

School of Computer Science and Engineering

CURRICULUM AND SYLLABI

(2023-2024)

M.Tech. Computer Science and Engineering (Information Security)

School of Computer Science and Engineering

M.Tech. Computer Science and Engineering (Information Security)

CURRICULUM AND SYLLABUS

(2023-24 Admitted Students)





VISION STATEMENT OF VELLORE INSTITUTE OF TECHNOLOGY

Transforming life through excellence in education and research.

MISSION STATEMENT OF VELLORE INSTITUTE OF TECHNOLOGY

World class Education: Excellence in education, grounded in ethics and critical thinking, for improvement of life.

Cutting edge Research: An innovation ecosystem to extend knowledge and solve critical problems.

Impactful People: Happy, accountable, caring and effective workforce and students.

Rewarding Co-creations: Active collaboration with national & international industries & universities for productivity and economic development.

Service to Society: Service to the region and world through knowledge and compassion.

VISION STATEMENT OF THE SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

To be a world-renowned centre of education, research and service in computing and allied domains.

MISSION STATEMENT OF THE SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

- To offer computing education programs with the goal that the students become technically competent and develop lifelong learning skill.
- To undertake path-breaking research that creates new computing technologies and solutions for industry and society at large.
- To foster vibrant outreach programs for industry, research organizations, academia and society.



School of Computer Science and Engineering

M.Tech (CSE) - Specialization in Information Security

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

1. Graduates will be engineering professionals who will engage in technology development and deployment with social awareness and responsibility.

2. Graduates will function as successful practising engineer / researcher / teacher / entrepreneur in the chosen domain of study.

3. Graduates will have holistic approach addressing technological, societal, economic and sustainability dimensions of problems and contribute to economic growth of the country.



M. Tech Computer Science and Engineering Specialization in Information Security

PROGRAMME OUTCOMES (POs)

PO_01: Having an ability to apply mathematics and science in engineering applications.

PO_03: Having an ability to design a component or a product applying all the relevant standards and with realistic constraints, including public health, safety, culture, society and environment

PO_04: Having an ability to design and conduct experiments, as well as toanalyze and interpret data, and synthesis of information

PO_05: Having an ability to use techniques, skills, resources and modern engineering and IT tools necessary for engineering practice

PO_06: Having problem solving ability- to assess social issues (societal, health, safety, legal and cultural) and engineering problems

PO_07: Having adaptive thinking and adaptability in relation to environmental context and sustainable development

PO_08: Having a clear understanding of professional and ethical responsibility

PO_11: Having a good cognitive load management skills related to project management and finance



School of Computer Science and Engineering M.Tech (CSE) - Specialization in Information Security

PROGRAMME SPECIFIC OUTCOMES (PSOs)

1. The ability to design and develop computer programs/computer-based systems in the advanced level of areas including algorithms design and analysis, networking, operating systems design etc.

2. The ability to investigate and analyze using appropriate methodologies as well as security principles and apply ethically acceptable security solutions to mitigate cyber security threats.

3. Ability to bring out the capabilities for research and development in contemporary issues and to exhibit the outcomes as technical report.



M. Tech Computer Science and Engineering Specialization in Information Security

CREDIT STRUCTURE

Category-wise Credit distribution

| Discipline Core | 24 |
|-------------------------|----|
| Specialization Elective | 12 |
| Projects and Internship | 26 |
| Open Elective | 3 |
| Skill Enhancement | 5 |
| Total Credits | 70 |



CURRICULUM

M.Tech.-CSE (Information Security) - (2023)

| Discipline Core | Specialization Elective | Projects and Internship | Open Elective | Skill Enhancement | Total Credits |
|-----------------|-------------------------|-------------------------|----------------------|-------------------|---------------|
| 24 | 12 | 26 | 3 | 5 | 70 |

| | | Discipline Core | ! | | | | | | |
|----------------|-------------|--|-------------|---------|---|---|---|----------|------|
| S. No. | Course Code | Course Title | Course Type | Version | L | Т | Р | J | С |
| 1 | MCSE501L | Data Structures and Algorithms | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 2 | MCSE501P | Data Structures and Algorithms Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 3 | MCSE502L | Design and Analysis of Algorithms | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 4 | MCSE502P | Design and Analysis of Algorithms Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 5 | MCSE503L | Computer Architecture and Organisation | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 6 | MCSE503P | Computer Architecture and Organisation Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 7 | MCSE504L | Operating Systems | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 8 | MCSE504P | Operating Systems Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 9 | MCSE505L | Computer Networks | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 10 | MCSE505P | Computer Networks Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 11 | MCSE506L | Database Systems | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 12 | MCSE506P | Database Systems Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| | | Specialization Elec | tive | | | | | | |
| S. No. | Course Code | Course Title | Course Type | Version | L | Т | Р | J | С |
| 1 | MCSE608L | Information Security and Risk Management | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 2 | MCSE609L | Cryptosystems | Theory Only | 1.0 | 2 | 0 | 0 | 0 | 2.0 |
| 3 | MCSE609P | Cryptosystems Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 4 | MCSE610L | Penetration Testing and Vulnerability Assessment | Theory Only | 1.0 | 2 | 0 | 0 | 0 | 2.0 |
| 5 | MCSE610P | Penetration Testing and Vulnerability Assessment Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 6 | MCSE611L | Malware Analysis | Theory Only | 1.0 | 2 | 0 | 0 | 0 | 2.0 |
| 7 | MCSE611P | Malware Analysis Lab | Lab Only | 1.0 | 0 | 0 | 2 | 0 | 1.0 |
| 8 | MCSE612L | Cyber Security | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 9 | MCSE613L | Digital Forensics | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| | | Projects and Interns | hip | | | | | | |
| S. No. | Course Code | Course Title | Course Type | Version | L | Т | Р | J | С |
| 1 | MCSE696J | Study Oriented Project | PROJECT | 1.0 | 0 | 0 | 0 | 0 | 2.0 |
| 2 | MCSE697J | Design Project | PROJECT | 1.0 | 0 | 0 | 0 | 0 | 2.0 |
| 3 | MCSE698J | Internship I/ Dissertation I | PROJECT | 1.0 | 0 | 0 | 0 | 0 | 10.0 |
| 4 | MCSE699J | Internship II/ Dissertation II | PROJECT | 1.0 | 0 | 0 | 0 | 0 | 12.0 |
| | - | Open Elective | | | | | - | _ | - |
| S. No. | Course Code | Course Title | Course Type | Version | L | Т | Р | J | С |
| 1 | MFRE501L | Francais Fonctionnel | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 2 | MGER501L | Deutsch fuer Anfaenger | Theory Only | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| 3 | MSTS601L | Advanced Competitive Coding | Soft Skill | 1.0 | 3 | 0 | 0 | 0 | 3.0 |
| | | Skill Enhanceme | nt | | | I | I | <u> </u> | 1 |
| S. <u>No</u> . | Course Code | Course Title | Course Type | Version | L | Т | Р | J | C |
| 1 | MENG501P | Technical Report Writing | Lab Only | 1.0 | 0 | 0 | 4 | 0 | 2.0 |
| 2 | MSTS501P | Qualitative Skills Practice | Soft Skill | 1.0 | 0 | 0 | 3 | 0 | 1.5 |
| 3 | MSTS502P | Quantitative Skills Practice | Soft Skill | 1.0 | 0 | 0 | 3 | 0 | 1.5 |

Discipline Core

| Course code | Course title | L T P C | | | | | | |
|--------------------------|---|----------------------|-----------------|--------|------------------------|-------|--|--|
| MCSE501L | Data Structures and Algorith | nms | 3 | 0 | 0 | 3 | | |
| Pre-requisite | NIL | | Sylla | abus | vers | sion | | |
| | | | | | v. | 1.0 | | |
| Course Objectives | | | | | | | | |
| 1. To familiari | ze the concepts of data structures and algo | rithms focusing or | n spa | ce a | nd t | ime | | |
| complexity. | | | | | | | | |
| 2. To provide a | deeper insight into the basic and advanced dat | a structures. | | | | | | |
| 3. To develop | 3. To develop the knowledge for the application of advanced trees and graphs in real- world | | | | | | | |
| scenarios. | | | | | | | | |
| | | | | | | | | |
| Course Outcomes | | | | | | | | |
| After completion of | this course, the student shall be able to: | | | | | | | |
| 1. Understand a | and analyze the space and time complexity of the | he algorithms. | | | | | | |
| 2. Identification | n of suitable data structure for a given problem. | | | | | | | |
| 3. Implementat | ion of graph algorithms in various real-life app | lications. | | | | | | |
| 4. Implementat | ion of heaps and trees for querying and searchi | ng. | | | | | | |
| 5. Use of basic | data structures in advanced data structure oper | ations. | | | | | | |
| 6. Use of search | ning and sorting in various real-life application | S. | | | | | | |
| Madulas1 Cuarr | th of Francisco | | | | 2 6 0 | | | |
| Module:1 Grow | th of Functions | : 41 | D | • • • | 3 n 0 | urs | | |
| Derformence enclusion | riance of algorithms and data structures- Algor | nd Thete notation, I | Recui | rsion | i, ina | | | |
| Style Pefinement of | f Coding Time Space Trade Off Testing Dat | nd Theta holation, F | rogra | 111111 | mg | | | |
| Style, Kernellient 0 | T Couling - Time-Space Trade Off, Testing, Dat | a Abstraction. | | | 6 ho | 11100 | | |
| Array Steels Queue | Linked list and its types. Various Depresent | ations Operations | Pr 1 m | nlia | 0 IIU | | | |
| Allay, Slack, Queue | e, Linked-fist and its types, various Represent | ations, Operations a | x Ap | prica | ation | \$ 01 | | |
| Module·3 Sortir | ag and Searching | | | | 7 ho | urs | | |
| Insertion sort mero | e sort sorting in linear Time-Lower bounds | for sorting Radix | sort | Rito | $\frac{7}{\text{nic}}$ | ort | | |
| Cocktail sort Media | ans and Order Statistics-Minimum and maximu | im Selection in ext | sort, pecter | l line | ar ti | me | | |
| Selection in worst-c | ase linear time, linear search. Interpolation sear | rch. Exponential sea | rch | 1 1111 | Jui ti | me, | | |
| Module:4 Trees | | | | | 6 ho | urs | | |
| Binary trees- Proper | ties of Binary trees. B-tree, B-Tree definition- | Operations on B-Tre | ee: Se | earch | ing a | a B- | | |
| tree, Creating, Splitt | ing, Inserting and Deleting, B+-tree. | 1 | | | 0 | | | |
| Module:5 Adva | nced Trees | | | | 8 ho | ours | | |
| Threaded binary tre | es, Leftist trees, Tournament trees, 2-3 tree, Sp | lay tree, Red-black | trees, | Ran | ge tr | ees. | | |
| Module:6 Grap | hs | | | | 7 ho | ours | | |
| Representation of g | raphs, Topological sorting, Shortest path algo | orithms- Dijkstra's | algor | ithm | , Flo | oyd- | | |
| Warshall algorithm, | Minimum spanning trees - Reverse delete algo | orithm, Boruvka's al | goritl | ım. | | - | | |
| Module:7 Heap | and Hashing | | | | 6 ho | ours | | |
| Heaps as priority qu | eues, Binary heaps, binomial and Fibonacci he | aps, Heaps in Huffn | nan c | odin | g, | | | |
| Extendible hashing. | | 1 | | | | | | |
| Module:8 Cont | emporary Issues | | | | 2 ho | urs | | |
| | | I | | | | | | |
| | Total Lecture hours: | | | 4 | l5 ho | urs | | |

| Tex | Text Book(s) | | | | | | | |
|-----|---|--------------------|------------|--------------------------------|--|--|--|--|
| 1. | Cormen, Thomas H., Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to | | | | | | | |
| | algorithms. MIT press, 2022. | | | | | | | |
| Ref | Reference Books | | | | | | | |
| 1. | Skiena, Steven S. "The Algorithm Design Manual (Texts in Computer Science)." 3rd edition, 2020, | | | | | | | |
| | Springer. | | | | | | | |
| 2. | Brass, Peter. Advanced data structure | es. Vol. 193. Camb | ridge: Cam | bridge University Press, 2008. | | | | |
| Mod | de of Evaluation: CAT / Written Assig | gnment / Quiz / FA | Г | | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | | | |
| App | proved by Academic Council | No. 67 | Date | 08-08-2022 | | | | |

| Course codeCourse titleLTF | | | | | Р | С | | |
|----------------------------|--|-----------------------|----------------|-----------------|---------|-------|--------|------|
| MCSE501P | Data St | ructures and Algo | orithms LA | B | 0 | 0 | 2 | 1 |
| Pre-requisite | NIL | | | | Sylla | abus | vers | sion |
| | | | | | | | v. | 1.0 |
| Course Objectives | | | | | | | | |
| 1. To fami | liarize the concepts of | of data structures | and algorit | hm focusing of | on spa | ace a | and t | ime |
| complex | complexity. | | | | | | | |
| 2. To provi | 2. To provide a deeper insight on the basic and advanced data structures. | | | | | | | |
| 3. To deve | 3. To develop the knowledge for application of the advanced trees and graphs in real world | | | | | | | |
| scenario | S. | | | | | | | |
| Course Outcome | | | | | | | | |
| After completion of | this course, the stude | ent shall be able to: | 1 | 1 1.1 | | | | |
| 1. Understa | and and analyze the sp | pace and time com | plexity of the | he algorithms. | | | | |
| 2. Identific | ation of suitable data | structure for a give | en problem. | | | | | |
| 3. Impleme | intation of graph algo | rithms in various r | eal-life app | lications. | | | | |
| 4. Impleme | intation of heaps and | trees for querying | and search | ng. | | | | |
| 5. Use of b | asic data structures in | advanced data str | ucture oper | ations. | | | | |
| 6. Use of s | earching and sorting 1 | n various real-life | application | S. | | | | |
| Indicative Experim | nents | | | | | | | |
| 1. Analyzing the | e complexity of iterati | ve and recursive a | lgorithms | | | | | |
| 2. Implement Li | near data structures (| Stacks, Oueues, Li | nked Lists) | | | | | |
| 3. Linear time so | orting techniques | | | | | | | |
| 4. Interpolation | search & Exponential | search | | | | | | |
| 5. Binary tree & | Tree traversals | | | | | | | |
| 6. B-trees & B+ | trees | | | | | | | |
| 7. Advanced Tre | ees: 2-3 tree, splay tre | e, red black tree et | с. | | | | | |
| 8. Advanced Tre | ees: Threaded Binary | trees, tournament | rees | | | | | |
| 9. Graph travers | als (BFS, DFS, Topol | logical sorting) | | | | | | |
| 10. Determining | the Shortest path betw | veen pair of nodes | in the giver | ı graph | | | | |
| 11. Minimum Spa | anning trees- reverse | delete & Boruvka' | s algorithm | | | | | |
| 12. Heaps & Has | hing | | | | | | | |
| | | | Total Lab | oratory Hours | 301 | nours | 5 | |
| Text Book(s) | | | | | | | | |
| 1. Cormen, Thom | nas H., Charles E. Leis | serson, Ronald L. I | Rivest, and | Clifford Stein | . Intro | duct | ion to | С |
| algorithms. MI | T press, 2022. | | | | | | | |
| Reference Books | | | . ~ | | | | | |
| 1. Skiena, Steven | S. "The Algorithm D | esign Manual (Tex | ts in Comp | uter Science).' | ' 3rd e | ditic | on, 20 |)20, |
| Springer. | 1 11. | 11 1 100 0 | | 1 * 1 ** * | • | | | |
| 2. Brass, Peter. A | dvanced data structur | res. Vol. 193. Cam | bridge: Can | nbridge Unive | rsity ł | ress | , 200 | 8. |
| Mode of Evaluation | : CAT / Mid-Term La | ad/ FAT | | | | | | |
| Recommended by H | Soard of Studies | 26-07-2022 | D | 00.00.000 | | | | |
| Approved by Acade | emic Council | No. 67 | Date | 08-08-2022 | | | | |

