Study Scheme of

Post Graduate Diploma

in

CYBER SECURITY AND DIGITAL FORENSIC

Batch 2020 onwards

By

Shaheed Bhagat Singh State Technical Campus, Ferozepur

POST GRADUATE DIPLOMA IN CYBER SECURITY AND DIGITAL FORENSICS (PGDCSDF)

Duration: 12 Months (one year) Total credits: 45

1st Semester PGDCSDF

Theory

Course Code	Course Type	Course Title	L	T	P	Internal	External	Total	Credit
PGDCSDF-101	Core Theory	Mathematics	3	0	0	30	70	100	03
PGDCSDF-103	Core Theory	Fundamentals of Computer and Programming in Python	3	0	0	30	70	100	03
PGDCSDF-105	Core Theory	Introduction to Cyber Security	3	0	0	30	70	100	03
PGDCSDF-107	Core Theory	Network and Application Security	3	0	0	30	70	100	03
PGDCSDF-109	Core Theory	Operating System	3	0	0	30	70	100	03
		Total Theory Credits			**15**				

Laboratory

PGDCSDF-111	Core Practical/Lab	Fundamentals of Computer and Programming in Python	0	0	4	70	30	100	02
PGDCSDF-113	Core Practical/Lab	Cyber Security Lab	0	0	4	70	30	100	02
PGDCSDF-115	Core Practical/Lab	Network and Application Security Lab	0	0	4	70	30	100	02
PGDCSDF-117	Core Practical/Lab	Operating System Lab	0	0	4	70	30	100	02
		Total Laboratory Credits			**08**				
		TOTAL SEMESTER CREDITS			**23**				
		Total	15	0	16	430	470	900	23

2nd Semester PGDCSDF

Theory

Course Code	Course Type	Course Title	L	T	P	Internal	External	Total	Credit
PGDCSDF-102	Core Theory	Digital Forensics	3	0	0	30	70	100	03
PGDCSDF-104	Core Theory	Malware Analysis and Reverse Engineering	3	0	0	30	70	100	03
PGDCSDF-106	Core Theory	Ethical Hacking	3	0	0	30	70	100	03
PGDCSDF-108	Core Theory	Incident Response Management	3	0	0	30	70	100	03
		Total Theory Credits			**12**				
Laboratory									
PGDCSDF-110	Core Practical/Lab	Digital Forensics Lab	0	0	4	70	30	100	02
PGDCSDF-112	Core Practical/Lab	Malware Analysis and Reverse Engineering Lab	0	0	4	70	30	100	02
PGDCSDF-114	Core Practical/Lab	Ethical Hacking Lab	0	0	4	70	30	100	02
PGDCSDF-116	Core Practical/Lab	Major Project	0	0	8	70	30	100	04
		Total Laboratory Credits			**10**				
		TOTAL SEMESTER CREDITS			**22**				
		Total	12	0	20	470	430	900	22

1ST SEMESTER

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-101 MATHEMATICS

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

The objective of this course is to provide basic knowledge of mathematics.

Course Outcomes: After undergoing this course students will be able to

- **Represent data using various mathematical notions.**
- **Explain different terms used in Basic Calculations**
- **Describe various Operations and Formulas used to solve variety of Mathematical Problems.**

Part-A

Number System: Introduction to (Natural number, Integer Number, Real Number, Rational Number and Irrational number), Sum and Products of Rational numbers, Multiplying & Dividing Powers (Integer Exponents), Powers of Products & Quotients (Integer Exponents), Radicals (Introduction to Square Root, Simplifying Square Root, Introduction to Cube Root, Simplifying Cube Root).

Set: Set Introduction, Objectives, Representation of Sets (Roster Method, Set Builder Method), Types of Sets (Null Set, Singleton Set, Finite Set, Infinite Set, Equal Set, Equivalent Set, Disjoint Set, Subset, Proper Subset, Power Set, Universal Set) and Operation with Sets (Union of Set, Intersection of Set, Difference of Set, Symmetric Difference of Set),Universal Sets, Complement of a Set.

Part-B

Logic Statement: Connectives, Basic Logic Operations (Conjunction, Disjunction, Negation) Logical Equivalence/Equivalent Statements, Tautologies and Contradictions.

Matrices : Matrices Introduction, Objectives, Meaning, Types of Matrix (Row Matrix, Column Matrix, Rectangular Matrix, Square Matrix, Diagonal Matrix, Scalar Matrix, Unit Matrix, Triangular Matrix, Null Matrix, Comparable Matrix, Equal Matrix) Algebra of Matrices (Scalar Multiplication, Negative of Matrix, Addition of Matrix, Difference of two Matrix, Multiplication of Matrices, Transpose of a Matrix).

Text Books:

1. Discrete Mathematics and Its Applications by Kenneth H. Rosen, Mc Graw Hill, 6th Edition.
2. College Mathematics, Schaum Series, TMH.

Reference Books:

1. Elementary Mathematics, Dr. RD Sharma
2. Comprehensive Mathematics, Parmananad Gupta
3. Elements of Mathematics, ML Bhargava

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-103 Fundamentals of Computer and Programming in Python

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:
This course will provide the in-depth knowledge of basic computer system and Programming skills in Python language.

Course Outcomes:

After undergoing this course students will be able to

- **Learn the functional units and classify types of computers, how they process information and how individual computers interact with other computing systems and devices.**
- **Understand an operating system and its working, and solve common problems related to operating systems**
- **Familiar with Python environment, data types, operators used in Python.**
- **Compare and contrast Python with other programming languages.**
- **Learn the use of control structures and numerous native data types with their methods.**

Part A

Functional Units of Computer System: Concepts of Hardware and Software; Data and Information, CPU, registers, system bus, main memory unit, cache memory, Motherboard, Ports and Interfaces, expansion cards, memory chips, processors.

Devices: Input and output devices (with connections and practical demo), keyboard, mouse, joystick, scanner, OCR, OMR, bar code reader, web camera, monitor, printer, plotter.

Memory: Primary, secondary, auxiliary memory, RAM, ROM, cache memory, storage disks.

Data Representation: Bit, Byte, Binary, Decimal, Hexadecimal, and Octal Systems, Conversions and Binary Arithmetic (Addition/ Subtraction/ Multiplication)

Concept of Computing: Types of Languages: Machine, assembly and High level Language; Operating system as user interface, utility programs.

Applications of IT and Impact of Internet on Society

Introduction to Bluetooth, Cloud Computing, Big Data, Data Mining, Mobile Computing and Internet of Things (IoT)

Introduction to Python Programming Language: Programming Language, History and Origin of Python Language, Features of Python, Limitations, Major Applications of Python, Getting, Installing Python, Setting up Path and Environment Variables, Running Python, First Python Program, Python Interactive Help Feature, Python differences from other languages.

Python Data Types & Input/Output: Keywords, Identifiers, Python Statement, Indentation, Documentation, Variables, Multiple Assignment, Understanding Data Type, Data Type Conversion, Python Input and Output Functions, Import command.

Operators and Expressions: Operators in Python, Expressions, Precedence, Associativity of Operators, Non Associative Operators.

Control Structures: Decision making statements, Python loops, Python control statements.

Python Native Data Types: Numbers, Lists, Tuples, Sets, Dictionary, Functions & Methods of Dictionary, Strings (in detail with their methods and operations).

PART B

Python Functions: Functions, Advantages of Functions, Built-in Functions, User defined functions, Anonymous functions, Pass by value Vs. Pass by Reference, Recursion, Scope and Lifetime of Variables.

Python Modules: Module definition, Need of modules, Creating a module, Importing module, Path Searching of a Module, Module Reloading, Standard Modules, Python Packages.

Exception Handling: Exceptions, Built-in exceptions, Exception handling, User defined exceptions in Python.

File Management in Python: Operations on files (opening, modes, attributes, encoding, closing), read() & write() methods, tell() & seek() methods, renaming & deleting files in Python, directories in Python.

Classes and Objects: The concept of OOPS in Python, Designing classes, Creating objects, Accessing attributes, Editing class attributes, Built-in class attributes, Garbage collection, Destroying objects.

