Python

Practical 11: Implement Atbash Cipher Encryption-Decryptuon in python

Practical 12: Implement RSA encryption-Decryption in Python

Practical 13: Implement RSA Encryption-Decryption on paper

Practical 14: Perform Diffie-helmen Key exchange on Paper

Practical 15: Write a Program to generate SHA-256/512 in Python

Practical 16: Set up Bitcoin Wallet

CSF 408

Cyber Forensic and Investigation

Unit I- Introduction to Cyber Crime Investigation & Cyber Forensics

Cyber Crime Investigation, Cyber Warfare, Terrorism & Social Networking, Cyber Forensics and Incident Handling, Case Study, Cyber Forensic Basics, Storage Fundamentals, File System Concepts

Unit II- Investigating Real World Cyber Crimes

Investigating Social Media Profile Impersonation cases, Phishing Cases, Data Theft Cases, Corporate Espionage Cases, Email Fraud Cases, Credit Card Fraud Cases, Cyber Pornography Cases, Denial of Service Attacks Cases, Cyber Defamation Cases, Real Life Case Studies

Unit III- IT ACT, Offenses and Penalties

Offences under the Information and Technology Act 2000, Penalty and adjudication, Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed), Limitations of Cyber Law

Unit IV- Data Recovery Tools, Process, and Ethics & Cyber Forensics Investigation

Gathering Evidence, Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Data Protection and Privacy, Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, Encryption and Decryption methods, Search and Seizure of Computers, Work on Open Source, Commercial tools and Cyber range

Practical List-

Practical 01: Performing method to create image of hard disk and removable storage media.

Practical 02: Performing Recovery of Internet Usage Data

Practical 03: Use Exif tool for extracting metadata from image file.

Practical 04: Working with Forensic Toolkit.

Practical 05: Evidence Collection from live system.

Practical 06: Performing Deleted File Recovery using the forensic tool.

Practical 07: Performing tracking on E-Mail, IP Tracking

Practical 08: Performing the E-Mail Recovery

Practical 09: Password Cracking, Cracking with GPU Systems (Hashcat).

Practical 10: Write the report of digital analysis with an example of cyber crime case.

CSF 409

Cloud Security

Unit I- Introduction to Cloud Computing

Cloud Computing definition, Private, public and hybrid cloud, Cloud types: IaaS, PaaS, SaaS, Benefits and challenges of cloud computing, Public vs private clouds, Role of virtualization in enabling the cloud, Business Agility: Benefits and challenges to Cloud architecture, Application availability, Performance, Security and disaster recovery, Next generation Cloud Applications

Unit II- Cloud Application Architecture and security

Technologies and the processes required when deploying web services, Deploying a web service from inside and outside a cloud architecture, Advantages and disadvantages, Introduction to Cloud Technology, Container: Features, Architecture, Lifecycle, Docker: Architecture, Objects, Operations, Kubernetes: Features, Architecture

Unit III- Implementing Cloud Application, Services and security

Reliability, Availability and security of services deployed from the cloud, Performance and scalability of services, Cloud Economics: Cloud Computing infrastructures available for implementing cloud-based services, Cloud security controls, Dimensions of cloud security, Cloud Vulnerability and Penetration Testing, Data security, Encryption, Compliance

Unit IV- Cloud Application Development & IT Model & Importance of Cloud Technology in Corporates

Service creation environments to develop cloud-based applications, Development environments for service development: Amazon, Azure, Google App, Applicability of laws to data stored outside the nation's boundary, Economics of choosing a Cloud platform for an organization - Based on application requirements, economic constraints, and business needs - Discuss industry cases including open sources

Practical List-

PRACTICAL 01: Building and Deploying JAVA/NODE.js based application on public cloud-based application

PRACTICAL 02: Perform Blackbox penetration testing on Cloud applications to get an access to internal cloud resources.

PRACTICAL 03: Performing cloud configuration review on a public cloud platform.

PRACTICAL 04: Performing LAMP technology for developing application using cloud.

PRACTICAL 05: Performing s3 bucket enumeration using lazy3.

PRACTICAL 06: Performing s3 bucket enumeration using s3scanner.

PRACTICAL 07: Install and setup cloud goatlab for cloud vulnerability practice.

PRACTICAL 08: To exploit reverse tabnabbing on vulnerable cloud domain.

PRACTICAL 09: To exploit web domain takeover vulnerability on vulnerable cloud domain.

PRACTICAL 10: To perform XSS attack on vulnerable cloud domain.

