MANAV RACHNA
vidyanatariksha

MANAV RACHNA UNIVERSITY
FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED A GRADE INSTITUTION
Declared as State Private University under section 2f of the UGC act, 1956

Manav Rachna University

FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE & TECHNOLOGY

Scheme & Syllabus

B.TECH-COMPUTER SCIENCE & ENGINEERING WITH SPECIALIZATION IN CYBER SECURITY& THREAT INTELLIGENCE IN ASSOCIATION WITH QUICKHEAL (CSU04) (2020-24)

MANAV RACHNA
vidyanatariksha

MANAV RACHNA UNIVERSITY
FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION
Declared as State Private University under section 2f of the UGC act, 1956

MANAV RACHNA UNIVERSITY
FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE&TECHNOLOGY
SYLLABUS & SCHEME
B.TECH-COMPUTER SCIENCE & ENGINEERING WITH SPECIALIZATION IN CYBER SECURITY& THREAT INTELLIGENCE IN ASSOCIATION WITH QUICKHEAL (CSU04) (2020-24)

Apart from the courses that have been picked from B.Tech CSE the specialization courses for Cyber Security& Threat Intelligence are as follows:

CSU04- Semester-I

SUBJECT CODES	SUBJECT NAME	PRE-REQUISITE	OVERLAPPING/EQUIVALENT COURSES	**OFFERING DEPARTMENT	*COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)	COURSE TYPE (Core/Elective)	L	T	P	O	NO. OF CONTACT HOURS PER WEEK	NO. OF CREDITS
CHH144-T&P	CHEMISTRY-I	NIL	NA	CH	HARD	CORE	3	1	2	0	6	5
ECH103B-T/P	BASICS OF ELECTRICAL & ELECTRONICS	NIL	NA	EC	HARD	CORE	3	1	2	0	6	5
CSH101B-T&P	PROGRAMMING FOR PROBLEM SOLVING USING C	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH109B-T&P	INTRODUCTION TO INFORMATION SECURITY	NIL	NA	CS	HARD	CORE	3	0	2	0	5	4
MEW102B	ENGINEERING GRAPHICS & DRAWING	NIL	NA	ME	WORKSHOP	CORE	0	0	3	0	3	1.5
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						**12**	**3**	**11**	**0**	**26**	**20.5**

DETAILED SYLLABUS
CSU04- Semester-I

Course Title/ Code	Introduction to Information Security
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(3-0-2-0)
Objectives	Students are able to understand the fundamentals of Information Security and Infrastructure

Syllabus	Sections	Weightage
	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

What is Information Security, Goals of Information Security: Integrity Models, Availability Models, and Security is not just VAPT, Security Models: Security Model Work, Confidentiality, Integrity, and Availability (CIA) Triad, Parkerian hexad, Real World Examples, Examples of Breach Incidents

Section-B

Domains of Cyber Security, Morals and Ethics, Cyber Law and Cyber Security: IT Act 2000 and Amendments, Cybercrime Motives, Psychological Profiling, Sociology of Cyber Criminals, Social Engineering, Cyber Stalking, Botnets Attack Vector, Real World Cases, Career in Information Security: Roles and Responsibilities, Entry Level Positions in Cyber Security, Current & Expected Growth in Cyber Security Industry

Section-C

Information Security Jargons: Jargon for Businesspeople, Countering Cyber Criminals, Knowing your Adversaries: Taking an Enemy Perspective, Adopting “Inside-Out” Security, Putting It All Together, Script Kiddies, Hacktivists, Nation State Actors, etc.

Section-D

Access Control: Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data, Discretionary Access Control (DAC): Discretionary Access Control (DAC) is a type of access control in which a user has complete control over all the programs it owns and executes, and also determines the permissions other users have those files and programs. , Mandatory Access Control (MAC): MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users, Role-based Access Control (RBAC): Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control.

LIST OF EXPERIMENTS:

1. Lab Setup and Installation of Virtual Machine
    - Different types of Virtual Machines: VirtualBox and VMware
    - Different types of OS file installation: Linux, Windows (ova/ovf/iso image)

2. Practice on following concepts
    - Confidentiality (Encryption, Steganography)
    - Integrity (Hash, Checksum etc.)
    - Availability (Backups)
    - Bash commands
3. Various Case Studies on Cyber Crimes and IT Act.

Books

1. Information Security: The Complete Reference by Mark Rhodes-Ousley
2. Computer Networking with Internet Protocols and Technology by William Stallings
3. Getting an Information Security Job for Dummies by Peter H. Gregory

Help Pages

1. Breaking into InfoSec: A beginner's guide to all things Cyber Security

Wikipedia Pages

1. Information Security: https://en.wikipedia.org/wiki/Information_security

Tool Web Sites

1. VMware: https://www.vmware.com/in.html
2. VirtualBox: https://www.virtualbox.org/
3. Kali: https://www.kali.org/downloads/

Web Tutorials

4. SANS: https://www.sans.org/information-security/
5. Geeksforgeeks: https://www.geeksforgeeks.org/what-is-information-security/
6. Info-Guard: https://www.infoguardsecurity.com/what-is-information-security-definition-principles-and-policies/

