3. Program to execute matrix multiplication using pthreads.
4. Program to execute matrix multiplication using OpenMP and comparison with pthread program.
5. Program to execute Pi computation and prefix sum using OpenMP.
6. Program to execute section, task and synchronization constructs of OpenMP.
7. Case Study of Cluster building steps - MPI Cluster setup and overview of different routines.
8. Program to implement point to point communication using MPI routines.
9. Program to implement collective communication using MPI routines.
10. Program to implement Map-Reduce parallelism for Warehouse Scale Computer.

Reference Books

- Peter S. Pacheco, "An Introduction to Parallel Programming", Morgan Kaufmann, Morgan Kaufmann, 2011, ISBN: 978-0-12-374260-5.
- Michael Quinn, "Parallel Programming in C with MPI and OpenMP", McGraw-Hill Edition, 2003, ISBN13: 978-0072822564.

This is a suggested list. The instructor is expected to continuously update it.

(CT(DE)-22017) Cyber Security

Teaching Scheme:
Lectures : 3 Hrs/week

Examination Scheme:
Assignment/Quizzes – 40 marks
End Sem Exam - 60 marks

Course Outcomes:

Students will be able to:

1. Define the need of Cyber Security.
2. Explain the IT act, Application Security vulnerabilities and its mitigation techniques.
3. Demonstrate the knowledge of penetration testing, and social networking security.
4. Analyse the malwares, social networking websites and impact of cyber-crime on e-commerce.

Unit I:Introduction: Nature and scope of computer crime, Understanding how cyber criminals and hackers work, Different types of cyber-crimes, Introduction to digital signatures, Cryptography, Digital certificate and public key infrastructure, IT Act., Impact of cyber-crime on e-governance and e-commerce.

[6 Hrs]

Unit II: Malware reverse engineering: Overview of malware reverse engineering, Types of malware, Malicious code families, Latest trends in malware analysis, Basic static and dynamic analysis, Malware analysis techniques, Case study.

[6 Hrs]

Unit III:Web application security: Introduction to web application security: Attacks, vulnerabilities and mitigation, Client-side security, Server-side security, Application security: HTTPS, HSTS etc., Security engineering: Passwords and their limitations, Attacks on passwords: CAPTCHA, OTP.

[8 Hrs]

Unit IV:Advanced security topics: Secure email systems: PGP, SMIME, DKIM, DMARC, DNSSec, SMTP STS etc., Privacy and security for online social networks, Database security, Browser security, Mobile device security.

[8 Hrs]

Unit V: Ethical hacking and penetration testing: Security Technologies: IDS, IPS, Ethical hacking, Penetration testing fundamentals: Reconnaissance, scanning, gaining access, maintaining access, Covering tracks.

[6 Hrs]

Unit VI:Case studies: Cloud security, Operating system security, Security of social networking websites, IoT devices security, E-commerce websites security.

[6 Hrs]

Text Books

- Hossein, "Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management", Wiley, Volume 3 edition, ISBN-13: 978-0470323069.
- Georgia Weidman, "Penetration testing: A Hands-On Introduction to Hacking", No Starch Press, 2014, ISBN-13: 978-1593275648.
- Michael Sikorski and Andrew Honig, " Practical Malware Analysis", No Starch Press, 1st Edition, 2012, ISBN-13: 978-1593272906

Reference Books

- "Practical Internet of Things Security" by Brian Russell, Drew Van Duren, Packt publishing, 2016, ISBN: 9781785889639
- T. Mather, S. Kumaraswamy, S. Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Series, 2009, ISBN-13: 978-0596802769.
- "Cyberlaw: the Indian perspective"; Pavan Duggal; Saakshar Law Publications, 1st edition, 2002, ISBN: 8189121022, 9788189121020.

(CT(DE)-22026) Cyber Security Laboratory

Teaching Scheme:
Laboratory : 2 Hrs/Week

Examination Scheme:
Continuous evaluation: 50 Marks
Assignments/Mini Project: 20 marks
End Semester Exam: 30 Marks

List of Assignments:

1. Perform literature survey of recent research papers on cyber security.
2. Perform case study of any two cyber-crime cases in India and write a report illustrating Indian cyber laws (IT Act, IT Act 2008. IPC) relevant to these cases.
3. Perform malware reverse engineering in an isolated environment using sandbox and document the findings.
   a. Use any sample malware file.
   b. Study malware behaviour: its working, how it spreads. Find its features/characteristics.
   c. Identify the changes made by malware on the system. (for e.g., changes in event log, registry etc.). Difference between infected and normal system.
   d. Describe detection method or alert system for malware
   e. Write down steps to remove the malware and make system safe again.
4. Perform penetration testing using Kali Linux on virtual machine and write a report.Follow each stage of penetration testing: Planning and reconnaissance, scanning, gaining access, maintaining access and analysis.Once the Kali is installed, use following tools. Submit a report answering following questions:
      a. Maltego: How did you perform the following things?
   - Associate an e-mail address to a person
   - Associate websites to a person
   - Verify an e-mail address
   - Gather details from Twitter, including geolocation of pictures
      b. Vega: Provide a target website and scan that website for vulnerabilities.
      c. NMAP: Scan your local network and provide screenshot of the report
      d. Tamper Data plugin in FireFox: Gather information of GET and POST request for gmail.com
      e. Metasploit framework: List out all the exploits provided by metasploit framework. Explain preconditions and expected end results for each one.
5. Provide screenshots also. Do not use any exploit without proper permission.
6. Implement any IDS/IPS system.

This is an illustrative list of assignments. The instructor is expected to update the list.

Departmental Elective – IV

(CT(DE)-22027) System Administration

Teaching Scheme	**Examination Scheme**
Lectures: 3 Hrs./week	Assignment/Quizzes: 40 marks End Semester Exam: 60 marks

Course Outcomes

Students will be able to:

1. Carry out the following tasks, with special emphasis on GNU/Linux based systems: