ಮಂಗಳೂರು ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

MANGALORE UNIVERSITY

(Accredited by NAAC with 'A' Grade)

ಕ್ರಮಾಂಕ/ No.:MU/ACC/CR 59/2020-21/A2

ಕುಲಸಚಿವರ ಕಛೇರಿ
ಮಂಗಳಗಂಗೋತ್ರಿ – 574 199
Office of the Registrar
Mangalagangothri – 574 199
ದಿನಾಂಕ/Date: 18.10.2022

NOTIFICATION

Sub: Regulations and Syllabus governing Post Graduate Diploma Programme in Cyber Security and Ethical Hacking

Ref: 1. Approval of the Academic Council meeting held on 23.12.2020 vide Agenda No.ಎಸಿಸಿ:ಶೈ.ಸಾ.ಸ.2:09(2020–21)

2. Government letter No.ED 05 UDS 2021 dated 19.09.2022

*****

The Regulations governing Post Graduate Diploma Programme in Cyber Security and Ethical Hacking is assented by the Honorable Chancellor on 15.07.2022 as communicated in Government letter cited to ref.(2) above and the syllabus thereon is approved by the Academic Council meeting held on 23.12.2020. Hence, the regulations and syllabus are hereby notified for implementation with effect from the academic year 2022-23 and onwards.

REGISTRAR

1. The Registrar (Evaluation), Mangalore University
2. The Chairman, Dept. of Electronics, Mangalore University, Mangalagangothri
3. The Chairman, P.G.BOS in Electronics, Dept. of Electronics, Mangalore University.
4. The Principal of the Colleges concerned.
5. The Assistant Registrar (ACC), O/o the Registrar, Mangalore University
6. The Superintendent (ACC), O/o the Registrar, Mangalore University.
7. A4/A6/A7 Case workers (ACC) O/o the Registrar, Mangalore University.
8. The Director, DUIMS, Mangalore University – with a request to publish in the website.

8. Guard File.

MANGALORE UNIVERSITY

REGULATIONS GOVERNING POST GRADUATE DIPLOMA PROGRAMME IN CYBER SECURITY AND ETHICAL HACKING

(Framed as per Section 44 (1) (c) of K.S.U. Act 2000)

Preamble

The main aim of National Education Policy -2020 is to increase the employability skill of a student while pursuing any kind of programme of his choice. It will provide an active link between education system and the industry and provide the skill sets in a job oriented specialized programme.

Cyber Security awareness is the combination of both knowing and doing something to protect information assets. When an enterprise's employees are cyber security aware, it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent cyber -crime infiltrating their online workspace. In all these circumstances Mangalore University has proposed to start Post Graduate Diploma in Cyber Security and Ethical Hacking.

1. Title and Commencement

1.1 These regulations shall be called "Regulations governing Postgraduate Diploma in Cyber security and Ethical Hacking".

1.2 These regulations shall come into force from the date of assent of the Chancellor.

2. Eligibility for Admission

2.1 Candidates who have passed any Bachelor's Degree examination or an examination recognized by the University as equivalent shall be eligible for this Post Graduate Diploma Programme.

2.2 Selection shall be on the basis of merit-cum-reservation and according to the Government's reservation policy existing at the time of implementation.

2.3 Those who are pursuing any Masters's degree programme in Mangalore University are eligible to pursue this programme as a part time programme along with their Master's programme which will be stretched for 2 years.

2.4 Working professionals can also apply for the programme and pursue it on part time basis.

3. Duration of the Programme

One year – full time

Two years – part time

4. Medium of Instruction

The medium of instruction and examination shall be English.

5. Attendance

Each course shall be treated as an independent unit for the purpose of attendance. A student shall attend a minimum of 75% of the total instruction hours in a course including tutorials and seminars. If the student does not satisfy the above condition, he/she shall be required to repeat the programme in a subsequent year.

6. Maximum period for Completion of the Programme

The candidate shall complete the programme within the period prescribed in the regulations governing maximum period for completing various degree/diploma programmes of Mangalore University.

7. Mode of delivery, Hours of Instruction and Scheme of Examinations

The mode of delivery can be one among online or offline or blended modes, whichever is suitable at the time of the implementation of a batch.

The details of hour of instruction and the scheme of examination shall be as stated below.