	SEMESTER - 2											
SUBJECT CODES	**SUBJECT NAME**	**PRE-REQUISITE**	**OVERLAPPING/EQUIVALENT COURSES**	****OFFERING DEPARTMENT**	***COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)**	**COURSE TYPE (Core/Elective)**	**L**	**T**	**P**	**O**	**NO. OF CONTACT HOURS PER WEEK**	**NO. OF CREDITS**
PHH101B - T&P	QUANTAM MECHANICS FOR ENGINEER	NIL	NA	PH	HARD	CORE	3	1	2	0	6	5
CSH110B	INTRODUCTION TO STANDARDS, FRAMEWORKS AND KEY TECHNOLOGY CONCEPTS	NIL		CS	HARD	CORE	5	0	0	0	5	5
HLS104B/HLS103B	PROFESSIONAL ENGLISH BASIC/ PROFESSIONAL ENGLISH	NIL	NA	ED	SOFT	ELECTIVE	2	0	2	0	4	3

	ADVANCE											
CSW208B	PROGRAMMING FOR PROBLEM SOLVING USING PYTHON	NIL	NA	CS	Workshop	CORE	0	0	3	0	3	1.5
MAH101B-T & P	CALCULUS & LINEAR ALGEBRA	NIL	NA	MA	HARD	CORE	3	1	2	0	6	5
CHH137	ENVIRONMENTAL STUDIES	NIL	NA	CH	AUDIT	CORE	2	0	0	2	2	0
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						**15**	**2**	**9**	**2**	**26**	**19.5**
CSO104B	Post 2nd Sem Summer Training (Mandatory) (Project Management)											2

Course Title/ Code	**Introduction to Standards, Frameworks and Key Technology Concepts**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(5-0-0-0)
Objectives	Students will have the understanding of Basic Standards, Framework and Guidelines

	Sections	**Weightage**
Syllabus	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

Introduction to Cyber Security Standards, Framework Basics and Guidelines Covered, Baseline IT Security Policy, IT Security Guidelines, Practice Guide for Security Risk Assessment & Audit, Practice Guide for Information Security Incident Handling, ISO 27000 Series, IT Act, Copyright Act, Patent Law, ISO 27001, IPR, CoBit: What is The COBIT Framework? Planning & Organization, Delivering and Support, Acquiring & Implementation, Monitoring & Evaluating, Various Components of Cobit: Framework, Process Descriptions, Control Objectives, Maturity Model, Management Guidelines, COBIT 5.0 the Most Celebrated Version

Section-B

PCI DSS: What is Payment Card Industries, Defining PCI-DSS, How does taking credit cards by phone work with PCI?, PCI DSS Compliance levels, PCI DSS requirements, PCI compliance, Getting started with PCI DSS, Business Continuity Plan: Open discussion on BCP, Business Continuity Plans, Key to Cybersecurity, Ways to get started, Cybersecurity and Business Continuity Are Co-dependent, Integrating Cybersecurity Practices with Business Continuity Management Strategies, Differences in Roles between Business Continuity Management and Disaster Recovery Teams.

Section-C

Risk Management Standards: Introduction to various risk management standards, ISO Risk management standard and process, evaluating the risk management framework, Risks affecting organizations, Risk Assessment Techniques, Standard Deviations: A Risk Practitioner Guide to ISO, Why Use Risk Management Standards, and Standards as Risk Management Tools.

Section-D

Access Control: Basic concepts in access control, Security/Emerging issues in Access Control, Network Security: Basic concepts in network security, Network Security Technology, Software Development Security: Basic concepts in software development security, Emerging issues in software development security, Cryptography: Basic concepts in cryptography, Emerging issues in cryptography, Physical and Environment Security, Basic concepts in physical and Environment Security, Emerging issues in Basic concepts in physical and Environment Security

LIST OF EXPERIMENTS:

1. Development and Preparation of ISO 27001 checklist for Audit
2. ISO 27001 – Understanding all policy documents
3. Practical's on OSI 7 Layers (Common Network Protocols)
4. Practical's on Security Protocols

Books

1. Information Security Policies, Procedures, and Standards: A Practitioner's Reference by Douglas J. Landoll
2. Getting an Information Security Job for Dummies by Peter H. Gregory

Help Pages

1. https://www.iso27001security.com/html/27001.html

Wikipedia Pages

1. ISO/IEC 27001: https://en.wikipedia.org/wiki/ISO/IEC_27001
2. PCI DSS: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
3. COBIT: https://en.wikipedia.org/wiki/COBIT
4. Information Technology Act, 2000: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

Tool Web Sites

1. ISO/IEC 27001: https://www.iso.org/isoiec-27001-information-security.html
2. PCI DSS: https://www.pcisecuritystandards.org/pci_security/
3. COBIT: https://www.isaca.org/resources/cobit
4. Ministry of Electronics & Information Technology: https://meity.gov.in/content/information-technology-act-2000

Web tutorials

1. Tutorials Point: https://www.tutorialspoint.com/auditing/auditing_internal_audit.htm
2. SANS: https://www.sans.org/reading-room/whitepapers/leadership/paper/33169
3. IT GOVERNANCE: https://www.itgovernance.co.uk/cyber-security-audit