PRACTICAL 11: To create container and perform various task using docker.

PRACTICAL 12: Performing vulnerability assessment on EC2 container using Nessus.

PRACTICAL 13: Performing vulnerability assessment on Docker using Nessus.

PRACTICAL 14: Performing signature rapping attacks and side channel attacks in cloud-based applications.

PRACTICAL 15: Security Controls in Cloud and Tools used for Security Control Implementation

.

CSF 410

Reverse Engineering and Malware Analysis

Unit I- Malware Analysis Fundamentals:

What is a Reverse Engineer, Assembling a toolkit for effective malware analysis, Analysis Flow for Malware Analysis, Examining static properties of suspicious programs, Performing behavioral analysis of malicious Windows executables, Performing static and dynamic code analysis of malicious Windows executables, Interacting with malware in a lab to derive additional behavioral characteristics

Unit II- Reversing Malicious Code:

Understanding core x86 assembly concepts to perform malicious code analysis, Opcodes and Instructions, Registers, Identifying key assembly logic structures with a disassembler, Following program control flow to understand decision points during execution, Calling a function, Recognizing common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers), Extending assembly knowledge to include x64 code analysis

Unit III- Malicious Web and Document Files:

Introduction, Types of Malware, Interacting with malicious websites to assess the nature of their threats, De-obfuscating malicious JavaScript using debuggers and interpreters, Analyzing suspicious PDF files, Examining malicious Microsoft Office documents, Including files with macros, Analyzing malicious RTF document files

Unit IV- In-Depth Malware Analysis:

Recognizing packed malware, Getting started with unpacking, Using debuggers for dumping packed malware from memory, Analyzing multi-technology and file-less malware, Code injection and API hooking, Using memory forensics for malware analysis

Practical List-

Practical 01: Getting started with various Reverse Engineering methodologies.

Practical 02: Installation and configuration of the following tools

Practical 03: Understanding the reconnaissance and Weaponization stages

Practical 04: Working with Spear phishing Emails & Delivery Mechanisms.

Practical 05: Create a fake phishing page with a fileless malware link in it.

also analyze the link for the traces of malware.

Practical 06: Analyse the Malicious Office File Using Oledump

Practical 07: Analyse the Malicious OLE Files using Oletools

Practical 08: Working with Wireshark Display filters.

Practical 09: To implement an attempt to do the Static Analysis with Floss.

Practical 10: Perform full Static analysis of the malware sample(trojan/macro) and create a well-documented report for the same.

Practical 11: Create a Trojan and get control of the windows system.

Practical 12: Create a Triage Analysis.

Practical 13: Create an example of Dynamic Analysis.

CSF 411 PR Practical 1 (CSF 407 and CSF408)

CSF 412 PR Practical 2 (CSF 409 and CSF410)

MSc Cyber Security and Forensics Semester III

Syllabus

CSF 501

Security Monitoring

Unit I- Security Monitoring fundamentals:

What is Security Operations, Finding the sweet spot, Security and Control, Security Goals, Reliability vs Security, Typical Security Flaws, Basics of SOC infrastructure

Unit II- Log management:

Computer Security Log Management, Log Management Infrastructure, Log Management Planning, Log Management Operational Process

Unit III- Security Information & Event Management:

Introduction to SIEM, SIEM Architecture, Logs and Events, Understanding logs, Various formats, Log Baselining, Aggregation and normalization, Event Collection and Event Correlation, Correlation Rules

Unit IV- Incident Response Plan and handling steps:

Purpose of Incident Response Plan, Requirements of Incident Response Plan, Preparation, Incident Recording, Initial Response, Communicating the Incident, Containment, Formulating a Response Strategy, Incident Classification, Incident Investigation, Data Collection, Forensic Analysis, Evidence Protection, Notify External Agencies, Eradication, Systems Recovery, Incident Documentation, Incident Damage and Cost Assessment, Review and Update the Response Policies

Practical List-

Practical 01- Perform Installation deployment of SIEM systems
Practical 02: Log Management and Analysis
Practical 03: Perform operations with smart connectors to manage IT assets.
Practical 04: Perform security operation/investigations on different types of security events.
Practical 06: Perform threat hunting using Splunk.
Practical 07: Perform vulnerability management using SIEM.
Practical 08: Perform orchestration of common security related events and investigations.
Practical 09: SOAR
Practical 10: Perform incidence recovery for threat mitigation using SIEM.