Courses	Instruction Hrs. Per course/Week	Duration of exam (hrs.)	IA	Exam	Total	Credit
I Semester						
3 Courses (Hard Core)	3x4	3x3	3x30	3x70	3x100	3x4
2 courses (Soft Core)	2x3	2x3	2x30	2x70	2x100	2x3
2 Practicals	2x4	2x3	2x30	2x70	2x100	2x2
Total			**210**	**490**	**700**	**22**
II Semester						
3 Courses (Hard Core)	3x4	3x3	3x30	3x70	3x100	3x4
2 courses (Soft Core)	2x3	2x3	2x30	2x70	2x100	2x3
2 Practicals	2x4	2x3	2x30	2x70	2x100	2x2
1 Seminar	1x1	-	15	35	50	1x1
Total			**225**	**525**	**750**	**23**

8. Internal Assessment:

8.1 The Internal assessment marks shall be based on tests and assignments.

8.2. Marks scored in the internal assessment shall be indicated separately in the Marks card.

8.3 Internal assessment marks of a failed candidate shall be retained and carried forward to his/her subsequent examination.

9. Registering for Examination:

A candidate shall register for all the courses/papers in the programme when he/she appears for the examination for the first time.

10. Minimum for Pass:

10.1 No candidates shall be declared to have passed in the examination unless he/she has obtained not less than 40% marks in the University Examination in each Course. Further, the candidate shall have obtained a cumulative of 40% marks in examination and internal assessment.

10.2 There shall be no minimum in respect of internal assessment.

10.3 A candidate who fails in any of the theory courses shall reappear in that theory course and pass the examination subsequently.

11. Classification of successful candidates:

11.1 The results of successful candidates shall be classified on the basis of aggregate marks obtained.

11.2 The candidates who pass the examinations in the first attempt are eligible for ranks provided they secure at least 60%.

Percentage of marks for declaring class:

First class with Distinction	70% and above
First Class	60% and above, but less than 70%
Second Class	50% and above, but less than 60%
Pass Class	40% and above, but less than 50%

12. Improvement of Results

12.1 A candidate may be permitted to improve the results of the whole examination, within 30 days after the publication his/her result or 10 days from the date of dispatch of his/her Marks cards by the Registrar (E) to the department whichever is later, and reappear for improvement. Course-wise improvement shall not be permitted.

12.2 The improvement option shall be exercised only once and the rejection once exercised cannot be revoked.

12.3 Application for improvement along with the payment of prescribed fee shall be submitted through the department together with the original statement of marks.

12.4 The internal assessment marks secured by the candidate during the programme shall be carried forward.

12.5 A Candidate who appears for improvement is eligible only for class and not for ranking.

(Assented by the Honorable Chancellor on 15.07.2022 as communicated in Government letter No.ED 05 UDS 2021 dated 19.09.2022 and notified under Notification No.MU/ACC/CR 59/2020-21/A2 dated 18.10.2022)

Sd/-
REGISTRAR

PG Diploma in Cybersecurity and Ethical Hacking Programme Structure

Semester I		
Sl. No	**Course Name**	**Credits**
	Hard Core	
1	PGDCSEH001: Information Security Management Systems	4
2	PGDCSEH002: Networking	4
3	PGDCSEH003: Ethical Hacking	4
	Soft Core	
4	PGDCSES001: Cloud Security	3
5	PGDCSES002: Mobile Application Security and Penetration Testing	
6	PGDCSES003: Linux Fundamentals	
7	PGDCSES004: Malware Analysis	
	Practical's	
8	PGDCSEP001: Networking Laboratory	2
9	PGDCSEP002: Ethical Hacking Laboratory	2
	Total	**22**

Semester II		
Sl. No	**Course Name**	**Credits**
	Hard Core	
1	PGDCSEH004: Network Penetration Testing	4
2	PGDCSEH005: Web Application Security	4
3	PGDCSEH006: Cyber Law, Data Privacy and Cyber Forensics	4
	Soft Core	
4	PGDCSES005: Artificial Intelligence and Machine Learning	3
5	PGDCSES006: Blockchain	
6	PGDCSES007: Network Security	
7	PGDCSES008: Internet of Things (IoT) Security	
	Practicals	
8	PGDCSEP003: Network Penetration Testing Laboratory	2
9	PGDCSEP004: Web Application Security Laboratory	2
	Seminar	
10	CSCS 461: Seminar on latest trends and techniques in Cyber security	1