| Course code | ę | Course title | L T P C | | | | | |
|---|---|--|--------------------------------------|--------------------|----------------|-------------|--|--|
| MCSE502L | 1 | Design and Analysis of Algorithms | 3 | 0 | 0 | 3 | | |
| Pre-requisit | te | NIL | Sylla | abus | vers | sion | | |
| | | | | | v. | 1.0 | | |
| Course Obj | ectives | | | | | | | |
| 1. T 2. T 3. T | To provide a mathematical framework for the design and analysis of algorithms. To disseminate knowledge on how to create strategies for dealing with real-world problems. To develop efficient algorithms for use in a variety of engineering design settings. | | | | | | | |
| Course Out | comes | | | | | | | |
| On completi 1. Appl 2. Appl 3. Demo 4. Under 5. Appl 6. Expla | On completion of this course, student should be able to: Apply knowledge of computing and mathematics to algorithm design. Apply various algorithm paradigms to solve scientific and real-life problems. Demonstrate the string matching and network flow algorithms relating to real-life problems. Understand and apply geometric algorithms. Apply linear optimization techniques to various real-world linear optimization problems. | | | | | | | |
| 1 | | | | | | | | |
| Module:1 | Greed | y, Divide and Conquer Techniques Introduction | | | 6 ha | ours | | |
| Overview a problem, Id techniques: Karatsuba's | nd Impo entifyin Graph C fast mul | ortance of Algorithms - Stages of algorithm development: Descr g a suitable technique, Design of an algorithm, Illustration of Des Coloring Problem, Job Sequencing Problem with Deadlines- Di- tiplication method, the Strassen algorithm for matrix multiplicat | ibing t ign Sta ivide a ion | he Iges nd (| - Gre Conq | edy uer: | | |
| Module:2 | Dynai | mic Programming, Backtracking and Branch & Bound | | | 9 ho | ours | | |
| | Techn | iques | | | | | | |
| Dynamic pro Queens prob methods. | ogramm olem, S | ing: Matrix Chain Multiplication, Longest Common Subsequenc ubset Sum, Graph Coloring- Branch & Bound: A-Star, LIFO | e. Bacl -BB ar | ktrac nd F | king IFO | : N- BB | | |
| Module:3 | Amor | tized analysis and String Matching Algorithms | | | 6 ha | ours | | |
| Stack operat potential me Karp Algorit | ion and thod, an thm, Str | Incrementing Binary counter -The aggregate method, the account ad Dynamic tables. Naïve String matching Algorithms, KMP algorithms matching with Finite Automata. | nting m orithm | netho , Ra | od, tł bin- | ie | | |
| Module:4 | Netwo | ork Flow Algorithms | | | 6 ha | ours | | |
| Flow Netwo | rks, <mark>M</mark> a | ximum Flows: Ford-Fulkerson, Edmond-Karp, Push relabel Alg | orithm | , Th | e | | | |
| relabel-to-fro | ont algo | rithm, Minimum Cost flows – Cycle Cancelling Algorithm. | | | | | | |
| Module:5 | Comp | utational Geometry | | | 5 ho | ours | | |
| Line Segme | nts – pro | operties, intersection; Convex Hull finding algorithms- Graham' | s Scan | , Jar | vis's | | | |
| March Algo | rithm. | | | | | | | |
| Module:6 | Linea | r Optimization and Randomized algorithms | • | 11 | 5 ho | urs | | |
| Finding the g | amming global N | g problem - Simplex Method-Big M Method, LP Duality- The hi Ainimum Cut. | ring pi | oble | em, | | | |
| Module:7 | NP C | Completeness and Approximation Algorithms | | | 6 ha | ours | | |
| The Class P 3CNF, Indep salesman. | - The C bendent | lass NP - Reducibility and NP-completeness - Circuit Satisfiabi Set, Clique, Approximation Algorithm: Vertex Cover, Set Cove | lity pro | oblei Trave | n-SA elling | ۸Т ç | | |
| Module:8 | Cont | emporary Issues | | | 2 ho | urs | | |
| | | Total Lecture hours: | | 4 | 5 ho | ours | | |
| | | | | | - | | | |

| Tex | Text Book(s) | | | | | | | |
|---|--|---------------------|--------------|-----------------------|--|--|--|--|
| 1. | Cormen, Thomas H., Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to | | | | | | | |
| | algorithms. MIT press, 2022. | | | | | | | |
| Ref | Reference Books | | | | | | | |
| 1. | . Rajeev Motwani, Prabhakar Raghavan; "Randomized Algorithms, Cambridge University | | | | | | | |
| | Press, 1995 (Online Print — 2013). | | | | | | | |
| 2. | Ravindra K. Ahuja, Thomas L. Mag | nanti, and James B | . Orlin, Net | twork Flows: Theory, | | | | |
| | Algorithms, and Applications, 1st Ed | dition, Pearson Edu | cation, 201 | 14. | | | | |
| 3. | Jon Kleinberg and EvaTardos, Algor | rithm Design, Pears | son Educat | ion, 1"Edition, 2014. | | | | |
| Mo | de of Evaluation: CAT / Written Assi | gnment / Quiz / FA | Т | | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | | | |
| Approved by Academic Council No. 67 Date 08-08- | | | | 08-08-2022 | | | | |

| Course code Course title L T P Q | | | | | С | | | | |
|--|---|----------------------------|----------------------|--------------|-----------------|---------------|-------|--------|------|
| MCSE | 502P | Design a | nd Analysis of Al | gorithms I | Lab | 0 | 0 | 2 | 1 |
| Pre-re | quisite | NIL | | 5 | | Syll | abus | s vers | sion |
| | • | | | | | v | | v. | 1.0 |
| Course | e Objectives | | | | L. L. | | | | |
| 1. | To provide a | a mathematical frame | work for the desig | n and analy | ysis of algorit | hms. | | | |
| 2. | To dissemin | ate knowledge on ho | w to create strategi | ies for deal | ing with real- | world | proł | olems | s. |
| 3. | To develop | efficient algorithms f | or use in a variety | of engineer | ring design se | ttings | | | |
| | | | | | | | | | |
| Course | e Outcome | | | | | | | | |
| On co | mpletion of t | this course, student sl | nould be able to: | 1 . 1 | | | | | |
| 1. | Apply know | ledge of computing a | and mathematics to | algorithm | design. | | | | |
| 2. | Apply vario | us algorithm paradigi | ms to solve scientil | fic and real | -life problem | S. -1 1:£- | | | |
| 5. | problems | e the string matching | and network flow | argorithms | relating to re | ai-me | | | |
| Δ | Understand | and apply geometric | algorithms | | | | | | |
| 5 | Apply linear | r optimization technic | ues to various rea | l-world line | ear optimizati | on | | | |
| 5. | problems. | | 1405 00 7411045 104 | | our optimizuti | 011 | | | |
| 6. | Explain the | hardness of real-worl | d problems with re | espect to al | gorithmic des | ign. | | | |
| | - | | - | - | - | - | | | |
| | | | | | | | | | |
| Indica | tive Experin | nents | | | | | | | |
| 1. C | Greedy Strate | gy : Graph Coloring | Problem, Job Sequ | encing Pro | blem with De | eadline | es | | |
| 2. E | Divide and Co | onquer : Karatsuba's | fast multiplication | method, the | he Strassen al | gorith | m fo | or ma | trix |
| n | nultiplication | 1 | | | | | | | |
| 3. E | Dynamic Pro | gramming: Matrix | Chain Multiplicat | ion, Longe | est Common | Subse | eque | nce, | 0-1 |
| K | Knapsack | | | | | | | | |
| 4. E | Backtracking: | N-queens, Subset su | Im | | | | | | |
| 5. E | Branch and B | ound: Job selection | T7 41 1.1 | | •.• | | | | |
| 6. S | tring Matchi | ng Algorithms: Rabi | n Karp Algorithm, | KMP Algo | orithm | •.1 | | | |
| /. N | Network Flow | vs : Ford -Fulkerson a | and Edmond – Kar | p, Cycle ca | ancelling algo | rithm | | | |
| 8. N | Annimum Co | st flows – Cycle Can | celling Algorithm | | | | | | |
| 9. L | linear progra | mming: Simplex met | hod | | | | | | |
| 10. R | Randomized A | Algorithms: Las Veg | as and Monte carlo |) | | | | | |
| 11. P | olynomial ti | me algorithm for ver | itication of NPC pi | oblems | | | | | |
| 12. <i>P</i> | Approximatic | on Algorithm: Vertex | cover, Set cover a | nd TSP | | 20 | | | |
| Torrt D | $a a \mathbf{l} \mathbf{r}(a)$ | | | Total Lab | oratory Hours | 30 | nour | S | |
| 1 ext B | OOK(S) | and U. Charles E. La | icoreon Donald I | Divect on | d Clifford St | in In | tradi | latio | |
| 1. Co | algorithms | MIT press 2022 | iseison, Konalu L. | Kivest, all | | | noui | letioi | .1 |
| Refere | nce Books | wiii piess, 2022. | | | | | | | |
| 1 Ra | aieev Motwa | ni. Prabhakar Raghay | an: Randomized A | lgorithms. | Cambridge I | Iniver | sitv | | |
| Pr | ess, 1995 (O | nline Print — 2013). | | , | | | | | |
| 2 Ra | avindra K. Al | huja, Thomas L. Mag | manti, and James I | B. Orlin, No | etwork Flows | : Theo | ory, | | |
| Al | lgorithms, an | d Applications, 1^{st} E | dition, Pearson Edu | ication, 20 | <u>14.</u> | ••• | 4 | | |
| 3 Jo | n Kleinberg | and Eva Tardos, Algo | rithm Design, Pear | rson Educa | tion, l"Editic | n, 201 | 14. | | |
| Mode o | Mode of Evaluation: CAT / Mid-Term Lab/ FAT | | | | | | | | |
| Recom | mended by E | Board of Studies | 26-07-2022 | D | 00.00.0000 | | | | |
| Approv | ved by Acade | emic Council | NO. 6/ | Date | 08-08-2022 | | | | |

| Course code Course title | | | | | Р | С |
|--|--|--|----------------------------|-----------------------|--------------------------|---------------------|
| MCSE503L | | Computer Architecture and Organization | 3 | 0 | 0 | 3 |
| Pre-requisit | e | NIL | Syl | labus | s vers | sion |
| | | | J | | v. | 1.0 |
| Course Obj | ectives | | | | | |
| 1. T fc 2. T 0 3. T 0 Course Out After comple | o provid o design o design o evalua ptimizat | de knowledge on the basics of computer architectures and organiz on to study high-performance architectures n and develop parallel programs using parallel computing platform, CUDA ate the performance using profiling tools and optimize parallel co- cion techniques this course, the student shall be able to: | aralle | that ch as sing | lays s vario | the ous |
| Outline the developments in the evolution of computer architectures and parallel programming paradigms Comprehend the various programming languages and libraries for parallel computing platforms Use of profiling tools to analyze the performance of applications by interpreting the given data Evaluate efficiency trade-offs among alternative parallel computing architectures for an efficient parallel application design Develop parallel programs using OpenMP and CUDA and analyze performance parameters such as speed-up, and efficiency for parallel programs against serial programs | | | | | | n |
| | a | | | | ~ 1 | |
| Module:1 | Comp | uter Evolution And Performance | | | $\frac{5 \text{ ho}}{1}$ | ours |
| architecture, Multi-thread | Harvard Harvard ing, Col nce Me | d Architecture CISC & RISC, Flynn's Classification of Computer mparisons of Single Core, Multi Processors, and Multi-Core arch asurement | nts, v ers, N nitect | on N Aoor ures, | eum e's L Met | ann aw, trics |
| Module:2 | Memo | ory Hierarchy | | | 8 ho | ours |
| Key Charac Performance | cteristic: , Cache | s of Memory systems, Memory Hierarchy, Cache Design Coherence, Snoopy Protocols, Cache coherence protocols, MSI, | pol MES | icies I, M | , Ca OES | iche I |
| Module:3 | Paral | lel Computers | | | 8 ho | ours |
| Instruction L Parallelism (| level Pa TLP), T | rallelism(ILP), Compiler Techniques for ILP & Branch Predict hreading Concepts, Shared Memory, Message Passing, Vectoriz | ion, [ation | Threa | ad Le | evel |
| Module:4 | Multi | threaded Programming using OpenMP | | | 7 ho | ours |
| Introduction | to Ope | enMP, Parallel constructs, Runtime Library routines, Work-s | harin | g co | nstru | icts, |
| Scheduling c | lauses, | Data environment clauses, atomic, master Nowait Clause, Barrier | Con | struc | t | , |
| Module:5 | Prog | amming for GPU | | | 6 ho | ours |
| Introduction CUDA & Ex | to GPU ecution | J Computing, CUDA Concepts, CUDA Programming Model, Pro Methods for operations on Device Memory, Thread Organization | ogran on. Ex | n Stru amp | uctur les | e of |
| Module:6 | Perfo | rmance Analyzers | , | -1 | 6 h | ours |
| Performance | Evalua | tion, performance bottlenecks, Profiling categories; Profiling to | ols: T | race | analy | yzer |
| and collector | r (ITAC PP) | C), VTune Amplifier XE, Energy Efficient Performance, Integr | ated | Perf | orma | ince |
| 1 1111111VES (1 | | | | | | |

| Mo | dule:7 | Energy Efficient Architectures | 5 hours |
|-----|-----------|--|-------------------------|
| Ove | erview of | f power issues, CMOS Device-level Power dissipation basics, S | sources of energy |
| Con | sumption | , Strategies to save power or Energy, Low power designs, Power manag | gement techniques |
| Mo | dule:8 | Contemporary Issues | 1 hours |
| | | | |
| | | | |
| | | Total Lecture hours: | 45 hours |
| | | | |
| Tex | t Book(s |) | |
| 1. | William | Stallings, Computer Organization and Architecture: Designing for Perf | formance, |
| | Pearson | , 2022, 11 th Edition, Pearson | |
| 2 | Gerassii | nos Barlas, Multicore and GPU Programming: An Integrated Approach | , 2022, 2 nd |
| | edition, | Morgan Kaufmann | |
| Ref | erence B | ooks | |
| 1. | J.L. Her | inessy and D.A. Patterson. Computer Architecture: A Quantitative Appr | roach. 5th Edition, |
| | 2012, M | organ Kauffmann Publishers. | |
| 2. | Shamee | m Akhter, Jason Roberts, Multi-core Programming: Increasing Performation | ance Through |
| | Softwar | e Multi-threading, 2010, Intel Press, BPB Publications | - |
| Mo | de of Eva | luation: CAT / Written Assignment / Quiz / FAT | |
| Rec | ommende | ed by Board of Studies 26-07-2022 | |
| App | proved by | Academic CouncilNo. 67Date08-08-2022 | |

| Cour | se code | Course title | L | Т | Р | С | |
|-----------|--|---|---------------|-------|--------|------|--|
| MCS | E503P | Computer Architecture and Organization LAB | 0 | 0 | 2 | 1 | |
| Pre-r | requisite | NIL | Sylla | abus | vers | sion | |
| | | | | | v. | 1.0 | |
| Cour | se Objectives | | | | | | |
| | 1. To provi | de knowledge on basics of computer architectures and organiza | tion tha | t lay | 'S | | |
| | foundatio | on to study high performance architectures | | | | | |
| | 2. To desig | n and develop parallel programs using parallel computing platf | orms su | ch as | 5 | | |
| | OpenMP | P, CUDA | | | | | |
| | 3. To evaluate the performance using profiling tools and optimize parallel codes using various | | | | | | |
| ~ | optimiza | tion techniques | | | | | |
| Cour | se Outcome | | | | | | |
| After | completion of | this course, the student shall be able to: | | | | | |
| 1. | Outline the c | levelopments in the evolution of computer architectures and pa | rallel pr | ogra | mmı | ng | |
| 2 | paradigms | 1.4 | | 1 | | | |
| 2. | Comprehend | the various programming languages and libraries for parallel c | computii | ng pi | | rms | |
|) 3. 4 | Evaluate off | ing tools to analyze the performance of applications by interpre- | eturoa fo | giv | en da | ita | |
| 4. | efficient par | allel Application design | | n an | | | |
| 5 | Develop para | allel programs using OpenMP and CUDA and analyze perform | ance na | ame | eters | | |
| | such as spee | d-up, efficiency for parallel programs against serial programs | unee pu | unne | | | |
| | | | | | | | |
| Indic | ative Experim | nents | | | | | |
| | • | | | | | | |
| 1. | Set-up an envi | ironment for OpenMP Programming: | | | | | |
| | Activities: cre | eate a Project using Visual Studio, Writing Sample OpenMp | Progran | ı, Se | etting | g up | |
| | properties, co | mpile & Execute OpenMP program, OpenMP manual study | , Creati | on o | of Lo | ogin | |
| | credential on] | Intel for Intel Parallel Studio | | | | | |
| 2. | OpenMP prog | ram using following construct and describe scenario for the new | ed of co | nstru | ıct | | |
| | Use of Paralle | el Construct, Determine the Number of processors in a paral | lel Regi | on, | Find | the | |
| - | thread ID of e | ach processor | | | | | |
| 3. | Computation | of Execution Time | | | | | |
| 4 | Using OpenM | P clock, Using windows clock | | | | • | |
| 4. | OpenMP Pro | gram using various Environment Routines to access the | proces | sor | run-t | ime | |
| 5 | Information an | ha write interesting observations by comparing various routines | s monio fo | n tha | | dof | |
| э. | construct | rain using tonowing worksharing Constructs and describe see | mario 10 | i une | - nee | u oi | |
| | loon construct | sections construct single construct | | | | | |
| 6 | OpenMP prov | gram using following schedule clauses and describe scenario fo | r the ne | ed o | f clai | ise | |
| 0. | Static Dynam | ic. Guided | i the ne | | i ciu | 150 | |
| 7. | Develop paral | lel programs for given serial programs and profile the program i | ising Vt | une | Anal | vsis | |
| | tool | | | | | J~-~ | |
| | Matrix-Matrix | multiplication, Matrix-Vector multiplication | | | | | |
| 8. | Develop paral | lel programs for given serial programs and profile the program u | using Vt | une | Anal | ysis | |
| | tool | | 2 | | | - | |
| | Quicksort, M | inimum Spanning Tree | | | | | |
| 9. | CUDA-platfor | rm setup on NVIDIA / Google Colab | | | | | |
| 10. | Write a CUDA | A C/C++ program that add two array of elements and store the | result i | n thi | rd ar | ray | |
| 11. | Write a CUDA | A C/C++ program that Reverses Single Block in an Array; CUI | DA C/C- | ++ | | | |
| 12. | Write a CUDA | A C program for Matrix addition and Multiplication using Shar | ed mem | ory | | | |
| | | Total Laboratory Hours | 30 hou | rs | | | |

