

## Cyber Security & Ethical Hacking

### Modules, Details & Fees

Duration :- 6 Months

Modules :- 30 (Highest in Industry)


Course Fees :- 49,000/- (Pay in Installments also)

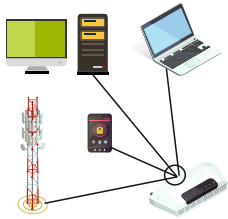
<b>Batches Options</b>	Regular Batches	Monday to Thursday
	Alternate Batches	3 Days a Week
	Weekend Batches	Saturday & Sunday
	Sundays Bahches	Only Sunday
<b>Online Classes Also Available</b>		


### 10 Reasons you Should Join DICCC


1. Beginner to Elite Level Training
2. Experienced and Certified Trainer
3. Modules Covered: 30 - 2023
4. 80% Practical Training
5. Software Toolkits + Study Material
6. Flexible Timings
7. 100% Placement Support
8. Backup Classes Available
9. Future Support for Students
10. Certifications


- 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 →
- 25 IoT Hacking →
- 26 Cloud Computing →
- 27 Firewalls, and Honeypots →
- 28 Challenges →
- 29 Cryptography →
- 30 Penetration Testing →


 <p>Introduction</p>	<ul style="list-style-type: none"> <li>• Important Terminology</li> <li>• Ethical Hacking vs. Hacking</li> <li>• Effects of Hacking on Business</li> <li>• Why Ethical Hacking Is Necessary</li> <li>• Skills of an Ethical Hacker</li> <li>• What Is Penetration Testing?</li> </ul>
---	---

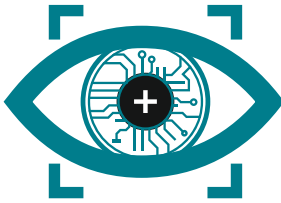
 <p>Networking Concepts</p>	<ul style="list-style-type: none"> <li>• Various types of network topologies</li> <li>• Dissimilar type of Network Devices</li> <li>• Protocols &amp; Port numbers</li> <li>• IP Addressing and its classes</li> <li>• VPN Network, DHCP Server</li> <li>• DNS Server, OSI Model</li> <li>• Server Configuration</li> </ul>
--	---

 <p>Virtualization (Lab Setup)</p>	<ul style="list-style-type: none"> <li>• Windows, Linux OS for Usage &amp; Test</li> <li>• Setting up Vulnerable Machines</li> <li>• Create Network in VMs</li> <li>• Share Data in Network</li> <li>• Android Lab Virtualization</li> <li>• Problem Handling</li> <li>• Various types of Virtualization Programs</li> </ul>
--	--

 <p>Kali Linux</p>	<ul style="list-style-type: none"> <li>• Kali Linux Vs Other Pen Testing OS</li> <li>• Installation and setup of Kali Linux</li> <li>• System Architecture of Kali Linux</li> <li>• Network Configuration of Kali Linux</li> <li>• Essential Commands of Kali Linux</li> </ul>
---	--

 <p>CyberLaws</p>	<ul style="list-style-type: none"> <li>• Introduction to Cyber laws</li> <li>• What is IT Act 2000</li> <li>• Types of Cyber crimes</li> <li>• Evolution of Cyber Law in India</li> </ul>
--	---

 <p>Reconnaissance</p>	<ul style="list-style-type: none"> <li>• Gathering Information</li> <li>• IP Mapping and Tracing IP address</li> <li>• Active and Passive Methods</li> <li>• Detecting Web Server and there Location</li> <li>• Find Login Pages, eMail Login, Cpanel, Admin</li> <li>• Hacking Using Google and other Search Engines</li> </ul>
---	--



### Scanning

- 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



### Enumeration

- 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



### Anonymity

- 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




### Vulnerability Assessment


- Types of vulnerability assessments
- Network-based scans
- Host-based scans
- Wireless network scans
- Application scans
- Database scans




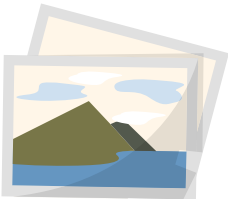
### System Hacking

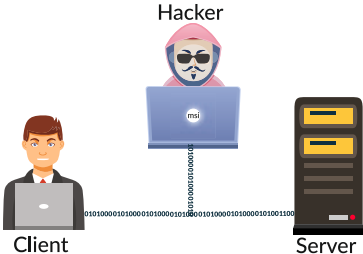
- OS Authentication Architecture
- OS Hash BruteForcing
- OS Password Cracking
- Windows Login Bypass
- OSX Login Bypass
- BadUSB Attacks

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

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

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

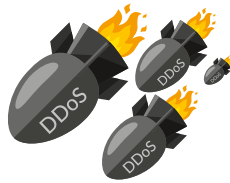
 <p><b>Steganography</b></p>	<ul style="list-style-type: none"> <li>• How Steganography Works</li> <li>• Types Of Steganography</li> <li>• Steganography In Image</li> <li>• Steganography In Audio</li> <li>• Steganography In Video</li> <li>• Online challenge</li> <li>• Countermeasures and detection</li>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

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



## Phishing

- Social Engineering
- Desktop Phishing
- Spear Phishing
- SEToolKit
- Punycode url



## Denial-of-Service

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



## Session Hijacking

- Session Hijacking Concepts
- Key Session Hijacking Techniques
- Session Hijacking Process
- Packet Analysis of a Local Session Hijack
- Session Hijacking Tools



## Hacking Web Servers

- Webserver Concepts
- Website Defacement
- Webserver Attacks
- Attack Methodology
- Webserver Attack Tools



## 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



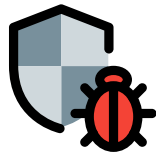
## (XSS) Cross Site Scripting

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



## 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



## Bug Bounty

- Pick a program
- Find a target via recon
- Hit the target and find a vulnerability
- Write the report
- Get paid



## IoT Hacking

- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools



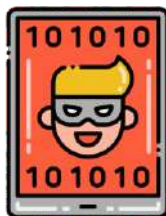
## Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Security
- Cloud Security Tools



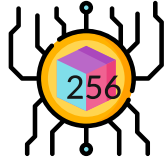
## Firewalls, and Honeypots


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



## Challenges

- 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?

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

 <b>Penetration Testing</b>	<ul style="list-style-type: none"> <li>• Need of Penetration Testing?</li> <li>• Types of Pen Testing</li> <li>• Pen Testing Techniques</li> <li>• Security Audit</li> <li>• Vulnerability Assessment</li> <li>• Black Box Pen Testing</li> <li>• Gray Box Pen Testing</li> </ul>
---	---

<p>SOME <b>TOOLS</b> we use</p>			
			
			
			
			
			
			
			
			
<p><b>and many more...</b></p>			