Credit Distribution

Semester	Main Course Credits
I	22
II	23
Grand Total	45

Scheme of Examination for M.Sc. in Cyber Security

Semester I

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
Hard Core (All are Compulsory)							
PGDCSEH001	Information Security Management Systems	04	04	3 hours	30	70	100
PGDCSEH002	Networking	04	04	3 hours	30	70	100
PGDCSEH003	Ethical Hacking	04	04	3 hours	30	70	100
Soft Core (Two to be chosen by the student)							
PGDCSES001	Cloud Security	03	03	3 hours	30	70	100
PGDCSES002	Mobile Application Security and Penetration Testing	03	03	3 hours	30	70	100
PGDCSES003	Linux Fundamentals	03	03	3 hours	30	70	100
PGDCSES004	Malware Analysis	03	03	3 hours	30	70	100
Practicals							
PGDCSEP001	Networking Laboratory	02	04	03 hours	30	70	100
PGDCSEP002	Ethical Hacking Laboratory	02	04	03 hours	30	70	100
Total		-	-	-	**210**	**490**	**700**

Semester II

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
Hard Core (All are Compulsory)							
PGDCSEH004	Network Penetration Testing	04	04	3 hours	30	70	100

PGDCSEH005	Web Application Security	04	04	3 hours	30	70	100
PGDCSEH006	Cyber Law, Data Privacy and Cyber Forensics	04	04	3 hours	30	70	100
Soft Core							
PGDCSES005	Artificial Intelligence and Machine Learning	03	03	3 hours	30	70	100
PGDCSES006	Blockchain	03	03	3 hours	30	70	100
PGDCSES007	Network Security	03	03	3 hours	30	70	100
PGDCSES008	Internet of Things (IoT) Security	03	03	3 hours	30	70	100
Practicals							
PGDCSEP003	Network Penetration Testing Laboratory	02	04	03 hours	30	70	100
PGDCSEP004	Web Application Security Laboratory	02	04	03 hours	30	70	100
Seminar							
CSCS 461	Seminar on latest trends and techniques in Cyber security	01	01	-	15	35	50
Total					**225**	**525**	**750**

Marks Distribution Semester Wise

Semester	Credits	Marks
I	22	700
II	26	750
Total	**48**	**1450**

SEMESTER I

PGDCSEH001: Information Security Management Systems

UNIT - I

Introduction to Cyber Security: Security Principles, Confidentiality, Integrity, Availability, Cyber Attacks, Security Standards & Guidelines: Standards, Guidelines, Frameworks, Policies, Procedures, HIPAA, NIST, ISO 27001:2013 Standard: 14 Domains and 114 Controls of the Standard

(16 hours)

UNIT - II

PCI DSS Standard: 12 Requirements of the PCI DSS Standard, GDPR Regulation, Data Protection Act 2021, Risk Management PRACTICALS : Risk, Threat, Risk Assessment, Quantitative & Qualitative Risk Assessment, Security Auditing & Testing

(16 hours)

UNIT - III

PRACTICALS: Audit Types, SOC Audits, Test of Design, Test of Effectiveness, Compliance Management PRACTICALS: Compliance, Managing Compliance in Organization, GRC Tools, Security Architecture and Roles & Responsibilities: Security Domains & Departments, Roles & Responsibilities, Organizational Structure

(16 hours)

TextBooks:

1. Certified Information Systems Security Professional Official Study Guide Eighth Edition
2. CISSP Eighth Edition by Shon Harris and Fernando Maymi
3. ISO/IEC 27001:2013 Standard Reference
4. PCI DSS Standard Reference

PGDCSEH002: Networking

UNIT - I

Network Layers: OSI Layers, TCP/IP Layer (From Security Perspective), Port numbers and Protocols: Port Numbers, Protocols, Networking commands PRACTICALS: PING, NETSTAT, TRACERT, IpConfig, NSLookUp, Nslookup, **nbtstat,**

(16 hours)

UNIT - II

IP Addressing & Subnetting : IP Address Types & Categories, IP Working, Subnetting, Routing, Networking Devices and their functionalities, PRACTICALS: Routing Protocols, RIP v1, RIP v2, OSPF, EIGRP, Switching PRACTICALS : Switching and Switches, IP Sec protocol, Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) – 802.1w, VLAN,

(16 hours)

UNIT - III

Network Architecture Designing and Types PRACTICALS: Configuring networks using CISCO Packet Tracer, Network Address Translation & Wide Area Networks : Static NAT & Dynamic NAT, Port Address Translation PAT, WAN Networks, Frame Relays, SDN (Software Defined networks)

(16 hours)

TextBooks:

1. CCNA Routing and Switching Complete Study Guide: By Todd Lammle
2. CEH v10 EC-Council Certified Ethical Hacker Complete Training Guide