Recommended Text and Reference Books

1. Introduction to Information Technology, ITL Education Solutions limited, Pearson Education
2. Fundamentals of Computers, P. K.Sinha & P. Sinha, BPB Publishers.
3. Computer Fundamentals, A. Goel, 2010, Pearson Education.
4. Programming in Python, Pooja Sharma, BPB Publications, 2017.
5. Core Python Programming, R. Nageswara Rao, 2nd Edition, Dreamtech.
6. Python in a Nutshell, A. Martelli, A. Ravenscroft, S. Holden, OREILLY.

Reference Books:

1. “Introduction to Computers”, Peter Norton
2. Computers Today, D. H. Sanders, McGraw Hill.
3. “Computers”, Larry long & Nancy long, Prentice Hall.
4. Python, The complete Reference, Martin C. Brown, Mc Graw Hill Education.

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-105 Introduction to Cyber Security

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

This course will provide fundamental knowledge in Cyber Security which is very much required to understand the current status of Cyber World.

Course Outcomes: After undergoing this course students will be able to

CO1 Understand the importance and challenges of Cyber Security

CO2 Analyze and evaluate the cyber security needs of an organization.

CO3 Apply methods for authentication, access control, intrusion detection and prevention.

CO4 Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools

CO5 Design operational and strategic cyber security strategies, policies and conduct research in

cyber security

Unit I: Introduction to Cyber Security

Overview of Cyber Security, Information Systems, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Cyber Security and Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

Unit II: Cyber Security Vulnerabilities and Cyber Security Safeguards

Introduction to Cyber Attacks, Classification of Cyber Attacks, Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

Unit III: Different types of Security

Basic Security for Windows, User Account Security and Password, Wi Fi Security, Web Security, Email Security, Mobile Device and Cloud Security Social media security, Online Banking, Credit Card and UPI Security, IOT Security and Cyber Physical System Security.

Unit IV: Securing Web Application, Services and Servers

Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

Unit V: Intrusion Detection and Prevention

Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

Unit VI: Cryptography and Network Security

Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.

Recommended Text and Reference Books

1. Donaldson, S., Siegel, S., Williams, C.K., Aslam, A., Enterprise Cyber security -How to Build

a Successful Cyber defense Program Against Advanced Threats, A-press

2. Nina Godbole, Sumit Bela pure, Cyber Security, Willey

3. Hacking the Hacker, Roger Grimes, Wiley

4. Cyber Law By Bare Act, Govt Of india, It Act 2000.

5. J. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC press, 2008.
6. Menezes, et.al, Handbook of Applied Cryptography, CRC Press, 2004.
7. Golreich O, Foundations of Cryptography, Vol.1.2, Cambridge University Press, 2004

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-107 Network and Application Security

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

This course will provide the in-depth knowledge of Network and Application Security related concepts.

Course Outcomes:

After undergoing this course students will be able to

- **Examine the concepts related to fundamentals of cryptography including symmetric cryptography, asymmetric cryptography, and digital signatures.**
- **Identify the Authentication requirements and functions for security over the network.**

- **Analyze and evaluate the Application level security and vulnerabilities**
- **Apply methods for authentication, access control, intrusion detection and prevention.**
- **Understand the concepts of Ethical Hacking, Digital Signature, Penetration testing and forensics, Cyber laws.**

UNIT-I

Overview of Network Security: Basic concepts: confidentiality, integrity, availability, security policies, security mechanisms, assurance, Review of Cryptography: Secret key Cryptography, Public Key Cryptography, Encrypting large messages (ECB, CBC, OFB,CFB, CTR), Examples DES, RSA. Message Digests: Applications, Strong and weak collision resistance, The Birthday Paradox, MD5, SHA-1 [8]

UNIT-II

Network security: Firewalls, Network intrusion detection, Transport security: Mechanisms of TLS, SSL, IPSec: IPsec: AH and ESP, IPsec: IKE [8]

UNIT-III:

System Security-Desktop Security, Programming Bugs and Malicious code, Database Security, Operating System Security: Designing Secure Operating Systems, OS Security Vulnerabilities.

UNIT-IV:

Security Management-Disaster recovery, Digital Signatures, Ethical Hacking, Phases and its Techniques, Penetration Testing techniques, Computer Forensics techniques.

UNIT-V:

Introduction to Cyber Laws and Standards-ISO 27001, Cyber Law (Information Technology Act, 2000), International Standards maintained for Cyber Security

1. C. Kaufman, R. Perlman amd M. Speciner, “Network Security Private Communication in Public World”, PHI Learning Private Limited
2. W. Stallings, “Cryptography and Network Security: Principles and Practice” Prentice Hall
3. W. Stallings, “Network Security Essentials: Applications and Standards”PearsonPublications
4. R. Bragg, M. P. Ousley and K.Strassberg, “The Complete Reference:Network Security”, Tata McGraw-Hill
5. Ethical hacking and Penetration testing by Rafay Bloach, CRC Press, Taylor and Francis, 2015
6. Basics of Ethical Hacking, Manthan Desai, Hacking Tech, 2010

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-109 OPERATING SYSTEM

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

This course will provide the in-depth knowledge of basic concepts of an Operating System with case studies of Windows and Linux Operating Systems.

Course Outcomes:

After undergoing this course students will be able to

The student will be able to:
1. Understand and implement basic services and commands of Windows operating System
2. Implement commands for files and directories;
3. Understand Linux Operating System and its structure
4. **Shells of Linux OS and installation of different software services in Linux**

PART A

Fundamentals of Operating system: What is Operating system? Functions of an operating system. Operating system as a resource manager. Structure of operating system (Role of kernel and Shell). Views of operating system. Evolution and types of operating systems.
Process management: Definition of process, process states, Process Control Block, Scheduling Queues, Schedulers, context switch.
Inter Process Communication: Communication/message passing mechanisms, threading, multithreading models, multicore programming, Fundamental concepts of OpenMP.
Process Synchronization: Cooperating process, critical section problem, mutex locks, semaphores, deadlock and starvation, bounded buffer problem, reader-writer problem.
CPU scheduling: Basic concepts, Scheduling criteria, single processor scheduling, multiprocessor scheduling, real time scheduling, Algorithm Evaluation.
Deadlock: Definition, necessary conditions, Resource Allocation Graph, Prevention, Avoidance, Detection and Recovery.

Part-B

Memory Management: Address binding, Dynamic linking and loading, Contiguous memory allocation techniques (fixed and variable sized partitions), Fragmentation and its types, Non-Contiguous memory allocation techniques, Paging, Segmentation, paging with segmentation, Need of Virtual memories, Demand paging, performance measuring of demand paging, Page replacement Algorithms, allocation of frames, Concept of Thrashing.
Device Management: Secondary storage structure, disk scheduling, Disk management, RAID structure, Role of I/O traffic controller, scheduler.
File Management: File concepts, access methods, directory and disk structure, file system structure, file system and directory implementation, Protection and Security.

Case Studies:

LINUX Operating System and Windows Operating System.

Text Books:
1. Operating System Principles by Abraham Silberschatz and Peter Baer Galvin, Seventh Edition, Published by Wiley-India.
2. Operating Systems by Stuart E. Madnick, John J. Donovan, Published by Mac-Graw-Hill.

Reference Books:
1. Principals of Operating System by Naresh Chauhan, Published by OXFORD University Press, India.
2. Operating Systems by Sibsankar Haldar and Alex A. Aravind, Published by Pearson Education.
3. Operating system by Stalling, W., Sixth Edition, Published by Prentice Hall (India)

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-111

Fundamentals of Computer and Programming in Python Laboratory Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		0	0	4	2

Course Objectives:

This course will provide the in-depth knowledge of basic and advanced Programming skills in Python language.

Course Outcomes:

After undergoing this course students will be able to

- Solve simple to advanced problems using Python language.
- Develop logic of various programming problems using numerous data types and control structures of Python.
- Implement different data structures using Python.
- Implement modules and functions using Python.
- Design and implement the concept of object oriented programming structures.
- Implement file handling

List of Experiments

1. Compute sum, subtraction, multiplication, division and exponent of given variables input by the user.
2. Compute area of following shapes: circle, rectangle, triangle, square, trapezoid and parallelogram.
3. Compute volume of following 3D shapes: cube, cylinder, cone and sphere.
4. Compute and print roots of quadratic equation ax2+bx+c=0, where the values of a, b, and c are input by the user.
5. Print numbers up to N which are not divisible by 3, 6, 9,, e.g., 1, 2, 4, 5, 7,….
6. Write a program to determine whether a triangle is isosceles or not?
7. Print multiplication table of a number input by the user.
8. Compute sum of natural numbers from one to n number.
9. Print Fibonacci series up to n numbers e.g. 0 1 1 2 3 5 8 13…..n
10. Compute factorial of a given number.
11. Count occurrence of a digit 5 in a given integer number input by the user.
12. Print Geometric and Harmonic means of a series input by the user.
13. Evaluate the following expressions:

a. x-x2/2!+x3/3!- x4/4!+… xn/n!

b. x-x3/3!+x5/5!- x7/7!+… xn/n!

