Ethical Hacking

Introduction to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Top Information Security Attack Vectors
- Motives, Goals, and Objectives of Information Security Attacks
- Information Security Threats
- Information Warfare
- Hacking Concepts
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?
- Hacker Classes
- Hacktivism
- Hacking Phases
- Types of Attacks
- Types of Attacks on a System
- Operating System Attacks
- Misconfiguration Attacks
- Application-Level Attacks
- Skills of an Ethical Hacker
- Defense in Depth
- Incident Management Process
- Information Security Policies
- Classification of Security Policies
- Structure and Contents of Security Policies

Footprinting and Reconnaissance

- Foot printing Concepts
- Foot printing Terminology
- What is Foot printing?
- Why Foot printing?
- Objectives of Foot printing
- Foot printing Threats
- Foot printing through Search Engines
- Finding Company's External and Internal URLs
- Mirroring Entire Website
- Website Mirroring Tools
- Extract Website Information from
- http://www.archive.org
- Monitoring Web Updates Using Website Watcher
- Finding Resources Using Google Advance Operator
- Google Hacking Tool: Google
- Hacking Database (GHDB)
- Google Hacking Tools
- WHOIS Footprinting
- WHOIS Lookup
- DNS Footprinting
- Extracting DNS Information
- DNS Interrogation Tools
- Network Footprinting
- Locate the Network Range
- Determine the Operating System
- Footprinting through Social Engineering

Scanning Networks

- Check for Live Systems
- Checking for Live Systems - ICMP Scanning
- Ping Sweep
- Check for Open Ports
- Scanning Tool: Nmap
- Hping2 / Hping3
- Scanning Techniques
- Scanning Tool: NetScan Tools Pro
- Scanning Tools
- Do Not Scan These IP Addresses (Unless you want to get into trouble)
- Port Scanning Countermeasures
- Banner Grabbing Countermeasures
  Disabling or Changing Banner
- Hiding File Extensions from Web Pages
- Scan for Vulnerability
- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack

Enumeration

- What is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- NetBIOS Enumeration
- NetBIOS Enumeration Tool:SuperScan
- NetBIOS Enumeration Tool: Hyena
- NetBIOS Enumeration Tool:Winfingerprint
- NetBIOS Enumeration Tool:NetBIOS Enumerator
- Enumerating User Accounts

System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
- CrackingPasswords
- Password Cracking
- Password Complexity
- Password Cracking Techniques
- Types of Password Attacks
- Distributed Network Attack
- Default Passwords
- Manual Password Cracking (Guessing)
- Stealing Passwords Using Keyloggers
- Spyware
- How to Defend Against Keyloggers
- Anti-Spywares
- What Is Steganography?
- Least Significant Bit Insertion

Trojans and Backdoors

- Trojan Concepts
- What is a Trojan?
- Trojan Infection
- Types of Trojans
- Command Shell Trojans
- Command Shell Trojan: Netcat
- GUI Trojan: MoSucker
- GUI Trojan: Jumper and Biodox
- Document Trojans
- E-mail Trojans
- E-mail Trojans: RemoteByMail
- Trojan Detection
- How to Detect Trojans
- Scanning for Suspicious Ports
- Trojan Horse Construction Kit
- Anti-Trojan Software

Viruses and Worms

- Virus and Worms Concepts
- Introduction to Viruses
- Virus and Worm Statistics
- Types of Viruses
- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses

- Stealth/Tunneling Viruses
- Encryption Viruses
- Polymorphic Code
- Computer Worms
- Malware Analysis
- Online Malware Testing: VirusTotal
- Online Malware Analysis Services
- Anti-virus Tools

Sniffers

- Sniffing Concepts
- Wiretapping
- Lawful Interception
- Packet Sniffing
- Sniffing Threats
- SPAN Port
- MAC Attacks
- MAC Flooding
- MAC Address/CAM Table
- How CAM Works
- DHCP Attacks
- How DHCP Works
- DHCP Request/Reply Messages
- IPv4 DHCP Packet Format
- ARP Poisoning
- What Is Address Resolution Protocol(ARP)?
- ARP Spoofing Techniques
- ARP Spoofing Attack
- Spoofing Attack
- Spoofing Attack Threats
- DNS Poisoning
- DNS Poisoning Techniques

Social Engineering

- Social Engineering Concepts
- What is Social Engineering?
- Behaviors Vulnerable to Attacks
- Social Engineering Techniques
- Types of Social Engineering
- Human-based Social Engineering
- Technical Support Example
- Authority Support Example
- Social Networking Sites
- Social Engineering Through
- Impersonation on Social
- Networking Sites
- How to Detect Phishing Emails
- Anti-Phishing Toolbar: Netcraft
- Anti-Phishing Toolbar: PhishTank
- Identity Theft Countermeasures

Denial of Service

- DoS/DDoS Concepts
- What is a Denial of Service Attack?
- What Are Distributed Denial ofService Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Bandwidth Attacks
- Service Request Floods
- SYN Attack
- SYN Flooding
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Application Level Flood Attacks
- Botnet
- Botnet Propagation Technique
- DDoS Attack
- DDoS Attack Tool:LOIC
- DoS Attack Tools

Session Hijacking

- Session Hijacking Concepts
- What is Session Hijacking?
- Dangers Posed by Hijacking
- Why Session Hijacking is Successful?
- Key Session Hijacking Techniques
- Brute Forcing Attack
- Network-level Session Hijacking