PGDCSEH003: Ethical Hacking

UNIT - I

Introduction to Ethical Hacking: Hacking vs Ethical Hacking, Hackers and Hacking Groups, Vulnerabilities, CVE, Hacking Types, Introduction to Kali Linux and other Ethical Hacking Operating Systems (PRACTICALS) : Kali Linux Installation, Various Tools in Kali Linux, Parrot OS, BackBox, Ethical Hacking Phases – Reconnaissance PRACTICALS : Reconnaissance Methodology, Active Reconnaissance, Passive Reconnaissance, Google Dorks, Shodan, OSINT Framework, Nmap, Subdomain finding, Ethical Hacking Phases – Scanning & Gaining Access PRACTICALS : OS Fingerprinting & Banner Grabbing, Scanning methods, Scanning Tools - Vega, OWASP ZAP, Nessus, Burp Suite,

(16 hours)

UNIT - II

System Exploitation, Creating Malwares to gain access, Ethical Hacking Phases – Maintaining Access & Clearing Tracks PRACTICALS: System Hacking Methodology, Using Metasploit, Exploitation using Github Sripts, Meterpreter Password Cracking, Stealing internal Credentials using Lazagne, Creating Backdoor Clearing Audit Policies on Windows, : Clearing Logs on Windows,

(16 hours)

UNIT - III

Cyber Attacks PRACTICALS : Sniffing, DDos, Eavesdropping, Mobile Attacks, Wifi Hacking Social Engineering, Vulnerability Assessment & Penetration Testing : VA vs PT, VA Methodology, PT Methodology, Scoping, Documentation & Report Writing PRACTICALS: VAPT Report Writing and Documentation

(16 hours)

TextBooks:

1. CEH v10 EC-Council Certified Ethical Hacker Complete Training Guide
2. Web Application Security – A beginner's guide by Bryan Sulivan Vincent Liu
3. CEH V10 Certified Ethical Hacker Study Guide - Book by Ric Messier

PGDCSES001: Cloud Security

UNIT I

Introduction to cloud computing: Introduction to cloud computing, characteristic of cloud computing, cloud computing models: Service model and deployment model, cloud services and technologies, research challenges, cloud computing reference architecture, network recruitment for cloud computing Cloud Computing Security Baseline: Overview of computer security, vulnerabilities, and attacks, privacy and security in cloud storage services, privacy and security in multi-clouds, cloud accountability, Understanding the Threats, Classification and countermeasures: Infrastructure and host threats, service provider threats, generic threats, threat assessment

(12 hours)

UNIT II

Security Challenges in Cloud Computing: Creating a Safe Environment, Access control, The CIA model: Confidentiality, Integrity, Availability, A real-world example, The principles of security: The Principle of Insecurity, The Principle of Least Privilege, The Principle of Separation of Duties, The Principle of Internal Security, Data center security: Select a good place, Implement a castle-like structure, Secure your authorization points Securing Network in Cloud: The Open Systems Interconnection model: Layer 1 – the Physical layer, Layer 2 – the Data link layer, Address Resolution Protocol (ARP) spoofing, MAC flooding and Content Addressable Memory table overflow attack, Dynamic Host Configuration Protocol (DHCP) starvation attack, Cisco Discovery Protocol (CDP) attacks, Spanning Tree Protocol (STP) attacks, Virtual LAN (VLAN) attacks, Layer 3 – the Network layer, Layer 4 – the Transport layer, Layer 5 – the Session layer, Layer 6 – the Presentation layer, Layer 7 – the Application layer, TCP/IP, Architecting secure networks, Different uses means different network, The importance of firewall, IDS, and IPS, Firewall, Intrusion detection system (IDS), Intrusion prevention system (IPS)

(12 hours)

UNIT III

Securing Cloud Storage and Cloud Forensics: Different storage types,: Object storage, Block storage, File storage, Securing the Hypervisor :Various types of virtualization, Full virtualization, Paravirtualization, Partial virtualization, Comparison of virtualization levels, Hypervisors: Kernelbased Virtual Machine, Xen, VMware ESXi, Hyper-V, BareMetal, Containers, Docker, Linux Containers, Criteria for choosing a hypervisor : Team expertise, Product or project maturity, Certifications and attestations, Features and performance, Hardware concerns, Hypervisor memory optimization, Additional security features, Hardening the hardware management: Physical hardware – PCI passthrough, Virtual hardware with Quick Emulator, virtualization, Hardening the host operating system, DARE (Data At Rest Encryption Cloud Elements & its Security: Seeing Infrastructure as a Service, Exploring Platform as a Service, Using Software as a Service, Understanding Massively Scaled Applications and Business Processes, Setting Some Standards Web Services Delivered from the Cloud, Building Cloud Networks, Federation, Presence, Identity, and Privacy in the Cloud, Security in the Cloud

