iEHCS™

i3indya Ethical Hacking & Cyber Security

i3indya™ Technologies

Innovation • Intelligence • Information

One of the FAVOURITE PLACE of Engineers/Professionals..!

i3indya Ethical Hacking & Cyber Security

Course	:	i3indya Ethical Hacking & Cyber Security (iEHCS)
Certification	:	Participation Certificate by i3indya™ Technologies
Study Material	:	Books & CD Free to each participant

FEES & DURATION

1. For iEHCS **(Advance Module 1.1)**
Duration: 15 Days/45 hrs
Fees: INR 5,700/- (including taxes) per candidate

2. For iEHCS **(Advance Module 1.1 + 1.2)**
Duration: 30 Days/90 hrs
Fees: INR 11,628/- (including taxes) per candidate

3. For iEHCS **(Advance Module 1.1 + 1.2 + 2)**
Duration: 40 Days/120 hrs
Fees: INR 16,188/- (including taxes) per candidate

ADVANCE MODULE 1.1 – Ethical Hacking & Cyber Security   **(15 Days)**

DAY	TOPICS	TIMING
1	**Fundamental of Ethical Hacking** • Hacking Vs. Ethical Hacking • Types of Hackers • Skill Profile of a Hacker • Some Famous Hackers and Groups • Cyber World • Advantage and Disadvantage of Cyber world • Cyber World as a Home of hackers	**3 Hours**
2	**Overview of Cyber Law** • Introduction To Cyber Law • Cyber Laws Indian • Technical Aspect Of Indian Cyber Law • IT ACT 2000 & 2008 • Internet Crimes And Frauds • Cyber Law Cases In India • Organization Under Cyber Laws • Advantages Of Cyber Laws	**2 Hours**
3	**Information Gathering** • What Is Information Gathering & Why Hackers Need This? • Types Of Information Gathering • Information Gathering Using Websites • Information Gathering Using Software • Information Gathering Using Add-Ons • Search Engines- Smart Way Of Information Gathering • Scanning And Enumeration • Tracing - E-Mail, Mobile Phone, Intruder	**5 Hours**

4	**Virtualization & System Cloning**
	• Introduction Of Virtualization
	• Need & Use Of Virtualization
	• Virtualbox
	    • Installation
	    • Configuration
	    • Maintenance
	• Installing OS On Virtual Machines
	• Networking In Virtual Machines
	• System Cloning
	• Troubleshooting
	• Other Tools For Virtualization
		3 Hours

DAY	TOPICS	TIMING
5	**Windows Hacking & Security (Win 8 & Win 7)** • Windows OS & Security • Hacking Into System By Changing Passwords • Getting Access To System By Elevating Privileges • Finding Out The Passwords Of Windows • Bypassing The Windows Security • Hack from Guest to Admin • Password in Plain Text Directly • Hacking By USB Devices • Mitigation Of System Attacks • Setting Up A Secure System	5 Hours
6	**Password Cracking Techniques** • What is Password Cracking • Types of Password Cracking Techniques • How Different Password Crackers Work • Windows Password Cracking • FTP / Network Password Cracking • Zip/ RAR Password Cracking • Doc & PDF Password Cracking • Using GPU For Password Cracking • Password Security	3 Hours
7	**Data Hiding Techniques** • What Is Steganography • How Attacker Hides His Data In Images And Other Formats • How To Find Data Which Are Hidden • What Is Cryptography • Advanced Cryptography Tools • How Are Programs And Data Wrapped • Secure Measures To Protect Our Data	3 Hours

8	**Hacking By Batch Programming & Scripting**
	• Basics Of Scripting
	• Languages Used In Scripting
	• Writing Your First Program
	• Malacious Program Scripting
	    • Process Killer
	    • Firewall Killer
	    • Antivirus Killer
	    • System killer
	• Session Hijacking Using Batch Scripting
	• Data Theft Using Batch Script
	• Automation Using Scripting
	• Designing Tools Using Scripting
	• Developing Security Tools Using Scripting.
		3 Hours

DAY	TOPICS	TIMING
9	**Hacking by Viruses, Trojans, Keyloggers & Spywares** • What is Trojan? • Trojans Attack Big Famous Cases • Types Of Trojans • Different way a Trojan Can Get Into A System • How We Create A Trojan and Control System • How Attacker Bypass Your Antivirus By Trojans • Analysis Of Trojans/Virus • How we remove Trojans Manually • Security Against Trojans	**4 Hours**

10	**Malware Analysis & Fake Antivirus Detections**
	• Introduction of Malware
	• Types of Malware
	• Common Malwares In Cyber
	• Types of Malware Analysis
	    • Behavior Analysis
	    • Code Analysis
	• Manual Malware Analysis
	• Tools for Malware Analysis
	• Countermeasures
		3 Hours