CSF 502 EA

ISO 27001: INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

Unit 1: Introduction to ISO 27001 and ISMS

Overview of ISO 27001, Importance of information security, Key concepts and principles of ISMS, Asset and Information Security, Vulnerability and Threat, Information Security risk, Types of Vulnerabilities, Types of threat, Risk management process, PDCA model, Structure and requirements of ISO 27001 (Clauses 4-10), Benefits of implementing ISO 27001.

Clause 4: Context of the Organization

Clause 5: Leadership

Unit 2: Risk Assessment and Treatment, Implementation

Clause 6: Planning, Understanding risk assessment in ISO 27001, Risk assessment methodologies, Identifying and analyzing risks, Risk treatment options, Developing a risk treatment plan

Clause 7: Support

Clause 8: Operation

Unit 3: Monitoring, Review, and Continuous Improvement

Monitoring and measuring ISMS performance, Internal audits and management reviews, Corrective and preventive actions, Continual improvement of ISMS, Preparing for ISO 27001 certification audit

Clause 9: Performance Evaluation

Clause 10: Improvement

Unit 4: Annex A Reference Control Objectives and Controls (A.5 to A.18)

A.5- Information Security Policies, A.6- Organization of Information Security, A.7- Human Resource Security, A.8- Asset Management, A.9- Access Control, A.10- Cryptography, A.11- Physical and Environmental Security, A.12- Operations Security, A.13- Communications Security, A.14 – System Acquisition, Development & Maintenance, A.15 – Supplier Relationships, A.16 – Information Security Incident Management, A.17 – Information Security Aspects of Business Continuity Management, A.18 – Compliance

CSF 502 EB

PCI DSS: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Unit 1: Introduction to PCI DSS and Cardholder Data Environment (CDE)

Objective and Structure of International Standards, Importance of ISMS, Standard and Regulatory Framework, Certification Process, Fundamental principle of Information Security, Asset and Information Security, Confidentiality, Integrity and Availability, Vulnerability and Threat, Information Security risk, Types of Vulnerabilities, Types of threat, Risk management process, PDCA model

Introduction to PCI DSS

Overview of PCI DSS, Importance of protecting cardholder data, Key concepts and principles of PCI DSS, PCI DSS standards and requirements, Scope of PCI DSS: Cardholder Data Environment (CDE), Build and Maintain a Secure Network and Systems.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Unit 2: Protecting Cardholder Data and Vulnerability Management

Protecting stored cardholder data, Encryption and secure transmission of cardholder data, Vulnerability management program, Use of anti-virus software, Secure systems and applications, Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks, Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Unit 3: Access Control Measures and Monitoring Networks

Implementing strong access control measures, restricting access to cardholder data, Authentication mechanisms, Monitoring and testing networks, Regular testing of security systems and processes, Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 8: Identify and authenticate access to system components

Requirement 9: Restrict physical access to cardholder data, Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Unit 4: Information Security Policy and Maintaining Compliance

Importance of maintaining an information security policy**,** Developing and maintaining an information security policy**,** Compliance monitoring and enforcement**,** Preparing for PCI DSS audits and assessments**,** Continuous improvement of PCI DSS compliance**,** Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

CSF 502 EC

ISMS- PRIVACY INFORMATION MANAGEMENT SYSTEM

Unit 1: Introduction to Information Security and Privacy

Concept of Information Security: Importance and objectives of confidentiality, integrity, and availability.
Overview of Information Security Management System (ISMS): Definition, importance, key concepts.
Privacy Information Management System (PIMS): Definition, relevance, and the relationship between privacy and security.
Regulatory and Compliance Landscape: ISO/IEC 27001, ISO/IEC 27701, GDPR, HIPAA, and other relevant standards.
Risk Management Concepts: Understanding risks, vulnerabilities, and threat landscapes.

Unit 2: ISMS Framework and Implementation

ISMS Planning and Scope: Establishing ISMS scope, identifying information assets, and defining boundaries.
ISMS Policy and Controls: Developing security policies, objectives, and control measures.
Risk Assessment and Treatment: Risk identification, analysis, and management strategies.
Implementation of ISMS Controls: Key domains like access control, asset management, physical security, incident management.
Monitoring and Continuous Improvement: Auditing and reviews, internal audits, and ISMS lifecycle.