(12 hours)

TextBooks

1. Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Doston
2. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide by Brian T O'Hara
3. OpenStack Cloud Security Paperback by Alessandro Locati Fabio, PacktPub
4 Cloud Computing Security: Foundations and Challenges edited by John R Vacca, CRC Press
5 Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L Krutz, Russell Dean Vines, John Wiley & Sons

PGDCSES002: Mobile Application Security and Penetration Testing

UNIT I

Mobile Devices Overview: Mobile Platforms Android, iOS, Why Mobile Security, Taxonomy of Security Threats: OWASP Top 10 Mobile Risks, Physical Security, Poor Keyboards, User Profiles, Web Browsing, Malwares, Malware History, Malware Spreading, Patching and Updating Mobile OS Architectures & Security Models: Android Architecture, Android Security Models, Privilege Separation and Sandboxing, File System Isolation, Storage and Database Isolation, Application Signing, Permission Model, Memory Management Security Enhancement, Components, Google Bouncer, Rooting Devices

(12 hours)

UNIT II

Android -Setting up a Test Environment: Android SDK, Windows OS and Linux OS, Eclipse IDE, AVD and Actual Devices, Start AVD, Edit Virtual Devices Definitions, Create New Virtual Device, Run and Interact with Virtual Devices, Improve Virtual Devices Performance, Connect Actual Devices via USB, Interact with the Devices, Android Debug Bridge and Gather Device Information, ADB Shell, Browse the Device, Read Databases, Move Files from/to the Device, Sqlite3, DDMS File Explorer, Mount Device Disk, Install / Uninstall Application with adb, Install and Run Custom Application, BusyBox, SSH, VNC

(12 hours)

UNIT III

Android -Reverse Engineering and Static Analysis: Decompiling and Disassembling apk files, Smali, Decompile apk to jar files, from jar to Source Code, Decompiling/Disassembling Overview Android-Dynamic / Runtime Analysis: Monitoring process activity, Observing file access, Monitoring network connectivity, Analyzing logs using logcat, Memory dumps and analysis, Smali Debugging, Setting breakpoints, Native debugging with IDA (building signatures, types etc), Runtime instrumentation and manipulation using ReFrameworker Android Network Analysis: Traffic Sniffing, Proxying Emulators and Actual Devices, Intercept Application and SSL Traffic, Intercept with Rooted Device and ProxyDroid, Traffic Manipulation

(12 hours)

TextBooks

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov, No Starch Press Publication (2015)
2. Android Hacker's Handbook by Joshua J Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A Ridley, Collin Mulliner, Wiley Publication (2014)
3. Learning Pentesting for Android Devices by Aditya Gupta, Packt Publication (2014)
4. Android Apps Security Mitigate Hacking Attacks and Security Breaches by Sheran Gunasekera, Apress Publication (2020)
5. The Mobile Application Hacker's Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, Wiley Publication (2015)

PGDCSES003: Linux Fundamentals

UNIT I

Introduction to Linux: Introduction to Linux, An overview of the Linux system, Virtualization, Installing VirtualBox and CentOS, Working with VirtualBox, Connecting VMs through SSH (Headless Mode) The Linux Command Line: Introducing the command line, File globbing Quoting commands, working with the Linux shell, Understanding standard streams, Understanding regular expressions, Working with sed, Working with awk, Navigating the Linux filesystem

(12 hours)

UNIT II

The Linux Filesystem: Understanding the filesystem, working with file links, searching for files, working with users and groups, working with file permissions, working with text files, working with VIM text editor Working with the Command Line: Essential Linux commands, Additional programs, Understanding processes, Signals, Working with Bash shell variables, Introduction to bash shell scripting

(12 hours)

UNIT III

More Advanced Command Lines and Concepts: networking with linux, installing new software and updating the system, Introduction to services, Basic system troubleshooting and firewalling, Introducing ACLs, setuid, setgid and sticky bit

(12 hours)

TextBooks

(1). "Linux Command Line and Shell Scripting Bible", Richard Blum, Wiley Publishing, Inc, 2008.

(2) "Mastering Linux - Fundamentals", Paul Cobbaut, Samurai Media Limited 2016

(3). "Linux Administration Handbook", Evi Nemeth, Garth Snyder & Trent R. Hein, Second Edition, Prentice Hall, 2006

Semester-II

PGDCSEH004: Network Penetration Testing

UNIT I

Introduction to Network Penetration Testing, The Mindset of the Professional Pen Tester, Types of Penetration Testing, Penetration testing methodology, Reconnaissance of the Target Organization, Infrastructure, and Users, Scoping, Ports, and Services.