| Tex | Text Book(s) | | | | | |
|--|---|--------------------|----------|-------------------------------|--|--|
| 1. | Gerassimos Barlas, Multicore and GPU Programming: An Integrated Approach, 2022, 2 nd | | | | | |
| | edition, Morgan Kaufmann | | | | | |
| Ref | erence Books | | | | | |
| 1. | Shameem Akhter, Jason Roberts, | Multi-core Progra | mming: I | ncreasing Performance Through | | |
| | Software Multi-threading, 2010, Inte | el Press, BPB Publ | ications | | | |
| Mo | de of Evaluation: CAT / Mid-Term La | ab/ FAT | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | |
| Approved by Academic CouncilNo. 67Date08-08-2022 | | | | 08-08-2022 | | |

| Course code | Course title | L | Т | Р | С | |
|--|----------------------------|---|-----------|-------------|---------------|------------------|
| MCSE504L | MCSE504L OPERATING SYSTEMS | | | | | |
| Pre-requisit | e | Nil | Svlla | ibus | vers | sion |
| | - | | | | v. | 1.0 |
| Course Obj | ectives | | | | | |
| 1. T | 'o focus | the core functionalities required to develop and manage operating | ; syst | ems. | | |
| 2. T | 'o encon | npass process management, synchronization strategies, memory m | ianag | eme | nt, fi | ile |
| S | ystems, | device management, and virtualization. | | | | |
| 3. T | 'o introd | luce the concepts and features of real-time operating systems as w | ell as | | | |
| V | irtualiza | ition. | | | | |
| | | | | | | |
| Course Out | comes | | | | | |
| After comple | etion of | this course, the student shall be able to: | | | | |
| 1. U | Indersta | nd the fundamental operating system abstractions, including proce | esses, | thre | eads, | |
| Se | emapho | res, and file systems. | | | | |
| 2. Ir | npleme | nt scheduling, devising and addressing synchronization issues. | | | | |
| 3. G | fain an i | inderstanding of memory management tasks. | | | | |
| 4. D | Develop | real-time working prototypes of different small-scale and medium | i-scal | e en | ibed | ded |
| S S | ystems. | | <i>.</i> | | | |
| 5. C | ompreh | end the basics of virtualization and differentiate types of virtualiz | ation | • | | |
| Modulo.1 | Introd | notion to Operating Systems | 1 | | 1 ha | |
| Computer O | rgonizo | tion and Arabitacture OS definition OS history OS Operat | iona | 0 | 4 no 5 do | aign |
| issues Oper | rating s | usiant Architecture - OS definition – OS history – OS Operat | rnol (| -0 | o ach | Sigii |
| Building and | l bootin | g an OS | | appr | Jacin | 6 8 – |
| Modulo:2 | Drogog | g and Schoduling | 1 | | 6 ha | 11PC |
| Process state | rides s Stat | e transitions with suspend and resume Process control block C | ntov | tow | <u>itchi</u> | ng |
| Processes on | s – Stat | - Process scheduling - CPU scheduling: Non-preemptive preempt | five - | 1-5w Mul | ti_ar | ng - |
| scheduling - | Multi_l | evel feedback queue scheduling | .1 v C - | wiu | u-qu | icuc |
| Module·3 | Synch | pronization | | | 9 hc | nirs |
| IPC · Shred n | nemorv | message passing - Race condition – Critical section problem - Pet | tersoi | n's so | <u>- luti</u> | n = 1 |
| Bakery Algo | orithm - | Mutex locks - Semaphores – Classical synchronization proble | ensor | - M | onito | ors - |
| Thread synch | hronizat | ion – Multi-threading Models. Deadlocks – Resource allocation g | raphs | – D | eadle | ock: |
| prevention. a | voidan | ce. detection and recovery. | - up iiis | - | | |
| Module:4 | Memo | orv Management | | | 5 ho | ours |
| Address bind | ling – F | ragmentation - Pinning Memory – Paging – Structure of the page | table | - S | wapt | oing |
| - Segmentati | on - De | mand Paging – Copy-on-write - Replacement – Thrashing – Work | ing s | et – | Men | nory |
| compression | – Alloc | cating kernel memory. | 0 | | | 5 |
| Module:5 | Mana | ging Devices, Files, Security and Protection | | | 9 ho | ours |
| I/O Manager | nent – I | OMA - Delayed write - Disk scheduling algorithms: Seek-time and | rotat | iona | l late | ency |
| based - File | control | block – Inode – Access method – Directory structure - Directory | imple | eme | ntatio | on – |
| File allocation | on meth | ods - Free space management – Program and network threats – C | Crypt | ogra | phy | as a |
| security tool – Domains of protection – Access matrix – Capability based systems | | | | | | |
| Module:6 | Real- | time Operating Systems | | | 5 ho | ours |
| RTOS Intern | nals - F | Real-Time Scheduling - Task Specifications - Performance Me | etrics | of | RTC |) S - |
| Schedulabili | ty Analy | ysis – RTOS Programming Tools. | | | | |
| Module:7 | Virtu | alization | | | 5 ho | ours |
| Need for virt | ualizati | on - Virtual machines and architectures – Hypervisors - Virtualizat | ion T | echr | nolog | gies: |
| Para Virtua | lization, | Full Virtualization - Virtualization types: Server virtualization | tion, | Ap | plica | tion |
| virtualization | n, Storag | ge virtualization. | | | | |
| Module:8 | Cont | emporary Issues | | | 2 ho | ours |
| ı | | | <u> </u> | | | |
| | | Total Lecture hours: | | 4 | 15 ho | ours |

| Tex | Text Book(s) | | | | | | | |
|-----|--|-----------------------------------|-------------|---|--|--|--|--|
| 1. | Abraham Silberschatz, Peter B. Ga | lvin, Greg Gagne, | "Operatin | g System Concepts", 2018, 10 th | | | | |
| | Edition, Wiley, United States. | | | | | | | |
| Ref | erence Books | | | | | | | |
| 1. | Arpaci-Dusseau, R. H., & Arpaci-Dusseau, R. H. | usseau, A. C, "Ope | rating Syst | ems: Three easy pieces, 2018, | | | | |
| | 1 st Edition, Boston: Arpaci-Dusseau | Books LLC. | | | | | | |
| 2. | Kamal, R, Embedded Systems: Arcl | hitecture, Program | ming and I | Design, 2011, 1 st Edition, Tata | | | | |
| | McGraw-Hill Education. | | | | | | | |
| 3. | Portnoy, M, "Virtualization Essentia | lls", 2012, 2 nd Editi | ion, John W | Viley & Sons, New Jersey, USA. | | | | |
| Mo | de of Evaluation: CAT / Written Assi | gnment / Quiz / FA | Т | | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | | | |
| App | proved by Academic Council | No. 67 | Date | 08-08-2022 | | | | |

| Course code | Course title | L | Τ | P | С |
|---|---|-----------------|-------------|--------|--------|
| MCSE504P | OPERATING SYSTEMS LAB | 0 | 0 | 2 | 1 |
| Pre-requisite | Nil | Sylla | abus | vers | sion |
| | | | | v. | 1.0 |
| Course Objectives | | | | | |
| 1. To encomp | ass process management, synchronization strategies, memory man | nagen | nent, | file | |
| systems, de | vice management, and virtualization. | | | | |
| 2. To introduc | the concepts and features of real-time operating systems as well | l as vi | rtual | izati | on. |
| Course Outcome | | | | | |
| After completion of | f this course, the student shall be able to: | | | | |
| I. Implement | scheduling, devising and addressing synchronization issues. | | | | |
| 2. Gain an un | derstanding of memory management tasks. | 1 | | | |
| 3. Develop re | al-time working prototypes of different small-scale and medium-s | cale e | mbe | dded | |
| systems. | d the basics of virtualization and differentiate types of virtualization | . | | | |
| 4. Comprehen | in the basics of virtualization and unterentiate types of virtualization | 011. | | | |
| Indicativa Evnarin | nonts | | | | |
| 1 Investigate th | e fundamental Unix/Linux commands | | | | |
| 2 Obtaining the | OS system data file and its associated information | | | | |
| 3 Shell Program | nming | | | | |
| 4 Create utility | programs that use I/Ω system calls to simulate operations such a | ns ls | cn o | ren | and |
| others | programs that use 1/0 system cans to simulate operations such a | 15 15, | cp, g | siep, | ana |
| 5. Create child. | Orphan and Zombie processes using suitable system calls such | as fo | ork() | . exe | ec(). |
| wait(), kill(), | sleep() and exit() system calls. | | | , | - () / |
| 6. Create a pro | gram that mimics the CPU Scheduling algorithms including | multi | -leve | el qu | leue |
| scheduling al | gorithm. Ex: Assume that all processes in the system are divided in | nto tw | o ca | tegor | ries: |
| system proce | sses and user processes. System processes are to be given higher | prioi | ity t | han ı | ıser |
| processes. Us | e FCFS scheduling for the processes in each queue. | | | | |
| 7. Implement th | e deadlock-free solution to Dining Philosophers problem using Se | emaph | ore. | | |
| 8. Simulation of | f Bankers algorithm to check whether the given system is in safe | state | or r | not. A | Also |
| check whethe | r addition resource requested can be granted immediately. | | | | |
| 9. Parallel Thre | ad management using Pthreads library. Implement a data parall | elism | usin | ıg mı | ılti- |
| threading. Ex | x: An application should have a thread created with synchron | zatio | n an | d thr | ead |
| termination. Every thread in the sub-program must return the value and must be synchronized w | | | | v1th | |
| the main func | tion. Final consolidation should be done by the main (main function) | on). | | | |
| 10. Dynamic mer | nory allocation algorithms – First-fit, Best-fit, Worst-fit algorithm | is. | | | |
| 11. Page Replace | File looking machanism | | | | |
| 12. Implement a | December Monitoring and Controlling System Monitoring Co | llasti | na d | oto f | |
| 15. KIUS Based | ratameter Monitoring and Controlling System – Monitoring: Conterface display devices/actuators using a microcontroller. Control | mecti olling | ng a | ata fi | |
| alert when the | nerrae uspray usyles/actuators using a microcontroller. Contra- e received data reaches a certain threshold value | June | 5. г | ovide | 2 all |
| 14 Virtualization | Setup: Type-1 Type-2 Hypervisor (Detailed Study Report) | | | | |
| | Total Laboratory Hours | 301 | hour | s | |

| Tex | Text Book(s) | | | | | | |
|-----|---|---------------------|--------------|--|--|--|--|
| 1. | Vijay Mukhi, "The C Odyssey: UNIX: v. 3", 2004, 3 rd Edition, BPB Publications, New Delhi, | | | | | | |
| | India. | | | | | | |
| Ref | erence Books | | | | | | |
| 1. | Stevens, W. R., & Rago, S. A. (2013 |). Advanced Progra | amming in | the UNIX Environment: Advanc | | | |
| | Progra UNIX Envir_p3. Addison-W | esley. | | | | | |
| 2. | Love, Robert, "Linux System Progra | amming: talking dir | ectly to the | e kernel and C library", 2013, 2 nd | | | |
| | Edition, O'Reilly Media, Inc, United | l States. | | - | | | |
| Mod | Mode of Evaluation: CAT / Mid-Term Lab/ FAT | | | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | | |
| App | proved by Academic Council | No. 67 | Date | 08-08-2022 | | | |

| Course code | Course title | L | Т | Р | C | | | |
|--|---|-------------------|----------|--------|------------|--|--|--|
| MCSE505L | E505L Computer Networks 3 0 (| | | | | | | |
| Pre-requisite | uisite NIL Syllabus versi | | | | | | | |
| | v. 1. | | | | | | | |
| Course Object | ves | | | | | | | |
| 1. To learn | various network models, layers and their protocols. | | | | | | | |
| 2. To gain | a fundamental understanding of routing algorithms. | | | | | | | |
| 3. To comp | rehend the basics of wireless as well as mobile networks and their of | charact | eristi | ICS. | | | | |
| | | | | | | | | |
| Course Outcon | | | | | | | | |
| After completio | n of this course, the student shall be able to: | | | | | | | |
| 1. Explore | the basics of Computer Networks and various performance metrics. | | | | | | | |
| 2. Interpret | the application layer services and their protocols. | 1 | | | | | | |
| 3. Evaluate | the requirements for reliable services and implications of congestion. | on at th | e tra | nspo | rt | | | |
| layer ser | vices. | 11 | | | | | | |
| 4. Analyse | various functionalities required in the control and data plane at networks and their see | vork la | yer s | ervic | es. | | | |
| 5. Inter the | characteristics of wireless as well as mobile networks and their sec | urity st | anda | iras. | | | | |
| Modulo 1 C | mnutar Natworks and the Internet | <u> </u> | | 7 . | | | | |
| Internet: A Nut | and Polts Description Network Protocols. The Network Edge: A | | Notu | / II(| ond | | | |
| Dhysical Modia | -and-Bolts Description - Network Flotocols - The Network Edge. A | work c | f Nc | two | anu .ko | | | |
| Physical Meula | Throughput in Decket Switched Networks Drotocol Levers and T | work u hair Sa | ruiou | | KS - | | | |
| Modulo:2 | nilication Layer | | IVICE | 5 h | | | | |
| Dringinlag of N | phication Layer | icos ' | Tho ' | 5 III | and | | | |
| HTTD Electro | nic Mail in the Internet DNS. The Internet's Directory Service | D_{00} | r to r | Door | Filo | | | |
| Distribution S | nic Main in the internet - DNS—The internet's Directory Service | | 1-10-1 | r eei | rne | | | |
| Module-3 | ensport I aver | <u> </u> | | 7 h | nire | | | |
| Relationship Be | tween Transport and Network I avers - Overview of the Transport | Laveri | n the | Inte | rnet | | | |
| - Multiplexing a | nd Demultiplexing - Connectionless Transport: UDP - Reliable Data | Transt | fer (| -R | ack- | | | |
| N (GRN) and | Selective Repeat (SR) - Connection-Oriented Transport: TCP | Flow | Cor | trol | and | | | |
| Congestion Con | trol | 11000 | Con | 11101 | una | | | |
| Module:4 N | etwork Laver: Data Plane | | | 5 hc | mrs | | | |
| Network Laver | - Router - The Internet Protocol (IP): IPv4 Addressing and | IPv6 - | Ge | neral | ized | | | |
| Forwarding and | SDN | 11 10 | 00 | lioiui | 1200 | | | |
| Module:5 N | etwork Laver: Control Plane | | | 5 ha | ours | | | |
| Control Plane: | Per-router control and logically centralized control - Routing Algo | orithms | - L | ink-S | state | | | |
| (LS) Routing A | lgorithm, Distance-Vector (DV) Routing Algorithm, Intra-AS Rou | iting in | the | Inter | met: | | | |
| OSPF and Rou | ing Among the ISPs: BGP - SDN Control Plane | 0 | | | | | | |
| Module:6 Li | nk Layer and LANs | <u> </u> | | 8 ha | ours | | | |
| Overview of L | ink Laver Services - Error-Detection and -Correction Technique | ues: Pa | arity | Che | cks. | | | |
| Checksum and | CRC - Multiple Access Links and Protocols: Channel Partitio | ning F | roto | cols | and | | | |
| Random-Access | Random-Access Protocols - Switched Local Area Networks: Link-Laver Addressing and ARP - Virtual | | | | | | | |
| Local Area Networks | | | | | | | | |
| Module:7Wireless and Mobile Networks-Security6 hours | | | | | | | | |
| Elements of a w | vireless network - Wireless Links and Network Characteristics - Wi | iFi: 802 | 2.11 | Wire | eless | | | |
| LANs - Mobilit | y Management: Principles - Wireless and Mobility: Impact on Hig | her-La | yer J | Proto | col- | | | |
| Security in Cor | nputer Network- Message Integrity and Digital Signatures - Network | ork-La | yer (| Secu | rity: | | | |
| IPsec and Virtua | l Private Networks | | | | | | | |
| Module:8 | Contemporary Issues | | | 2 ho | ours | | | |
| | | | | | | | | |
| | Total Lecture hou | irs: | 4 | 45 ha | ours | | | |
| | | | | | | | | |

| Tex | Text Book(s) | | | | | | | |
|---|--|--------------------|---|--|--|--|--|--|
| 1. | James F. Kurose, Keith W. Ross, " | Computer Network | omputer Networking: A Top-Down Approach", 2022, 8 th | | | | | |
| | Edition (Paperback), Pearson, United | d Kingdom. | | | | | | |
| Ref | erence Books | | | | | | | |
| 1. | Larry Peterson and Bruce Davie, "C | Computer Network | s: A Syster | ns Approach", 2019, 6 th Edition, | | | | |
| | Morgan Kaufmann, United States of | America. | | | | | | |
| 2. | Andrew S. Tanenbaum, "Computer | Networks", 2013, | 6 th Edition, | Pearson, Singapore. | | | | |
| Mo | de of Evaluation: CAT / Written Assig | gnment / Quiz / FA | Т | | | | | |
| Rec | Recommended by Board of Studies 26-07-2022 | | | | | | | |
| Approved by Academic Council No. 67 Date 08-08-2022 | | | | 08-08-2022 | | | | |

| Course o | code | | Course title | | | L | Т | Р | С |
|-----------|--------------|------------------------|-----------------------|--------------|-------------------|--------|--------------------|------------------|------|
| MCSE5 | 05P | C | Computer Networl | ks Lab | | 0 | 0 | 2 | 1 |
| Pre-requ | uisite | NIL | • | | | Sylla | abus | vers | sion |
| • | | | | | | | | v. | 1.0 |
| Course | Objectives | I | | | | | | | |
| 1 | . To introc | luce the computer net | twork concepts and | l provide sl | kills required to | trou | ble s | hoot | the |
| | network | devices. | | | | | | | |
| 2 | . To descr | ibe the basic knowled | lge of VLAN. | | | | | | |
| 3 | . To devel | op the knowledge for | application of soft | ware defin | ed networks. | | | | |
| Course | Outcome | | | | | | | | |
| After con | npletion of | this course, the stude | ent shall be able to: | | | | | | |
| 1 | . Understa | and the types of netwo | ork cables and prac | tical imple | mentation of cr | oss-v | virec | l and | |
| | straight t | hrough cable. | | | | | | | |
| 2 | . Design a | nd implementation of | f VLAN. | | | | | | |
| 3 | . Analyze | and apply network ac | ldress translation u | sing packe | t tracer and net | work | sim | ulato | rs. |
| 4 | . Design a | nd develop software | defined networks. | | | | | | |
| | | | | | | | | | |
| Indicativ | ve Experin | nents | | | | | | | |
| 1. | Hardware | e Demo(Demo session | n of all networking | hardware a | and Functionali | ities) | | | |
| | OS Com | nands(Network confi | guration command | s) | | | | | |
| 2. | Error dete | ection and correction | mechanisms | | | | | | |
| | Flow con | trol mechanisms | | | | | | | |
| 3. | IP address | sing Classless address | sing | | | | | | |
| 4. | Network | Packet Analysis using | g Wireshark | | | | | | |
| | i. P | acket Capture Using | Wire shark | | | | | | |
| | ii. S | tarting Wire shark | | | | | | | |
| | iii. V | viewing Captured Tra | ffic | | | | | | |
| | iv. A | nalysis and Statistics | & Filters. | | | | | | |
| | | | | | | | | | |
| 5. | Socket pr | ogramming(TCP and | UDP) Multi client | chatting | | | | | |
| 6. | Networki | ng Simulation Tool – | Wired and Wireles | S | | | | | |
| 7. | SDN App | olications and Use Ca | ses | | | | | | |
| 8. | Security i | n Network- Use case | 8 | | | | | | |
| 9 | Performan | ce evaluation of routi | ng protocols using | simulation | tools. | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Referen | ce Books | | | | | | | | |
| 1. Jam | es F. Kuro | ss, Keith W. Ross, " | Computer Networ | king, A To | op-Down Appr | oach' | ", 8 ^{tl} | ¹ Edi | tion |
| (Pap | perback), Pe | earson Education, 202 | 22. | | | | | | |
| Mode of | Evaluation | : CAT / Mid-Term La | ab/ FAT | | | | | | |
| Recomm | ended by B | Board of Studies | 26-07-2022 | · | 1 | | | | |
| Approve | d by Acade | mic Council | No. 67 | Date | 08-08-2022 | | | | |

| Course code | ourse code Course title | | | | Р | С | | |
|--------------------|---|----------|------------------|-------|-------------|------------------|--|--|
| MCSE506L | 6L DATABASE SYSTEMS | | | | 0 | 3 | | |
| Pre-requisite | NIL | 2 | Sylla | bus | vers | ion | | |
| | | | | | v. | 1.0 | | |
| Course Obje | ctives | | | | | | | |
| 1. To | o understand the underlying principles of Relational Database Manag | gemei | nt Sy | stem | is | | | |
| 2. To | focus on the modeling and design of secured databases and usage of | of adv | ance | d da | ta | | | |
| m | odels | | | | | | | |
| 3. To | implement and maintain the structured, semi-structured, and unstru | icture | d dat | a in | an | | | |
| eft | Ficient database system using emerging trends | | | | | | | |
| | | | | | | | | |
| Course Outc | omes | | | | | | | |
| On completio | n of this course, students must be able to | | | | | | | |
| 1. De | esign and implement a database depending on the business requ | ireme | ents, | con | sider | ring | | |
| va | rious design issues | | | | | | | |
| 2. Ui | nderstand the concepts of Indexing, Query optimization, tran | sactio | on n | iana | gem | ent, | | |
| со | ncurrency control, and recovery mechanisms | | | | | | | |
| 3. Le | arn to apply parallel and distributed databases in Real-time scenario | S | | | | | | |
| 4. Ca | tegorize and design the structured, semi-structured, and unstructured | d data | abase | s | | | | |
| 5. Cł | haracterize the database threats and their countermeasures | | | | | | | |
| | | | | | <u></u> | | | |
| Module:1 | Design and Implementation of Relational Model | | 1 | 1 | <u>6 ho</u> | | | |
| Database Sys | tem Concepts and Architecture, Entity-Relationship (ER) Modellin | ng, R | elati | onal | Mo | del- | | |
| Keys, and Int | egrity Constraints, Mapping ER model to Relational Schema, Norm | alizat | 10n, | воу | ce Co | odd | | |
| Normal Form | , Multi-valued dependency and Fourth Normal form | | | | (] | | | |
| Storega and I | Query Processing and Transaction Management | Tron | anti | ~ ** | 0 110 | urs | | |
| Storage and F | Concurrency Control Bosovery | Tran | sactio | on | | | | |
| Modulo:3 | Parallal Databases and Distributed Databases | | | | 8 ho | iirc | | |
| Parallel Data | architecture Data partitioning strategy Inter-Ouery and Intra- | Quer | v Dar | أماله | <u>ism</u> | uis | | |
| Distributed D | atabase Features Distributed Database Architecture Fragmentation | Ren | y 1 ai licati | on | 13111, | | | |
| Distributed D | uery Processing Distributed Transactions Processing | , nep | iicati | on, | | | | |
| | Snatial and Multimedia Databases | | | | 6 ho | urs | | |
| Spatial databa | ase concepts. Spatial data types, and models. Spatial operators and | aueri | es. | Inde | exing | $\frac{1}{2}$ in | | |
| spatial databa | ses, Multimedia database concepts. Automatic Analysis of Images. | Obie | ct Re | COgi | nitio | n in | | |
| Images, Sema | intic Tagging of Images | | | - 01 | | | | |
| Module:5 | Semi-Structured Databases | | | | 6 ho | urs | | |
| Semi Structur | ed databases- XML Schema-DTD- XPath- XQuery, Semantic Web, | RDF | , RD | FS | | | | |
| Module:6 | Cloud and NoSQL Databases | | | (| 5 hoi | urs | | |
| Cloud databas | ses- Data Storage Systems on the Cloud, Data Representation, Partit | ionin | g and | l Re | triev | ing | | |
| Data, Challen | ges with Cloud-Based Databases- NoSQL Data model: Aggregate N | Aodel | s, Do | ocun | nent | • | | |
| Data Model, | Data Model, Key-Value Data Model, Columnar Data Model, Graph-Based Data Model | | | | | | | |
| Module:7 | Database Security | | | | 5 ho | urs | | |
| Database Sec | urity Issues, Security Models, Different threats to databases, Chal | lenge | s to | mai | ntain | ing | | |
| database secu | rity | | | | | | | |
| | | | | | | | | |
| Module:8 | Contemporary Issues | | | | 2 ho | urs | | |
| | | | | | | | | |
| | | | | | | | | |
| | Total Lecture hou | irs: | | 4 | 5 ho | urs | | |
| | | | | | | | | |

| Tex | xt Book(s) | | | | | |
|----------------------|--|---------------|--------------|--|--|--|
| 1 | Abraham Silberschatz, Henry F. Korth, and S. Sudharsan, "Database System Concepts", 7 ^h | | | | | |
| | Edition, McGraw Hill, 2019. | | | | | |
| 2 | R. Elmasri and S. Navathe, | Fundamentals | of Databa | ase Systems, 7 th Edition, Addison-Wesley, | | |
| | 2016 | | | | | |
| Ref | ference Books | | | | | |
| 1 | Fawcett, Joe, Danny Ayers, | and Liam RE | Quin. "Bo | eginning XML", Wiley India Private Ltd., 5 th | | |
| | Edition, 2012 | | | | | |
| 2 | Rigaux, Ph, Michel Scholl, | and Agnes V | oisard." | Spatial databases: with application to GIS". | | |
| | Morgan Kaufmann, 2002. | | | | | |
| 3 | Dunckley L. Multimedia da | tabases: An o | bject rela | ational approach. Addison-Wesley Longman | | |
| | Publishing Co., Inc.; 2003 Jan | n 1. | | | | |
| Mo | ode of Evaluation: CAT / Writte | en Assignment | t / Quiz /] | FAT | | |
| Rec | commended by Board of | 26-07-2022 | | | | |
| Stu | idies | | | | | |
| Approved by Academic | | No. 67 | Date | 08-08-2022 | | |
| Cou | uncil | | | | | |

| Course code | | Course title | L | Т | Р | С |
|-------------|------------------|--|---------|-------|--------|------|
| MCS | SE506P | DATABASE SYSTEMS LAB | 0 | 0 | 2 | 1 |
| Pre- | requisite | NIL | Sylla | bus | ver | sion |
| | | | | | v. | 1.0 |
| Cou | rse Objectives | | | | | |
| | 1. To under | stand the underlying principles of Relational Database Managem | ent Sy | vster | n. | |
| | 2. To focus | on the modeling and design of secure databases and usage of ad- | vancec | l dat | a | |
| | models. | | | | | |
| | 3. To imple | ment and maintain the structured, semi structured and unstructur | ed data | a. | | |
| Cou | rse Outcome | | | | | |
| After | completion of | this course, the student shall be able to: | | | | |
| | 1. Construc | t database queries using Structured Query Language (SQL) | | | | |
| | 2. Design a | nd implement applications that make use of distributed fault-tole | rant da | itaba | ases. | |
| | 3. Apply Sp | patial and Multimedia Database concepts to solve real-world prob | olems. | | | |
| | 4. Impleme | nt applications that work with structured, semi-structured, and ur | struct | ured | | |
| | databases | S | | | | |
| | 5. Create ap | oplications that use cloud storage technologies and relevant distri | buted | file | syste | ms |
| | | | | | | |
| Indic | cative Experim | ients | | | | |
| 1. | Study of Basic | c SQL Commands. | | | | |
| 2 | Model any giv | en scenario into ER/EER Model | • | 1 | 1 | |
| 2. | Table creation | with constraints, alter schema, insert values, aggregate functions | s, simp | ole a | nd | |
| 2 | complex quer | les with joins, views, Subqueries. | | | | |
| 3. | PL/SQL-Proce | edures, Cursors, Functions, Triggers | | 1 | 6.41 | |
| 4. | Partition a giv | en database based on the type of query and compares the executi | on spe | ed o | of the | ; |
| 5 | Query with/wi | thout parallelism. | datab | 000 | | |
| 5. | Ouery the dist | ributed database scenario, insert values, magnetit and replicate the | ualad | ase | | |
| 6 | Consider a sch | notice database | | | | |
| 0. | Consider a ser | tend that contains the following table with the key undermied. | | | | |
| | Employee (En | o, Ename, Desg, Dno). Assume that we horizontally fragment th | e table | as f | follo | ws: |
| | I - J (| | | | | |
| | Employee1(E | no; Ename; Desg; Dno), where 1<= Dno <=10 | | | | |
| | Employee2(E | no; Ename; Desg; Dno), where 11 <= Dno <=20 | | | | |
| | Employee3(E | no; Ename; Desg; Dno), where 21 <= Dno <=30 | | | | |
| | | | | | | |
| | In addition, as | sume we have 4 sites that contain the following fragments: | | | | |
| | • Site | e1 has Employee1 | | | | |
| | • Site | e2 has Employee2 | | | | |
| | • Site | e3 has Employee2 and Employee3 | | | | |
| | • Site | e4 has Employee1 | | | | |
| | Implement at | least 5 suitable queries on Employee fragments. Add relations to | the da | taba | se as | \$ |
| | per your requi | rements. | | | | |
| 7. | Plot points, lir | nes, and polygons using Spatial Databases such as Oracle Spatial | , Postg | reS | QL, | |
| | Microsoft SQ | L Server etc | | | | |
| 8. | • Use Sp | batial Databases to store data using Latitude and Longitude, find | the dis | tanc | e | |
| | betwee | en two spatial objects, find the area of a polygon | | | | |
| | • Store a | and retrieve images from a multimedia database | | | | |
| 9. | Create an XM | L document and validate it against an XML Schema/DTD. | | | | |
| | Use XQuery t | o query and view the contents of the database | | | | |
| 10. | Execute XPA | TH expressions on a database. | | | | |

| 11. | . Perform the following using a MongoDB Database | | | | | |
|-----|---|--|--|--|--|--|
| | • Create an Employee Collection and insert a few documents (sample document given below for reference) | | | | | |
| | { "name" : "Satish", "salary" : 30000, "address" : "Vellore", "school" : "SCOPE" } | | | | | |
| | Display all employees whose address is vellore and salary is greater than 30000 Undate the salary for an employee by name 'Pam' as 40000 | | | | | |
| | Opticate the satisfy for all employee by hame. Kall as 40000 Display only name and salary for all employees in the collection. | | | | | |
| | Display only name and safary for an employees in the conection Display all employees who are not from 'SCOPE' school | | | | | |
| | Display an employees who are not from Secore school Display only documents that contains the address property. | | | | | |
| 12 | Create an application that interacts with a cloud database | | | | | |
| 12. | Total Laboratory Hours 30 hours | | | | | |
| Tex | t Book(s) | | | | | |
| 1. | D Abraham Silberschatz, Henry F. Korth, S. Sudarshan "Database System Concepts" 7th Edition | | | | | |
| | McGraw Hill, 2021 | | | | | |
| Ref | erence Books | | | | | |
| 1. | Elmasri and Navathe "Fundamentals of Database Systems", 7th Edition Addison Wesley, 2014 | | | | | |
| 2. | Thomas Connolly, Carolyn Begg "Database Systems: A Practical Approach to Design, | | | | | |
| | Implementation and Management" 6 th Edition, Pearson India, 2015 | | | | | |
| | | | | | | |
| 3. | Mishra, Sanjay, and Alan Beaulieu. Mastering Oracle SQL: Putting Oracle SQL to Work. O'Reilly | | | | | |
| N/ | Media, Inc., 2004. | | | | | |
| NIO | le of Evaluation: CA1 / Mid-Term Lab/ FAT | | | | | |
| Ann | reved by Academic Council No. 67 Data 08.08.2022 | | | | | |
| Арр | Toved by Academic Council No. 07 Date 08-08-2022 | | | | | |