Unit 3: PIMS Framework and Implementation

Understanding Privacy Management: Data privacy principles, personal data lifecycle management.
PIMS Policies and Procedures: Development of privacy policies, data subject rights, consent management.
Risk Management in PIMS: Privacy Impact Assessments (PIA), risk assessments specific to privacy.
Key Controls in PIMS: Data minimization, anonymization, encryption, breach notification, and third-party processing.
PIMS Governance: Roles, responsibilities, and accountability for privacy management.

Unit 4: Case Studies and Practical Considerations

Case Studies on ISMS and PIMS Implementations: Real-world examples of ISMS and PIMS adoption across industries.
Challenges in ISMS/PIMS Implementation: Common pitfalls, lessons learned, and best practices.
Technology Trends Impacting ISMS/PIMS: Cloud security, IoT, Artificial Intelligence, and their influence on information security and privacy.

CSF 503 EA

Vulnerability Assessment and Penetration Testing

UNIT I

Need for Vulnerability Assessment, Risk prevention, Compliance requirements, The life cycles of Vulnerability Assessment and Penetration Testing: scoping, information gathering, vulnerability scanning, false positive analysis, vulnerability exploitation (Penetration Testing), and report generation. Scan prerequisites, Scan-based target system admin credentials, Direct connectivity without a firewall, scanning window to be agreed upon, Backup of all systems including data and configuration, Creating a scan policy as per target system OS and information, Configuring a scan policy to check for an organizations security policy compliance, Gathering information of target systems, Active and Passive information gathering, Social Engineering Attacks, Port scanning tools.

UNIT II

Scan, Vulnerability and Management: Scan Result analysis, Report interpretation, Hosts Summary (Executive), Vulnerabilities By Host, Vulnerabilities By Plugin, False positive analysis, Understanding an organizations environment, Target-critical vulnerabilities, Port scanning tools, Vulnerability analysis: False positives, Risk severity Applicability analysis, Fix recommendations, Vulnerability Exploitation: Metasploit, Buffer overflow, Fuzzing, Advanced binary exploitation: Reverse engineering, Static code analysis. Vulnerability Assessment reports, Stages of vulnerability management Identify, Assess, Remediate, Report, Improve, Monitor, Vulnerability management tools : Nessus, report customization, report automation, audit policies, Compliance reporting, auditing infrastructure, Compliance check for different OS and databases.

UNIT III

Phases of Penetration Testing, methodologies (Black Box/White Box/Fuzz), penetration testing for Software (Operating system, services, application), Hardware, Network, Processes, End-user behaviour, tools used for penetration testing, Virtual box, Configuration, Reading: Sample PenTest Report, Sample test cases or scenarios.

UNIT IV

Case Studies and Tools

Penetration Testing types: Social Engineering Test, Web Application Test, Physical Penetration Test, Network Services Test, Client-side Test, Tools: Nmap, Nessus, Metasploit, Wireshark, OpenSSL, Acunetix, Intruder, Burpsuite

CSF 503 EB

Advanced Malware Analysis

UNIT – I

Introduction to Malware and Malware Analysis: Malware Definition and Types, Malware Analysis, Forensic Importance of Malware Analysis, Introduction to different analysis techniques, Malware Behavior, Setting up malware analysis laboratory. Static Analysis: Hashing, Finding Strings, Decoding Obfuscated Strings Using FLOSS,

UNIT- II

PE Files Headers and Sections, PE View, Linked Libraries and Functions, Dependency Walker, CFF Explorer, Resource Hacker, Malware signature and Clam AV Virus Signature, YARA Signatures, Dynamic Analysis: Sandboxes, Running and Monitoring a Malware, Process Monitor, Process Explorer, RegShot, faking a network, Using Wireshark for Packet Analysis.

UNIT – III

Behaviors of Malware Common malware behaviors include Process Injection, Process Replacement, Hook Injection, Data Encoding, anti-disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, and Packing and Unpacking.

UNIT - IV

Volatile Data Examination from Windows and Linux Systems: Understanding processes, threads, ports, handles etc. Identifying services and drivers, determining scheduled tasks. Discovering and extracting malware and associated artifacts from Windows and Linux Systems.

Practical list-

1. Identifying Malware Using Hashing and Strings
2. Analyzing PE File Headers and Sections
3. Linked Libraries and Function Analysis Using Dependency Walker
4. Resource Analysis with Resource Hacker
5. Creating and Analyzing YARA Signatures
6. Dynamic Analysis Using Sandboxes
7. Monitoring Malware Behavior with Process Monitor and Process Explorer
8.Static Analysis of Malware Using the CAPA Tool (Remnux)

CSF 503 EC

SCADA & IOT

UNIT I

Evolution of Internet of Things, IoT and Digitization, Enabling Technologies, Challenges of IoT, M2M Communication, The oneM2M IoT Standardized Architecture, IoT World Forum (IoT WF) standardized architecture, Simplified IoT Architecture, Core IoT Functional Stack, IoT Data Management and Compute Stack- Fog, Edge and Cloud in IoT.

