

Certified Ethical Hacking Program

for Cyber Security

Modules, Details & Fees

Total Modules- 30 (Highest in Industry)
Duration- 2-3 Months
Full Course Fees- 18,000/- (Pay in two Installments - 9500*2)

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

10 Reasons you Should Join DICC

1. Advance Level Ethical Hacking
2. EC-Council Certified Trainer
3. Modules Covered: 30 - 2020 Updated
4. 90% Practical Training
5. Latest Software Toolkits + Study Material
6. Flexible Timings
7. 100% Placement Support
8. Free demo Class available
9. Future Support for Students

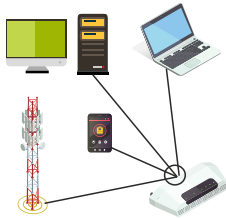
10. DICC Institute Certification

01	Introduction to Hacking	→	
02	Networking Concepts	→	
03	Virtualization (Lab Setup)	→	
04	Kali Linux	→	
05	CyberLaws	→	
06	Reconnaissance	→	
07	Scanning Networks	→	
08	Enumeration	→	
09	Anonymity	→	
10	Vulnerability Assessment	→	
11	System Hacking	→	
12	Mobile Hacking	→	
13	Virus and Worms	→	
14	Trojans & Payloads	→	
15	Steganography	→	
16	Sniffing Spoofing	→	
17	Phishing	→	
18	Denial-of-Service	→	
19	Session Hijacking	→	
20	Hacking Web Servers	→	
21	SQL Injection	→	
22	(XSS) Cross Site Scripting	→	
23	Wi-Fi Hacking	→	
24	Bug Bounty Process	→	
25	IoT Hacking	→	
26	Cloud Computing	→	
27	Firewalls, and Honeypots	→	
28	(CTF) Penetration Testing	→	
29	Cryptography	→	
30	Live Project Work	→	



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?



Networking Concepts

- 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



Virtualization (Lab Setup)

- Windows, Linux OS for Usage & Test
- Setting up Vulnerable Machines
- Create Network in VMs
- Share Data in Network
- Android Lab Virtualization
- Problem Handling
- Various types of Virtualization Programs



Kali Linux

- 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



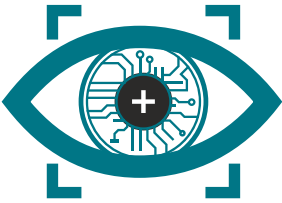




CyberLaws


- Introduction to Cyber laws
- What is IT Act 2000
- Types of Cyber crimes
- Evolution of Cyber Law in India





Reconnaissance

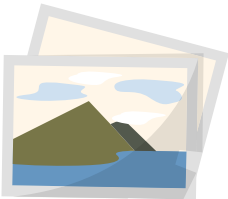
- Gathering Information
- IP Mapping and Tracing IP address
- Active and Passive Methods
- Detecting Web Server and there Location
- Find Login Pages, eMail Login, Cpanel, Admin
- Hacking Using Google and other Search Engines

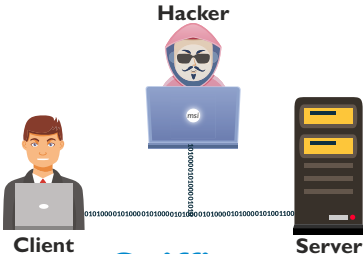
 <p>Scanning</p>	<ul style="list-style-type: none"> • Detection of Alive IP Addresses • Port scanning techniques • Advance Trace route • Discovering with SYN,ACK, UDP, ICMP,ARP • ARP (MAC Address scanning) • Packet Crafting • Aggressive detection
 <p>Enumeration</p>	<ul style="list-style-type: none"> • Extract User Names Using Email Ids • Extracting Information Using the Default Passwords • Brute Force Active Directory • Extract Username Using SNMP • Extract Information Using DNS Zone Transfer • Running services Detection
 <p>Anonymity</p>	<ul style="list-style-type: none"> • How hackers hide their identity • Working with Proxy Server & Configuration • Types HTTP,HTTPS, SOCK Protocols • OpenVPN Client & Server Setup • Proxy Chains & RELAYING the Traffic • Understanding of TOR & Deepweb Network • Anonymous Browsers
 <p>Vulnerability Assessment</p>	<ul style="list-style-type: none"> • Types of vulnerability assessments • Network-based scans • Host-based scans • Wireless network scans • Application scans • Database scans
 <p>System Hacking</p>	<ul style="list-style-type: none"> • OS Authentication Architecture • OS Hash BruteForcing • OS Password Cracking • Windows Login Bypass • OSX Login Bypass • BadUSB Attacks







