Faculty:ScienceandTechnology

Syllabus Prescribed for3YearB.Sc. CyberSecurity UG Programme [CBCS]

SEMESTER: III

Programme: B.Sc.Cyber Security

Title: Incident Response

Type:AEC

Credits: 3

TotalMarks-50		CourseCode:3CS1	(TotalNumberofPeriods)Hrs
TheoryExamMarks:40	InternalMarks:10	MinPassing:20	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Learnhowtohandletheincidentresponsemanagement.
2. Performlivedatacollectionandforensicduplication.
3. Identifynetworkevidence.
4. Analyzedatatocarryoutinvestigation.

Unit	Content
Unit-1Introduction: (09 HRS)	Preparing for the Inevitable incident: Real world incident, IR management incident handbook, Pre-incident preparation, Preparing the Organization for Incident Response, Preparing the IR team, Preparing the Infrastructure forIncident Response. Incident Detection and Characterization: Getting the investigation started on the right foot, collecting initial facts, Maintenance ofCase Notes, Understanding Investigative Priorities. Discovering the scope of incident: Examining initial data, Gathering and reviewing preliminary evidence, determiningacourseofaction,Customerdatalossscenario,Automated clearingfraudscenario.
Unit-2 Data Collection: (09 HRS)	Live Data Collection: When to perform live response, Selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-Based Systems. Forensic Duplication:ForensicImageFormats,Traditionalduplication,Livesystem duplication,DuplicationofEnterpriseAssets.
Unit-3 Network Evidence: (09 HRS)	The case for network monitoring, Types for network monitoring, Setting Up a Network Monitoring System, Network Data, Analysis, Collect Logs Generated fromNetworkEvents.EnterpriseServices:NetworkInfrastructureServices, EnterpriseManagementApplications,Webservers,DatabaseServers
UNIT-4 Data Analysis: (09 HRS)	Analysis Methodology: Define Objectives, Know your data, Access your data, Analyseyourdata,EvaluateResults.InvestigatingWindowsSystems:NTFS and File System analysis, Prefetch, Event logs, Scheduled Tasks, The Windows Registry,OtherArtifactsofInteractiveSessions,MemoryForensics,Alternative PersistenceMechanisms.

UNIT-5 Investigating Mac OS X Systems: (09 HRS)	HFS+ and File System Analysis, Core Operating systems data. Investigating Applications: What is Application Data?, Where is application data stored?, GeneralInvestigationmethods,WebBrowser,EmailClients,InstantMessage Clients.

TextBook:

1. "Incident Response and Computer Forensics", Jason T. Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents", Eric. C. Thompson, Apress.

ReferenceBook:

1. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk", N.K. McCarthy, Tata McGraw-Hill.

Programme: B.Sc.CyberSecurity

Title: Cryptography

Type:DSE

Credits: 4

TotalMarks-100		CourseCode:3CS2(E1)	(TotalNumberofPeriods)Hrs
TheoryExamMarks:80	InternalMarks:20	MinPassing:40	60

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Classifythesymmetricencryptiontechniques
2. Illustratevariouspublickeycryptographictechniques
3. Evaluatetheauthenticationandhashalgorithms.
4. Discussauthenticationapplications
5. Summarizetheintrusiondetectionanditssolutionstoovercometheattacks.
6. Understandbasicconceptsofsystemlevelsecurity

Unit	Content
Unit-1(12HRS)	Attacks on Computers and Computer Security: Introduction, Need for Security, Security Approaches, Principles of Security, Types of Attacks. Cryptography: Concepts and Techniques Introduction, Plain Text and Cipher Text, Substitution and Transposition Techniques, Encryption and Decryption, Symmetric and AsymmetricKeyCryptography,Stenography,KeyRangeandKeySize, Possible TypesofAttacks
Unit-2(11HRS)	SymmetricKey Algorithmsand AES:Introduction, AlgorithmTypesand Modes, An Overview of Symmetric Key Cryptography, Data Encryption Standard(DES),InternationalDataEncryptionAlgorithm(IDEA),RC4,RC5, Blowfish,AdvancedEncryptionStandard(AES).

Unit-3(12HRS)	AsymmetricKeyAlgorithms,DigitalSignaturesandRSA:Introduction, History and Overview of Asymmetric Key Cryptography, The RSA Algorithm, SymmetricandAsymmetricCryptography,DigitalSignatures,Knapsackand otherAlgorithms.
UNIT-4(15HRS)	Digital Certificates and Public Key Infrastructure (PKI): Introduction, Digital Certificates, Private Key Management, The PKIX Model, Public Key CryptographyStandards(PKCS),XML,PKIandSecurity,CreatingDigital Certificate.
UNIT-5(10HRS)12	Internet Security Protocols: Introduction, Concepts, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Hypertext Transport Protocol(SHTTP), TimeStampingProtocol(TSP),SecureElectronicTransaction(SET),SSL Versus SET, 3-D Secure Protocol, Electronic Money, Email Security, Wireless Application Protocol(WAP)Security, Security in GSM, Security in 3G User Authentication and Kerberos: Introduction, Authentication Basics, Passwords, Authentication Tokens, Certificate-based-Authentication, Biometric Authentication,Kerberos,KeyDistributionCenter(KDC),SecurityHandshake Pitfalls,SingleSignOn(SSO)Approaches.