UNIT II

Sensors, Actuators, Smart Objects and Sensor Network, Connecting Smart Objects. IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, 802.11ah and Lora WAN Protocols, Comparison of IEEE 802.15.4 and IEEE 802.11ah, 6LoWPAN, Application Layer Protocols: CoAP and MQTT.

UNIT III

Evolution of SCADA, SCADA definitions, SCADA Functional requirements and Components, SCADA Hierarchical concept, SCADA architecture, General features, SCADA Applications, Benefits

UNIT IV

Remote Terminal Unit (RTU), Interface units, Human- Machine Interface Units (HMI), Display Monitors/Data Logger Systems, Intelligent Electronic Devices (IED), Communication Network, SCADA Server, SCADA Control systems and Control panels

PRACTICAL LIST-

1. To study different physical layer technologies used in wireless communication.
2. To configure and test MAC layer parameters using simulation tools.
3. To set up and analyze different wireless network topologies using simulation tools.
4. To assess vulnerabilities and implement mitigation techniques using free tools.
5. To configure IP versions in constrained IoT devices using simulation.
6. To set up and analyze 6LoWPAN networks using simulation.
7. To set up a SCADA system using simulation tools.
8. To perform real-time data transmission and alarm handling using simulation tools.
9. To implement CoAP for data exchange and device control using simulation tools.
10. To implement MQTT for data exchange and interoperability using free tools.

CSF 504 EA

Security Operation Center

Unit 1:
Introduction to Security Operations Center - Overview of SOC: Definition, purpose, and importance of SOC. - SOC Roles and Responsibilities: Key roles within a SOC, including SOC analysts, incident responders, and SOC managers. - SOC Architecture: Components and layout of a SOC. - Introduction to Cyber Threats: Types of cyber threats and attack vectors.

Unit 2:
Monitoring and Detection - Security Information and Event Management (SIEM): Introduction to SIEM tools and their role in SOC. - Log Management: Importance of log management, types of logs, and log sources. - Threat Intelligence: Basics of threat intelligence and its integration into SOC operations. - Hands-on Labs: Setting up and configuring a SIEM tool, analyzing logs, and integrating threat intelligence feeds.

Unit 3:
Incident Response - Incident Response Lifecycle: Phases of incident response (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned). - Incident Detection and Analysis: Techniques for detecting and analyzing security incidents. - Response and Mitigation: Strategies for responding to and mitigating security incidents. - Hands-on Labs: Simulating security incidents and practicing incident response procedures.

Unit 4:
SOC Management and Compliance - SOC Metrics and Reporting: Key performance indicators (KPIs) and metrics for SOC performance. - Compliance and Legal Issues: Overview of compliance requirements (e.g., GDPR, HIPAA) and legal considerations. - SOC Best Practices: Best practices for managing and operating a SOC. - Hands-on Labs: Creating SOC reports, ensuring compliance, and implementing best practices.

CSF 504 EB

Digital Forensics

Unit 1:
Introduction to Advanced Digital Forensics
Overview of Digital Forensics: Definition and Importance, History and Evolution, Types of Digital Forensics, Legal and Ethical Considerations. Legal Framework and Regulations: Ethical Issues in Digital Forensics, Chain of Custody and Evidence Handling. Advanced Forensic Techniques and Tools: Advanced Data Recovery Techniques, Forensic Imaging and Bitstream Copies, Overview of Forensic Tools (myFRT, FTK, Autopsy, etc.), Digital Evidence and Data Acquisition: Collection and Preservation of Digital Evidence, Handling Volatile and Non-Volatile Data, Live Acquisition and Dead Acquisition.

Unit 2:
In-depth Analysis Techniques
File System Forensics: File System Structures (FAT, NTFS, EXT, HFS+), File Carving Techniques, Metadata Analysis. Network Forensics: Network Traffic Analysis, Packet Sniffing and Protocol Analysis, Intrusion Detection and Prevention Systems.
Malware Forensics: Malware Identification and Classification, Reverse Engineering Malware, Dynamic and Static Analysis Techniques. Memory Forensics: Introduction to Memory Forensics, Volatility Framework, Analysis of
Memory Dumps.