	SEMESTER - 3											
SUBJECT CODES	SUBJECT NAME	PRE-REQUISITE	OVERLAPPING/EQUIVALENT COURSES	**OFFERING DEPARTMENT	*COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)	COURSE TYPE (Core/Elective)	L	T	P	O	NO. OF CONTACT HOURS PER WEEK	NO. OF CREDITS
MAH202B-T & P	PROBABILITY & STATISTICS	NIL	NA	MA	HARD	CORE	3	1	2	0	6	5
CSH103B-T&P	DATA STRUCTURES & ALGORITHMS	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH202B-T&P	DATABASE MANAGEMENT SYSTEM	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH213B-T&P	SECURE CODING IN in C/C++	NIL	NA	CS	HARD	CORE	1	1	3	0	5	3.5
EDS288/EDS289/EDS235	APP. PHILOSOPHY/APP. PSYCHOLOGY/ APP. SOCIOLOGY	NIL	NA	ED	SOFT	ELECTIVE	1	0	2	0	3	2
FLS101/FLS102/FLS103	FOREIGN LANGUAGE (SPANISH-I/ GERMAN-I/ FRENCH-I)	NIL	NA	FL	AUDIT	ELECTIVE	1	1	0	0	2	0
CDO201	PROFESSIONAL COMPETANCY ENHANCEMENT-I	NIL	NA	CDC	OUTCOME BASED	CORE	0	0	1	0	1	0.5
RDO501	INTRODUCTION TO RESEARCH	NIL	NA	RESEARCH	OUTCOME BASED	CORE	0	0	0	1	1	0.5
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						12	5	12	1	30	21.5

Course Title/ Code	Secure Coding in C/C++
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(0-0-5-0)
Objectives	Students will have the understanding of secure development through c/c++

Syllabus	Sections	Weightage
	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

Introduction to programming: Coding Standards Dirty Code and Dirty Compiler Introduction to C and C++ A brief history Identifying problem with C, Legacy code and other languages, Difference between C and C++Procedure vs. Object oriented Programming, Covering Basics of programming C & C++Introducing the Threat in Coding, Fundamentals of Security Concepts, Development Platforms, Basics of Compiler, Fundamentals of Operating System

Strings, Character Strings and Problem associated, String as a Class, Common string Manipulation Errors, Bounded String: Null Termination, String Vulnerability and Exploits, Security Flaws: Password Security, Buffer Overflow: String vs Character Array, Attacks using different type string injection, Handling string inputs, associated standard function for basic string, String handling functions

Pointers: Basics of pointers, Different program structures suing pointers, Type of pointers: Security Perspective, Pointers data location, Function pointers, Object pointers, Exception Handling: Basics programs, Type of exception Handling

Section-B

Dynamic Memory Management, C Memory management, Standard Memory management functions, Common C Memory Management Errors, Initialization Errors, Failing to Check Return Values, Memory Leaks, C++ Dynamic Memory Management, Allocation Functions / Deallocation Functions, Garbage Collection, Common C++ Memory Management Errors, Memory Managers, Doug Lea's Memory Allocator, Double-Free Vulnerabilities, Mitigation Strategies.

Section-C

Business Continuity Page Integer Security, Introduction to Integer Security, Integer Data Types, Integer Conversions, Integer Operations, Integer Vulnerabilities, Conversion and Truncation Errors, Nonexceptional Integer Logic Errors, Mitigation Strategies, Integer Type Selection, Formatted Output, Variadic Functions, Formatted Output Functions, Stack Randomization, Mitigation Strategies, Notable Vulnerabilities, Concurrency, Multithreading, Parallelism: Data and Task, Performance Goals, Common Errors: Race Conditions, Mitigation Strategies, and Notable Vulnerabilities.

Section-D

File I/O, File I/O Basics, File Systems, Special Files, File I/O Interfaces, Data Streams, Opening and Closing Files, POSIX Notation, File I/O in C++Access Control, UNIX File Permissions, File Identification, Race Conditions, Mitigation

Strategies, Eliminating the Race Object, Recommended Practices, The Security Development Lifecycle, Security Training, Secure Coding Standards, Design, Implementation and Verification, Verification, Static Analysis, Penetration Testing, Fuzz Testing and Code Audits.

Text Books:

1. Secure Coding in C and C++, Robert C. Seacord
2. Object Oriented Programming by E Balaguruswamy

Reference Books:

1. C++ How To Program 10th Edition by Paul Deitel and Harvey M Deitel

LIST OF EXPERIMENTS:

1. Scratch: Covering Concepts of
    - Basics of C and C++
    - How C is Different from C++
    - How to build any program using Debugging environment using C/C++
    - Secure Coding with Structured Environment
2. Lab Setup and Installation Different Compilers
    - Different types of Compilers and Debugging tools for C/C++
    - Different types of environment setup for Executing and Running Program Using Object File
    - Buffer Management, Null Termination and Code Mitigation: Secure Coding
3. Case Studies: Code Review Environment and Secure Code Structure

Help Pages

- Asset File Book Help Page Digital: resources.sei.cmu.edu/asset_files/BookChapter/2005_009_001_52710.pdf
- Introduction to Secure Coding: levelup.gitconnected.com/introduction-to-secure-coding-in-c-and-c-d8ece627facb
- Online Secure Coding Reference: www.nccgroup.com/us/online-secure-coding-in-c-and-c-course/
- Document Library: https://www.ibm.com/support/pages/xl-cc-linux-documentation-library