Discipline Elective

| MANAGEMENT 3 0 0 3 Pre-requisite Nil Syllabus version v.1.0 Course Objectives v.1.0 Syllabus version v.1.0 Course Objectives 1. To learn about security policies and their impacts. | Course code | | INFORMATION SECURITY AN | ND RISK | | L | Т | P | C |
|--|---|---|--|------------------|---------|-----------|-------|--------------|--------------|
| MCSUGOL Syllabus version Pre-requisite Nil Syllabus version Course Objectives v.1.0 Course Objectives v.1.0 Course Outcome v.1.0 Upon completion of this course, the student will be able to: v.1.0 I. To larn about security risk calculations and mitigating them by using various policies. v.1.0 Course Outcome Upon completion of this course, the student will be able to: v.1.0 I. Understand the principles and policies of information security. A nalyze and explore the information security controls. A nalyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security Framework 7 hours 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Rescurity Standards and Procedures. Module:3 Security Life Cycle and Controls Module:3 Security Management Models and Performance 8 hours Information Security Life Cycle and Controls Systems Development and Support - General Controls - People Security - User Access Controls. 8 hou | MCSECOOL | | MANAGEMENT | | | 2 | 0 | 0 | 2 |
| Interception Synabols velocities 0. Course Objectives v.1.0 1. To learn about security policies and their impacts. v.1.0 2. To assess the framework, lifecycle and controls of security under a variety of scenarios. 3. To analyze the security risk calculations and mitigating them by using various policies. Course Outcome Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Information Security Principles 6 hours Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Incident Management - Legal Framework: Security Standards and Procedures. Nodule:3 Module:3 Security Life Cycle and Controls 8 hours Information Security Uffe Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - Virferent Uses of Controls. Module:3 Module:4 Security Managemen | MCSE008L | | Nii | | Sylle | 3 shua | U | U | 3 |
| Course Objectives 9,110 1. To learn about security policies and their impacts. 2. To assess the framework, lifecycle and controls of security under a variety of scenarios. 3. To analyze the security risk calculations and mitigating them by using various policies. Course Outcome Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security Pramework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Uncident Management - Legal Framework is Cortrols - Systems Development and Support - General Controls - Poople Security Use of Controls - Systems Development and Support - General Controls - Poople Security - Standards and Performance 6 hours Module:3 Security Management Models and Performance 6 hours Medule:4 Security Management Models and Performance 6 hours Module:5 Risk Assessment 6 hours Module:6 Risk Analysis - Risk Evaluation - Risk Control - Risk - Calculation of Overa | Pre-requisite | • | | | Sylla | abus | ver | <u>sion</u> | 1.0 |
| 1. To learn about security policies and their impacts. 2. To assess the framework, lifecycle and controls of security under a variety of scenarios. 3. To analyze the security risk calculations and mitigating them by using various policies. Course Outcome Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security Pranework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Information Assurance Programme Implementation - Security Information Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls 8 hours 8 hours Information Security Management Models and Performance 6 hours 8 hours Information Security Management Models and Performance 6 hours Measurement Module:3 Security Management Models and Performance 6 hours Module:4 Security Management Models and Performance 6 hours< | Course Obie | ctives | | | | | | v | .1.0 |
| 2. To assess the framework, lifecycle and controls of security under a variety of scenarios. 3. To analyze the security risk calculations and mitigating them by using various policies. Course Outcome Upon completion of this course, the student will be able to: Understand the principles and policies of information security. Analyze and explore the information security controls. Assess and evaluate the risk management practices of information security. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security Pramework Thours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Assurance Programme Implementation - Security Incident Module:3 Security Life Cycle and Controls Shours Information Assurance Programme Implementation - Security - Protection fromation Security Life Cycle and Controls - Systems Development and Support - General Controls - People Security - Different Uses of Controls. Module:4 Security Management Models and Performance | 1. To lea | rn abou | t security policies and their impacts. | | | | | | |
| 3. To analyze the security risk calculations and mitigating them by using various policies. Course Outcome Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles formation Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Module:3 Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls. 8 hours Information Security Models and Performance 6 hours Module:4 Security Management Models and Performance 6 hours Measurement Information - Risk Analysis - Risk Evaluation - Risk Control - Risk Treatmetio - Risk Reduction - Risk Analysis - Risk Evaluation - Ri | 2. To ass | sess the | framework, lifecycle and controls of security | under a variety | v of sc | cena | rios. | | |
| Course Outcome Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles Information Security Principles 6 hours Information Security Principles 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Covernance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Information Security Life Cycle and Controls 8 hours Information Security Policy Concels - Systems Development and Support - General Controls - People Security - User Access Controls - Systems Development and Support - General Controls - People Security - Different Uses of Controls. Module:3 Security Management Models and Performance 6 hours Measurement Informatio | 3. To ana | alyze th | e security risk calculations and mitigating the | n by using var | ious r | oolic | ies. | | |
| Course Outcome Upon completion of this course, the student will be able to: Understand the principles and policies of information security. Analyze and explore the information security controls. Assess and evaluate the risk management practices of information security. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Incident Management - Legal Framework: Security Standards and Procedures. Module:3 Security Life Cycle and Controls Network and Procedures. Module:3 Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Systems Development and Support - General Controls - People Security - Different Uses of Controls. Module:4 Security Management Models and Performance 6 hours Measurement. Module:5 Risk Assessment 6 hours Measurement. Module:5 Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - R | | | | , , | | | | | |
| Upon completion of this course, the student will be able to: 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. 7 hours Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Standards and Procedures. 8 hours Information Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls 8 hours Information Security Life Cycle and Security - Different Uses of Controls - Systems Development and Support - General Controls - People Security - Different Uses of Controls. Module:4 Security Management Models and Performance 6 hours Measurement Measurement. 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Vario | Course Outc | ome | | | | | | | |
| 1. Understand the principles and policies of information security. 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security- Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. 7 hours Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle - Resting, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Meanus Measurement 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Module:6 Risk Management 4 hours Risk Management Methoologies. Management | Upon comple | tion of | this course, the student will be able to: | | | | | | |
| 2. Analyze and explore the information security controls. 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. 6 hours Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls. 8 hours Module:4 Security Management Models and Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Module:5 Risk Assessment 6 hours Threats and its Categories - Vulnerabilities and its Categories - Risk Teratination - Risk Reduction - Risk Tansfer - Risk Tolerance - Overall Risk Assessment. 6 hours Module:5 Risk Management 4 hours Risk Management Framework and Process - Manag | 1. Under | stand th | e principles and policies of information secur | rity. | | | | | |
| 3. Assess and evaluate the risk management practices of information security. 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. 6 hours Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls 8 hours 8 hours Information Security Life Cycle and Security - User Access Controls - Systems Development and Support - General Controls - People Security - User Access Controls. 8 hours Module:4 Security Management Models and Performance Measurement 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Information - Risk Analysis - Risk Evaluation - Risk Control - Risk Treatment- Alternative Risk Management - Risk Tolerance - Overall Risk Asse | 2. Analy | 2. Analyze and explore the information security controls. | | | | | | | |
| 4. Identify the disasters and recovering from them with appropriate decisions. Module:1 Information Security Principles 6 hours Information Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. 7 hours Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls 8 hours Information Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls. 6 hours Module:4 Security Management Models and Performance Measurement 6 hours Blueprints - Frameworks and Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Threats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Management 6 hours Module:6 Risk Management General Methoologies. 6 hours Module:6 Risk Management | 3. Assess | s and ev | valuate the risk management practices of infor | mation security | y. | | | | |
| Module:1Information Security Principles6 hoursInformation Security- Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security.Module:2Information Security Framework7 hoursModule:2Information Security Framework7 hoursOrganization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures.8 hoursModule:3Security Life Cycle and Controls8 hoursInformation Security Life Cycle and ControlsSystems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls.6 hoursModule:4Security Management Models and Performance Maagement6 hoursModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursModule:5Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.6 hoursModule:6Risk Management4 hoursRisk Management Hethodologies.Module:7Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Risklience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hours <td>4. Identit</td> <td>fy the d</td> <td>isasters and recovering from them with appro</td> <td>priate decision</td> <td>s.</td> <td></td> <td></td> <td></td> <td></td> | 4. Identit | fy the d | isasters and recovering from them with appro | priate decision | s. | | | | |
| Module:1Information Security Principles6 hoursInformation Security - Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security.Security Risk and Impact - Information SecurityModule:2Information Security Framework7 hoursOrganization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures.Nodule:3Module:3Security Life Cycle and Controls8 hoursInformation Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from MaliciousSoftware - Physical Security - Different Uses of Controls.Module:4Security Management Models and Performance MeasurementG hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.G hoursModule:5Risk AssessmentG hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Ralysis - Risk Evaluation - Risk Control - Risk Tremination - Risk Reduction - Risk Management Framework and Process - Managing Risk - Risk Treatment - Alternative Risk ManagementModule:6Risk Management Approaches Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for | | | | | | | | | |
| Information Security- Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. Module:2 Information Security Framework 7 hours Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. 8 hours Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Security - Protection from Malicioux Software - Physical Security - Different Uses of Controls. Module:4 Security Management Models and Performance Measurement 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Threats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Management 4 hours Risk Management Models e Security and Business Continuity Management Hethodologies. 6 hours Module:6 Risk Management Alternative Risk Module:7 Di | Module:1 | Inform | nation Security Principles | | | | | 6 ha | urs |
| Policy Concepts - Need for Information Security.7 hoursModule:2Information Security Framework7 hoursOrganization and Responsibilities: Organizational Policy, Standards and Procedures - Information Assurance Programme Implementation - Security IncidentManagement - Legal Framework: Security Standards and Procedures.8 hoursModule:3Security Life Cycle and Controls8 hoursInformation Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls.Module:4Security Management Models and Performance MeasurementBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.Module:5Risk AssessmentModule:6Risk Analysis - Risk Evaluation - Risk Control - Risk Control - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.Module:7Disaster Recovery and Business Continuity Management Methodologies.Module:8Issater Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentatior - Maintenance and Testing.Module:8Contemporary Issues2 hours | Information S | Security | - Assets and Types - Threat, Vulnerability, Ri | isk and Impact | - Info | rma | tion | Secu | rity |
| Module:2Information Security Framework7 hoursOrganizationand Responsibilities: Organizational Policy, Standards and Procedures - InformationSecurity Governance - Information Assurance Programme Implementation - Security IncidentManagement - Legal Framework: Security Standards and Procedures.Module:3Security Life Cycle and ControlsShoursInformationSecurity Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - Gerral Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of ControlsSecurity Management Models and Performance MeasurementModule:4Security Management Models and Performance | Policy Conce | pts - Ne | ed for Information Security. | 1 | | | | | |
| Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. Module:3 Security Life Cycle and Controls Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls. Module:4 Security Management Models and Performance Measurement Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. Module:5 Risk Assessment 6 hours Module:6 Risk Management Assessment. 6 hours Module:6 Risk Management 4 hours Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 2 hours Module:8 Contemporary Issues 2 hours< | Module:2 | Inform | nation Security Framework | | | | | 7 ho | urs |
| Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures. Module:3 Security Life Cycle and Controls 8 hours Information Security Life Cycle and Controls - People Security - User Access Controls - Systems Development and Support - General Controls - People Security - Different Uses of Controls. Review and Controls. Module:4 Security Management Models and Performance Measurement 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Threats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Kolerance - Overall Risk Assessment. 6 hours Module:6 Risk Management 4 hours Risk Management Methodologies. 0 6 hours Module:6 Risk Management 6 hours Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentatior - Maintenance and Testing. 0 Module:8 Contemporary Issues 2 hours | Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information | | | | | | | | |
| Management - Legal Framework: Security Standards and Procedures.Module:3Security Life Cycle and Controls8 hoursInformation Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls.Module:4Security Management Models and Performance Measurement6 hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.6 hoursModule:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Tremination - Risk Reduction - Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Modologies.4 hoursModule:6Risk Management4 hoursDisaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.6 hoursModule:8Contemporary Issues2 hours | Security Gov | vernanc | e - Information Assurance Programme I | mplementation | - S | ecur | ity | Incie | lent |
| Module:3Security Life Cycle and Controls8 hoursInformation Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious- Technical Security - ProtectionModule:4Security Management Models and Performance Measurement6 hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Module:56 hoursModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Transfer4 hoursRisk Management-4 hoursRisk Management-6 hoursModule:6Risk Management-Module:7Disaster Recovery and Business Continuity Management-Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity | Management | - Legal | Framework: Security Standards and Procedure | res. | | | | | |
| Information Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls.Module:4Security Management Models and Performance Measurement6 hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Module:56 hoursModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.4 hoursModule:6Risk Management4 hoursRisk Management Methodologies.6 hoursModule:7Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hoursModule:8Contemporary Issues2 hours | Module:3 Security Life Cycle and Controls | | | | | | | 8 ho | urs |
| Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls. Module:4 Security Management Models and Performance Measurement 6 hours Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement. 6 hours Module:5 Risk Assessment 6 hours Module:6 Risk Assessment 6 hours Threats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Transfer - Risk Tolerance - Overall Risk Assessment. 4 hours Module:6 Risk Management 4 hours Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies. 6 hours Module:7 Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 2 hours Module:8 Contemporary Issues 2 hours | Information S | Security | Life Cycle - Testing, Audit, Review and C | Controls - Syste | ems D | Deve | lopn | nent | and |
| from Malicious Software - Physical Security - Different Uses of Controls.Module:4Security Management Models and Performance Measurement6 hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.6 hoursModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.4 hoursModule:6Risk Management4 hoursRisk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies.6 hoursModule:7Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hoursModule:8Contemporary Issues2 hours | Support - Gei | neral Co | ontrols - People Security - User Access Control | rols - Technica | l Secu | urity | - Pr | otec | tion |
| Module:4Security Management Models and Performance Measurement6 hoursBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.Models - Various Access ControlModule:5Risk Assessment6 hoursModule:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Tolerance - Overall Risk Assessment.4 hoursModule:6Risk Management4 hoursRisk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Wethodologies.6 hoursModule:7Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hoursModule:8Contemporary Issues2 hours | from Maliciou | us Softv | vare - Physical Security - Different Uses of C | ontrols. | | | | | |
| MeasurementMeasurementBlueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.Module:5Risk AssessmentModule:5Risk AssessmentModule:5Risk AssessmentThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.Module:6Risk ManagementModule:7Risk ManagementModule:7Disaster Recovery and Business Continuity ManagementDisaster Recovery and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.Module:8Contemporary Issues2 hoursModule:8Contemporary Issues45 hours | Module:4 | Secur | ity Management Models and Performance | | | | | 6 ho | urs |
| Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access ControlModels - Information Security Performance Measurement.Models - Information Security Performance Measurement.Module:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - RiskIdentification of Overall Risk - Risk Reduction -Threats and its Categories - Nulnerabilities and its Categories - Risk Control - Risk Termination - Risk Reduction -Risk Termination - Risk Reduction -Risk Transfer - Risk Tolerance - Overall Risk Assessment.Module:6Risk Management - Overall Risk Assessment.Module:6Risk ManagementFramework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies.Ontinuity ManagementDisaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.Ontenance and Testing.Module:8Contemporary Issues2 hoursModule:8Contemporary Issues2 hours | | Measu | irement | | | | | 9 | |
| Models - Information Security Performance Measurement.Module:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.6 hoursModule:6Risk Management4 hoursRisk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies.6 hoursModule:7Disaster Recovery and Business Continuity Management6 hoursDisaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hoursModule:8Contemporary Issues2 hours | Blueprints - F | ramew | orks and Security Models - Security Architect | ure Models - V | ariou | s Ac | cess | Con | trol |
| Module:5Risk Assessment6 hoursThreats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk - Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment.Risk Termination - Risk Reduction - Risk Termination - Risk Reduction - Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies.4 hoursModule:7Disaster Recovery and Business Continuity Management6 hoursDisaster Recovery and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.2 hoursModule:8Contemporary Issues2 hours | Models - Info | rmation | Security Performance Measurement. | Γ | | | | <u> </u> | |
| Module:6 Risk Management 4 hours Module:6 Risk Management 4 hours Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk 4 hours Module:7 Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 6 hours Module:8 Contemporary Issues 2 hours Module:8 Contemporary Issues 2 hours | Module:5 | Risk A | Assessment | | 6.0 | - | 1.D. | <u>6 ho</u> | urs |
| Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction - Risk Reduction - Risk Transfer - Risk Tolerance - Overall Risk Assessment. Module:6 Risk Management 4 hours Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies. 4 hours Module:7 Disaster Recovery and Business Continuity Management 6 hours Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 2 hours Module:8 Contemporary Issues 4 hours | Threats and it | ts Categ | ories - Vulnerabilities and its Categories - Ris | k - Calculation | of Ov | veral | I R18 | 3K - F | X 1SK |
| Misk Transfer - Risk Tolerance - Overall Risk Assessment. Module:6 Risk Management 4 hours Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management- Alternative Risk Management Methodologies. Disaster Recovery and Business Continuity Management 6 hours Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 2 hours Module:8 Contemporary Issues 2 hours | Identification | - K1SK | Analysis - Risk Evaluation - Risk Control - | Risk Terminati | ion - I | K1SK | Red | luction | on - |
| Module:6Kisk Management4 noursRisk ManagementFramework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies.Alternative RiskModule:7Disaster Recovery and Business Continuity Management6 hoursDisaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for | Risk Transfer | - K1SK | Tolerance - Overall Risk Assessment. | | | | | 41 | · · · · · |
| Risk Management Framework and Process - Managing Risk - Risk Treatment- Alternative Risk Management Methodologies. Disaster Recovery and Business Continuity 6 hours Management Disaster Recovery and policy - Relationship between Disaster Recovery and Business Continuity 6 hours Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. Contemporary Issues 2 hours Module:8 Contemporary Issues 45 hours | Module:6 | | Vlanagement | | | A 1/ | | 4 ho | urs |
| Management Methodologies. Module:7 Disaster Recovery and Business Continuity Management 6 hours Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. Module:8 Contemporary Issues 2 hours Module:8 Total Lecture hours: 45 hours | Risk Manage | ement I | ramework and Process - Managing Risk | - Risk Treatm | ent- | Alte | rnati | ve I | X 1SK |
| Module:7 Disaster Recovery and Business Continuity Management 6 hours Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. 6 hours Module:8 Contemporary Issues 2 hours Total Lecture hours: | Management | Niethoc | | | | | | | |
| Management Management Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. Module:8 Contemporary Issues 2 hours Total Lecture hours: | Module:7 | Disast | er Recovery and Business Continuity | | | | | 6 no | urs |
| Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity Management - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing. Module:8 Contemporary Issues 2 hours Total Lecture hours: | Disector | Mana | gement | | - 1 D | | C | | |
| Management - Resinence and Redundancy - Approaches to writing and implementing Plans - Need for Documentation - Maintenance and Testing. Module:8 Contemporary Issues 2 hours Total Lecture hours: 45 hours | Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business Continuity | | | | | | | | |
| Module:8 Contemporary Issues 2 hours Total Lecture hours: 45 hours | Management - Residence and Redundancy - Approaches to writing and implementing Plans - Need for | | | | | | | | |
| Module:s Contemporary issues 2 hours Total Lecture hours: 45 hours | Modulo:8 | Conte | morary Issues | | | | | 2 ho | |
| Total Lecture hours: 45 hours | | Conte | | | | | | <i>4</i> II0 | u1 S |
| 1 Utal Lecture nours, 45 nours | | | Tatal Laatura haura | | | | / | 5 ho | lira |
| | | | Total Lecture nours. | | | | - | 5 110 | ui 3 |

| Text Book(s) | | | | | | | |
|-----------------|---|--|--|--|--|--|--|
| 1. | Andy Taylor, David Alexander, Amanda Finch and David Sutton, "Information Security | | | | | | |
| | Principles",2020, Third Edition, BCS, United Kingdom. | | | | | | |
| 2. | Michael E. Whitman and Herbert J. Mattord, "Management of Information Security", 2018, | | | | | | |
| | Sixth Edition, Cengage Learning, United States of America. | | | | | | |
| Reference Books | | | | | | | |
| 1. | Calder, A., and Watkins, S. G., "Information security risk management for | | | | | | |
| | ISO27001/ISO27002", 2018, Third Edition, IT Governance Ltd, United States of America. | | | | | | |
| 2. | Susanto, H., and Almunawar, M. N, "Information security management systems: A novel | | | | | | |
| | framework and software as a tool for compliance with information security standards", 2018, First | | | | | | |
| | Edition, Apple Academic Press, New York. | | | | | | |
| Mod | le of Evaluation: CAT / Assignment / Quiz / FAT | | | | | | |
| Reco | ommended by Board of Studies 26-07-2022 | | | | | | |
| App | roved by Academic Council No.67 Date 08-08-2022 | | | | | | |