TestBook:

1. AtulKahate,"CryptographyandNetworkSecurity",McGrawHill,SecondEdition

ReferenceBook:

1. William Stallin gs, "Cryptography and Network Security, Principles and Practice", PHI Fourth Edition. Behrouz A.
2. Forouzan and Debdeep Mukhopadhyay,"Cryptography and Network Security", McGrawHill, Second Edition.
3. MattBishop,"ComputerSecurityArtsandScience",PearsonEducation.
4. DouglasRStinson,"Cryptography,TheoryandPractice"CRCPress.
5. Keith M Martin, "Everyday Cryptography, Fundamental Principles and Applications", Oxford University Press, Second Edition.

Programme: B.Sc.CyberSecurity

Title: Cloud Computing

Type:DSE

Credits: 4

TotalMarks-100		**CourseCode:3CS2(E2)**	**(TotalNumberofPeriods)Hrs**
TheoryExamMarks:80	**InternalMarks:20**	**MinPassing:40**	**60**

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Understand different computing paradigms and potential of the paradigms and specifically cloud computing
2. Understand cloud service types, cloud deployment models and technologies supporting and driving the cloud

3. Acquire the knowledge of programming models for cloud and development of software application that runs the cloud and various services available from major cloud providers
4. Understandthesecurityconcernsandissuesincloudcomputing
5. Acquiretheknowledgeofadvancesincloudcomputing.

Unit	Content
Unit-1Cloud Computing Fundamentals (10 HRS)	ComputingParadigms,CloudComputingFundamentals,CloudComputing Architecture and Management
Unit-2 Models (14 HRS)	CloudDeploymentModels,CloudServiceModels,TechnologicalDriversfor CloudComputing:SOAandCloud,MulticoreTechnology,Web2.0andWeb 3.0,PervasiveComputing,OperatingSystem, ApplicationEnvironment
Unit-3Virtualization (12HRS)	Virtualization,ProgrammingModelsforCloudComputing:MapReduce,Cloud Haskell,SoftwareDevelopmentinCloud
UNIT-4Networking for Cloud Computing (12HRS)	NetworkingforCloudComputing:Introduction,OverviewofDataCenter Environment,NetworkingIssuesinDataCenters,TransportLayerIssuesin DCNs,CloudServiceProviders
UNIT-5 Security in Cloud Computing (12 HRS)	SecurityinCloudComputing,andAdvancedConceptsinCloudComputing

TextBook:

1. Chandrasekaran,K.Essentialsofcloudcomputing.CRCPress,2014.

ReferenceBook:

1. Cloud Computing: Principles and Paradigms, Editors: Rajkumar Buyya, James Broberg,Andrzej M. Goscinski, Wiley, 2011
2. Enterprise Cloud Computing - Technology,Architecture, Applications, Gautam Shroff, Cambridge University Press, 2010
3. CloudComputingBible,BarrieSosinsky,Wiley-India,2010.

Programme:B.Sc.CyberSecurity

Title:WebTechnologies&Development Type:

Core Skill

Credits:4

TotalMarks-100		CourseCode:3CS3	(TotalNumberofPeriods)Hrs
TheoryExamMarks:80	**InternalMarks:20**	**MinPassing:40**	**60**

CourseOutcome(CO):

Aftersuccessfulcompletionofthecourse,studentswillableto:

1. ConstructabasicwebsiteusingHTMLandCascadingStyleSheets
2. Builddynamic web page with validation using Java Script objects and by applying different event handling mechanisms.
3. Developserver-sideprogramsusingServletsandJSP.

4. ConstructsimplewebpagesinPHP andtorepresentdatainXMLformat.
5. Developinteractivewebapplications.

Unit	Content
Unit-1WEBSITE BASICS,HTML5, CSS 3, WEB 2.0 (14 HRS)	Web Essentials: Clients, Servers and Communication – The Internet – Worldwideweb–HTTP RequestMessage–HTTP ResponseMessage–WebClients – Web Servers – HTML5 – Tables – Lists – Image – HTML5 control elements – DragandDrop– Audio– Videocontrols-CSS3–Inline,embeddedand external style sheets – Rule cascading – Inheritance – Backgrounds – Border Images–Colors–Shadows–Text–Transformations–Transitions–Animations.BootstrapFramework
Unit-2 CLIENT SIDE PROGRAMMING (13HRS)	JavaScript:AnintroductiontoJavaScript–JavaScriptDOMModel-Exception Handling-ValidationBuilt-inobjects-EventHandling-DHTMLwithJavaScript-JSONintroduction–Syntax–FunctionFiles.
Unit-3 SERVER SIDE PROGRAMMING (12HRS)	Servlets:JavaServlet Architecture-ServletLifeCycle-FormGETandPOST actions-Session Handling-UnderstandingCookies-DATABASECONNECTIVITY:JDBC.
UNIT-4 PHPand XML (11 HRS)	An introduction to PHP: PHP- Using PHP- Variables- Program control- Built-in functions-FormValidation.XML:BasicXML-DocumentTypeDefinition-XMLSchema,XMLParsersandValidation,XSL,
UNIT-5 INTRODUCTION TO ANGULAR and WEB APPLICATIONS FRAMEWORKS (10 HRS)	Introduction to AngularJS, MVC Architecture, Understanding ng attributes, Expressions and data binding, Conditional Directives, Style Directives, Controllers, Filters, Forms, Routers, Modules, Services; Web Applications Frameworks and Tools – Firebase- Docker- Node JS- React- DjangoUI & UX.