- The 3-Way Handshake
- Sequence Numbers
- Session Hijacking Tools
- Session Hijacking Tool: Zaproxy
- Session Hijacking Tool: Burp Suite
- Session Hijacking Tool: JHijack
- Session Hijacking Tools

Hacking Webservers

- Webserver Concepts
- Webserver Market Shares
- Open Source WebserverArchitecture
- Attack Methodology
- Webserver Attack Methodology
- Webserver Attack Methodology:Information Gathering
- Webserver Attack Methodology:Webserver Footprinting
- Counter-measures
- Countermeasures: Patches and Updates
- Countermeasures: Protocols
- Countermeasures: Accounts
- Countermeasures: Files and Directories
- How to Defend Against Web Server Attacks
- How to Defend against HTTP
- Response Splitting and Web Cache
- Poisoning
- Web Server Penetration Testing

Hacking Web Applications

- Web App Concepts
- Web Application Security Statistics
- Introduction to Web Applications
- SQL Injection Attacks
- Command Injection Attacks
- Web App Hacking Methodology
- Footprint Web Infrastructure
- Footprint Web Infrastructure:ServerDiscovery
- Hacking Web Servers
- Web Server Hacking Tool:WebInspect
- Web Services Probing Attacks
- Web Service Attacks: SOAP Injection
- Web Service Attacks: XML Injection
- Web Services Parsing Attacks
- Web Service Attack Tool: soapUI

SQL Injection

- SQLInjection Concepts
- SQL Injection
- Scenario
- SQL Injection Threats
- What is SQL Injection?
- SQL Injection Attacks
- SQL Injection Detection
- Types of SQL Injection
- Simple SQL Injection Attack
- Union SQL Injection Example
- SQL Injection Error Based
- Blind SQL Injection
- What is Blind SQL Injection?
- SQL Injection Methodology
- Advanced SQL Injection
- Information Gathering
- Extracting Information through ErrorMessages
- Interacting with the FileSystem
- SQL Injection Tools
- SQL Injection Tools: BSQLHacker
- SQL Injection Tools: Marathon Tool
- SQL Injection Tools: SQL PowerInjector
- SQL Injection Tools: Havij
- SQL Injection Tools

Hacking Wireless Networks

- Wireless Concepts
- Wireless Networks
- Wi-Fi Networks at Home and Public Places
- Types of Wireless Networks
- Wireless Encryption
- Wireless Threats
- Wireless Threats: Access Control Attacks
- Wireless Threats: Integrity Attacks
- Footprint the Wireless Network
- Attackers Scanning for Wi-Fi Networks
- Bluetooth Hacking
- Bluetooth Threats

Evading IDS, Firewalls, and Honeypots

- IDS, Firewall and Honeypot Concepts
- How IDS Works?
- Ways to Detect an Intrusion
- Denial-of-Service Attack (DoS)
- ASCII Shellcode
- Other Types of Evasion
- Evading Firewalls
- IP Address Spoofing
- Source Routing
- Website Surfing Sites
- Detecting Honeypots
- Detecting Honeypots

Buffer Overflow

- Buffer Overflow Concepts
- Buffer Overflow
- Shellcode
- No Operations (NOPs)
- Buffer Overflow Methodology
- Overflow using Format String
- Smashing the Stack
- Once the Stack is Smashed...
- Buffer Overflow Security Tools
- BoF Security Tool: BufferShield
- BoF Security Tools

Cryptography

- Cryptography Concepts
- Cryptography
- Types of Cryptography
- Government Access to Keys (GAK)
- Encryption Algorithms
- Ciphers
- Advanced Encryption Standard (AES)
- Public Key Infrastructure(PKI)
- Public Key Infrastructure (PKI)Certification Authorities
- Email Encryption
- Digital Signature
- SSL (Secure Sockets Layer)
- Transport Layer Security (TLS)
- Disk Encryption Tools
- Cryptanalysis Tool: CrypTool
- Cryptanalysis Tools
- Online MD5 Decryption Tool

Penetration Testing

- Pen Testing Concepts
- Security Assessments
- Security Audit
- Vulnerability Assessment
- Limitations of Vulnerability Assessment
- Introduction to Penetration Testing
- Penetration Testing
- Why Penetration Testing?
- Testing Locations
- Types of Pen Testing
- Types of Penetration Testing
- External Penetration Testing
- Internal Security Assessment
- Black-box Penetration Testing
- Grey-box Penetration Testing
- White-box Penetration Testing

Partners : ORACLE WORKFORCE DEVELOPMENT PROGRAM | redhat. CERTIFIED TRAINING PARTNER | UBI Unica Business and Innovation Centre | edexcel | Java

DUCAT®
development | consultancy | training

E-mail: info@ducatindia.com
Visit us: www.ducatindia.com
www.facebook.com/ducateducation

NOIDA
A-43 & A-52, Sector-16,
Noida - 201301, (U.P.) INDIA
70-70-90-50-90
+91 99-9999-3213

GHAZIABAD
1, Anand Industrial Estate,
Near ITS College, Mohan Nagar,
Ghaziabad (U.P.)
70-70-90-50-90

PITAMPURA (DELHI)
Plot No. 366, 2nd Floor,
Kohat Enclave, Pitampura,
(Near- Kohat Metro Station)
Above Allahabad Bank,
New Delhi- 110034.
70-70-90-50-90

SOUTH EXTENSION (DELHI)
D-27,South Extension-1
New Delhi-110049
70-70-90-50-90
+91 98-1161-2707

GURGAON
1808/2, 2nd floor old DLF,
Near Honda Showroom,
Sec.-14, Gurgaon (Haryana)
70-70-90-50-90