Cyber Attacks & Network Security
(October 11-12, 2018)
Mr A S Kalyana Kumar : Programme Director

Introduction & Objectives

Cyber Attacks & Network Security training focuses on Various Cyber Attacks, Vulnerability Discovery, Testing Network Devices to ensure the security and auditing on enterprise networks.

This course will starts with different attack methods used by real time network intruders and further discuss on how to review network architecture, devices and configuration of multiple devices with a good amount of practical hands-on exercises.

This programme will provide you the latest developments to mitigate the attacks on Network level and ensuring Security from Cyber attacks. Through presentation and discussions with industry experts, you will gain a thorough understanding of the standards that will underpin and support your work.

Programme Content

- Information Security & Cyber Forensics
- Fundamentals of Ethical Hacking
- Stages of Hacking
- Understanding the attacks
- Vulnerability Analysis (Intro & Demo): Nessus, GFI Languard, MBSA
- Penetration testing in a nut shell (Internal Pen-testing (White & Grey Box Testing), External Pen-testing (Black Box Testing), Analysis
- Crash Course: NMap, Wireshark, Metasploit Framework (including SET & Armitage)
- Basics on Cyber security Distros and Frameworks (Veil Framework, Nexpose Framework, Introduction to Viper VAST, Tail, Black Arch etc.

Target Group

This course will be beneficial for network administrators, architects, network engineers, testers, auditors and other enthusiasts want to learn about network security and understand potential digital threats to enterprise networks. This course is also to meet the requirements all Lower/Middle/Upper level officers/managers/executives those who are looking for technological awareness and skill development in this domain.