| Course cod | e | CRYPTOSYSTEMS | | | L | Т | P | С | | |
|---|--------------------------------------|--|-------------------|------------|------|--------|-------------|-------------|--|--|
| MCSE609I | | | | | 2 | 0 | 0 | 2 | | |
| Pre-requisi | te | NIL | | S | ylla | bus ' | vers | sion | | |
| | | | | | | | v | .1.0 | | |
| Course Ob | jectives | 5 | | | | | | | | |
| 1. To l | earn the | e concept of Cryptosystems. | | | | | | | | |
| 2. To u | Indersta | nd the design of cryptanalytics and security a | algorithms. | | | | | | | |
| 3. To e | xplore | various authentication and hashing algorithm | 18. | | | | | | | |
| | | | | | | | | | | |
| Course Ou | tcome | | | | | | | | | |
| Upon comp | letion o | f this course, the student will be able to: | | | | | | | | |
| 1. Understand the fundamental of Cryptosystems requirements. | | | | | | | | | | |
| 2. Identify and apply the concept of Cryptographic algorithms. | | | | | | | | | | |
| 3. Analy | ze and | explore the use of authentication and hashing | g. | | | | | | | |
| 4. Gain a | a deep i | nsight into attacks and emerging security alg | orithms. | | | | | | | |
| 5. Explo | re and a | analyze of signature and key exchange algori | thms. | | | | | | | |
| | | | | | | | 4 1 | | | |
| Module:1 | Math | ematical Foundations of Cryptosystems | F1 1 7 | T 1 | | | <u>i ho</u> | | | |
| Cryptographic attacks – Modular arithmetic – Fermat's Theorem, Euler's Theorem, Extended | | | | | | | | | | |
| Euclidean A | Algorith An Matl | m, Chinese Remainder Theorem - Solovay S | Straseen Test - T | ne Ja | acoi | 51 S y | mo | 01 – 10 | | |
| Pollard's Rho Method, Pollard's p-1 Method, Pollard's Kangaroo Algorithm. | | | | | | | | | | |
| Cryptosystems: Affine Cipher Vigenere Cipher Hill Cipher Linear Feedback Shift Register (LESR) | | | | | | | | | | |
| Cryptosystems: Affine Cipher, Vigenere Cipher, Hill Cipher and J ESP | | | | | | | | | | |
| - Cryptanarysis on Annie Cipher, vigenere Cipher, fill Cipher and LFSK. | | | | | | | | | | |
| WIOUULE:5 DIOCK CIPITERS and Stream Cipiters 4 nours Shonnon's Theory Linear Cruptonalusis Differential Cruptonalusis Description | | | | | | | | | | |
| of DES Description and Analysis of AES Modes of Operation | | | | | | | | | | |
| Module:4 | Hash | Functions and Message Authentication | | | | 4 | 1 ho | urs | | |
| Hash Functi | ions and | 1 Data Integrity – Security of Hash Function | s - MD5 - SHA | 512 | – N | leste | d M | AC | | |
| and HMAC | – CBC | MAC. | 5 1120 5111 | | - | | | | | |
| Module:5 | Publi | c Key Cryptography and Discrete | | | | 4 | 1 ho | urs | | |
| | Loga | rithms | | | | | | | | |
| RSA Crypto | osystem | - Shanks' Algorithm - Elliptic Curves Over | the Reals – Elli | ptic | Cur | ves] | Mod | lulo | | |
| a Prime – E | lliptic (| Curves Over Finite Fields – ElGamal Crypto | systems on Ellip | otic C | Curv | 'es - | Elli | ptic | | |
| Curve Diffi | e – Hell | man. | | | | | | | | |
| Module:6 | Signa | ture Schemes and Post-Quantum | | | | 5 | 5 ho | urs | | |
| | Cryp | tography | | | | | | | | |
| Number Th | eory R | esearch Unit (NTRU): Basics, Lattices and | Security of N | ΓRU | - (| Code | e Ba | ised | | |
| Cryptograp | ny – N | IcEliece Cryptography – Lamport Signatu | re Scheme – W | Vinte | rnit | z Si | gna | ture | | |
| Scheme – M | Ierkle S | signature Scheme. | | | | | | | | |
| Module:7 | Key | Distribution and Key Agreement | | | | 2 | 1 ho | urs | | |
| | Schei | nes | 11 0 1 1 | 0.1 | | 17 | 1 | | | |
| Key Predist | r1but101 | 1 - Session Key Distribution Schemes: Need | anam Schroeder | Sch | eme | э, Ке | | ros, | | |
| Cruntoquate | gaway | scheme – Dime-Heilman Key Agreement | - MII Key A | gree | mei | 1l - | Pail | mer | | |
| Cryptosystem – Argeoraic Suucinies – Group and King. | | | | | | | | | | |
| Modulare | Modulo:8 Contemporary Issues 1 hours | | | | | | | | | |
| moune:0 | Cont | any or at y abbach | | | | | 110 | ul S | | |
| | | | | | | | | | | |
| | | Total Lecture hours | | | | 3(|) ho | lire | | |
| | | i otar Decture nours. | | | | 50 | , 110 | u 13 | | |
| | l | | | | | | | | | |

| Text | Text Book(s) | | | | | | | | |
|-----------------|---|---------------------|------------|--------------------------------|--|--|--|--|--|
| 1. | Douglas R. Stinson, "Cryptogr | aphy: Theory and | Practice", | 2018, 4th Edition, CRC Press, | | | | | |
| | United states. | | | | | | | | |
| Reference Books | | | | | | | | | |
| 1. | Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source code in C", 2017, | | | | | | | | |
| | 20 th edition, John Wiley & Sons, New York. | | | | | | | | |
| 2. | Behrouz A Forouzan, Debdeep | Mukhopadhyay, "Ci | ryptograph | y and Network Security", 2011, | | | | | |
| | Tata Mcgraw Hill education priv | vate limited, India | | | | | | | |
| Mod | e of Evaluation: CAT / Assignme | ent / Quiz / FAT | | | | | | | |
| Reco | ommended by Board of Studies | 26-07-2022 | | | | | | | |
| Appi | roved by Academic Council | No.67 | Date | 08-08-2022 | | | | | |
| | | | | | | | | | |

| Cou | rse code | | CRYPTOSYSTE | MS LAI | 3 | L | Τ | P | С | |
|---|--|-----------------------------|----------------------|------------|-----------------|----------|-------|-----------------|------|--|
| MCS | SE609P | | | | | 0 | 0 | 2 | 1 | |
| Pre- | requisite | NIL | | | | Sylla | bus v | vers | ion | |
| | | | | | | | | v. | 1.0 | |
| Cou | rse Objective | S | | | | | | | | |
| 1. | To learn the | e concept of Crypto | osystems. | | | | | | | |
| 2. | To understa | and the design of cr | yptanalytics and se | ecurity al | gorithms. | | | | | |
| 3. | To explore | various authenticat | tion and hashing al | gorithms. | | | | | | |
| | | | | | | | | | | |
| Course Outcome | | | | | | | | | | |
| Upor | n completion | of this course, the s | student will be able | to: | • • | | | | | |
| | Gain a deep | insight into attacks | and emerging sec | urity algo | prithms. | | | | | |
| 2. | Explore and | analyze of signatu | re and key exchang | ge algorit | nms. | | | | | |
| Indi | cative Experi | iments | 1:56 | | | | | | | |
| 1. | Implement a | client and a server | r on different comp | outers. Pe | rform the com | municati | lon | | | |
| 2 | between these two entities by using KSA cryptosystem. | | | | | | | | | |
| Ζ. | hat has a two antities by using digital signature counters. Perform the authentication of sender | | | | | | | | | |
| 3 | between these two entities by using digital signature cryptosystem | | | | | | | | | |
| <u>э.</u> Л | Implementi | $1 a H \Delta_{-512}$ messa | ge digest algorithm | | y exchange arg | omunn | | | | |
| - 1 . 5 | Demonstrate | the classical crypt | tography algorithm | S | | | | | | |
| 6. | Implement I | Data Encryption Sta | andard algorithm. | .0 | | | | | | |
| 7. | Implement a | session key agree | ment algorithm. | | | | | | | |
| 8. | Demonstrate | e the hash-based m | essage authenticati | on code (| HMAC) algori | ithm. | | | | |
| 9. | Implement I | ElGamal cryptosyst | tems on elliptic cur | ves | | | | | | |
| 10. | Implement A | Advanced Encrypti | on Standard algorit | thm | | | | | | |
| | ↓ | | | | | | | | | |
| | | | Total Lecture | hours: | | | 30 |) ho | urs | |
| | | | | | | | | | | |
| Text | Book(s) | | | | | | | | | |
| 1. | Douglas R. | Stinson, "Cryptog | raphy: Theory and | Practice | ", 2018, 4th E | dition, | CRC | Pro | ess, | |
| | United states | 3. | | | | | | | | |
| Refe | rence Books | (s) | | | 1 10 | | | | 1.5 | |
| 1. | Bruce Schne | eier, "Applied Cryp | tography: Protocol | s, Algori | thms and Source | e code i | n C' | [,] 20 | 17, | |
| 2 | 20^{ch} edition, | John Wiley & Son | s, New York. | ٦ | | - 1- C | ····, | , 20 | 11 | |
| ۷. | Denrouz A F | v Hill education and | wuknopaanyay, " | ryptogra | ipny and Netwo | Jrk Secu | rity | , 20 | 11, | |
| Mode of Evaluation: Continuous Assessment / EAT | | | | | | | | | | |
| Recommended by Board of Studies 26.07.2022 | | | | | | | | | | |
| Ann | roved by Δcar | demic Council | No 67 | Date | 08-08-202 | 2 | | | | |
| Luhh | loved by Acal | | 110.07 | Date | 00-00-202 | 4 | | | | |

| Course cod | e | PENETRATION TESTING AND VULNERABILITY | L | Τ | P | С | | | | |
|---|---|---|--------|----------------|-------------------|---------|--|--|--|--|
| | | ASSESSMENT | | | | | | | | |
| MCSE610L | 4 | | 2 | 0 | 0 | 2 | | | | |
| Pre-requisi | te | NIL | S | <u>/llab</u> | us v | ersion | | | | |
| | | | | | | v.1.0 | | | | |
| Course Obj | jective | es | | | | | | | | |
| 1. To c | ompre | chend the security framework related occurrences and knowl | edge | on e | xpec | cted | | | | |
| protections, and countermeasures against normal vulnerabilities. | | | | | | | | | | |
| 2. To ic | dentify | y security weaknesses in a network, machine, and in software | e. | | | | | | | |
| 3. To make students familiarization with cyber kill-chains. | | | | | | | | | | |
| Course Ordennes | | | | | | | | | | |
| Upon compl | lotion | of this course, the student will be able to: | | | | | | | | |
| | | of this course, the student will be able to: | voto | man | roto | | | | | |
| 1. Iden | ury na | aws and vulnerabilities in applications, websites, networks, s | yste | ns, p | 1010 | cois, | | | | |
| 2 Depl | ov an | d test exploits over targeting operating systems and services | | | | | | | | |
| 3 Rich | know | d test exploits over targeting operating systems and services dedge on legal and ethical issues related to vulnerability and | nen | etrati | on te | esting | | | | |
| 4 Abili | itv to | perform pentest on target and generate a report based on the | test : | and c | leter | mine | | | | |
| the s | ecurit | v threats and vulnerabilities in computer networks. | cest (| ina c | 101011 | lillile | | | | |
| 5. Usin | g the | acquired knowledge into practice for testing the vulnerabiliti | es ai | nd id | entif | ving | | | | |
| threa | its. | | | | | J8 | | | | |
| | | | | | | | | | | |
| Module:1 | Pent | esting and Information Security | | | 4 | hours | | | | |
| Pentester – Types of Hackers – Pentest Methodology – Pentest Types – Vulnerability Scanning – | | | | | | | | | | |
| Vulnerabilit | y Ass | essments – Pentest Target and Specializations - Asset Manag | geme | nt: C | T AI | Triad – | | | | |
| Security Co | ntrols | - Access Controls - Incident Responses - Malware - A | Adva | nced | Per | sistent | | | | |
| Threats – Cy | yber K | Kill Chain – Air-gapped Machines – Dark Web. | | | | | | | | |
| Module:2 | Reco | on and Hijacking | | | 4 | hours | | | | |
| Reconnaissa | nce – | External ¬- Dumpster Diving – Social Media – Social Eng | ineer | ing - | Inte | ernal – | | | | |
| Sniffing and | Scan | ning – De-Authentication of Attacks – Detection Mechanism | - Ses | sion | Hija | cking: | | | | |
| Blind and N | on-Bl | ind Spoofing - Detection and Prevention Mechanisms. | r | | | | | | | |
| Module:3 | Netv | vork and Wireless Mayhem | | | 4 | hours | | | | |
| WEP Theor | y – SS | SID - WPA – WPS - MAC Filtering – Port Security – IPsec | - Wa | r Div | ving: | Basic | | | | |
| Web Crack | ıng – | Detecting Wireless Attacks - Fake Authentication – H | ands | hake | The | eory - | | | | |
| Bypassing F | irewa | Ils – Evading Intruder Detection System - Securing Network | tror | n Att | tacks | | | | | |
| Module:4 | Web | Server Attacks | ļ | | 4 | hours | | | | |
| Understandi | ng W | eb Languages - Web Architecture - Webpage Spoofing – Inf | orm | ation | Gat | hering | | | | |
| From Target | web | sites – Finding Subdomains – Files Based Analysis - Cook | ies F | Iandi | ling | - web | | | | |
| Page Attack | $\frac{S - Al}{Injoe}$ | tion Vulnershility | IVIF | Code | <u>3 mje</u> 4 | bound | | | | |
| Databases | Tostir | uon Vuinerability Securing SOI Server Detecting | Dat | ahass | 4 > \ \ ff | nours | | | | |
| Protection Ac | result vainst l | Database Attacks - File Unload Vulnerability – Inclusion Vulnerab | ility. | abase . Cod | s Au e Exe | acks – | | | | |
| – Local File – | – Rem | ote File – Mitigation Strategies. | mey | Cou | C LA | Jourion | | | | |
| Module:6 | Gain | ing Access | | | 5 | hours | | | | |
| Introduction | to Gai | ning Access – Server Side – Client Side – Post – Exploitation S | Serve | r Sid | e Att | tacks – | | | | |
| Metasploit ar | nd MS | FS - Scripting Vulnerabilities - Automatic Vulnerability Compli | ance | s usir | ng O | WASP | | | | |
| ZAP. | | | | | - | | | | | |
| Module:7 | Escal | ation | | | 4 | hours | | | | |
| Trojan, Viru | ises an | d Backdoor Applications - Detection Mechanism - Unix Permissi | on ar | id Ro | ot A | ccess | | | | |
| - Butter ov | - Buffer overflow - Memory Architecture - Examples - Escalation - Linux - Window - Preventing | | | | | | | | | |
| Modulo 9 | -DD(| JS – Detection and Prevention – 100is. | | | 1 | hours | | | | |
| moune:0 | COII | comportary 155005 | | | 1 | nours | | | | |
| | | Tatal Lactura hourse | | | 30 | hours | | | | |
| | | Total Lecture nours: | | | 50 | 110013 | | | | |

| Text Book(s) | | | | | | | |
|-----------------|---|------------------------|---|-----------------------|--|--|--|
| 1. | Phillip L. Wylie, Kim Crawley, "The | e Pentester BluePrint | : Starting a Career as | s an Ethical Hacker", | | | |
| | 2020, Wiley, United States. | | | | | | |
| 2. | Sabih, Zaid, "Learn Ethical Hacking | from Scratch: Your s | from Scratch: Your stepping stone to penetration testing", 2018 | | | | |
| | Packt Publishing Ltd, United Kingdom. | | | | | | |
| Reference Books | | | | | | | |
| 1. | Diogenes, Yuri, and Erdal Ozkaya, "Cybersecurity??? Attack and Defense Strategies: Infrastructure | | | | | | |
| | security with Red Team and Blue Tea | am tactics", 2018, Pac | ckt Publishing Ltd, U | nited Kingdom. | | | |
| 2. | Andrew Whitaker, and Daniel P. New | man. "Penetration Te | esting and Network I | Defense", 2005, Cisco | | | |
| | Press, New Jersey. | | - | | | | |
| Mod | e of Evaluation: CAT / Assignment | / Quiz / FAT | | | | | |
| Reco | ommended by Board of Studies | 26-07-2022 | | | | | |
| Appi | roved by Academic Council | No.67 | Date | 08-08-2022 | | | |