Wikipedia Pages

1. CERT C Standards: https://en.wikipedia.org/wiki/CERT_C_Coding_Standard
2. C++ Reference: https://en.wikipedia.org/wiki/C%2B%2B
3. Secure Coding: https://en.wikipedia.org/wiki/Secure_coding

Tool Web Sites

1. DevC++: https://www.bloodshed.net/dev/devcpp.html
2. TurboC: https://archive.codeplex.com/?p=turboc
3. CPPHeck: http://cppcheck.sourceforge.net
4. Clang: https://clang-analyzer.llvm.org
5. Eclipse, https://eclipse.org/users/
6. Git, http://git-scm.com/
7. GCC, https://gcc.gnu.org/onlinedocs/gcc-4.9.3/gcc/

Web Tutorials

1. Lynda: https://www.lynda.com/C-tutorials/Secure-Coding-C/2242047-2.html
2. Class Central: https://www.classcentral.com/course/identifying-security-vulnerabilities-c-p-14509
3. Accelebrate: https://www.accelebrate.com/training/c-secure-coding
4. Infosec Institute: https://www.infosecinstitute.com/courses/secure-coding-for-c/
5. Coursera: https://www.coursera.org/specializations/secure-coding-practices

SEI: https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=V35

	SEMESTER - 4											
SUBJECT CODES	SUBJECT NAME	PRE-REQUISITE	OVERLAPPING/EQUIVALENT COURSES	**OFFERING DEPARTMENT	*COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)	COURSE TYPE (Core/Elective)	L	T	P	O	NO. OF CONTACT HOURS PER WEEK	NO. OF CREDITS
CSH205B-T&P	COMPUTER NETWORKS	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH206B-T&P	OPERATING SYSTEMS	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH201B-T&P	OOPS USING JAVA	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
CSH214B-T&P	DIGITAL FORENSICS	NIL	NA	CS	HARD	CORE	2	0	3	0	5	3.5
FLS105/FLS106/ FLS107	FOREIGN LANGUAGE	NIL	NA	FL	AUDIT	ELECTIVE	1	0	0	0	1	0
LWS324	INDIAN CONSTITUTION	NIL	NA	LW	AUDIT	CORE	1	0	0	0	1	0
EDS240	ESSENCE OF INDIAN TRADITIONAL KNOWLEDGE	NIL	NA	ED	AUDIT	CORE	1	0	0	0	1	0
CDO202	CDC	NIL	NA	CDC	OUTCOME	CORE	0	0	1	0	1	0.5
RDO502	RESEARCH & INNOVATION-1	NIL	NA	RESEARCH	OUTCOME	CORE	0	0	0	1	1	0.5
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						**14**	**3**	**10**	**1**	**28**	**19.5**
CSO215B	SUMMER TRAINING POST 4TH SEMESTER											2

Course Title/ Code	**Digital Forensics**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(1-0-4-0)
Objectives	Students will have the understanding implementation of forensics and investigation techniques.

Syllabus	Sections	Weightage
	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

Introduction to Digital Forensics, What is Digital Forensics, Uses of Digital Forensics, What skills should a computer forensic expert have, Locard's exchange principle, Key Technical Concepts, Storage Types, Hard Disk Structure, File System overview, Allocated, Unallocated Space, Slack Space, Free Space, etc., File f. Deleted vs. Wiped

Section-B

Digital Evidence Acquisition Essentials: Identifying Disk Regions That May Contain Evidence, Potential Limitations of Sifting Collectors, Digital Forensics of Different services, Digital Forensics analysis, what is an Image, Evidence Acquisition Basics, Acquisition Types and Methods: Forensic acquisition methods for various platforms, Chain of Custody, Evidence Handling, and Evidence Integrity?

Section-C

Digital Forensics Analysis Process: Analysis of Digital Evidence, Scope of Analysis, Logical and/or Deleted Data, Acquisition to Reporting Cycle, Registry Forensics: Registry File Acquisition, Access Data FTK Imager, Registry Structure, Issues in Registry Analysis

Section-D

Windows Artifacts Analysis: Windows registry structure, Registry Hive vs Supportive Hive, Registry Files, Windows System Artifacts, USB Device Forensics: USB Flash Drives, Flash Drives Store Data, USB Flash Drive Forensics, Recovering Data from Broken or Destroyed USB Flash Drives, Retrieving Data from Monolithic USB Flash Drives

LIST OF EXPERIMENTS:

1. Installation of various tools used in Digital Forensics.
2. Practice of extraction of information from a forensic image.
3. Practical on reconnaissance
4. Collecting evidence
5. Network forensics
6. Practice on CTF challenges for the forensic investigations.
7. Report and Summary formation post an investigation with POC.