 <p>Mobile Hacking</p>	<ul style="list-style-type: none"> • Hacking Android OS • Android Rooting Tools • Hacking Networks Using Network Spoofer • Android-based Sniffers • Mobile Spyware • Android Trojans • Securing Android Devices • Mobile Pen Testing Toolkit
--	--


 <p>Virus and Worms</p>	<ul style="list-style-type: none"> • Types of Viruses and Worms • Creation of Viruses and Worms • Ransomware Analysis • Detection of Viruses and Worms • Recover from Ransomware Attack
---	--


 <p>Trojans & Payloads</p>	<ul style="list-style-type: none"> • Making of Trojan(RAT) • Embed Trojan Word/Excel Macro- Files • Non-Macro Office Files - DDE • Shellcode vs DLLs • Migrating Processes • Bypass AV and Network Detection • Hidden Encrypted Payloads
---	---


 <p>Steganography</p>	<ul style="list-style-type: none"> • How Steganography Works • Types Of Steganography • Steganography In Image • Steganography In Audio • Steganography In Video • Online challenge • Countermeasures and detection
---	--


 <p>Sniffing Spoofing</p>	<ul style="list-style-type: none"> • Introduction to Network Sniffing • Man in the Middle Attacks • MAC spoofing & Flooding • ARP Poisoning • Rogue DHCP • SSL Stripping • DNS Spoofing
---	--


 <p>Phishing</p>	<ul style="list-style-type: none"> • Social Engineering • Desktop Phishing • Spear Phishing • SEToolKit • Punycode url
 <p>Denial-of-Service</p>	<ul style="list-style-type: none"> • How DoS Attack Works • Indications of DoS Attacks • DoS Attack Techniques • Tools for DDoS Attacks • Detection of Attacks
 <p>Session Hijacking</p>	<ul style="list-style-type: none"> • Session Hijacking Concepts • Key Session Hijacking Techniques • Session Hijacking Process • Packet Analysis of a Local Session Hijack • Session Hijacking Tools
 <p>Hacking Web Servers</p>	<ul style="list-style-type: none"> • Webserver Concepts • Website Defacement • Webserver Attacks • Attack Methodology • Webserver Attack Tools
 <p>SQL Injection</p>	<ul style="list-style-type: none"> • 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
 <p>(XSS) Cross Site Scripting</p>	<ul style="list-style-type: none"> • How XSS Attacks Work • XSS Attack via Email • Stealing Cookies via XSS • XSS Attack in Comment Field • Blog Post via XSS Attack • CSRF Attacks


 <p>Wi-Fi Hacking</p>	<ul style="list-style-type: none"> • 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
---	--

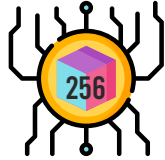
 <p>Bug Bounty Process</p>	<ul style="list-style-type: none"> • Pick a program • Find a target via recon • Hit the target and find a vulnerability • Write the report • Get paid
--	--


 <p>IoT Hacking</p>	<ul style="list-style-type: none"> • IoT Concepts • IoT Attacks • IoT Hacking Methodology • IoT Hacking Tools
---	---

 <p>Cloud Computing</p>	<ul style="list-style-type: none"> • Cloud Computing Concepts • Cloud Computing Threats • Cloud Security • Cloud Security Tools
---	---

 <p>Firewalls, and Honeypots</p>	<ul style="list-style-type: none"> • Introduction to Firewalls • Network Firewalls • Web Application Firewalls • Weakness in Firewalls • Honey Pots and Security Misconfiguration
--	--

 <p>Catch the flag (CTF)</p>	<ul style="list-style-type: none"> • What is capture the flag hacking? • CTF Preparedness • Types of Events • Types of Challenges • How To Participate in a CTF Event? • Examples • How Can I Learn More About CTF?
--	--

 Cryptography	<ul style="list-style-type: none"> • Introduction to Cryptography • Key terms • Symmetric cryptography: • Asymmetric cryptography/Public key cryptography • Hash Algorithms
---	--

 Live Project Work (PenTest)	<ul style="list-style-type: none"> • Need of Penetration Testing? • Types of Pen Testing • Pen Testing Techniques • Security Audit • Vulnerability Assessment • Black Box Pen Testing • Gray Box Pen Testing
---	---

<p style="text-align: center;">SOME TOOLS we use</p>			
 Nessus vulnerability scanner	 Metasploit		
 SHODAN	 OWASP ™		
 nexpose ®	 w3af <small>Web Application Attack and Audit Framework</small>		
 WireShark	 Zaproxy		
 BURPSUITE PROFESSIONAL	 Hydra		
 acunetix	 netcat	 AIRCRAK-NG	 OWASP
 NMAP	 EeEF	 OpenVAS <small>Open Vulnerability Assessment System</small>	
 VEIL	 John the Ripper	 Bettercap	 Ettercap
<p style="text-align: center;">and many more...</p>			