14.Print all possible combinations of 4, 5, and 6.

15.Determine prime numbers within a specific range.

16.Count number of persons of age above 60 and below 90.

17.Compute transpose of a matrix.

18.Perform following operations on two matrices.

1) Addition 2) Subtraction 3) Multiplication

19.Count occurrence of vowels.

20.Count total number of vowels in a word.

21.Determine whether a string is palindrome or not.

22.Perform following operations on a list of numbers:

1) Insert an element 2) delete an element 3) sort the list 4) delete entire list

23.Display word after Sorting in alphabetical order.

24. Perform sequential search on a list of given numbers.

25. Perform sequential search on ordered list of given numbers.

26.Maintain practical note book as per their serial numbers in library using Python dictionary.

27.Perform following operations on dictionary

1) Insert 2) delete 3) change

28. Check whether a number is in a given range using functions.

29. Write a Python function that accepts a string and calculates number of upper case letters and lower case letters available in that string.

30. To find the Max of three numbers using functions.

31. Multiply all the numbers in a list using functions.

32. Solve the Fibonacci sequence using recursion.

33. Get the factorial of a non-negative integer using recursion.

34. Write a program to create a module of factorial in Python.

35. Design a Python class named Rectangle, constructed by a length & width, also design a method which will compute the area of a rectangle.

36. Design a Python class named Circle constructed by a radius and two methods which will compute the area and the perimeter of a circle.

37. Design a Python class to reverse a string ‘word by word’.

38. Write a Python program to read an entire text file.

39. Design a Python program to read first n lines of a text file.

40. Construct a Python program to write and append text to a file and display the text.

Text Books:

1. Core Python Programming, R. Nageswara Rao, 2ndEdiiton, Dreamtech.
2. Python in a Nutshell, A. Martelli, A. Ravenscroft, S. Holden, OREILLY.
3. Programming in Python, Pooja Sharma, BPB Publications, 2017.

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-113	Cyber Security Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		0	0	4	2

Course Objectives:

The objective of this course is to provide knowledge about the design and implementation of various attacks and Security techniques using Security tools.

Course Outcomes: After undergoing this course students will be able to

CO1 Understand the importance and challenges of Cyber Security in Kali Linux

CO2 Analyze and implement secure password credentials using SSL and DNS.

CO3 Implement various Hacking Techniques using tools.

CO4 Understand and Implement sniffing using toolkit

CO5 Understand and implement various Security tools

Suggested List of Experiments:

1. Install VM Workstation in Ubuntu and set up windows and kali.

2. Set up nginx and provide password credentials with Secure Socket Layer.

3. Write a program to sniff packet sent over the local network.

4. To perform DNS Pharming attack using any method on computers in a LAN Environment.

5. Implement system hacking using tools and Malware Analysis.

6. Create virus with python script and implement attack and analyze the effect of various viruses.

7. Sniffing Website Credentials using Social Engineering Toolkit.

8. Security tools

    1. Introduction to Packet sniffing tools
    2. Penetration testing tools
    3. Internet security protocols validation tool – AVISPA
    4. Network intrusion detection and prevention system – Snort
    5. IOT tool kit

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-115 Network and Application Security Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		0	0	4	2

Course Objectives:
This course will provide the in-depth knowledge of Network and Application Seccurity

Course Outcomes:

After undergoing this course students will be able to

- Demonstrate the working of Open SSL in various domains.
- Predict the concept of Authentication and Encryption to secure the network transmission.
- Implement the wireless audit and decryption strategy for Routing a packet over the network.
- Analyze the functionality of various e-commerce services along with various issues associated with it.
- Design a Honey Pot over the network for secured transmission of packets.
- **Understand the importance and challenges of Application Security**
- **Protect documents using passwords and recovering passwords**
- Implement various techniques to protect databases