Books

1. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey
2. Windows Forensic Analysis Toolkit by Harlan Carvey
3. The Basics of Digital Forensics by John Sammons

Help Pages

1. Digital forensics: A cheat sheet: https://www.techrepublic.com/article/digital-forensics-the-smart-persons-guide/
2. Computer Forensics: https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf

Wikipedia Pages

1. Digital Forensics: https://en.wikipedia.org/wiki/Digital_forensics
2. Computer Forensics: https://en.wikipedia.org/wiki/Computer_forensics

3. List of Digital Forensics tools: https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

Tool Web Sites

1. FTK Imager: https://accessdata.com/product-download/ftk-imager-version-4-2-1
2. Autopsy: https://www.autopsy.com/
3. Strings: https://docs.microsoft.com/en-us/sysinternals/downloads/strings
4. HashMyFiles: https://www.nirsoft.net/utils/hash_my_files.html
5. Encase: http://www.guidancesoftware.com/encase-forensic
6. Kali Linux: https://www.kali.org/

Web tutorials

1. Hacking Tutorials: https://www.hackingtutorials.org/category/digital-forensics/
2. NICCS: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/digital-forensics
3. NIJ ORG: https://nij.ojp.gov/digital-evidence-and-forensics

	SEMESTER - 5											
SUBJECT CODES	**SUBJECT NAME**	**PRE-REQUISITE**	**OVERLAPPING/EQUIVALENT COURSES**	****OFFERING DEPARTMENT**	***COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)**	**COURSE TYPE (Core/Elective)**	**L**	**T**	**P**	**O**	**NO. OF CONTACT HOURS PER WEEK**	**NO. OF CREDITS**
CSH329B-T&P	NETWORK SECURITY	NIL	NA	CS	HARD	CORE	2	0	3	0	5	3.5
CSH311-B-T&P	THEORY OF AUTOMATA & COMPILER DESIGN	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
ECH308B-T/P	Digital Electronics & Microcontroller	NIL	NA	EC	HARD	CORE	3	1	2	0	6	5
CSW308B	ADVANCED JAVA	OOPs using JAVA	NA	CS	WORKSHOP	CORE	0	0	3	0	3	1.5
CHS234/ECS306B/ CSS325B- T&P	ENVIRONMENTAL ETHICS & SUSTAINABLE DEVELOPMENT/ GREEN COMPUTING/ E-WAStE MANAGEMENT	NIL	NA	CH/EC	SOFT	ELECTIVE	1	0	2	0	3	2
LWS321/LWS323	CYBER LAW/ LAW RELATING TO	NIL	NA	LW	SOFT	ELECTIVE	2	0	0	0	2	2

	INTELLECTUAL PROPERTY RIGHTS											
MOOC	NPTEL Courses from MOOC											
CDO305	PROFESSIONAL COMPETANCY ENHANCEMENT-III	NIL	NA	CDC	OUTCOME	CORE	0	0	1	0	1	0.5
RDO601	RESEARCH & INNOVATION-II	NIL	NA	RESEARCH	OUTCOME	CORE	0	0	0	1	1	0.5
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						**11**	**2**	**13**	**0**	**26**	**20**

Course Title/ Code	**Network Security**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(2-0-3-0)
Objectives	Students will have the understanding and hands on expertise to live network associated attack vectors and threats

	Sections	**Weightage**
Syllabus	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

Network Security: Related challenges, Different attacks vectors and network threats: DDOS, MITM, Packet Analysis, Port Forwarding, And Implementation of prevention from network attacks, Wireless Security: Wireless Attacks, WEP, WPS, WPA/WPA2, Attacking a Wireless network: Aircrack-ng, Airmon, Airodump, reaver etc. Improving Wireless Security, Access control: IAM, Control Mechanism, 2 Factor Authentication, Multifactor Authentication, Antivirus and antimalware software: AV Software Structure, AV database and AI, Stuxnet, Morris Worm, Mellissa Worm, Application security, Behavioural analytics, Cloud Security: Cloud Infrastructure, Common cloud platforms, Software as a service risk

Section-B

Data loss prevention: Data Vs Information, Information Systems, Threat related to information Systems, Data Recovery and Backup, Email security: Tradition Email Technology, SMTP, Email Encryption, Email Header, Analysing email

headers, Firewalls: Fire wall definition Roles and Responsibility in any network, Statefull vs Stateless firewall, Intrusion prevention systems: Intrusion Detection vs Prevention methodology, Honeypots, Mobile device security: Mobile platforms threats, local storage, security policies, jail-breaking, rooting your device, mobile backdoors, Network segmentation, Security information and event management, Application and operating system security, Connected Web and Network Security

Section-C

OSI vs TCP Model: Security Risks with respect to each layer supported protocols, Packet Analysis Fundamentals: Packet Analysis and Network Basics Tapping into the Wire, Introduction to Wireshark, Working with Captured Packets, Common Lower-Layer Protocols Common Upper-Layer Protocols Basic Real-World Scenarios Fighting a Slow Network Packet Analysis for Security Wireless Packet Analysis, HTTP vs HTTPS Traffic, SSL vs TLS versions, Socket Layer implementation and necessity, Traffic Relay Attacks, Introduction to Interceptors: Burpsuite, Zed Attack Proxy (ZAP) OWASP etc.