TextBook:

1. Deitel and Deitel and Nieto, Internet and World WideWeb - How to Program, Prentice Hall, 5th Edition, 2011.
2. Jeffrey C and Jackson, Web TechnologiesA Computer Science Perspective, Pearson Education, 2011.
3. Angular6forEnterprise-ReadyWebApplications,DoguhanUluca,1stedition,PacktPublishing

ReferenceBook:

1. StephenWynkoopandJohnBurke—RunningaPerfectWebsite¦,QUE,2ndEdition,1999.
2. Chris Bates, Web Programming – Building Intranet Applications, 3rd Edition, Wiley Publications, 2009.
3. GopalanN.P.andAkilandeswariJ.,—WebTechnology¦,PrenticeHallofIndia,2011.
4. UttamK.Roy,—WebTechnologies¦,OxfordUniversityPress,2011.
5. Angular:UpandRunning:LearningAngular,StepbyStep,ShyamSeshadri,1stedition,O′Reilly

Programme: B.Sc. Cyber Security

Title:Wireless andMobile Security

Type: Core Skill

Credits:3

TotalMarks-100		CourseCode:3CS4	(TotalNumberofPeriods)Hrs
TheoryExamMarks:80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Aftersuccessfulcompletionofthecourse,studentswillableto:

1. Familiarize with the issues and technologies involved in designing a wireless and mobile system thatis robust against various attacks.
2. Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoff in protecting networks.
3. Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thusenhancing their potential to do research or pursue a career inthisrapidly developingarea.
4. Learn various security issues involved in cloud computing. 5. Learn various security issues related to GPRS and 3G..

Unit	Content
Unit-1(10HRS)	Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications,SecurityforMobileApplications,Advantagesand DisadvantagesofApplication–levelSecurity.
Unit-(8HRS)	Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Securityfor1GWi-Fi Applications,Securityfor2GWi-FiApplications,Recent SecuritySchemesforWi-FiApplications
Unit-3(8HRS)	Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications,GPRSSecurityforapplications,UMTSsecurityforapplications, 3Gsecurityforapplications,SomeofSecurityandauthenticationSolutions.
UNIT-4(10HRS)	Application Level Security in MANETs: MANETs, Some applications of MANETs,MANETFeatures,SecurityChallengesinMANETs,Security AttacksonMANETs,ExternalThreatsforMANETapplications,Internal threats for MANET Applications, Some of the Security Solutions. Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC,andSecurityAttacksonUCnetworks,Someofthesecuritysolutionsfor UC.
UNIT-5(9HRS)	DataCenterOperations-Securitychallenge,implement“FivePrincipal CharacteristicsofCloudComputing,DatacenterSecurityRecommendations EncryptionforConfidentialityandIntegrity,Encryptingdataatrest,Key

	ManagementLifecycle,CloudEncryptionStandards.

TextBook:

1. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill,2010.
2. FrankAdelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.

ReferenceBook:

1. Randall k. Nichols, Panos C. Lekkas : "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. BrucePotterandBobFleck:"802.11Security",1stEdition,SPDO'REILLY 2005.
3. James Kempf: "Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols", 1st Edition, Cambridge University Press, 2008.

Programme:B.Sc.CyberSecurity

Title:Wireless andMobile Security -LAB

Type: SEC/LAB

Credits:2

TotalMarks-50		CourseCode:3CS5	(TotalNumberofPeriods)Hrs
ExternalMarks:25	InternalMarks:25	MinPassing:20	60

ListofPractical's:

NOTE: The listsuggestssampleprogramset.Hence,theconcernedstaffmay modify thelistasneeded (Minimum 15).

1. Simulateandanalyzesecurityprotocolsinwiredvs.wirelessnetworks,withafocusonidentifying vulnerabilities.
2. Practicalexerciseonsecuritytrade-offsbetweendevice-levelandapplication-levelsecurity.
3. settingupsecurityconfigurationsformobiledevices,includingpasswordpoliciesandbiometric authentication.
4. PracticalimplementationofWPA2,WPA3,andotherwirelesssecurityprotocolsonalocalnetwork.
5. SettingupandsecuringaserverformobilecommunicationswithSSL/TLSandaccesscontrols.
6. DemonstratecommonWLANattacktechniques(e.g.,eavesdropping,MITM)andcountermeasures.
7. Overviewofsecurityprotocolsacrossgenerations(GSM,GPRS,UMTS,3G,4G,5G)throughnetwork simulators.
8. Practicalonidentifyingandcounteringpotentialattacksincellularnetworks(e.g.,cloning,denialof service).
9. Hands-onexplorationofsecuritychallengesinMANETsandsimulationofexternal/internalthreats.
10. Set up a MANET environment and demonstrate common security attacks like Blackhole, Wormhole, and Sybil attacks.
11. Explorecountermeasuresforspecificattacksin MANETs,includingroutingprotocolslike AODV.
12. Practiceencryptingdataatrestandintransit,withanemphasisonkeymanagementbestpractices.