Unit 3:
Specialized Forensics Domains
Mobile Device Forensics: Mobile OS and File System Structures, Data Acquisition Techniques for Mobile Devices, Analysis of Mobile Applications and Data.
Cloud Forensics: Challenges in Cloud Forensics, Data Acquisition from Cloud Services, Analysis of Cloud Storage and Services. Internet of Things (IoT) Forensics: IoT Device Ecosystem, Forensic Challenges in IoT, Data Acquisition and Analysis Techniques. Advanced Persistent Threat (APT) Forensics: Understanding APTs, Detection and Analysis of
APTs, Mitigation and Response Strategies.

Unit 4:
Case Studies and Practical Applications
Real-world Case Studies: Analysis of Famous Digital Forensics Cases, Lessons Learned and Best Practices. Forensic Report Writing and Presentation: Structuring Forensic Reports, Communicating Findings Effectively, Legal Implications and Expert Witness Testimony.
Hands-on Practical Sessions: Practical Exercises in Digital Forensics, Using Forensic Tools and Techniques, Simulated Forensic Investigations.

CSF 504 EC

Cloud Security

Unit 1:
Introduction to Cloud Security - Overview of Cloud Computing: Basics of cloud computing, types of cloud services (IaaS, PaaS, SaaS), and deployment models (public, private, hybrid). - Cloud Security Fundamentals: Key concepts, importance of cloud security, and common security challenges. - Cloud Service Providers: Introduction to major providers like AWS, Azure, and Google Cloud, and their security features.

Unit 2:
Identity and Access Management (IAM) - IAM Basics: Understanding IAM, its importance, and how it works in the cloud. - Authentication and Authorization: Methods and best practices. - IAM Tools and Services: Overview of IAM tools provided by AWS, Azure, and Google Cloud. - Hands-on Labs: Setting up IAM policies and roles.

Unit 3:
Cloud Infrastructure Security - Network Security: Securing cloud networks, firewalls, VPNs, and security groups. - Data Security: Encryption, data protection strategies, and secure data storage. - Monitoring and Logging: Tools and techniques for monitoring cloud environments and logging activities. - Hands-on Labs: Configuring network security and encryption.

Unit 4:
Threats and Incident Response - Common Cloud Threats: Identifying and understanding common threats like DDoS attacks, malware, and insider threats. - Incident Response: Steps to take during a security incident, creating an incident response plan. - Compliance and Legal Issues: Understanding compliance requirements (e.g., GDPR, HIPAA) and legal considerations. - Hands-on Labs: Simulating a security breach and responding to it.

Practical List-

1. Set up a Free Tier Account: Create a free tier account on AWS, Azure, or Google Cloud. Document the steps and initial security configurations.

2. Explore Security Features: Identify and document the security features available in the free tier of your chosen cloud provider.

3. Create IAM Users and Groups: Set up IAM users and groups with different permissions using AWS Free Tier. Test access to various resources based on these roles.

4. Enable Multi-Factor Authentication (MFA): Practice MFA for an IAM user and demonstrate the login process.

5. Configure IAM Policies: Write and apply a custom IAM policy that restricts access to specific resources. Use AWS IAM Policy Simulator to test the policy.

6. Set up a Virtual Private Cloud (VPC): Create a VPC with subnets, route tables, and security groups using AWS Free Tier. Demonstrate how to secure the VPC.

8. Encrypt Data at Rest and in Transit: Practice encryption for data stored in an AWS S3 bucket and for data being transmitted between services.

9. Monitor and Log Activities: Enable and configure logging and monitoring services using AWS CloudWatch. Analyze the logs to identify any unusual activities.

10. Simulate a DDoS Attack: Practice AWS Shield (included in the free tier) to simulate a DDoS attack and demonstrate how to mitigate it.

11. Respond to a Security Incident: Create a scenario where a security breach occurs. Develop and execute an incident response plan using AWS Incident Response Playbook.

12. Ensure Compliance: Identify and implement compliance controls for a specific regulation (e.g., GDPR) within your cloud environment using AWS Artifact.

CSF 505 PR Practical 1 (CSF 501 & CSF 502)

CSF 506 PR Practical 2 (CSF 503 & CSF 504)

MSc Cyber Security and Forensics Semester IV

CSF 507 Internship

CSF 508 Final Dissertation / Project

GRANT TOTAL (I+II+III+IV SEMESTERS) = 2400 MARKS

……