Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL					
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*	L	T	P	CREDITS
MSCFN401		Malware Analysis	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Course Objectives:
The student will have ability:
1. To understand malware analysis concept
2. To understand advanced malware analysis

Course Outcomes:
After studying this course, the students will :
1. To know to analysis of malware using tools
2. To get overviews of malware analysis

UNIT IBasic Static Malware Analysis-I
Introduction to Malware, Types of malware – Virus, Worm, Trojan, Backdoor,Ransomware, The Goals of Malware Analysis, Malware Analysis Techniques,

UNIT IIBasic Static Malware Analysis- II
Basic Static Techniques: Hashing, Finding Strings, Packed and ObfuscatedMalware, PortableExecutable File Format, Linked Libraries and Functions, PEFile Header and Sections,Virtual Machines for Malware Analysis

UNIT III Advanced Static Malware Analysis
Introduction to x86 Disassembly: Architecture, Main Memory, Instructions,Opcodes and Endianness, Operands, Registers, Simple Instructions, Stack,Conditionals, Branching,Analyzing Malicious Windows Programs: WindowsAPI, Windows Registry, Networking APIs, Kernel vs User Mode, Native API.

UNIT IV: Advanced Dynamic Malware Analysis
Debugging: Source Level vs Assembly Level Debuggers, Kernel vs User modeDebugging, Using Debugger – OllyDbg/IDA Pro, Exceptions, Modifyingexecution with Debugger, Malware Behavior: Reverse Shell, RAT, Botnet,Process Injection, Hook Injection, APC Injection

UNIT VDynamic Malware Analysis
Basic Dynamic Analysis: Executing Malware Analysis in safe environment,Monitoring with Process Monitor, Viewing Processes with Process Explorer,Comparing Registry Snapshots with Regshot, Faking a Network, Packet Sniffingwith Wireshark

Experiments
1. Assembling a toolkit for effective malware analysis
2. Examining static properties of suspicious programs
3. Understanding core x86 assembly concepts for malicious code analysis
4. Recognizing common malware characteristics at the Windows API level
5. Malicious PDF file analysis, including the analysis of suspicious websites; VBA macros in Microsoft Office documents
6. Using debuggers for dumping packed malware from memory; Analyzing multi-technology and "fileless" malware
7. Code injection and API hooking
8. How malware detects debuggers and protects embedded data
9. Unpacking malicious software that employs process hollowing
10. Bypassing the attempts by malware to detect and evade analysis tools
11. Handling code misdirection techniques, including SEH and TLS callbacks
12. Unpacking malicious executables by anticipating the packer's actions

Reference Books-:
1. Michael Sikorski, Andrew Honig : Practical Malware Analysis - The Hands-On Guide toDissecting Malicious Software, 1st Edition
2. Eldad Eilam : Reversing – Secrets of Reverse Engineering, Wiley Publishing

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL					
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*	L	T	P	CREDITS
MSCFN402		Social Network Analysis & Open Source Intelligence	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Course Objectives:
The student will have ability:
1. To learn about structure and evolution of networks, to build a framework of network analysis that covers measures.
2. To learn cyber ethics
3. To learn social media and network analysis

Course Outcomes:
After studying this course, the students will :
1. Be able to secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
2. Be able to understand dynamics and evolution of social networks.
3. Be able to understand the framework of network analysis.
4. Be able to understand how various social media networks are working and using SNA in their infrastructure.

UNIT 1Introduction to Social Network
What is Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social network, Cybercrimes related to social media and its awareness, scrapping of data from social media API's.
.
UNIT 2 Privacy in Social Network Analysis
Information privacy disclosure, revelation, and its effects in OSM and online social networks, Privacy issues related to location based services on OSM.

UNIT 3 Social Media Analysis

Chairperson	**Chairperson**	**Controller of Examinations**	**Registrar**
Board of Studies – Forensic Science Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Faculty of Studies - Science Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore

Tracking social footprint / identities across different social network, Identifying fraudulent entities in online social networks, Effective and usable privacy setting and policies on OSM, Policing & OSM

UNIT 4 Social Media Behaviour:
Social Media Forensics: Case Studies Open Source tools or social media analytics, Safety on social media, Legal Issues in world social media, Information Technology (Intermediary Guidelinesand Digital Media Ethics Code) Rules, 2021

UNIT 5 Social Network Behaviour Analysis
Detection and characterization of spam, phishing, frauds, hate crime, abuse and extremism via online social media, Data Collection & Analysis, Fake News & content on social media

Experiment-:
1. Case study of current IT act related cases.
2. Case study of Cyber Crimes.
3. Case study of IT law related real life examples.
4. Practical analysis of Social Networking sites.
5. Practical analysis of Networks.
6. Finding out the vulnerable data on Social Networking sites.
7. Find out attacks on social networking sites.
8. Practical analysis of Malwares in Social Networking sites.
9. Case study of Social Networking related crimes

Text Books -:
2) Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
3) John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.