Section-D

Countermeasures and increasing network security: Hardware countermeasure, Behavioral countermeasures, Implementing Control Systems and Access Control listing, Countermeasures for Each Layer (Secure Multipurpose Internet Mail Extensions (S/MIME), Privacy Enhanced Mail (PEM), Secure Shell (SSH)), Types of Countermeasures (hi-tech, lo-tech, and no-tech), Optimum Countermeasure Portfolio Selection, From User-Land to Kernel-Land Attacks

LIST OF EXPERIMENTS:

1. Installation and Practice on dummy network images for security testing.
2. Practical's on Network Security Protocols
3. Analyze and solve CTF challenges for the network security.
4. Monitoring and Analysis of live network to understand the various protocols and packets exchange system.
5. Report network intrusion incident with POC.
6. Practical on Zed Attack Proxy: Monitoring and Analyzing Modified Packets

Books

1. Network Security Essentials Applications and Standards by William Stallings
2. Network Security: The Complete Reference by Roberta Bragg

Help Pages

1. Network Security: https://www.sans.org/reading-room/whitepapers/basics/network-security-guide-small-mid-sized-businesses-1539
2. Cyber and Network Security: https://www.nist.gov/itl/cyber-and-network-security

Wikipedia Pages

1. Network Forensics: https://en.wikipedia.org/wiki/Network_forensics
2. Wireshark: https://en.wikipedia.org/wiki/Wireshark

Tool Web Sites

1. Wireshark: https://www.wireshark.org/
2. Network Miner: https://www.netresec.com/?page=NetworkMiner
3. Kali Linux: https://www.kali.org/

Web tutorials

1. Network Forensics: https://www.lynda.com/Wireshark-tutorials/Network-Forensics/806160-2.html
2. Geeksforgeeks: https://www.geeksforgeeks.org/computer-network-tutorials/
3. SANS: https://isc.sans.edu/presentations/first_things_first.html

	SEMESTER - 6											
SUBJECT CODES	SUBJECT NAME	PRE-REQUISITE	OVERLAPPING/ EQUIVALENT COURSES	**OFFERING DEPARTMENT	*COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/ Outcome)	COURSE TYPE (Core/Elective)	L	T	P	O	NO. OF CONTACT HOURS PER WEEK	NO. OF CREDITS
CSH330B-T&P	VULNERABILITY ASSESSMENT AND PENETRATION TESTING	NIL	NA	CS	HARD	CORE	1	1	3	0	5	3.5
CSH314B-T&P	Artificial Intelligence & Machine Learning	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
MCS368B	ENTREPRENEURSHIP	NIL	NA	MC			1	0	2	0	3	2
MOOC	NPTEL Courses from MOOC				SOFT	ELECTIVE						
CSW407B	USER EXPERIENCE	NIL	NA	CS	WORKSHOP	CORE	0	0	3	0	3	1.5
ECW204B/MEW314B / MEW315B / MEW316B /CSW317B	ELECTRONIC DESIGN WORKSHOP / Manufacturing Workshop/ 3-D Software/ CNC / AGILE TECHNOLOGIES	NIL	NA	EC/ME/ CS			0	0	3	0	3	1.5
MOOC	NPTEL Courses from MOOC				WORKSHOP	ELECTIVE						
ECW310B/MEH439/MEW318B/MEW319B/CSW318B	SENSORS & IOT/ Basic of Robotics/ 3 D Printing/ SAP/ R PROGRAMMING	NIL	NA	EC/ME/ CS			0	0	3	0	3	1.5
MOOC	NPTEL Courses from MOOC				WORKSHOP	ELECTIVE						

CDO306	PROFESSIONAL COMPETANCY ENHANCEMENT-IV	NIL	NA	CDC	OUTCOME	CORE	0	0	1	0	1	0.5
TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)							**5**	**2**	**17**	**0**	**24**	**15.5**
CSO320B	SUMMER TRAINING POST 6TH SEMESTER											3

Course Title/ Code	**Vulnerability Assessment and Penetration Testing**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(1-0-4-0)
Objectives	Students will have the understanding of core concept of VAPT with practical implementation

	Sections	**Weightage**
Syllabus	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

What is VAPT: VAPT Process Vulnerability Assessment Tools, Cyber Security Foundation, Essential Tools and Commands, Information Gathering: Active and Passive Ways, Vulnerability Scanning and Assessment, Buffer Overflows: Different Machine Perspective

Section-B

Client Side and Web Application Attacks, Password and Hashing: Generating and Cracking, John The Ripper, hashcat, hashkiller, Bypassing Antivirus Software, Penetration Testing, Network Penetration Testing: Nmap, Nessus,Web Application Penetration testing

Section-C

Web Application Penetration testing, Social Engineering Penetration Testing, Wireless Penetration Testing, Introduction to tools like, sqlmap shodan Aircrack-ng suite, Cloud Penetration Testing, Database Security and Penetration Testing: SQLMap, sqlninja

Section-D

Smartphone Penetration Testing Framework, Phase of Exploitation: Pre-Exploitation vs Post-Exploitations, Escalating an Attack with Exploitation: Metasploit framework guide, Cybersecurity Technologies: Introduction to Cryptography, Threat and Vulnerability Assessment

LIST OF EXPERIMENTS:

1. Lab Setup for the Vulnerability Assessment and Penetration Testing.
2. Practical's on Reconnaissance
3. Practical's on Scanning Various Targets
4. Practical's on Gaining Access
5. Practical's on Maintaining Access
6. Take walkthrough different retarded and live machines with vulnerabilities.
7. Solve CTF challenges with respect to information security.
8. Challenges to get root level access of the system and bypass it.
9. Practical's on Bypassing Firewall with the Help of Flagged TCP Packets

Books

1. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman
1. Basic Security Testing with Kali Linux 2 by Daniel W. Dieterle.

