DICC

Certified Ethical Hacking Course

Be a Certified Ethical Hacker

Modules, Details & Fees

Total Modules- **24 (highest in Industry)**
Duration- 2-Months
Full Course Fees- 15,000.00 (Pay in two Installments -8000*2)

Batches Options		
	Regular Batches	Mon-Fri
	Alternate Batches	3 Days a Week
	Weekend Batches	Saturday + Sunday
	Sundays Batches	Only Sundays
Online Classes Also Available		

Reasons you should join DICC

1. Advance Level Ethical Hacking Course
2. EC-Council Certified Trainer
3. Total Modules Covered: 24
4. 95% Practical Trainining
5. **Free Latest Software Toolkits + Study Material**
6. Flexible Timings (**Early Morning & Late Evening Availablle**)
7. 100% Placement Support
8. Free demo Class available
9. **DICC Certification Included**
10. **Affordable Fees**

Call: 9899127357 info@delhitrainingcourses.com

Chapter 1: Introduction to Hacking

- Important Terminology
- Ethical Hacking vs. Hacking
- Effects of Hacking on Business
- Why Ethical Hacking Is Necessary
- Skills of an Ethical Hacker
- What Is Penetration Testing?

Chapter 2: Networking Concepts

- What is Network?
- Various types of network topologies
- Dissimilar type of Network Devices
- Protocols & Port numbers
- IP Addressing and its classes
- VPN Network, DHCP Server
- DNS Server, OSI Model
- Server Configuration

Chapter 3: Virtualization (Lab Setup)

- Importance of Virtualization
- Features and Terminologies
- Create & Run Your First Virtual Machine OS
- Connect USB to Virtual Machine
- Network Adapter and More Settings
- Create Network in VMs
- Share Data in Network
- Special Features of Virtualization
- Problem Handling
- Various types of Virtualization Programs

Chapter 4: Foot printing

- Gathering Information Using Websites and Applications
- IP Mapping and Tracing IP address
- Active and Passive Methods
- Detecting Web Server
- Find weaknesses using Google
- Hacking Using Google and other Search Engines

Chapter 5: Scanning

- Detection of Alive IP Addresses
- Port scanning techniques
- Advance Trace route
- Discovering with SYN, ACK, UDP, ICMP, ARP
- Aggressive detection
- Proxy and VPN Servers
- Understanding of TOR & Deepweb Network

Chapter 6: Windows Hacking

- OS Authentication Architecture
- OS Hash BruteForcing
- OS Password Cracking
- Windows Login Bypass
- OSX Login Bypass
- Data Stealing Techniques

Chapter 7: Linux Hacking

- Kali Linux Vs Other Pen Testing OS
- Installation and setup of Kali Linux
- System Architecture of Kali Linux
- Network Configuration of Kali Linux
- Essential Commands of Kali Linux

Chapter 8: Virus and Worms

- Types of Viruses and Worms
- Creation of Viruses and Worms
- Difference Between Viruses and Worms
- Detection of Viruses and Worms
- Manual Removal of Viruses and Worms

Chapter 9: Trojans and RATS

- Different Type of Trojans
- Making of Trojan(RAT)
- Right Way to Configure Trojan
- Online Trojan propagation
- Analysis and Removal of Trojan

Chapter 10: Sniffing

- Introduction to Network Sniffing
- Man in the Middle Attacks
- MAC spoofing & Flooding
- ARP Poisoning
- Rogue DHCP
- SSL Stripping
- Session Hijacking

Chapter 11: Email Hacking

- Social Engineering
- Fake Emails
- Identify Fake Emails
- KeyLoggers
- Email Encryption
- Counter Measures

Chapter 12: Phishing

- Phishing Attacks
- Desktop Phishing
- Spear Phishing

Chapter 13: SQL Injection

- Introduction to SQL Database
- Types of SQL Injections
- Authentication Bypass Injection
- Blind Injections
- Error Based Injection
- Union Based Injection
- Stacked Query Injection
- Time Based Injection

Chapter 14: Wi-Fi Hacking

- Wi-Fi Technical Details
- Types of Encryptions
- MAC Spoofing
- Attacks on WEP, WPA, WPA2
- Forged Authentication Attack
- Replay Attack
- De-Synchronization Attack
- Evil Twin and Fake AP Attack

Chapter 15: Steganography

- Types of Steganography
- Techniques of Steganography
- How Steganography Works
- Image Steganography
- Working with Tools

Chapter 16: (XSS) Cross Site Scripting

- How XSS Attacks Work
- XSS Attack via Email
- Stealing Cookies via XSS
- XSS Attack in Comment Field
- Blog Post via XSS Attack
- CSRF Attacks

Chapter 17: iFrame Attacks

- Understanding an iFrame Attack
- New iFrame Injection Method
- Ads in hidden iFrame and pop-ups
- Redirecting to a malicious server
- Malicious script execution

Chapter 18: DoS and DDoS Attacks

- How DoS Attack Works
- Indications of DoS Attacks
- DoS Attack Techniques
- Tools for DDoS Attacks
- Detection of Attacks

Chapter 19: Mobile Hacking

- Understanding Android's Roots
- Android Rooting Tools
- Android Trojans
- Exploit Using apk File
- Detection of Weakness
- Understanding of Fake Cell Towers

Chapter 20: Penetration testing

- Need of Penetration Testing?
- Types of Pen Testing
- Pen Testing Techniques
- Security Audit
- Vulnerability Assessment
- Black Box Pen Testing
- Gray Box Pen Testing

Chapter 21: Reverse Engineering

- Introduction to RE
- Tools and Commands
- Monitoring Events and Exceptions
- Inspecting Processes and Modules

Chapter 22: Firewall & honeypots

- Introduction to Firewalls
- Network Firewalls
- Web Application Firewalls
- Weakness in Firewalls
- Honey Pots and Security Misconfiguration

Chapter 23: IDS / IPS

- Configure Rule sets
- Setup Network IDS/IPS
- Writing Custom Rules
- Logs Analysis
- DMZ Configuration
- Intrusion Detection Systems and weakness
- Intrusion Prevention Systems and weakness

Chapter 24: Cyber Laws