List of Experiments

1. Steps to ensure security of any one web browser (Mozilla Firefox/Google chrome)
2. Learn to install virtual box or any other equivalent software on the host OS.
3. Study of the features of firewall in providing network security and to set firewall security in windows.
4. Generating password hashes with OpenSSL.
5. Perform a wireless audit of an access point / router and decrypt WEP and WPA.
6. Setup a honeypot and monitor the HoneyPot on network
7. Analysis of the security vulnerabilities of e-commerce services.
8. Case Study on Authentication and Encryption
9. Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
10. Study the steps to protect a Microsoft Word Document of different version with different operating system.
11. Study the steps to remove Passwords from Microsoft Word
12. Study various methods of protecting and securing databases.
13. Study “How to make strong passwords” and “passwords cracking techniques”.
14. Study the steps to hack a strong password

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-117 OPERATING SYSTEM LAB

Mid-Sem	End-Sem	MM	L	T	P	C
70	30	100	0	0	4	2

Course Objectives:

This course will provide the in-depth knowledge of basic concepts and commands of Windows and Linux Operating Systems.

Course Outcomes:

After undergoing this course students will be able to

The student will be able to:

1. Understand and implement basic services and commands of Windows operating System
2. Implement commands for files and directories;
3. Understand Linux Operating System and its structure
4. **Shells of Linux OS and installation of different software services in Linux**

Case Study of Windows Operating System

Installation of Windows OS, My Computer, Recycle Bin, Desktop, Drives, create a directory/folder, rename/change to a directory/folder, creating a file in a directory/folder, Make the file read only, Make the file/directory hidden, Editing a file in a directory/folder, Delete a file in a directory/folder.

Listing the files in the directory, Create a file, Copy a file from one directory to the other, Deleting all files from a directory/folder, Deleting a director/folder, Formatting a hard disk and loading operating system, Domain, workgroup, Active Directory, User Management, Network Setting, Services, IIS Configuration.

Case Study of Linux Operating System

Installation of Linux OS, Distributions of Linux, Devices and drivers, File system Hierarchy, The components: Kernel, Distribution, XFree86, Sawfish, Gnome, The command line commands, File, management commands, Working with nano, Working with help (man).

SSH and X-forwarding, Managing compressed archives with zip and tar, Working with GNU screen, How to add users and groups, working with su, working with sudo, Changing user password, Printing, Installing software with Yum, Yast, Rpm, Installing webmin.

2nd SEMESTER

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-102 DIGITAL FORENSICS

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

Aim of this course is to teach deep understanding of security issues and digital forensics & incident response. In addition, this course also provides the students with specialist knowledge and experience of various digital forensics.

Course Outcomes:

After undergoing this course students will be able to

- **Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response.**
- **Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project**

Unit I: Introduction to Computer Forensics - Course overview - Understanding the need for computer forensics - Defining computer forensics – Computer Hardware - Understanding the computer components - Digital Media - Hard disk basics.

Unit II: The Forensic Toolkit - Forensic hardware - Hardware write/blockers - Hard drive acquisitions - Processing the scene Hard drive acquisition, Files and File Systems - Windows file systems - FAT32 - NTFS - Forensic file images.

Unit III: Forensic software - Overview of different software packages - EnCase - Autopsy EnCase introduction – Bookmarking and Searching - Creating basic search queries - Hex, Decimal, and Binary - ASCII – Unicode, Searching evidence for common keywords – Bookmarking and Searching - Creating basic search queries - Hex, Decimal, and Binary - ASCII – Unicode, Searching evidence for common keywords.

Unit IV: GREP - Understanding GREP - Building Regular Expressions - Creating GREP keywords - Viewing and managing keywords and cases E-mail Analysis - Viewing e-mail - Webmail - POP - File Signature Analysis - File signatures - File extensions - Differences between - Identifying Detecting file manipulation Hash Analysis - Understanding hash algorithms - Hashing files - Hash – Other Windows Artifacts - Common windows artifacts - Recycle bin - My Documents - Recent files - Installed programs.

Recommended Text and Reference Books

Hacking Exposed: Computer Forensics. Davis, Philipp, and Cowen ISBN: 0-07- 225675-3

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-104 Malware Analysis and Reverse Engineering

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:

This course will provide the in-depth knowledge of basic and advanced Programming skills in Python language.