(16 hours)

UNIT II

Port Scanning using Nmap, Nmap scripting engine, Vulnerability Assessment using Nessus, Identifying False positive, Gaining access using RCE, Gaining access using malware, Bind / Reverse shell, Buffer overflow, Gaining Initial Access, Exploitation using Metasploit, Meterpreter, Privilege escalation, on both Windows and Linux

(16 hours)

UNIT III

Hash dumping, Cracking windows and Linux passwords, Port forwarding, Pivoting, Active Directory Domain Mapping and Exploitation, Domain Privilege Escalation, Persistent Administrative Domain Access, Reporting, documenting all the proofs and Report writing.

(16 hours)

Textbooks:

(1). "Mastering Kali Linux for Advanced Penetration Testing", Vijay Kumar Velu , Robert Beggs, Packt, 2019

(2) "Metasploit: The Penetration Tester's Guide", Devon Kearns, Jim O'Gorman, David Kennedy, Mati Aharoni, No Starch Press, 2011

PGDCSEH005: Web Application Security

UNIT I

Introduction to Web Application Technologies: Three Tier Architecture, Web development platforms, Types of Web application Security testing, Web application Reconnaissance, Comprehensive study of Burpsuite, Web Based Vulnerabilities & Attacks, PRACTICALS: Testing Guidelines OWASP ASVS, MITM, Parameter Tampering,

(16 hours)

UNIT II

OWASP Top 10 – Part 1 PRACTICALS: SQL Injection, Cross Site Scripting, Broken Authentication & Session Management, Insecure Direct Object References, Cross Site Request Forgery, Broken Access Control, Security Misconfiguration, Insecure Cryptographic Storage, Failure to restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards.

(16 hours)

UNIT III

E Commerce Security: Client side validation, Payment gateway Attacks, Consumer Protection, Hashing & Digital Signatures : Hashing, SHA, MD5, Digital Signatures, CA, Secure Coding & Code Reviews using tools, Secure Software Development Life cycle, Input Validation, Authentication and Session Management, Error Handling, Logging, Security headers to Avoid major attacks

(16 hours)

TextBooks:

1. CEH v10 EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs

2. "The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws", Dafydd Stuttard and Marcus Pinto, Wiley 2011

PGDCSEH006: Cyber Law, Data Privacy and Cyber Forensics

UNIT I

Introduction to Cyber Law: Cyber Law, World wide cyber laws, Cyber law history and future scope, IT Act 2000 : Sections of the IT Act 2000, Data Privacy & it's regulations : Data Privacy & it's importance, GDPR, Privacy laws , Cyber Crime Case Studies PRACTICALS: Case Studies and Scenarios on Cyber Crimes,

(16 hours)

UNIT II

Digital Forensics Phases PRACTICALS: Identification, Preservation, Analysis, Documentation, Presentation, Legal Aspects of Computer Forensics : Investigation of cases, Complaint drafting, Investigation Reporting and Documenting, Windows Forensics : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, Logs & Event Analysis And Password Cracking : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers. Network Forensics : Introduction, Network Components And Their Forensics Importance, OSI, Forensics Information From Network, Log Analysis, Forensics Tools, Wireless Attacks : Introduction, Wireless Fidelity (Wi-fi)(802 11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems

(16 hours)

UNIT III

Mobile Device Forensics: Introduction, Challenges In Mobile Forensics, Mobile Communication, Evidences In A Mobile Device, Mobile Forensic Process, Forensic Acquisition Tools, Investigative Reports Cyber Forensics Using Tools – Part 1 PRACTICALS: Tools - Autopsy, Exiftool, Oxygen Forensics, Encase, Cyber Forensics using Tools – Part 2 PRACTICALS: Tools - CAINE, Sleuth Kit (+Autopsy), FTK Manager, Ease US

(16 hours)

Text Books:

(1) "Digital Forensics"- Dr Jeetendra Pande, Dr Ajay Prasad, Uttarakhand Open University, Haldwani - 2016

(2) "Computer Forensics and Cyber Crime an Introduction"- Marjie T Britz, Pearson, Third Edition, 2013

(3) "Learning Python for Forensics - Leverage the power of Python in forensic investigations", Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019 (4) "A Practical Guide to Computer Forensics Investigations", Dr Darren R Hayes, Pearson Education, 2015