| Соі | ırse code | PENETRATION TEST ASSESSMENT LAB | ING AND VULNERABI | LITY | L | ' | Г | P | С |
|------------|---|--|----------------------------|------------------------|----------|-----|-------------------|------|------|
| MCS | SE610P | | | | 0 | | 0 | 2 | 1 |
| Pre- | requisite | | | | Sylla | ab | us v | ers | ion |
| | | | | | | | | v. | 1.0 |
| Coi | ırse Objecti [,] | ves: | | | | | | | |
| 1. | To compre | hend the security framework | k related occurrences a | nd knowledge on e | xpecte | ed | | | |
| | protections | , and countermeasures again | nst normal vulnerabiliti | es. | | | | | |
| 2. | To identify | v security weaknesses in a ne | etwork, machine, and ir | n software. | | | | | |
| 3. | To make st | tudents familiarization with | cyber kill-chains. | | | | | | |
| Coi | arse Outcom | ie: | | | | | | | |
| Upoi | n completion | of this course, the student v | vill be able to: | | | | | | |
| 1. | Ability to p | perform pentest on target an | d generate a report base | ed on the test and d | eterm | in | e the | e | |
| | security the | reats and vulnerabilities in c | omputer networks. | | | | | | |
| 2. | Using the a | acquired knowledge into pra | ctice for testing the vul | nerabilities and ide | entifyi | ng | g thro | eat | s. |
| List | of Challeng | ing Experiments (Indicativ | /e) | | | | | | |
| 1. | Set up of Ka | li Linux in a Virtual machine a | and setup with DNS info a | and collection of | | | 3 | ho | urs |
| | local networ | ks | | | | | | | |
| 2. | Scan the net | work for Windows XP and Wi | ndows 7 Target machines | in local | | | 3 | ho | urs |
| | network and | virtual network | | | | | | | |
| 3. | Identify the | open ports and firewall rules se | etup | | | | 2 | ho | urs |
| 4. | Use passwor | d guessing tools to guess a pas | ssword. Use password str | engthening tools | | | 2 | ho | urs |
| | to strengther | the password. Try guessing th | e password and tabulate | the enhanced | | | | | |
| | difficulty du | difficulty due to length of password and addition of special characters. | | | | | | | |
| 5 | | | | | | | | ho | 1120 |
| 5. | Extract pass | word hashes from Windows X | P/NT machine. Use a pass | sword extraction | | | 2 | 110 | uis |
| | tool, using word list, single crack or external mode to recover the password. | | | | | | | | |
| | increase the | tomplexity of the password an | id determine the point at | which the | | | | | |
| 6 | Cracking Liu | nux passwords | | | | | 2 | ho | 1120 |
| 0. | Experiments | on SOL injections | | | | | $\frac{2}{2}$ | ho | urs |
| 7. | Analysis of | WEP flaws | | | | | $\frac{2}{2}$ | ho | urs |
| 0. | Experiments | on Wireless DDoS Attacks | | | | | $\frac{2}{2}$ | ho | urs |
| <i>9</i> . | Prevention a | gainst Cross Site Scripting Att | acks | | | | $\frac{2}{2}$ | ho | urs |
| 10. | Experiments | on Metasploit Framework | deks | | | | $\frac{2}{2}$ | ho | urs |
| 11. | Cross Site S | crinting | | | | | $\frac{2}{2}$ | ho | urs |
| 12. | Cross Site B | equest Forgery | | | | | $\frac{2}{2}$ | ho | urs |
| 13. 14 | File upload y | ulnerability on social engineer | inσ | | | | $\frac{2}{2}$ | ho | urs |
| Tot | al Laborato | ry Hours | | | | | 30 | hoi | irs |
| 100 | | iy iiou is | | | | | 501 | 100 | |
| Tex | t Book(s) | | | | | | | | |
| 1. | Phillip L. Wy | lie, Kim Crawley, "The Pentes | ster BluePrint: Starting a | Career as an Ethical | Hacke | r". | , 202 | 0, | |
| | Wiley, United | l States. | C C | | | | | | |
| 2. | Sabih, Zaid, " | Learn Ethical Hacking from S | cratch: Your stepping sto | ne to penetration test | ting", 1 | 20 | 18 P | ack | ct |
| | Publishing Lt | d, United Kingdom. | | | | | | | |
| Refe | rence Book(| s) | | | | | | | |
| 1. | Diogenes, Yu | ri, and Erdal Ozkaya, "Cybers | ecurity??? Attack and De | efense Strategies: Inf | rastruc | ctu | re se | ecui | rity |
| | with Red Tea | m and Blue Team tactics", 201 | 8, Packt Publishing Ltd, | United Kingdom. | | | | | |
| 2. | Andrew Whit | aker, and Daniel P. Newman. | "Penetration Testing and | Network Defense", | 2005, | С | isco | Pre | ess, |
| | New Jersey. | | | | | | | | |
| Mo | de of Evaluat | tion: Continuous Assessmen | nt / FAT | | | | | | |
| Rec | ommended by | Board of Studies | 26-07-2022 | | | | | | |
| App | proved by Ac | ademic Council | No. 67 | Date | 08-0 | 8- | $20\overline{22}$ | 2 | |

| MCSE611L Malware Analysis 2 0 0 2 Pre-requisite NIL Syllabus version v.1.0 Course Objectives v.1.0 v.1.0 1. To introduce malware taxonomy and life cycle. v.1.0 v.1.0 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. v.1.0 Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. 4 hours Module:1 Introduction to Malware 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - Pi: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEi dand TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware delaburey. Module:3 | Course code | Course title | L T P C | | | | | | | |
|--|---|---|----------|-------|--------|-------|--|--|--|--|
| Pre-requisite NIL Syllabus version Course Objectives v.1.0 1. To introduce malware taxonomy and life cycle. 2. 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. 3. 3. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: 1. 1. Apply the static and dynamic malware analysis on emerging samples. 2. 2. Analyze the executable file and malware classification. 3. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. 4. Explore the anti-malware analysis techniques. 5. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse 4 hours Infroduction to Malware Mack Life Cycle - The Combat Teams - Anti-malware low of the using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Atalysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module: | MCSE611L | Malware Analysis | 2 | 0 | 0 | 2 | | | | |
| Course Objectives v.1.0 1. To introduce malware taxonomy and life cycle. v.1.0 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 4 hours Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Module:4 Prepare for Reverse Engineering as process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:5 Build and Debug the Malware - Assembly of data - Encrypted data ident | Pre-requisite | NIL | Syll | abus | s vers | sion | | | | |
| Course Objectives 1. To introduce malware taxonomy and life cycle. 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. 3. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: . 1. Apply the static and dynamic malware analysis on emerging samples. . 2. Analyze the executable file and malware classification. . 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. . 4. Explore the anti-malware analysis techniques. . 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. . Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:3 Dynamic Malware Analysis 4 hours Module:4 Prepare for Reverse Enginecring as a process - Binary analysis tools, | | | | | v | 1.0 | | | | |
| 1. To introduce malware taxonomy and life cycle. 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. 3. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis Module:3 Dynamic Malware Analysis Module:4 Prepare for Reverse Engineering 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. | Course Objectives | | | | | | | | | |
| 2. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques. 3. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Samboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engincering as a process - B | 1. To introduce | malware taxonomy and life cycle. | | | | | | | | |
| 3. To detect and analyze obfuscation and anti-malware techniques. Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Molue:2 Static Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Istic Malware Analysis 4 hours Fingerprinting the Malware analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:5 Build and Debug the Malware 5 hours File Obfuscation Techniques - Dechiques - Assembly of data - Encrypted data identification - De | 2. To analyze m | alware samples using static, dynamic analysis, and reverse engined | ering te | chni | ques | • | | | | |
| Course Outcomes After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis Ingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis Module:4 Prepare for Reverse Engineering 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:6 Obfuscation Techniques A hours Low-Level Language: Registers, Memor | 3. To detect and | l analyze obfuscation and anti-malware techniques. | | | | | | | | |
| After completion of this course, the student shall be able to: 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Antack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis Fingerprinting the Malware Pice File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis Fingerprinting the Malware Pice File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis File Obtaing: Tools and Techniques - Virus Total. Module:4 Prepare for Reverse Engineering | Course Outcomes | | | | | | | | | |
| 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Module:2 Introduction to Malware and Obfuscation using emerging tools. Module:3 Introduction to Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware Analysis 4 hours Module:3 Dynamic Malware Analysis 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Module:5 Build and Debug the Malware 4 hours Module:6 Obfuscation Techniques Typical malware behavior - Malware delivery. Module:6 Obfuscation Techniques Assembly of data - Encrypted data identification - Decry | After completion of | this course, the student shall be able to: | | | | | | | | |
| 1. Apply the static and dynamic malware analysis on emerging samples. 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Malware Taxonomy - Malware Analysis 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. 4 hours Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. Module:7 <tr< td=""><td></td><td></td><td></td><td></td><td></td><td></td></tr<> | | | | | | | | | | |
| 2. Analyze the executable file and malware classification. 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Malware and Obfuscation using emerging tools. Module:2 Static Malware Antack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware Acception. Module:6 Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dsde - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis - Assembly of data - Encrypted data identification - Decrypting with x86dsde - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Contemporary Issues - DPD fil | 1. Apply the static and dynamic malware analysis on emerging samples. | | | | | | | | | |
| 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. 4. Explore the anti-malware analysis techniques. 5. Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 thours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. Module:6 Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis - PDF file analysis - SWFTools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Otheres - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Contemporary Issues 1 hours | 2. Analyze the e | executable file and malware classification. | | | | | | | | |
| Apply the reverse-engineering of malware and Obfuscation using emerging tools. Module:1 Introduction to Malware Malware and Obfuscation using emerging tools. Module:2 Static Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Samdboxing: Tools and Techniques - Virus Total. Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 and Encryption. Module:6 Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis - Asti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Contemporary Issues 1 Total Lecture hours: 30 hours | 3. Understand t | 3. Understand the disassemblers, debuggers, and decompilers in malware analysis. | | | | | | | | |
| Module:1 Introduction to Malware 4 hours Module:1 Introduction to Malware 4 hours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. Module:6 Module:7 Anti-Malware analysis - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours | 4. Explore the a | 4. Explore the anti-malware analysis techniques. | | | | | | | | |
| Module:1 Introduction to Malware 4 nours Malware Taxonomy - Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Reverse Engineering for Windows and Linux systems. 4 hours Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis Assembly of data - Encrypted data identi | J. Apply the rev | verse-engineering of marware and Objuscation using emerging tool | s. | | 1 h | | | | | |
| Matwate Factorionity - Matwate Attack Effe Cycle - The Combat Teams - Anti-Intatwate Froducts- Reverse Engineering for Windows and Linux systems. Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. 4 hours Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. Module:6 Obfuscation Techniques 5 hours File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis PDF file analysis - SWFTools - FLASM - Flare. Module:8 < | Moluora Tayonomy | Malwara Attack Life Cycle The Combet Teems Anti malwar | Drad | note | 4 nc | ora | | | | |
| Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware Analysis Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. 4 hours Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation Techniques Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis Assembly of gata - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis PDF file analysis - SWFTools - FLASM - Flare. | Engineering for Win | - Marware Attack Life Cycle - The Combat Teams - Anti-marwar | e Prou | ucts- | Rev | erse | | | | |
| Module:2 Static Malware Analysis 4 hours Fingerprinting the Malware - PE: File types, and header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. 4 hours Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification - and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation Techniques S hours 5 hours File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis Athi-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 <t< td=""><td>Module:2 Statio</td><td>Molware Analysis</td><td></td><td></td><td>1 h</td><td></td></t<> | Module:2 Statio | Molware Analysis | | | 1 h | | | | | |
| Pringerprinting the Malware - P.E. Frie types, and feader analysis, Excluding Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables. Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Samboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation Techniques Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. 1 hours Module:8 Contemporary Issues 1 hours | Fingerprinting the M | Woodule:2 Static Malware Analysis 4 nours Einemeinting the Melanary DE Eile tensor and handen analysis Charifering Melanary | | | | | | | | |
| Module:3 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - San⊎boxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation Techniques Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. Module:8 Contemporary Issues 1 hours | $\frac{1}{1}$ | · DEid and TrID MASTIFE DE executables | | ymg | wiarv | vale | | | | |
| Module:.5 Dynamic Malware Analysis 4 hours Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Samboxing: Tools and Techniques - Virus Total. 4 hours Module:4 Prepare for Reverse Engineering 4 hours Reverse engimeering as a process - Binary analysis tools, Disassemblers – Debuggers – Decompilers - Identificatiom and Extraction of Hidden Components - Typical malware behavior - Malware delivery. 4 hours Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours File Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. 1 hours Module:8 Contemporary Issues 1 hours | Module-3 Dyner | nie Malwara Analysis | | | 1 hc | MIPG | | | | |
| Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. 4 hours Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug - Windows API libraries - Packing and Encryption. 5 hours File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. 1 hours Module:8 Contemporary Issues 1 hours | Behavior Events An | alveis using ProcMon and Autorups - Detecting Code Injection - | Autom | ated | dyna | mic | | | | |
| Module:4 Prepare for Reverse Engineering 4 hours Reverse engineering as a process - Binary analysis tools, Disassemblers – Debuggers – Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 4 hours Module:6 Obfuscation Techniques S hours File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. 1 hours Module:8 Contemporary Issues 1 hours | analysis - Sandboxin | arysis using Proceeding Code injection - J | utom | aicu | uyna | unic | | | | |
| Reverse engineering as a process - Binary analysis tools, Disassemblers - Debuggers - Decompilers - Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery.Module:5Build and Debug the Malware4 hoursLow-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption.4 hoursModule:6Obfuscation Techniques5 hoursFile Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading.4 hoursModule:7Anti-Malware analysis4 hoursAnti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare.1000Module:8Contemporary Issues1 hours | Module 4 Prena | re for Reverse Engineering | | | 4 hc | mrs | | | | |
| Identification and Extraction of Hidden Components - Typical malware behavior - Malware delivery. Module:5 Build and Debug the Malware 4 hours Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption. 5 hours Module:6 Obfuscation Techniques Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. 4 hours Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. Module:8 Contemporary Issues 1 hours Total Lecture hours: 30 hours | Reverse engineering | as a process - Binary analysis tools Disassemblers – Debugge | rs – T | eco | nnile | ers - | | | | |
| Module:5Build and Debug the Malware4 hoursLow-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption.Module:6Obfuscation Techniques5 hoursModule:6Obfuscation Techniques- Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading Anti-Malware analysis4 hoursModule:7Anti-Malware analysis4 hoursAnti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare.1 hoursModule:8Contemporary Issues1 hours | Identification and Ex | traction of Hidden Components - Typical malware behavior - Mal | ware d | elive | rv. | 10 | | | | |
| Low-Level Language: Registers, Memory addressing, Opcode bytes - Builder and debugger: IDA Pro, Ollydebug -Windows API libraries - Packing and Encryption.Module:6Obfuscation Techniques5 hoursFile Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading.4 hoursModule:7Anti-Malware analysis4 hoursAnti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare.1 hoursModule:8Contemporary Issues1 hours | Module:5 Build | and Debug the Malware | | | 4 hc | ours | | | | |
| Ollydebug -Windows API libraries - Packing and Encryption. Module:6 Obfuscation Techniques File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. 1 hours Module:8 Contemporary Issues 30 hours | Low-Level Languag | e: Registers, Memory addressing, Opcode bytes - Builder and | lebugg | er: I | DA | Pro, | | | | |
| Module:6Obfuscation Techniques5 hoursFile Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading.OutputModule:7Anti-Malware analysis4 hoursAnti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare.1 hoursModule:8Contemporary Issues30 hours | Ollydebug -Window | s API libraries - Packing and Encryption. | | | | , | | | | |
| File Obfuscation - Binary Obfuscation Techniques - Assembly of data - Encrypted data identification - Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools - Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Contemporary Issues I hours 30 hours | Module:6 Obfus | cation Techniques | | | 5 ho | ours | | | | |
| Decrypting with x86dbg - Control flow flattening obfuscation - Garbage code insertion - Dynamic library loading. Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. Module:8 Contemporary Issues 1 hours Total Lecture hours: 30 hours | File Obfuscation - H | Binary Obfuscation Techniques - Assembly of data - Encrypted | data id | entif | icati | on - | | | | |
| Ioading. Module:7 Anti-Malware analysis 4 hours Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. Deadlisting - Information - Informatio - Information - Information - Information - Informa- | Decrypting with x86 | dbg - Control flow flattening obfuscation - Garbage code insertio | n - Dy | nami | ic lib | rary | | | | |
| Module:7Anti-Malware analysis4 hoursAnti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals SuiteTools - Deadlisting -Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare.1 hoursModule:8Contemporary Issues1 hoursTotal Lecture hours:30 hours | loading. | | - | | | - | | | | |
| Anti-debugging - Anti-VM - Anti-emulation - Anti-dumping - SysInternals Suite Tools – Deadlisting - Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. Module:8 Contemporary Issues 1 hours Total Lecture hours: 30 hours | Module:7 Anti-N | Aalware analysis | | | 4 ho | ours | | | | |
| Analysis of HTML scripts - MS Office macro analysis - PDF file analysis - SWFTools - FLASM - Flare. Module:8 Contemporary Issues 1 hours Total Lecture hours: 30 hours | Anti-debugging - A | nti-VM - Anti-emulation - Anti-dumping - SysInternals Suite To | ools – | Dead | dlisti | ng - | | | | |
| Module:8 Contemporary Issues 1 hours Total Lecture hours: 30 hours | Analysis of HTML s | Analysis of HTML scripts - MS Office macro analysis - PDF file analysis – SWFTools – FLASM – Flare. | | | | | | | | |
| Total Lecture hours: 30 hours | Module:8 Cont | emporary Issues | | | 1 ha | ours | | | | |
| Total Lecture hours: 30 hours | | | | | | | | | | |
| | | Total Lecture hours: | | • | 30 ha | ours | | | | |
| | | | | | | | | | | |

