Ethical Hacking and Cyber Security

[August 5-7, 2019]

Mr A Rakesh Phanindra - Programme Director

About the Programme

In today's global, digital world, data rule. Safeguarding intellectual property, financial information, and your company's reputation is a crucial part of business strategy. Yet with the number of threats and the sophistication of attacks increasing, it's a formidable challenge. Companies that understand the value that security brings to the business also ensure that they have a comprehensive strategy in place—and that they have the processes and procedures to back up their vision. The guiding principles for strategy are driven, in large part, by their data.

Securing vital resources and information in the network is the most challenging feat for system enterprise. As business has migrated to the digital world, criminals have, too. What has emerged is a sophisticated criminal ecosystem that has matured to the point that it functions much like any business—management structure, quality control, off shoring, and so on. While the hacking skills can be used for malicious purposes, this programme provides you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization. You leave with the ability to quantitatively assess and measure threats to information assets; and very good awareness stuff along with appropriate live demonstration also will be the part of this three day hands-on training programme on "Ethical Hacking & Cyber Security" at Institute of Public Enterprise (IPE), Hyderabad..

Programme Objective

- To update the knowledge on various Information and Cyber Security issues and solutions.
- Enriching awareness to identify the Hacker's attack points and to prevent in advance and combat them.

Programme Contents

- Introduction to Ethical Hacking, Importance of Cyber Security in public sector enterprises
- Intelligent threat analytics for Overlay networks
- Fake Block attack, Sybil attack
- Metasploit, Armitage, Traffic Classification
- Malicious attacks prevention, Security Threats & Vulnerabilities
- Cyber Forensics, Antivirus detection mechanism
- Online Frauds, Online Frauds, Hacking windows 7, Chinese PDF exploits, Vulnerability scanners, Rootkits, Spoofing attacks, Steganography, Nexpose, Bineders, facebook sniffers, Websites Hacking, Social Engineering, Web Shells
- Wi-Fi Cracking, WEP Cracking, WPA Cracking, WPA2 Cracking
- Computer Forensics & Honeypots, Social Engineering Toolkit Attacks
- Hacking windows 7, Chinese PDF exploits, Vulnerability scanners, Rootkits, Spoofing attacks, Steganography, Nexpose, Bineders, facebook sniffers, Websites Hacking, Social Engineering, Web Shells
- Attacks with Backtrack, Cross Site Scripting Attacks, Cookie Stealing and Session Hijacking
- Cyber-attacks & critical information, infrastructure protection
- Mobile Phone Exploits
- Network Reconnaissance & Information Gathering
- Cyber Security laws and standards
- Application, Internet and Mobile Platforms Security
- Network security –Firewalls, Gateway Devices, Antivirus, Anti-Spam, proxy,
- Intrusion Detection System and Intrusion Prevention System
- Security and Performance Evaluation of Security Protocols
- IEEE and CSI Case studies on Cyber Security
- Internet of Things
- Net Neutrality

Target People

This course is designed to meet the requirements of all Lower/Middle/Upper level officers/managers/executives working in Manufacturing, Defense, Atomic Energy, Works, Maintenance, Stores, Purchase, Finance, Commercial, Transport, Contracts and EDP Departments and Vigilance Officer those who are looking for technological awareness and skill development.