Course Outcomes:

After undergoing this course students will be able to

- To understand the concept of malware and reverse engineering
- Implement tools and techniques of malware analysis.

Unit I:

Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Goals of Malware Analysis, Malware types and Malware Analysis Techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM), Understanding Malware Threats, Malware indicators, Malware Classification. [10]

Unit II:

Static Malware Analysis: Collecting Malware and Initial Analysis, Hacking Malware, Basic Malware Analysis Static Techniques, Malware Analysis in Virtual machines. Case Study: IDAPro [8]

Unit III:

Dynamic Malware Analysis: Basic Dynamic malware Analysis techniques, Sandbox Approach, Running Malware, Monitoring with Process Monitor, Registry Analysis with Regshot, Viewing processes with Process Explorer, Packet Sniffing, Faking a Network, Case Study: Wireshark [8]

Unit IV:

Malware and Kernel Debugging: Source Level vs Assembly level debuggers, Kernal vs User mode Debugging, Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Case study: OllyDbg [8]

Unit V:

Anti Reverse Engineering: Anti Disassembly, Anti Debugging, Anti Virtual machine techniques, Packers and Unpacking [6]

Recommended Text and Reference Books

Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher William pollock

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-106 Ethical Hacking

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:
The mission of this course is to educate, introduce and demonstrate hacking tools for penetration testing purposes only.

Course Outcomes:

After undergoing this course students will be able to

- Introduction of Ethical hacking, issues and network scanning tools and techniques.
- Gain knowledge of system hacking and various Malware threats.
- Gain knowledge of various packet sniffing techniques, different types of DDoS attacks
- and Botnets.
- Illustrate the concept of a Firewall and various evasion techniques.

Unit-1 Ethical Hacking: Introduction to Ethical Hacking, Foot-printing and Reconnaissance, Network Scanning Techniques, Enumeration techniques and enumeration countermeasures.

Unit-2 System Hacking: Methodology, Steganography, Steganalysis attacks, and covering tracks.

Unit-3 Malware Threats: Working of viruses, virus analysis, computer worms, Malware analysis procedure, and countermeasures, Different types of Trojans, Trojan analysis, and Trojan Countermeasures.

Unit-4 Packet Sniffing: Techniques and how to defend against sniffing, Social Engineering techniques, identify theft, and social engineering countermeasures.

Unit-5 DoS/DDoS attacks: Techniques, Botnets, DDoS attack tools, and countermeasures.

Unit-6 Hacking Webservers: Different types of webserver attacks, attack methodology, and Countermeasures, Hacking Web Applications, SQL Injection.

Unit-7 Evasion Techniques: Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.

Recommended Text and Reference Books

1. Ethical Hacking For Beginners - Practical Approach by Toshendra Sharma
2. Learning Ethical Hacking from Scratch by Zaid Sabih
3. The complete Ethical hacking course by Ermin Kreponic

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-108	Incident Response Management

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		3	0	0	3

Course Objectives:
This course will enable students to Incident response team development and management, evidence handling, and the technical skills necessary to locate appropriate evidence.

Course Outcomes:

After undergoing this course students will be able to

- Obtain basic knowledge on dealing with system security related incidents. Differentiate events from incidents and classify incidents appropriately.
- Develop incident response policy and Explore network and host-based artifacts to help determine root cause.
- Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.
- Gain experience using tools and common processes in performing analysis of compromised systems and dynamic malware analysis.
- Obtain current knowledge of events and tools/support kits in the subject area.

Unit I: Preparing for the Inevitable Incident:
the IR process, investigation lifecycle, remediation, information tracking, the purpose of a Computer Emergency Response Team (CERT), why an organization needs a CERT, composition of a CERT team, and the incident response life cycle.

Unit II: Incident Detection and Characterization
investigative tips and techniques that contribute to a successful incident response. checklists, case notes, development of leads, creating indicators of compromise, and determining the scope of the incident.

Unit III: Data Collection
collecting data from both running and offline systems, the network, and from enterprise services. Data sources include memory, hard drives, network packet captures, and log files. Forensic Duplication

Unit IV: Data Analysis
general analysis approaches and then dive into specific operating systems. Investigate Microsoft Windows and Apple OS X. malware triage, primarily focusing on the Windows platform. report writing and provide a sample report template.

