|  |  |  |
| --- | --- | --- |
| **Course No 4** | **Item** | **Details** |
| (a) | *Title of the Course* | Introduction to Cyber Security |
| (b) | *Course Coordinator* | Prof. Sandeep Shukla  Department of Computer Science & Engineering  Indian Institute of Technology Kanpur |
| (c) | *Duration (1-3 weeks)* | Two weeks |
| (d) | *Eligibility Criteria (basic expected background)* | This introductory course will best serve people with Computer Science and Information Technology background who have never been exposed to the concept of cyber security in information systems, critical infrastructure, telecommunication and digital banking. This course will make the students about cyber security issues, cyber threats, their implications to their day-to-day operations as IT personnel, and prepare them for a more advanced course in cyber security. This course will not make them experts in cyber security or enable them to become the cyber security professionals. However, given that all engineers and IT personnel should be familiar with basic cyber security issues, this may bring them to a level of understanding that can further be enhanced by an advanced course (online courses, or direct taught courses). |
| (e) | *Tentative dates for the proposed event* | December 02- December 15, 2019 |
| (f) | *Objectives* | After completing this course the students will be able to:  • Explain the cyber borne threats to their IT systems, their mobile devices, devices used in home, factory, and office automation, and also be able to articulate the need for better cyber security control  • Explain the various sources of threats, and also be able to find sources of threat intelligence from various internet based sources to become more alert to known and reported vulnerabilities and threats  • Understand the system architecture of an IT system, a local network, and various computing assets at their disposal and understand how various threat vectors may affect various parts of the system, and why defense in depth is required  • Understand the threats in mobile devices, digital and mobile banking, and caution others about cyber hygiene and best practices  • Understand and articulate the threats to power systems, industrial control systems, and other systems germane to smart city, smart grid, smart transportation etc and raise awareness around them  • Understand the malware concepts, and how malware analysis helps in identifying malware (trojans, rootkits, spyware, ransomware etc)  • Explain to others the various tools and technologies available for cyber security including perimeter defenses (network firewall, web application firewall, intrusion detection systems etc), network defense, application level defenses, file system protections, memory protection  • Explain basic notions of side channel attacks and its various incarnations  • Explain basics of web security and vulnerabilities  • Explain basic idea of SSL/TLS for secure web communication  • Explain the difference between cryptography, and cyber security and their relationship  • Be knowledgeable in the vocabulary of cyber security |
| (g) | *Tentative list of topics to be covered* | * Cyber Security -- Confidentiality, Integrity and Availability * Basic Tool of Cyber Security -- Cryptography, Hash functions, Public vs. Private Keys, Public Key Infrastructure * IT system infrastructure -- architecture and threat vectors * Critical System infrastructure - architecture and threat vectors * Mobile phone and smart device architecture and threat vectors * Cyber Security Tools -- Perimeter Defense tools * Cyber Security Tools -- Defense in Depth at various layers of the system stack * Threat of malware and malware types and indicators * Basic Web protocols and secure web protocol SSL/TLS basics * Network security concepts and vulnerabilities * Antivirus, Malware analyzers, Intrusion detection, Firewalls * Side channels and the dangers of side channel attacks * Case studies from various well known attacks of recent past * Sources of further studies in cyber security |