Programme: B.Sc.CyberSecurity

Title: Web Development - LAB

Type: SEC/LAB

Credits:2

TotalMarks-50		CourseCode:3CS6	(TotalNumberofPeriods)Hrs
ExternalMarks:25	InternalMarks:25	MinPassing:20	60

ListofPractical's:

NOTE: The listsuggestssampleprogramset.Hence,theconcernedstaffmay modify thelistasneeded (Minimum 15).

1. Createawebpagewiththefollowingusing HTML.
   • Toembedanimagemapinawebpage.
   • To fixthehotspots.
   • Showalltherelatedinformationwhenthehotspotsareclicked.
2. Createawebpagewithalltypesof Cascadingstylesheets.
3. ClientSideScriptsforValidatingWebFormControlsusingDHTML.
4. InstallationofApacheTomcatwebserver.
5. WriteprogramsinJavausingServlets:
   ● ToinvokeservletsfromHTMLforms.
   ● SessionTracking

6. WriteprogramsinJavatocreatethree-tierapplicationsusingJSPandDatabases

   ● Forconductingon-lineexamination.

   ● For displaying student mark list.Assume that student information is available in a database which has been stored in a database server.

7. ProgramsusingXML–Schema–XSLT/XSL.

Programme: B.Sc.CyberSecurity

Title: LAB basedon 3CS2

Type:SEC/LAB

Credits: 2

TotalMarks-50		CourseCode:3CS7	(TotalNumberofPeriods)Hrs
ExternalMarks:25	InternalMarks:25	MinPassing:20	60

Minimum 15 experiments / programming assignments must be completed based on the respective syllabus (3CS2E1/ 3CS2 E2).

Programme: B.Sc.CyberSecurity

Title: Environment Studies

Type:VEC[CollegeLevelTheory]

Credits: 2

TotalMarks-50		CourseCode:3CS8	(TotalNumberofPeriods)Hrs
	InternalMarks:50	MinPassing:20	45

UnitI:(a)TheMultidisciplinarynatureofenvironmentalstudies:

Definition,Principles,Scopeandimportance,ManandEnvironment,Needforpublicawareness.

(b)NaturalResources:Renewableandnonrenewableresources:

Availability, use, overexploitation and associated environmental problems related to following Natural resource:

• Forestresources:

• Waterresources:.

• MineralResources:

• FoodResources:

• EnergyResources:

• LandResources:

• Roleofindividualinconservationofnaturalresources'

UnitII:Ecosystems:

• Conceptandcomponentsofanecosystem.

• Typesofecosystem

• Structureandfunctionofforestandpondecosystem.

• Energyflowintheecosystems.

• Foodchains,foodwebsandecologicalpyramids.

• Ecologicalsuccession:Generalmechanism

UNITIII:Biodiversityandit'sConservation:

• Introduction,definitionandtypesofbiodiversity.

• Bio-geographicalclassificationofIndia.

• Indiaasamega-diversitynation.

• Hot-spotsofbiodiversity.

• Threatstobiodiversity:habitatsloss,poachingofwildlife,manwildlifeconflicts.

• EndangeredandendemicspeciesofIndia.

• Conservationofbiodiversity:in-situandex-situconservationofbiodiversity.

UNITIV:EnvironmentalPollution:

• Definition, Causes, effects and control measures of: a.Air pollution b. Water pollution c. Soil pollution d. Noise pollution e. Nuclear hazards. • Solid waste Management: Principles, methods and significance • Disaster management: Floods, earth quake, cyclone and landslides.

UnitV:SocialissuesandtheEnvironment:

• From unsustainable to sustainable development • Urban problems related to energy • Water conservation:rainwaterharvesting,watershedmanagement•Environmentalethics:issuesandpossiblesolutions• Climate change, global warming, acid rain, ozone layer depletion and nuclear accidents • Wasteland reclamation • Environmental Legislation: Environment protectionAct (1986);Air (prevention and control of pollution) Act (1981-82); Water (prevention and control of pollution) Act (1974); Wildlife protection act (1972); Forest conservation act (1980),Issuesinvolved inenforcement ofenvironmental legislation

RecommendedBooks:

1. TextBookofEnvironmentalstudies,ErachBharucha,UGC.

2. FundamentalconceptsinEnvironmentalStudies,DDMishra,SChand&CoLtd.

3. EcologyandEnvironment,P.D.Sharma.

4. Ecology,M.P.Arora,HimalayaPublishingHouse.

Faculty:ScienceandTechnology

SyllabusPrescribed for3YearB.Sc.CyberSecurityUG Programme [CBCS]

SEMESTER:IV

Programme:B.Sc.CyberSecurity

Title: Identity andAccess Management

Type:AEC

Credits:3

TotalMarks-100		CourseCode:4CS1	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Buildanappropriatecloudarchitectureandidentifythecloudservices
2. Handlevarioussensorsandthetechnologies
3. DevelopIoTapplicationsusingcloudplatforms
4. IntegratetheIoTapplicationsintothecloudservices
5. Accessthesecurityissuesinapplicationsandnetworks

Unit	Content
Unit 1 CloudPlatformArchitecture and Services (9 HRS)	Coud computing and service models: Public, Private and Hybrid clouds, Infrastructure as a service(IaaS), Platfrom as a service(PaaS), Software as a service(SaaS) Architectural design of compute and storage clouds: Layered cloud architectural development, Architectural design challenges, Publiccloudplatforms:GAE,AWSandAzure
Unit-2 Programming IOT Devices for Cloud Interface (9HRS)	Basics of Sensors and actuators, examples and working principles of sensors and actuators, Cloud computing and IOT, Arduino/Equivalent Microcontroller platform. IoTCommunicationTechnologies,RFID,Bluetooth,Zigbee,Wifi,Wired Communication
Unit-3 Cloud PlatformsforIOT (9HRS)	Thinkspeak IoT Cloud Platform, Kaa Open Source Iot Cloud Platform, AWS IoT Cloud Platform,AWS IoT Device SDK, ArduinoAWS IoT development, RaspberryPi3,AWSIoTdevelopment
UNIT-4 Cloud Services forIOT (9HRS)	Service Management in Cloud Computing , Service LevelAgreements (SLAs), Managing IoT Data, Looking at Data, Scalability & Cloud Services, Database &DataStoresinCloud,LargeScaleDataProcessing.
UNIT-5 Security and Applications(9HRS)	Application Safety and Service Vulnerability in Cloud Network, IoT Securityand Privacy Preservation, Security and Challenges in Mobile Cloud Computing, ThevitalroleofFogcomputinginInternetofThings

TextBook:

1. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From parallel processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.
2. Raj Kamal, "Internet of Things:Architecture and Design Principles", McGraw-Hill Education Pvt. Ltd., 2018.
3. CharalamposDoukas,"BuildingInternetofThingswiththeArduino",CreateSpace, April2002.
4. AgusKurniawan"LearningAWSIoT"PacktPublishing(January29,2018)

ReferenceBook:

1. Dac-NhuongLe,ChintanBhatt,ManiMadhukar"SecurityDesignsfortheCloud,IoT,andSocialNetworking" John Wiley & Sons (11 October 2019).
2. HonboZhou,"TheInternetofThingsintheCloud:AMiddlewarePerspective",CRCPress,2013.
3. MarcoSchwatrz,"InternetofThingswithArduinoCookbook",PacktPublications,2016.
4. RajkumarBuyya,ChristianVecchiola.S.ThamaraiSelvi, "Mastering Cloud Computing",McGrawHill Education, 2013.
5. NickAntonopoulos and Lee Gillam, "Cloud Computing: Principles, Systems andApplications", Second Edition, Springer, 2017.

Programme: B.Sc.CyberSecurity

Title: Ethical Hacking

Type:CoreSkill Credits:

3

TotalMarks-100		CourseCode:4CS2	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Demonstrateanunderstandingoftheethicalandlegalimplicationsofhackingand penetration testing.
2. Identifyandexploitcommonsecurityvulnerabilitiesinsystemsandnetworks.
3. Useavarietyofhackingtoolsandtechniquestoassessthesecuritypostureoftargetsystems.
4. Analyzeandinterprettheresultsofethicalhackingassessmentstoprioritizeandremediate vulnerabilities.
5. Communicateeffectivelyaboutethicalhackingassessments,findings,andrecommendations

Unit	Content
Unit1Introductionto Ethical Hacking (9 Hrs)	Overviewofhackingandpenetrationtesting**,**Ethicalconsiderationsandlegal framework**,** Different types of hackers and their motivations, Introduction to ethical hacking methodologies and tools
Unit-2Information GatheringandFoot	Passiveandactivereconnaissancetechniques,Open-sourceintelligence (OSINT)gathering,Footprintingtoolsandmethodologies,Identifyingtarget

printing(9hrs)	assetsandattacksurface
Unit-3 Scanning and Enumeration (9hrs)	Network scanning techniques and tools, Host discovery and enumeration, Service enumeration and version detection, Vulnerability scanning and assessment
Unit-4 Exploitation and post-exploitation (9hrs)	Commonattackvectorsandexploitationtechniques,exploitingweb applications and servers, Privilege escalation and lateral movement, maintaining accessandcoveringtracks
Unit-5 Reporting and Ethics (9hrs)	Documentationandreportingofethicalhackingassessments,Ethicalguidelines and codes of conduct for ethical h ackers, Legal considerations and liabilities, Career paths and professional certifications in ethical hacking

ReferenceBooks:

