Course Overview:

This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, "To beat a hacker, you need to think like a hacker". This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver's seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach to help you identify when an attack has been used against your own targets. Why then is this training called the Ethical Hacker Course? This is because by using the same techniques as the bad guys, you can assess the security posture of an organization with the same approach these malicious hackers use, identify weaknesses and fix the problems before they are identified by the enemy, causing what could potentially be a catastrophic damage to your respective organization.

Throughout the course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

Benefits:

Upon completion of this course, students will be able to:

- Understand how intruders gain access to the victim machine.
- Understand Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Understand complete Ethical Hacking Concepts & Procedures.

Topics to be covered:

- Introduction to Ethical Hacking
- Cyber Laws
- Footprinting and Reconnaissance
- Google Hacking
- Scanning Networks
- Enumeration

- System Hacking
- Malware Threats
- Trojan & Backdoors
- Virus & Worms
- Sniffing
- Social Engineering
- Phishing
- Denial of Service
- DDoS
- Session Hijacking
- Hacking Web Servers
- Hacking Web Applications
- OWASP Top Ten
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- SQL Injection
- LDAP Injection
- Hacking Wireless Networks
- Cracking WEP
- Cracking WPA
- Cracking WPA-2
- Hacking Mobile Platforms
- Android Hacking
- iOS Hacking
- Evading IDS, Firewalls, and Honeypots
- Cloud Computing
- Cryptography
- Case Studies

Target Audience:

- Security Officers
- Auditors
- Network Administrators
- Firewall Administrators
- Security Professionals
- Anyone who is concerned about the integrity of the network infrastructure

Prerequisites:

- Strong knowledge of TCP/IP
- Information systems and security background
- Minimum of 12 months of experience in networking technologies

Course Length:

- 40 hours

Career Track & Roles:

- Network Administrator
- Systems Administrator
- Systems Engineer
- Systems Architect
- Network Security Specialist

Follow On Courses

- Delttas Web Application Security
- Delttas Mobile Application Security-Android & iOS

Course Price: USD 2,000 per person for a 40-hour course