Help Pages

1. https://www.kali.org

Wikipedia Pages

1. Vulnerability Assessment: https://en.wikipedia.org/wiki/Vulnerability_assessment
2. Penetration Test: https://en.wikipedia.org/wiki/Penetration_test

Tool Web Sites (Tools may vary or added as per current situation)

1. https://www.kali.org
2. https://www.zaproxy.org
3. https://nmap.org
4. https://www.metasploit.com
5. https://www.wireshark.org
6. https://www.openwall.com/john/
7. https://github.com/vanhauser-thc/thc-hydra
8. https://portswigger.net/burp

Web tutorials

1. https://www.opensourceforu.com/2017/06/basics-vulnerability-assessment-penetration-testing/
2. https://www.cybrary.it/course/advanced-penetration-testing/
3. https://www.tutorialspoint.com/penetration_testing/index.htm

	SEMESTER - 7											
SUBJECT CODES	SUBJECT NAME	PRE-REQUISITE	OVERLAPPING/EQUIVALENT COURSES	**OFFERING DEPARTMENT	*COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)	COURSE TYPE (Core/Elective)	L	T	P	O	NO. OF CONTACT HOURS PER WEEK	NO. OF CREDITS
CSH420B-T&P	SECURE SOFTWARE DEVELOPMENT AND MALWARE ANALYSIS AND REVERSE ENGINEERING (PART-1)	NIL	NA	CS	HARD	CORE	1	1	3	0	5	3.5

CSH415B-T&P	Internet of Things	NIL	NA	CS	HARD	CORE	3	1	2	0	6	5
EDH422	BIOLOGY	NIL	NA	ED	SOFT	CORE	2	0	0	0	2	2
ECH403B/ ECH401B-T/P/ MEH401B/ MEH402B/ME H403B	INTERFACING ANDROID WITH EMBEDDED SYSTEMS/ ROBOTICS IN AUTOMATION/ Non Conventional Energy Sources/ Heating, Ventilation and Air Conditioning (HVAC)/ Operation Research by Optimising Technique	NIL	NA	EC/ME/CS	HARD	ELECTIVE	3	1	2	0	6	5
MOOC	NPTEL Courses from MOOC											
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)						**9**	**3**	**7**	**0**	**19**	**15.5**

Course Title/ Code	**Secure Software Development and Malware Analysis and Reverse Engineering (Part 1)**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(2-0-3-0)
Objectives	Students will be able to understand the core technologies behind malware analysis and malware behavior

	Sections	**Weightage**
Syllabus	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

C/C++ from Reverse Engineering Perspective, Data Types and Memory layout, Windows Internals - Part 1, Windows Environment - User mode, Windows APIs, File System, Windows Registry, Process and Threads, Memory Management, Network functions, x86 Assembly Language, Registers, Instruction Types, Stack Basics

Section-B

Malware Analysis Lab Setup - Part 1, Malware Analysis - Part 1, Trojan, Worm, Backdoor, Virus, Spyware, Keylogger, Static Malware Analysis, Looking for uncommon and malicious traits, Dynamic Malware Analysis, Analysing behaviour with monitoring tools, Advance Assembly Language

Section-C

Windows Executable (PE) file format, PE File Header, Sections, Data Directories, Imports & Exports, Windows Internals - Part 2, Dynamic Link Libraries, Windows Services, Synchronization Objects, Windows Kernel mode, Malware Analysis Lab Setup - Part 2

Section-D

Debugger - Part 1, Malware Analysis - Part 2, Ransomware, Adware & Potentially Unwanted Applications, Network Analysis - Part 1, TCP/IP network stack, Common network protocols - SMTP, POP, FTP, HTTP, HTTPS, Network Monitoring tools – Wireshark, Automated Malware Analysis Tools.

**MARE – 2 Partial Syllabus may be covered in this module as in next module students will be working on the QHA Projects.

LIST OF EXPERIMENTS:

1. Malware Analysis and remote execution of malware in insolated environment. (Static and Dynamic Analysis)
2. Reverse Engineer and understand the functioning of a malware.
3. Solve the CTF challenges presented with relation to malware analysis.

Books

1. Practical Malware Analysis – The Hands–On Guide to Dissecting Malicious Software – Michael Sikorski
2. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

Help Pages

1. Malware Analysis: https://niccs.us-cert.gov/training/search/defense-cyber-investigation-training-academy/malware-analysis
2. Malware Analysis Submission: https://www.malware.us-cert.gov/

Wikipedia Pages

1. Malware Analysis: https://en.wikipedia.org/wiki/Malware_analysis
2. Malware Research: https://en.wikipedia.org/wiki/Malware_research

Tool Web Sites (Tools may vary or added as per current situation)

Static Malware Analysis

- Virus Total: https://www.virustotal.com/
- Hybrid Analysis: https://www.hybrid-analysis.com/
- Windows Sysinternal Tools: https://docs.microsoft.com/en-us/sysinternals/

Dynamic Malware Analysis

- IDA Pro: https://www.hex-rays.com/products/ida/
- Ollydbg: http://www.ollydbg.de/

Web tutorials

1. https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Paper/bh-dc-07-Kendall_McMillan-WP.pdf
2. https://www.csee.umbc.edu/courses/undergraduate/CMSC491malware/docEng2017.html
3. https://www.begin.re
4. https://hakin9.org/download/reverse-engineering-tutorials-hakin9-ondemand/