1. "CEHCertifiedEthicalHackerAll-in-OneExamGuide"byMattWalker
2. "TheWebApplicationHacker'sHandbook:FindingandExploitingSecurityFlaws"byDafydd Stuttard and Marcus Pinto
3. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, andMatiAharoni
4. "Hacking:TheArtofExploitation"byJonErickson
5. "PenetrationTesting:AHands-OnIntroductiontoHacking"byGeorgiaWeidman
6. "TheBasicsofHackingandPenetrationTesting:EthicalHackingandPenetrationTestingMade Easy" by Patrick Engebretson

Programme: B.Sc.CyberSecurity

Title: Cloud Security

Type:DSE

Credits: 3

TotalMarks-100		CourseCode:4CS3(E1)	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	**InternalMarks:20**	**MinPassing:40**	**45**

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Understandthecloudconceptsandfundamentals.
2. Explainthesecuritychallengesinthecloud.
3. DefinecloudpolicyandIdentityandAccessManagement.
4. Understandvariousrisksandauditandmonitoringmechanismsinthecloud.
5. Definethevariousarchitecturalanddesignconsiderationsforsecurityinthecloud

Unit	Content
Unit 1 Fundamentals Of Cloud Security Concepts (9Hrs)	Overview of cloud security- Security Services - Confidentiality, Integrity, Authentication, Nonrepudiation, Access Control - Basic of cryptography - Conventional and public-key cryptography, hash functions, authentication, and digital signatures.
Unit-2 Security DesignAnd ArchitectureFor Cloud (9hrs)	Security design principles for Cloud Computing - Comprehensive data protection - End-to-end access control - Common attack vectors and threats - Network andStorage - Secure Isolation Strategies - Virtualization strategies - Inter-tenant network segmentation strategies - Data Protection strategies: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation,PKIandKey
Unit-Access Control And Identity Management (9hrs)	Access control requirements for Cloud infrastructure - User Identification - Authentication and Authorization - Roles-based Access Control - Multi-factor authentication - Single Sign-on, Identity Federation - Identity providers and service consumers - Storage and network access control options - OS Hardening and minimization-Verifiedandmeasuredboot-IntruderDetectionandprevention
Unit-4 Cloud SecurityDesign Patterns(9hrs)	Introduction to Design Patterns, Cloud bursting, Geo-tagging, Secure Cloud Interfaces, Cloud ResourceAccess Control, Secure On-Premise Internet Access, SecureExternalCloud
Unit-5 Monitoring, AuditingAnd Management (9hrs)	Proactive activity monitoring - Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges - Events and alerts -Auditing – Record generation, Reporting and Management, Tamper-proofingauditlogs,Quality of Services, Secure Management, User management, Identity management, SecurityInformationandEventManagement

TextBook:

1. RajKumarBuyya,JamesBroberg,andrzejGoscinski,“CloudComputing:”,Wiley2013

2. Daveshackleford,“VirtualizationSecurity”,SYBEXawileyBrand2013.

3. Mather,KumaraswamyandLatif,“CloudSecurityandPrivacy”,OREILLY2011

ReferenceBook:

1. MarkC.Chu-Carroll—CodeintheCloud¦,CRCPress,2011

2. Mastering Cloud Computing Foundations and Applications Programming RajkumarBuyya, Christian Vechhiola, S. ThamaraiSelvi

Programme: B.Sc.CyberSecurity

Title: Network Security

Type:DSE

Credits: 3

TotalMarks-100		CourseCode:4CS3(E2)	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. Describecomputerandnetworksecurityfundamentalconceptsandprinciples.
2. Acquire the knowledge of various authentication protocols, key exchange mechanism, and digital certificates.
3. To get better knowledge on fundamental concepts of cryptography, encryption and hashing techniques.
4. Identify and assess different types of threats and attacks such as social engineering, rootkit, and botnets,etc.
5. Acquire Demonstrate the ability to select among available network security technology and protocols such as IDS, firewalls, SSL , TLS, etc.

Unit	Content
Unit 1Fundamendals Of Networking Security (9Hrs)	Overview of networking security- Security Services -Confidentiality, Authentication, Integrity, Nonrepudiation, access Control - Availability and Mechanisms- Security Attacks -Interruption, Interception ,Modification and Fabrication.
Unit-2 AuthenticationAnd Security (9hrs)	Authentication overview - Authentication protocols - Authentication and key establishment - key exchange - mediated key exchange - User Authentication – password based authentication - password security - CertificateAuthority and key management-digitalsignatures-digitalCertificates.
Unit-3 : Public-Key CryptographyAnd Message Authentication (9hrs)	Basics of cryptography -cryptographic hash functions - symmetric and public-key encryption - public key cryptography principles & algorithms - cipher block modes of operation - Secure Hash Functions – HMAC
Unit-4Security Attacks (9hrs)	Buffer overflow attacks & format string vulnerabilities - Denial-of-ServiceAttacks - Hijacking attacks : exploits and defenses - Internet worms – viruses – spyware – phishing – botnets - TCP session hijacking -ARP attacks - route table modification - UDPhijacking-man-in-the-middleattacks.
Unit-5 IPSecurity AndWebSecurity (9hrs)	Network defense tools: Firewalls,VPNs, Intrusion Detection, and filters - Email privacy: Pretty Good Privacy (PGP) and S/MIME - Network security protocols in practice- Introduction to Wireshark – SSL- IPsec, and IKE -DNS security- Secure Socket Layer (SSL) and Transport Layer Security (TLS) - Secure Electronic Transaction(SET).

TextBook:

1. NetworkSecurityEssentials(ApplicationsandStandards)byWilliamStallingsPearsonEducation.

ReferenceBook:

1. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, Wiley Dreamtech

2. CryptographyandnetworkSecurity,Thirdedition,Stallings,PHI/Pearson

3. AlookbackatSecurityProblemsintheTCP/IPProtocolSuite,S.Bellovin,ACSAC2004

Programme: B.Sc.CyberSecurity

Title: Digital Forensic

Type:CoreSkill Credits:

3

TotalMarks-100		CourseCode:4CS4	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. :Haveknowledgeondigitalforensics.
2. Knowaboutdigitalcrimeandinvestigations.
3. Beforensicready.
4. Investigate,identifyandextractdigitalevidencefromiOSdevices.
5. Investigate,identifyandextractdigitalevidencefromAndroiddevices.

Unit	Content
Unit-1Introduction ToDigitalForensics (9 Hrs)	ForensicScience–DigitalForensics–DigitalEvidence–TheDigitalForensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase
Unit-2DigitalCrime And Investigation (9hrs)	DigitalCrime–SubstantiveCriminalLaw–GeneralConditions–Offenses– Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence
Unit-3 Digital Forensic Readiness (9hrs)	Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Enterprise Digital Forensic Readiness – Challenges in Digital Forensics
Unit-4 iOS Forensics (9hrs)	Mobile Hardware and Operating Systems - iOS Fundamentals – Jailbreaking – File System – Hardware – iPhone Security – iOS Forensics – Procedures and Processes – Tools–OxygenForensics–MobilEdit–iCloud
Unit-5Android Forensics(9hrs)	Android basics – Key Codes – ADB – Rooting Android – Boot Process – File Systems – Security – Tools – Android Forensics – Forensic Procedures – ADB – Android Only Tools – Dual Use Tools – Oxygen Forensics – MobilEdit –Android AppDecompiling.

TextBook:

1. AndreArnes,"DigitalForensics",Wiley,2018.

2. ChuckEasttom,"AnIn-depthGuidetoMobileDeviceForensics",FirstEdition,CRCPress,2022.

ReferenceBook:

1. .Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

Programme: B.Sc.CyberSecurity

Title:Linux Operating System Type:

SEC

Credits:3

TotalMarks-100		CourseCode:4CS7	(TotalNumberofPeriods)Hrs
ExternalMarks(T):80	InternalMarks:20	MinPassing:40	45

CourseOutcome(CO):

Uponcompletionofthiscourse,thestudentsshouldbeableto:

1. FundamentalunderstandingoftheroleofOperatingSystems.
2. Tounderstandtheconceptofaprocessandthread.
3. Tounderstandthevariousmemorymanagementtechniques.
4. Toapplytheconsofprocess/threadscheduling.
5. Toapplytheconceptofprocesssynchronization,mutualexclusionandthedeadlock.
6. TorealizetheconceptofI/OmanagementandFilesystem.

Unit	Content
Unit 1 Overview Of Operating System (9 Hrs)	Operating System Objectives and Functions, The Evolution of Operating Systems, DevelopmentsLeadingtoModernOperatingSystems, VirtualMachines. BASH Shell scripting: Basic shell commands, shell as a scripting language.
Unit 2 - Process DescriptionAnd Control (9hrs)	Process: Concept of a Process, Process States, Process Description, Process Control (Processcreation, Waiting for the process/processes, Loading programs intoprocesses and Process Termination), Execution of the Operating System. Threads:ProcessesandThreads,ConceptofMultithreading,TypesofThreads, Thread programming Using Pthreads. Scheduling: Types of Scheduling, Scheduling Algorithms, and Thread Scheduling
Unit 3 - Concurrency Control(9hrs)	Process/thread Synchronization and Mutual Exclusion: Principles of Concurrency, RequirementsforMutualExclusion,MutualExclusion:HardwareSupport, Operating System Support (Semaphores and Mutex), Programming LanguageSupport (Monitors). Classical synchronization problems: Readers/Writers Problem, Producer and Consumer problem, Interprocess communication Deadlock: Principlesof Deadlock, Deadlock Modeling, Deadlock Prevention, Deadlock Avoidance, Deadlock detection and recovery.
Unit4-Memory,	MemoryManagement:MemoryManagementRequirements,MemoryPartitioning,

I/O & File Management (9hrs)	Buddy System, Relocation, Paging, Segmentation. Virtual Memory: Hardware and Control Structures, Operating System Software. I/O Management and Disk Scheduling: I/O Devices, Organization of the I/OFunction, Operating System Design Issues, I/O Buffering, Disk Scheduling, Disk Cache. File Management: Overview, File Organization and Access, File Directories, File Sharing, Record Blocking, Secondary Storage Management.
Unit5-TheLinux OperatingSystem Management(9hrs)	LinuxDesignPrinciples,LinuxBootingProcess,KernelModules,Process Management,Scheduling,MemoryManagement,FileSystems,InputandOutput, Inter-processCommunication.