PGDCSES005: Artificial Intelligence and Machine Learning

UNIT-I

Introduction to Mathematics for ML and Python Python: Setting up Environment, Basic Python Commands, Creating Python Scripts, Conditions, Loops, List, Dictionary, User Defined Functions, Introduction to Anaconda, Working with NumPy, Pandas and Matplotlib Mathematics for ML: Vectors, Matrices, Linear Equations, Mean, Median, Mod, Standard Deviation and Variance, Probability, Correlation, Regression, Handling and Representing Data Machine Learning (ML). Definition and History of AI, Defining Machine Learning, Applications of ML, Issues and Challenges in ML, Types of ML Basics of Supervised Learning, Prediction, Classification, Understanding Datasets, Feature Selection, Feature Normalization, Data Cleaning, Training, Testing & Validation Sets, Different Models of Supervised Learning, Hyperparameters, Measuring Performance, Accuracy and Loss Underfitting & Overfitting, Basics of Unsupervised Learning, Different Models of Unsupervised Learning

(12 hours)

UNIT-II

Neural Network Understanding Biological Brain, Defining Artificial Neural Network (ANN), Applications of ANN & DL Defining & Building a Perceptron, Feed Forward, Back propagation, Single-layer & Multi-layer ANNs, building an ANN Model, Activation & Loss Functions, Compiling & Evaluating a Model Convolutional Neural Networks (CNN): Understanding Convolutions, Pooling, Building & Fitting CNN Models, Evaluating Model Performance Recurrent Neural Networks (RNN): Basic RNN Architecture, Applications of RNN, Building & Fitting RNN Models, Evaluating Model Performance Long Short-Term Memory Networks (LSTM): LSTM Network Architecture, Understanding LSTM, Building LSTMs

(12 hours)

UNIT-III

Computer Vision and Natural Language Processing Computer Vision: Introduction, Object Detection and Image Segmentation, Detecting and Recognizing Faces, Tracking Objects, Pattern Recognition Natural Language Processing (NLP): Introduction, Language as Data, Building Custom Corpus, Text Vectorization & Transformation, Classification for Text Analysis, Clustering for text Similarity, Context-Aware Text Analysis, Text Visualization ML/DL for Cyber Security Introduction to Role of ML in Cyber Security, Malware Detection & Classification, Anomaly Detection, Pen Testing using ML, Social Engineering, ML based Intrusion Detection and other Applications of ML in Cyber Security

(12 hours)

Text Books :

1. Mathematics for Machine Learning 1st Edition by Marc Peter Deisenroth
2. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition by AurélienGéron
3. Python Machine Learning: Machine Learning and Deep Learning with Python, scikit-learn, and TensorFlow 2, 3rd Edition by Sebastian Raschka and Vahid Mirjalili
4. Hands-On Neural Networks with Keras: Design and create neural networks using deep learning and artificial intelligence principles 1st Edition by NiloyPurkait
5. Deep Learning with Keras: Implementing deep learning models and neural networks with the power of Python by Antonio Gulli, Sujit Pal
6. Practical Machine Learning for Computer Vision 1st Edition by Valliappa Lakshmanan, Martin Görner and Ryan Gillard
7. Learning OpenCV 4 Computer Vision with Python 3: Get to grips with tools, techniques, and algorithms for computer vision and machine learning, 3rd Edition by Joseph Howseand Joe Minichino
8. Natural Language Processing in Action: Understanding, analyzing, and generating text with Python 1st Editionby Hobson Lane, Hannes Hapke and Cole Howard
9. Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python by Emmanuel Tsukerman
10. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem by Soma Halder (Author), Sinan Özdemir

PGDCSES006: Block Chain

UNIT I

Cyber Threat Landscape and Security Challenges : Current threat landscape, Defender perspectives, Live attack execution, Emerging security challenges, Evolution of Security: The security ecosystem, The zero-trust approach, The assume breach approach, Evolution at the foundation layer, Introducing Blockchain and Ethereum : Introduction to blockchain, Internet versus blockchain, How blockchain works, The building blocks of blockchain, Ethereum, Private vs Public Blockchain, Business adaptation

(12 hours)

UNIT II

Hyperledger, the Blockchain for Businesses : Technical requirements, Hyperledger overview, Blockchain-as-a-service (BaaS), Architecture and core components, Hyperledger Fabric model, Bitcoin versus Ethereum versus Hyperledger, Hyperledger Fabric capabilities, Blockchain on the CIA Security Triad : Understanding blockchain on confidentiality, Blockchain on integrity, Understanding blockchain on availability, Deploying PKI-Based Identity with Blockchain : PKI, Challenges of the existing PKI model, How blockchain can help, Two-Factor Authentication with Blockchain: Introduction to 2FA, Blockchain for 2FA

