

Introduction:

Increased Internet penetration for applications such as e-Govern-ance, e-Commerce, e-Banking, digital payments, e-Learning, smart cities etc, has resulted in an exponential rise in sophisticated attacks on Information Technology (IT) infrastructure. This has led to Cyber Security as an important aspect to secure our computers and networks. Both government & industry are becoming the victims of cyber criminals, including companies working in security technology. Cyber Security is going to be much more serious problem in the coming years. Hence it becomes more important & essential to be aware of the challenges and methods to meet the new age attacks.

Course objective:

This Course Will Provide An Overview on Cryptography And Information Security, PKI And Digital Signature, IPV6 Addressing, Ethical Hacking, Various Attacks & Countermeasures, Wireless & Wi-Fi Security, Viruses, Trojans, Spywares, Security Issues In Android, Cyber Forensics.

Target Audience:

Officials of State/Central Govt departments, PSUs, Corporate, System / Network Administrators, Technical Officers, State & National Law agencies,

Pre-requisite: Knowledge of Computing & Internet

Intake: Participants will be limited to a max of Thirty (30) seats and on first-cum-first serve basis only

Methodology: The course will be for Five (5) days, followed by one day evaluation & certification (both written & Lab). Certification is not mandatory

Fees: Course fee is Rs 20,000/- + Rs. 5000/- (Evaluation & Certificate) per participant. Fee includes Training material & Refreshments.

How to Register:

URL for registration: <http://cybersec.cdacb.in/Regform/>

Course Contents (Theory Sessions)

Session 1.1: Cryptography and Information Security - Intro / Symmetric & Assymmetric Keys / Security threat & attacks / ITACT perspective , policy of GOI

Session 1.3: PKI and Digital Signature - Digital Signature Certificate / Authority / Trust model / Types / Classes / Lifecycle / eSign

Session 2.1: Computer Network and IPV6 Addressing - Networking Fundamentals / Segmentation / TCP/IP Utilities / IPv6 Addressing / IPV6 Application / Services / IANA

Session 2.3: INTRODUCTION TO ETHICAL HACKING - Ethical Hacker / Why Ethical Hacking / Terminology / Phases of Ethical Hacking / Information Gathering / Network Discovery / Various tools used for Scanning

Session 3.1: BRUTE FORCE ATTACK & COUNTER MEASURES - Brute Force Attack / Types of Password Attacks / Denial of Service (DoS) / Types of DoS Attacks / Symptoms for DoS Attack / MAC Address Spoofing

Session 3.3: DNS Hacking and Countermeasures - DNS Concepts and fundamentals / DNS Zones and Domains / DNS Hierarchy / Various Attacks on DNS Infrastructure

Session 4.1: Wireless & Wi-Fi Security - Wireless Attacks and Threats / Wireless Protocols / Wi-Fi Weaknesses / Wireless Security / Configuration and Network Isolation

Session 4.3: TROJAN, BACKDOOR & VIRUS and Android Hacking - Trojan, Backdoor & Virus / Tools Used / countermeasures / Password Crackers & Cracking Techniques

Session 5.1: Cyber Forensics - Principles / Forensics Analysis / Registry Analysis / Forensic Thumbs.db

Session 5.3: Memory Forensic - Live Forensic / Steganography / Network Forensics

Session 5.4: Container Security - Concepts of Container / Docker Demonstration / Security Concepts

** Theory sessions will be followed by hands-on session

C-DAC Profile:

The Centre for Development of Advanced Computing (C-DAC) is an autonomous Scientific Society under the Ministry of Communications & Information Technology, Government of India. established in 1988, as India's national initiative for design, development and delivery of high performance computing (Supercomputer) systems and solutions based on parallel processing technology, C-DAC has over the years diversified its activities, transferring the expertise it acquired and technologies it developed in the high-end computing to develop and deploy advanced Information Technology (IT) based solutions in the key sectors of economy.

C-DAC in Cyber Security:

Cyber Security & Cyber Forensics is one of the key thrust areas of R&D activity. C-DAC is focusing on developing solutions / products to fit into the Cyber security Ecosystem, in such a way that it can provide the needed expertise to various agencies at different levels of security architecture like biometrics, endpoint security, perimeter security, SCADA Security, Honeynets, web application security, malware detection & prevention solutions, unified threat management, wireless / mobile security and so on.

It offers services such as Information Security Consulting, Auditing, and w.r.t globally recognized and accepted standards such as ISO27001, Network Posture Assessment Services including Penetration Testing, Vulnerability Assessment, Web Application Security Assessment, Information Security Awareness and Training.

Venue:

Centre for Development of Advanced Computing

No. 68, 4th Cross, Electronic City Phase 1,
Hosur Road, Opp.BSNL Telephone Exchange

Bengaluru, Karnataka 560100

Telephone: +91-80-28523300

Contact Person:

Mr. Aswath Rao

Mobile No: +919449086827

Land Line: +91-80-66116545

email ID: aswath@cdac.in

Five-Day Certificate Course on Cyber Security & Ethical Hacking

Date: 04 - 08 February 2019

Time: 10.00 AM - 5.00 PM



Conducted by: C-DAC ACTS,
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC)
A Scientific Society of the Ministry of Electronics and Information Technology (MeitY)
C-DAC Knowledge Park, No. 1, Old Madras Road, Bengaluru-560038, Karnataka, India,
Tel: +91-80-25244059, Fax: +91-80-25246356, <http://www.cdac.in>