| Tex | Text Book(s) | | | | | | |
|-----------------|--|---|-------------|----------------------------------|--|--|--|
| 1. | Abhijit Mohanta, Anoop Saldanha, Ma | alware Analysis and | d Detection | Engineering a Comprehensive | | | |
| | Approach to Detect and Analyze Mod | lern Malware, 2020, 1st edition, Apress (ISBN 978-1-4842- | | | | | |
| | 6192-7), United States. | | | | | | |
| 2. | Reginald Wong, Mastering Reverse | e Engineering, 20 | 18, 1st ec | lition, Packt Publishing Ltd, | | | |
| | Birmingham, ISBN 978-1-78883-884-9, UK. | | | | | | |
| Reference Books | | | | | | | |
| 1. | M. Sikorski and A. Honig, Practical M | Ialware Analysis: | The Hands- | on Guide to Dissecting Malicious | | | |
| | Software. 2012, 1 st edition, No Starch | Press San Francisc | o, CA. (ISI | BN No.: 9781593272906), United | | | |
| | States. | | | | | | |
| Moo | de of Evaluation: CAT, assignment, Qui | iz and FAT | | | | | |
| Rec | commended by Board of Studies | 18-11-2022 | | | | | |
| App | proved by Academic Council | No. | Date | | | | |

| Course codeCourse titleLT | | | | | | С | | |
|--|---|---|-------|---------|-----------|-------|--|--|
| MCSE | E611P | Malware Analysis Lab 0 (| | | | 1 | | |
| Pre-re | equisite | NIL | S | llabu | s ver | sion | | |
| | 1 | | ~, | | <u>V.</u> | . 1.0 | | |
| | | | | | | | | |
| Cours | e Objectives | | | | | | | |
| 1. To | introduce malwa | re taxonomy and life cycle. | | | | | | |
| 2. To | analyze malware | samples using static, dynamic analysis, and reverse engineering t | techr | niques. | | | | |
| 3. To | detect and analyz | ze obfuscation and anti-malware techniques. | | | | | | |
| | | | | | | | | |
| Cours | e Outcome | | | | | | | |
| After o | completion of thi | s course, the student shall be able to: | | | | | | |
| I. Exp | plore the anti-mal | lware analysis techniques | | | | | | |
| 2. Ap | ply the reverse-ei | ngineering of malware and Obfuscation using emerging tools. | | | | | | |
| India | tivo Exnorimon | to | | | | | | |
| | Disassemble | Portable Executable (PE32) Files using PEid and ' | TrID |) 3 h | oure | | | |
| 1 | to identify | Tortable Exceduable (TE32) Thes using TER and | m | , 51 | Jours | | | |
| | • file compilation date | | | | | | | |
| imports/ exports, suspicious strings | | | | | | | | |
| | • run-tin | ne effect, procmon filter | | | | | | |
| hist -based signatures revealing files | | | | | | | | |
| | registry | v kevs processes services | | | | | | |
| | • networ | k-based signatures | | | | | | |
| 2 | Static and Dyna | amic Malware Analysis: | | 4 h | ours | | | |
| _ | Sandbox | xing the malware using SANDBOX tool: Cuckoo (open source) | | | | | | |
| | Sample | Malware analysis Virus Total | | | | | | |
| | • Registry | analysis using Any run | | | | | | |
| | Malwar | e analysis via hex code | | | | | | |
| 3 | Reverse-engine | ering the malware using IDA Pro: strings analysis, local varia | ables | s, 4 h | ours | | | |
| | graph mode to | cross-references, Analyzing Functions | | | | | | |
| 4 | Debug and Dis | assemble the malware using OllyDbg: Debug the malware, Vie | win | g 4 | | | | |
| | Threads and St | acks, OllyDbg Code-Execution Options, Breakpoints, Loading E |)LLs | , hou | ırs | | | |
| | Exception Hand | dling | | | | | | |
| 5 | MASTIFF is a | static analyzer framework (Linux and Mac) with the following | | 4 h | ours | | | |
| | plugins: | | | | | | | |
| | • ssdeep: | fuzzy hash, or context-triggered piecewise hashes (CTPH) to | | | | | | |
| | identify | nearly identical files for identifying variants of a malware family | r | | | | | |
| • pdftools: extracts information about PDF files. | | | | | | | | |
| • exiftool: This shows into, from image files. | | | | | | | | |
| | • disitool: | extract digital signatures from signed executables. | | | | | | |
| | • pyOLEscanner: extract information from OLE file types, such as Word | | | | | | | |
| | docume | nts and Excel spreadsheets | | 21 | | | | |
| 0 | Packing and o | | | 3 h | ours | | | |
| | • Pack an | a unpack the malware: UPX tool | | | | | | |
| | obfusca | tion and de-obfuscation of the malware using CFF explorer | | | | | | |

| 7 | Strings and API Analysis: | Strings and API Analysis: 4 ho | | | | | | |
|--------|--|--------------------------------|---------------------------|----------------------|-------------|-----------|--|--|
| | • SysInternals Suite's strings: T | This is a command-l | ine tool for | Windows that | at | | | |
| | shows the list of text strings i | in any type of file. | | | | | | |
| | • BinText: This is a GUI-based | l Windows tool that | can displa | y the ASCII a | ind | | | |
| | Unicode text strings for a giv | en file. | | | | | | |
| | • API Monitor: helps reverse e | ngineering by moni | toring API | calls as the | | | | |
| | program runs. | | | | | | | |
| 8 | Anti Malware analysis using: | | | | 4 ł | nours | | |
| | • WinDbg | | | | | | | |
| | IDA Pro / OllyDBG | | | | | | | |
| | SysInternals Suite Tools | | | | | | | |
| | Total Laboratory Hours 30 hours | | | | | | | |
| Text B | Text Book(s) | | | | | | | |
| 1. | Reginald Wong, Mastering Reverse | e Engineering, 2018 | , 1 st edition | , Packt Publis | shing Ltd, | | | |
| | Birmingham, ISBN 978-1-78883-8 | 84-9, UK | | | | | | |
| Refere | ence Books | | | | | | | |
| 1. | Abhijit Mohanta, Anoop Saldanha, | Malware Analysis a | and Detecti | on Engineerii | ng a | | | |
| | Comprehensive Approach to Detect | t and Analyze Mode | ern Malwar | e, 2020, 1^{st} ec | lition, Apr | ess | | |
| | (ISBN 978-1-4842-6192-7), United | States. | | | | | | |
| 2. | C. Eagle, The IDAPro Book: The U | Inofficial Guide to t | he worlds r | nost popular | Disassemb | oler, 2nd | | |
| | Ed. San Francisco: No Starch Press | San Francisco, CA | , 2011. (ISI | BN No. : | | | | |
| | 978-1-59327-289-0). | | | | | | | |
| Mode | of assessment: Continuous assessment | t and FAT | | | | | | |
| Recom | Recommended by Board of Studies 18-11-2022 | | | | | | | |
| Appro | ved by Academic Council | No. | Date | | | | | |

| Course code | Course title | L | Τ | P | C |
|-------------------------|--------------|------|-----|-------|--------|
| MCSE612L Cyber Security | | | | 0 | 3 |
| Pre-requisite | Nil | Syll | abu | s ver | sion |
| | | | | V | v. 1.0 |

Course Objectives

- 1. To understand key terms and concepts in Cyber security, Policies, Governance and Compliance.
- 2. To exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization.
- 3. To understand principles of cyber security and to guarantee a secure network by analyzing the nature of attacks through cyber forensics software or tools.

Course Outcome

After completion of this course, the student shall be able to:

- 1. Analyze and evaluate the cyber security needs of an organization.
- 2. Analyze the security issues in networks and computer systems to secure an infrastructure.
- 3. Design operational cyber security strategies and policies.
- 4. Apply critical thinking and problem-solving skills to detect current and future attacks on an organization's computer systems and networks.

| Module:1 | Introduction to Cyber Security | 6 hours | | | |
|--|--|-------------------------|--|--|--|
| Cyber Security- Layers of security, Vulnerability, Assets and Threat, Challenges and Constraints - | | | | | |
| Computer C | Computer Criminals - CIA Triad - Motive of attackers - Spectrum of attacks - Taxonomy of various | | | | |
| attacks - Cr | yptography - Security Governance – Challenges and Constraints, Secu | rity Models and Risk | | | |
| Managemen | t, Legacy Cyber security systems – Transformations in Cyber security | • | | | |
| Module:2 | Cyber Security Technologies | 6 hours | | | |
| Mobile Secu | urity – Advanced Data Security: Cloud Security, IoT Security - Incide | nt detection response | | | |
| - Penetration | testing – User Behavior Analytics (UBA) – Endpoint Detection and I | Response (EDR). | | | |
| Module:3 | Vulnerabilities and Safeguards | 6 hours | | | |
| Software Vu | Inerabilities - Complex Network Architectures, Open Access to Organ | izational Data, Weak | | | |
| Authenticati | on, poor cyber security awareness - Cyber Security Safeguards – Over | view, Access control, | | | |
| Audit, Auth | entication, Biometrics, Deception, Denial of Service Filters, Ethical | Hacking, Firewalls, | | | |
| Scanning, S | ecurity policy, Threat Management, Defending malicious software, | Applying software | | | |
| update and p | patches. | | | | |
| Module:4 | Securing Infrastructure and Local Host | 7 hours | | | |
| Infrastructur | e security in the real world and challenges – Understanding access co | ntrol and monitoring | | | |
| systems: Ac | cess control security policies, Physical security controls - Intrusion det | tection and Reporting | | | |
| systems – S | ecuring host device and challenges - Protecting the inner perimeter | - Protecting remote | | | |
| access: Loca | I protection tools, local intrusion detection tools, configuring browse | r security, Hardening | | | |
| operating sy | stems. | | | | |
| Module:5 | Cyber Security Tools | 6 hours | | | |
| Zenmap – H | ydra -Kismet - John the Ripper - Airgeddon - Deauther Board - Airc | rack-ng – EvilOSX. | | | |
| Module:6 | Cyber Security Strategies | 6 hours | | | |
| Need for built | ilding cyber strategy – Cyber-attack strategies (Red team) – Cyber de | fense strategies (blue | | | |
| team) – Int | roduction to Cyber security kill chain - Reconnaissance - Weapo | onization – Privilege | | | |
| Escalation - | Exfiltration - Threat Life cycle management phases. | | | | |
| Module:7 | Cybercrime Challenges | 6 hours | | | |
| Challenges | of fighting cybercrime- Opportunities, general challenges, and legal of | challenges - Capacity | | | |
| building- Cy | ber security and cybercrime: Capacity building methodology, Strates | gy as a starting point, | | | |
| the relevanc | e of policy, the role of regulators in fighting cybercrime, high star | ndards in developing | | | |
| countries. | | 1 0 | | | |
| Module:8 | Contemporary Issues | 2 hours | | | |
| | | | | | |
| | Total Lecture hours: | 45 hours | | | |

| Text Book(s) | | | | | |
|---|--|-----|------|--|--|
| 1. | Yuri Diogenes, Erdal Ozkaya, Cyber security - Attack and Defense Strategies, Packt Publishers, | | | | |
| | 2018. | | | | |
| 2. | Charles J. Brooks, Christopher Grow, Philip A. Craig, Donald Short, Cybersecurity Essentials, | | | | |
| | Wiley Publisher, 2018. | | | | |
| Ref | erence Books | | | | |
| 1. | William Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards, 1st | | | | |
| | edition, 2019. | | | | |
| 2. | Nina Godbole, Sunit Belapure, Cyber Security - Understanding cybercrimes, Computer Forensics | | | | |
| | and Legal Perspectives, Wiley, 2011. | | | | |
| Mode of Evaluation: CAT / Assignment / Quiz / FAT | | | | | |
| Rec | Recommended by Board of Studies 18-11-2022 | | | | |
| App | proved by Academic Council | No. | Date | | |
| | · · · · · · · · · · · · · · · · · · · | | | | |

| Course code | Course title | L | Т | Р | С | | |
|---|--|----------|-----------------|--------|--------|--|--|
| MCSE613L | Digital Forensics | | | 0 | 3 | | |
| Pro-requisite | Digital Forensics | | | | reion | | |
| rie-iequisite | | | Synabus version | | | | |
| Course Objectives | | | | | V.1.0 | | |
| 1 To understar | od the basics of digital forensics technology systems and se | rvices | | | | | |
| 2 To learn abo | ut data recovery data seizure digital evidence controls and | forens | ics a | nalve | sis | | |
| 3 To learn and | develop different tools for digital forensic acquisition and | analysi | | inary | ,15. | | |
| Course Outcomes | develop unterent tools for digital forensie acquisition and | anarysn | | | | | |
| After completion of | this course, the student shall be able to: | | | | | | |
| | | | | | | | |
| 1. Learn the fu | indamentals of digital forensics technology along with o | lifferen | t sv | stem | s and | | |
| services. | | | J | | | | |
| 2. Recover and | I seize data from a crime scene without damage, using | legal p | roce | dure | s and | | |
| standards. | | 0 1 | | | | | |
| 3. Exhibit know | wledge in forensic data acquisition and analysis and in | vestiga | te a | rtifa | cts in | | |
| different ope | erating systems. | U | | | | | |
| 4. Apply foren | sics tools and concepts on modern frameworks such as r | etwork | , em | nail, | smart | | |
| phones, clou | d and social media. | | | | | | |
| Module:1 Introd | uction to Digital Forensics | | | 6 I | nours | | |
| Digital forensics fu | ndamentals: Use of Computer Forensics - Benefits of P | rofessi | onal | Fore | ensics | | |
| Methodology - Step | s Taken by Computer Forensics Specialists - Case Studies | - Type | s of | Con | puter | | |
| Forensics Technolog | gy: Military, Law Enforcement, Business - Specialized Fo | orensics | s Teo | chnic | jues - | | |
| Hidden Data and H | low to Find It - Protecting Data from Being Compromis | ed - In | terne | et Tr | acing | | |
| Methods. | | | | | U | | |
| Module:2 Digital | Forensics Systems and Services | | | 61 | nours | | |
| Types of Computer | Forensics Systems: Firewall and IDS Security Systems - S | storage | Area | a Ne | twork | | |
| Security Systems - In | nstant Messaging (IM) Security Systems - Biometric Securit | y Syste | ms - | Com | puter | | |
| Forensics Services: | Occurrence of Cyber Crime - Cyber Detectives - Fighting C | yber C | rime | with | Risk | | |
| Management Tech | niques - Computer Forensics Investigative Services | - For | ensi | e Pr | ocess | | |
| Improvement. | | | | | | | |
| Module:3 Digita | l Forensics Evidence and Capture | | | 61 | nours | | |
| Data Recovery: Data | a Backup and Recovery, Data-Recovery Solution, Hiding ar | d Reco | veri | ng H | idden | | |
| Data - Evidence Col | lection and Data Seizure: Collection of Evidence and Optic | ons, Ob | stacl | es - [| Гуреs | | |
| of Evidence - The R | Rules of Evidence - Volatile Evidence - Volatile Memory H | Forensie | cs- C | ontr | olling | | |
| Contamination: The Chain of Custody, Reconstructing the Attack. | | | | | | | |
| Module:4 Data l | Preservation and Forensics Analysis | | | 71 | nours | | |
| Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene - Computer | | | | | | | |
| Evidence Processing Steps - Legal Aspects of Collecting and Preserving Evidence - Computer Image | | | | | | | |
| Verification and Authentication - Computer Forensics Analysis: Discovery of Electronic Evidence - | | | | | | | |
| Identification of Data - Reconstructing Past Events - disk and file system analysis. | | | | | | | |
| Module:5 Netwo | rk and Operating System Forensics | | | 61 | nours | | |
| Network forensics: | Investigation on virtual network and Email, Internet A | Artifact | s - 1 | Dam | aging | | |
| Computer Evidence - System Testing - Operating System Artifacts: Windows System Artifacts, Linux | | | | | | | |
| System Artifacts. | | | | | | | |
| Module:6 Mobil | e and Cloud Forensics | | | 61 | nours | | |
| Mobile Forensics: Acquisition Procedures for Mobile, Equipment, Tools, Internet of Anything - Cloud | | | | | | | |
| Forensics: Service Levels, cloud vendors, Legal Challenges and Technical Challenges, Acquisition, | | | | | | | |
| Investigation, Tools | : Open-Stack, F-Response, AXIOM. | | | - | | | |

| Mo | dule:7 | Forensics Tools | | | | 6 hours |
|---|--|------------------------------|-------------------|------------|-------------|-----------------------|
| Ope | Open source tools: The Sleuth Kit (TSK) and Autopsy - SANS SIFT Investigative tool - Voltality - | | | | | |
| CA | INE inve | estigative environment - win | ndows System inte | rnals-Com | mercial too | ols: Encase, FTK, PRO |
| Dis | cover Ba | sic, Nirsoft. | | | | |
| Mo | dule:8 | Contemporary Issues | | | | 2 hours |
| | | | | | | |
| | | | | | | |
| | | | T | otal Lectu | re hours: | 45 hours |
| | | | | | | |
| Tex | kt Book(| s) | | | | |
| 1. | John R | . Vacca, Computer Forens | sics: Computer Ci | rime Scen | e Investiga | tion, 2015, Second |
| | Edition | , Charles River Media, Inc. | (ISBN No.: 978- | 1-58450-3 | 89-7) | |
| 2. | 2. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools: Using Open Source | | | | | |
| | Platform Tools, 2011, First Edition, British Library Cataloguing-in-Publication Data. (ISBN | | | | | |
| | No.: 978-1-59749-586-8) | | | | | |
| Reference Books | | | | | | |
| 1. | 1. B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, Guide to Computer Forensics and | | | | | |
| | Investigations, 2019, Sixth Edition. CENGAGE, INDIA (ISBN: 9789353506261) | | | | | |
| Mode of Evaluation: CAT, assignment, Quiz and FAT | | | | | | |
| Recommended by Board of Studies 18-11-2022 | | | | | | |
| Approved by Academic Council No. Date | | | | | | |