(12 hours)

UNIT III

Blockchain-Based DNS Security Platform : Understanding DNS components, DNS structure and hierarchy, DNS topology for large enterprises, Challenges with current DNS, Blockchain-based DNS solution, Deploying Blockchain-Based DDoS Protection : DDoS attacks, Types of DDoS attacks, Challenges with current DDoS solutions, How blockchain can transform DDoS protection, Facts about Blockchain and Cyber Security: Decision path for blockchain, Leader's checklist, Challenges with blockchain, The future of cybersecurity with blockchain

(12 hours)

TextBooks:

(1) "Hands-On Cybersecurity with Blockchain", Rajneesh Gupta, Packt Publishing, 2018

(2) "Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions", Joseph J Bambara Paul R Allen, McGraw-Hill Education, 2018 (3) "Blockchain Enabled Applications", Vikram Dhillon, David Metcalf, Max Hooper, Apress, 2017

(4) "Blockchain Blueprint for a New Economy", Melanie Swan, O'Reilly Media, 2015

(5) "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Daniel Drescher, Apress, 2017

PGDCSES007: Network Security

UNIT I

Network Security Architecture & Devices : Network Security Requirement, Implementation & Devices, Working of Firewalls, Antivirus PRACTICALS: Firewall Implementation & Configuration, Antivirus working, IDS/IPS Configuration, SOC Management

(16 hours)

UNIT II

PRACTICALS: Introduction to SOC, SIEM Devices, SIEM Deployment , Cryptography : Symmetric & Asymmetric Cryptography, AES, DES, Diffie Hellman Key Exchange, Defense in Depth :Defense in Depth Architecture, Security Perimeter, Network Layers and Security Devices, End Point Security :System Attacks, Endpoint Security Controls & Devices,

(16 hours)

UNIT III

Wireless Security PRACTICALS: Wireless Security Overview, Wireless Standards, 802.11x WiFi Hacking, Network Security Threats PRACTICALS: Malware Types and Attacks, Network Intrusions, Network Segmentation

(16 hours)

TextBooks:

1. CISSP Eighth Edition by Shon Harris and Fernando Maymi
2. CEH v10 EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs

PGDCSES008:(IOT) Internet of Things Security

UNIT - I

Internet of Things : Introduction to Internet of Things, Reasons for IoT Security Vulnerabilities, Performing an IoT Pentest: Attack Surface Mapping, How to Perform Attack Surface Mapping, Structuring the Pentest, Analyzing Hardware : External Inspection, Finding Input and Output Ports, Internal Inspection, Radio Chipsets, UART Communication: Introduction to UART, Connections for UART Exploitation,

(12 hours)

UNIT – II

Exploitation Using I2C and SPI : Difference between I2C, SPI and UART, Serial Peripheral Interface, Exploiting I2C Security, Reading and writing from SPI EEPROM, Dumping Firmware Using SPI and Attify Badge, JTAG Debugging and Exploitation : Debugging with JTAG Open OCD, Setting Things up for JTAG Debugging, Performing JTAG Exploitation. Firmware Reverse Engineering and Exploitation: Understanding Firmware, Encrypted Firmware, Emulating a Firmware Binary, Backdooring Firmware, Working with Automated Firmware, Scanning Tools

(12 hours)

UNIT – III

Exploiting Mobile, Web, and Network for IoT : Mobile Application Vulnerabilities in IoT, Inside an Android Application, Reversing an Android Application, Hard-Coded Sensitive Values, Reversing Encryption, Network-Based Exploitation, Web Application Security for IoT. Software Defined Radio : Introduction to Software Defined Radio, Introduction to SDR 101, Common Terminology in SDR, GNU Radio for Radio Signal Processing, Identifying the Frequency of a Target, Using GNU Radio to Decode Data, Replaying Radio Packets. Exploiting ZigBee and BLE : ZigBee 101, Bluetooth Low Energy, Exploiting a BLE Smart Lock, Replaying BLE Packets

(12 hours)

TextBooks:

(1) "IoT Penetration Testing Cookbook: Identify Vulnerabilities and Secure Your Smart Devices" by Aaron Guzman and Aditya Gupta, by Packt Publishing 2017

(2) "The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things" by Aditya Gupta, by No Starch Press 2021

(3) "Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things" by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods, by Apress 2019