	SEMESTER - 8											
SUBJECT CODES	**SUBJECT NAME**	**PRE-REQUISITE**	**OVERLAPPING/EQUIVALENT COURSES**	****OFFERING DEPARTMENT**	***COURSE NATURE (Hard/Soft/ Workshop/ NTCC/Audit/Outcome)**	**COURSE TYPE (Core/Elective)**	**L**	**T**	**P**	**O**	**NO. OF CONTACT HOURS PER WEEK**	**NO. OF CREDITS**
MCS232/MCS231	INTRODUCTION TO FINANCE BASICS OF ECONOMICS	NIL	NA	MC	SOFT	ELECTIVE	1	0	2	0	3	2
CSH413B-T&P	PROJECT	NIL	NA	CS	NTCC	CORE	320 TO 360 HOURS					8
CSH421B-T&P	SECURE SOFTWARE DEVELOPMENT AND MALWARE ANALYSIS AND REVERSE ENGINEERING (PART-2)	NIL	NA	CS	HARD	CORE	1	1	3	0	5	3.5
CSH305B-T&P	NEURAL NETWORKS & FUZZY LOGIC	NIL	NA	CS	HARD	ELECTIVE						5
CSH324B-T&P	NATURAL LANGUAGE PROCESSING	NIL	NA	CS								
CSH416B-T&P	COMPUTER VISION & DATA VISUALIZA	NIL	NA	CS			3	1	2	0	6	

	TION											
MOOC	NPTEL Courses from MOOC											
	TOTAL (L-T-P-O/CONTACT HOURS/CREDITS)							**5**	**2**	**7**	**0**	**14**	**18.5**

Course Title/ Code	**QHA Project and Malware Analysis (Part 2)**
Course Type	Core (QHA)
Course Nature	Hard
L-T-P-O Structure	(0-0-6-0)
Objectives	Students will have the hands on experience on Secure Development and practical Malware Analysis

	Sections	**Weightage**
Syllabus	A	25%
	B	25%
	C	25%
	D	25%
	TOTAL	**100%**

Section-A

Fundamental Practices for Secure Software Development, Essential Elements of a Secure Development Lifecycle Program, Secure Design Principles, Standardize Identity and Access Management, Establish Log Requirements and Audit Practices, Need for Secure Software Development: The Importance of Secure Development, Secure Software Development Lifecycle Process: Secure Development Lifecycle, Secure Coding: Establish Coding Standards and Conventions

Section-B

Obfuscation Techniques, Understanding different Packers & Installers, Compression Algorithms - Zlib, ApLib, Debugger - Part 2, Malware Analysis - Part 3, Android Malware Analysis, ELF file format and Linux Malware, Network Analysis - Part 2, Network protocols - telnet, ssh, SMB, RDP, Network traffic analysis, Snort rules

Section-C

Network Monitoring tools - tcpdump, Wireshark, Fiddler, nmap, TCPViewer, Burp Suite, 64-bit Assembly Language, Using Python for Malware Analysis, Anti-Reverse Engineering techniques, Anti-debug, Anti VM techniques, Defeat Anti-Reverse Engineering techniques, Encryption Algorithms, RSA, AES etc.

Section-D

Social Engineering, Phising, Spamming, Malware Analysis - Part 4, Analysing Visual Basic, Delphi, .NET compiled programs, Rootkit, Bootkit Analysis, Advanced Persistent Threats, How Crypto-Currency works, Bitcoins etc., Mining, Vulnerabilities Exploit Analysis, File format vulnerabilities & exploits, Buffer Overflow, Stack Overflow, Memory Corruption, User after free vulnerabilities, PDF, SWF, RTF & OLE file analysis & tools, Script based malware analysis, Javascript, Powershell, Bash, Fuzzing Techniques, Brute Force, Debugger - Part 3.

****Training and Evaluation of this module will be based on following distribution**

- **25% of Malware Analysis and 75% of Allocated QHA Project**

LIST OF EXPERIMENTS:

1. Malware Analysis and remote execution of malware in insolated environment.
2. Reverse Engineer and understand the functioning of a malware.
3. Solve the CTF challenges presented with relation to malware analysis

Books

1. The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software (Developer Best Practices)
2. Practical Malware Analysis – The Hands–On Guide to Dissecting Malicious Software – Michael Sikorski
3. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

Help Pages

1. Malware Analysis: https://niccs.us-cert.gov/training/search/defense-cyber-investigation-training-academy/malware-analysis
2. Malware Analysis Submission: https://www.malware.us-cert.gov/

Wikipedia Pages

1. Malware Analysis: https://en.wikipedia.org/wiki/Malware_analysis
2. Malware Research: https://en.wikipedia.org/wiki/Malware_research

Tool Web Sites

Static Malware Analysis

- Virus Total: https://www.virustotal.com/
- Hybrid Analysis: https://www.hybrid-analysis.com/
- Windows Sysinternal Tools: https://docs.microsoft.com/en-us/sysinternals/

Dynamic Malware Analysis

- IDA Pro: https://www.hex-rays.com/products/ida/
- Ollydbg: http://www.ollydbg.de/

Web tutorials

1. http://fumalwareanalysis.blogspot.com/p/malware-analysis-tutorials-reverse.html
2. https://zeltser.com/reverse-engineering-malware-methodology/
3. https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques
4. https://www.onlinefreecourse.net/expert-malware-analysis-and-reverse-engineering-udemy-free-download/