Reference Books-:
1) Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011
2) Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013
3) Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
4) Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.
5) Understanding Social Networks: Theories, Concepts by Charles Kadushin
6. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew
.

Chairperson	**Chairperson**	**Controller of Examinations**	**Registrar**
Board of Studies – Forensic Science	Faculty of Studies - Science	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

MSCFN403 Security Auditing, Risk and Compliance

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN403		Security Auditing, Risk and Compliance	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based on the following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Course Objectives:
1. Different Information Assurance Standards
2. Auditing IT Infrastructures for Compliance
3. Audit Reporting
4. IT Audit: Purposes, Processes, and Practical Information

Course Outcomes: Upon completion of the subject students will be able to know the:
1. Understanding of Security Principles
2. Compliance Frameworks and Regulations
3. Risk Assessment and Management
4. Security Governance and Policies

Unit 1: Governance, Risk, and Compliance in Information Systems
Governance, Risk and Compliance, ISMS, Deming's Circle, IT Audit and Assurance Standards, Guidelines, and Tools and Techniques, Code of Professional Ethics, and other applicable standards. Risk assessment concepts and tools & techniques used in planning, examination, reporting, and follow-up.

Unit 2: Business Processes and Information Systems
Fundamentals of business processes: Purchasing, Payroll, Accounts Payable, accounts receivable, Role of IS in these processes. Control Principles in information systems, Introduction to information auditing standards, ISO 27000, ISO 27001 implementation, GDPR, HIPPA, PCI-DSS.

Unit 3: Risk-Based Audit Planning and Compliance
Risk-based audit planning and audit project management techniques. Applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits, the process of auditing information systems, information security program development and incident management, Risk management and compliance, Introduction to Data privacy bill India - PDPA, DPDP.

Chairperson
Board of Studies – Forensic Science
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Chairperson
Faculty of Studies - Science
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Controller of Examinations
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Registrar
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Unit 4: Evidence Collection and Forensic Audit Techniques

Evidence Collection Techniques: Observation, Inquiry, Inspection, Interview, Data Analysis, Forensic Investigation Techniques, and Computer-assisted audit techniques [CAATs] used to gather, protect and preserve audit evidence. Audit WRT Forensics: investigating website hacking, Data Breach Investigation, Introduction to cyber security frameworks – SANS – CIS, NIST, Industry 4.0 & CSA.

Unit 5: Audit Methodologies and Quality Assurance

Sampling methodologies and substantive/data analytical procedures. Reporting and Communication Techniques: Facilitation, Negotiation, Conflict Resolution, Audit report structure, issue writing, management summary, result verification. Audit Quality assurance (QA) systems and frameworks. Various types of audits: Internal, External, Financial, and methods for assessing and placing reliance on the work of other auditors and control entities.

List of Experiments:
1. Risk Assessment and Treatment Plan
2. ISMS (ISO 27001) Implementation Simulation
3. Audit Project Management and Evidence Collection
4. 5Forensic Investigation Simulation
5. Audit Report Writing and Communication

Suggested Readings:
1. "Auditor's Guide to IT Auditing" by Richard E. Cascarino
2. "IT Audit, Control, and Security" by Robert R. Moeller
3. "Human-Computer Interaction and Cybersecurity Handbook" edited by Abbas Moallem
4. IT Auditing Using Controls to Protect Information Assets, Third Edition by Mike Kegerreis, Mike Schiller, Chris Davis
5. Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance) by Martin Weiss, Michael G. Solomon
6. "The Information Audit: A Practical Guide", Susan Henczel, Information Services Management Series
7. The Basics of IT Audit: Purposes, Processes, and Practical Information", Stephen D. Gantz, Syngress. 2014

Chairperson	**Chairperson**	**Controller of Examinations**	**Registrar**
Board of Studies – Forensic Science	Faculty of Studies - Science	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								CREDITS
			THEORY			PRACTICAL					
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*	L	T	P	
MSCFN403		Internship	0	0	0	90	60	0	0	18	9

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Every student will carry out Internship in Organization/Private Lab/Govt. Lab of one month under the supervision of Supervisor/(s) (Internal/External). Every student will be required to present seminar talktowards the end of the semester and should submit a report of the same presenting the workcarried out by him/her in the semester.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

Chairperson
Board of Studies – Forensic Science
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Chairperson
Faculty of Studies - Science
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Controller of Examinations
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore

Registrar
Shri Vaishnav Vidyapeeth
Vishwavidyalaya, Indore