ReferenceBook:

1. William Stallings, Operating System: Internals and Design Principles, Prentice Hall, ISBN-10: 0-13-380591-3, ISBN-13: 978-0-13-380591-8, 8th Edition
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts, WILEY, ISBN 978-1-118-06333-0 , 9th Edition
3. Andrew S. Tanenbaum & Herbert Bos, Modern Operating System, Pearson, ISBN-13: 9780133592221, 4th Edition
4. "LinuxBible"byChristopherNegus
5. "HowLinuxWorks:WhatEverySuperuserShouldKnow"byBrianWard

Programme:B.Sc.CyberSecurity

Title:Legal and EthicalAspectsof CyberSecurity Type:

VEC

Credits:3

TotalMarks-100		CourseCode:4CS8	(TotalNumberofPeriods)Hrs
InternalMarks(T):50		MinPassing:20	45

CourseOutcome(CO):

1. Studentswillbeabletoidentifykeylegalframeworksthatgoverncyberactivities.
2. Studentswillbeabletoanalyzecybercrimesandapplybasicforensictechniques.
3. Studentswillbeabletoevaluateprivacyrisksandunderstanddataprotectionregulations.
4. Studentswillbeabletoaddressethicaldilemmasandapplyprofessionalconductincybersecurity.
5. Studentswillbeabletodiscussinternationalregulationsandassesslegalaspectsofcyberconflicts.

Unit	Topics
1.Introduction to Cyber Laws(9 Hrs)	Overview of Cyber Security laws, ITAct 2000,Amendments in ITAct, Cyber Crime Classification, Cyber Jurisdiction, Intellectual Property Rights in Cyber Space

2. Cyber Crimes and Investigation(9 Hrs)	Types of Cyber Crimes (hacking, phishing, online fraud, identity theft), Cyber Crime Investigation Tools, Cyber Forensics, Digital Evidence Collection, Case Studies in Cyber Crimes
3.PrivacyandData Protection(9 Hrs)	Personal Data Protection Bill, Data Privacy Laws (GDPR, HIPAA), Data Breach Management, Ethical Hacking and Penetration Testing Standards, Privacy Risks in Social Media
4. Ethics in Cyber Security(9Hrs)	Ethical Hacking and Code of Conduct, Cybersecurity Ethics inArtificial Intelligence and Machine Learning, Ethical Implications of Surveillance and Data Collection, Case Studies in Ethical Dilemmas
5. International Cyber Laws and Cyber Warfare(9 Hrs)	International Cybersecurity Regulations, Cyber Warfare Laws, UN Role in Cybersecurity, Cybersecurity in Cross-border Transactions, Future Trendsin Cyber Law and Ethics

Textbooks:

1. '*CyberLawandITProtection',*HarishChander,PHILearningPvt.Ltd.
2. **'** *Legal and Ethical Aspects of Cyber Security',* Michael E. Whitman, Herbert J. Mattord, Cengage Learning

ReferenceBooks

1. **'***CyberSecurityEssentials',*CharlesJ.Brooks,Sybex
2. **'***Cybersecurity and Cyberwar What Everyone Needs to Know',* P.W. Singer andAllan Friedman, Oxford University Press

Programme: B.Sc.CyberSecurity

Title: Digital Forensic - LAB

Type: SEC/LAB

Credits:2

TotalMarks-50		CourseCode:4CS5	(TotalNumberofPeriods)Hrs
ExternalMarks:25	InternalMarks:25	MinPassing:20	60

ListofPractical's:

NOTE: The listsuggestssampleprogramset.Hence,theconcernedstaffmay modify thelistasneeded (Minimum 15).

1.Installation of Sleuth Kit on Linux. List all data blocks.Analyze allocated as well as unallocated blocks of a disk image.

2. DataextractionfromcalllogsusingSleuthKit.

3. DataextractionfromSMSandcontactsusingSleuthKit.
4. InstallMobileVerificationToolkitorMVTanddecryptencryptediOSbackups.
5. Processandparserecordsfromtheir OSsystem.
6. ExtractinstalledapplicationsfromAndroiddevices.
7. ExtractdiagnosticinformationfromAndroiddevicesthroughtheadbprotocol.
8. Generateaunifiedchronologicaltimelineofextractedrecords,

Programme: B.Sc.CyberSecurity

Title: LAB basedon 4CS3

Type:SEC/LAB

Credits: 2

TotalMarks-50		CourseCode:4CS6	(TotalNumberofPeriods)Hrs
ExternalMarks:25	InternalMarks:25	MinPassing:20	60

Minimum 15 experiments / programming assignments must be completed based on the respective syllabus (3CS2E1/ 3CS2 E2).