Unit V: **Remediation**
remediation concepts, including a seven-step remediation process. Remediation case study.

Recommended Text and Reference Books

Textbooks (Required):

- **Computer Incident Response and Forensic Team Management,** Book, Leighton Johnson, ISBN: 978-1597499965

Reference Books/Resources:

- Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, 2nd Edition
- Cisco – 2017 Annual Cybersecurity Report • Read: Cisco – 2016 Midyear Cybersecurity Report
- The Internet Assigned Numbers Authority (IANA) web site (https://www.iana.org) and associated resources available on this web site

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-110 Digital Forensics Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		0	0	4	2

Course Objectives:
This course will provide the in-depth knowledge of basic and advanced Programming skills in Python language.

Course Outcomes:

After undergoing this course students will be able to

1. Learn the techniques of Hardware drive acquisition
2. Learn the vulnerabilities in Windows OS
3. Learn the vulnerabilities in Linux OS
4. Email Hacking

Lab I: Hard drive acquisition-Forensic hardware - Hardware write/blockers - Hard drive acquisitions - Processing the scene.

Lab II: Case Preparation-Windows file systems - FAT32 - NTFS - Forensic file images.

Lab III EnCase Introduction - Overview of different software packages.

Lab IV Searching evidence

Lab V- GREP Lab- Understanding GREP - Building Regular Expressions - Creating GREP keywords - Viewing and managing keywords and cases.

Lab VI- Email analysis lab- Viewing e-mail - Webmail - POP - IMAP.

Lab VII- Detecting File Manipulation

Lab-VIII- Hash Analysis Lab- Understanding hash algorithms - Hashing files - Hash libraries

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-112 Malware Analysis and Reverse Engineering Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	30	100		0	0	4	2

Course Objectives:
This course will provide the in-depth knowledge of basic and advanced Programming skills in Python language.

Course Outcomes:

After undergoing this course students will be able to

- To understand the concept of malware and reverse engineering
- Implement tools and techniques of malware analysis.

Expt 1. Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious programs.

Expt 2. Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment.

Expt 3. Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks.

Expt 4. Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis.

Expt 5. Use a disassembler and a debugger to examine the inner workings of malicious Windows executables.

Expt 6. Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst.

Expt 7. Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures.

Expt 8. Assess the threat associated with malicious documents, such as PDF and Microsoft Office files, in the context of targeted attacks.

Expt 9. Derive Indicators of Compromise from malicious executables to perform incident response triage.

Expt 10. Utilize practical memory forensics techniques to examine the capabilities of rootkits and other malicious program types.

Shaheed Bhagat Singh State Technical Campus, Ferozepur

PGDCSDF-114 Ethical Hacking Lab

Mid-Sem	End-Sem	MM		L	T	P	C
70	**30**	**100**		**0**	**0**	**4**	**2**

Course Objectives:
The mission of this course is to educate, introduce and demonstrate hacking tools for penetration testing purposes only.

Course Outcomes:

After undergoing this course students will be able to

- Introduction of Ethical hacking, issues and network scanning tools and techniques.
- Gain knowledge of system hacking and various Malware threats.
- Gain knowledge of various packet sniffing techniques, different types of DDoS attacks
- and Botnets.
- Illustrate the concept of a Firewall and various evasion techniques.

LIST OF PRACTICALS

1. To gather Live Network Information using open source tools (Nmap, Maltego etc.)
2. To demonstrate usage of Live Ethercap powerful attacking tools
3. To demonstrate Live active & passive scanning
4. To demonstrate Live DNS Hijacking (DNS Spoofing)
5. To Launch and Analyse a Live DoS attack
6. To Launch and Analyse a Live DDoS attack
7. To demonstrate Live Key Loggers attack
8. To demonstrate Sending of Fake Emails/ Email Forging
9. To demonstrate Fake calls/ Call Forging
10. To demonstrate Live Website hacking using SQL Injection
11. To demonstrate Live MTM attack (APR Spoofing)
12. To demonstrate Social Engineering Attacks (Credential Harvesting attack, java applet attack, tab nabbing attacks)
13. To demonstrate Windows Administrator account Password Hacking