11	**IDS, IPS and Honeypots** • Overview of IDS, IPS & Honeypot • Use of IDS & IPS • Installation of IDS & IPS • Prevention & Detection • Honeypot & its Types • Implementation - Honeypots • Honeypot Tools	**3 Hours**
12	**Proxy Server & Virtual Private Network (VPN) Technology** • Proxy And Types Of Proxies • Why Hackers Use Proxy? • How To Hide IP Address While Chatting • How To Open Block Website In College/Companies • Convert Your Machine As Proxy Server With HTTPS Proxy • Advantage And Disadvantage Of Proxy • Analyzing Proxy Bug • How Proxy Hack Your Passwords Etc • What Is Better Than Proxy • What Is VPN? • Why We Use VPN • Advantage & Disadvantage Of VPN • Free VPN • Countermeasures	**3 Hours**

DAY	TOPICS	TIMING
13	**Google Database Hacking** • Introduction And Working Of Search Engines • List Of Common Search Engines On Web • Comparing And Choosing Best Search Engine • Dorks For Hacking Search Engines • Tools For Search Engines Hacking • Web Ripping • Finding Admin Pages And Weakness In Site • Security Against Search Engine Hacking	**3 Hours**

ADVANCE MODULE 1.2 – Ethical Hacking & Cyber Security (15 Days)

DAY	TOPICS	TIMING
14	**Email Hacking & Security Issues** • World Famous Big Email Hacking Cases • IIT Bombay Alumni, Anil Ambani, Rahul, Gandhi, Facebook CEO Mark Zuckerberg (Case Study) • Analysis Email Attacks (Live Demo) Manually & Automatic • Cookies Stealing (Session Hijacking) of All Big Mail Servers • Phishing Attacks (Normal & Advanced) • Tab Nabbing Attack • Social Engineering Attack • Analyzing the Vulnerabilities of Email Servers • Analyzing Fake & Real Profiles & Email Accounts • Fake Mailing Attack • Email & Fake Profile Tracing • Hacker Email Backdoor Installing Technique For Future Access • Email Password Stealing By Plugins, Extensions Etc. • Email Hacking By Keylogger, Spywares & Malicious Softwares • Countermeasures	**6 Hours**

15	**Facebook Hacking, Security & Forensic**
	• World Famous Big Facebook Hacking Cases
	• Cookies Stealing of Facebook Accounts
	• Facebook Phishing Attacks
	    • Normal Phishing Attack
	    • Advanced Phishing Attack
	    • Normal & Advanced Security
	• Facebook Tab Nabbing Attack
	    • Normal & Advanced Tab Nabbing Attack
	    • Identify & Disable Tab Nabbing Attack
	    • Security Against Tab Nabbing Attack
		6 Hours

DAY	TOPICS	TIMING

	• Facebook Social Engineering Attack
	    • Facebook Forget Password Attack
	    • Facebook Guessing Attack
	    • Facebook Password Cracking With the Help of Social Engineering
	
	• Analyzing Fake & Real Profile of Facebook
	• Delete Spam Messages on Facebook
	• Facebook Fake Messaging Attack
	• Facebook Tracing Method Techniques (Basic & Advanced)
	• Facebook Backdoor Installing Technique For Future Access
	• Facebook Password Stealing By Plugins, Extensions Etc.
	• How to find if your Facebook Account has been hacked or not
	• Facebook Account security with Email & SMS Notifications
	• How to Hack Password using Facebook Hacker
	• Hack Facebook account password with key logger
	• Facebook Security & Forensics	

16	**Clickjacking & Tabnabbing Attacks** • What Is Clickjacking • How Does A Clickjacking Work • Facebook Likejacking • How Hacker Use Clickjacking • Execution Of Malicious Code Into Machine • Possibilities Of Clickjacking • Clickjacking Killer - The IFRAME Buster • How Protect From Being Clickjacked	**3 Hours**

17	**Advanced Methodology for Privacy on Internet**
	• Staying Safe in the Internet
	    • Browser Settings
	    • Using Add-ons & Plug-ins
	
	• Email Privacy
	• Malicious Link Security
	    • Behavior Based
	    • Code Based
	
	• Website Visit Privacy
	• Block Malicious Contents On Web
	• Antivirus Privacy
	• Automatic analyzing of Malicious Links
	• Internet Privacy Tools
		3 Hours

DAY	TOPICS	TIMING

18	**Social Engineering**
	• Introduction to Social Engineering
	• Types of Social Engineering
	    • Tools Based
	    • Manually
	• World's Biggest Social Engineering Cases
	• Web based Social Engineering
	• Vulnerability in Social Engineering
	• Analyzing a Social Engineering Attack
	• Security against Social Engineering
		3 Hours

19	**Android Hacking, Security & Forensics** • Introduction to Android • Android OS Structure • Overview of Android Apps • Android Rooting • Application Cracking of Android • Cracking PIN of Android Devices • Pattern Unlock Cracking • Android Security • Android Forensics • Countermeasures	5 Hours
20	**Credit Card Frauds & Cases** • Introduction of Plastic Money • Some Big Credit Card Cases Solved by i3indya Team • Type of Credit Card • Hacker's Credit card Theft Techniques • Online & Offline Credit Card Generators • Vulnerability In Credit Card & Payment Gateway • Big Credit Card Fraud Website on Internet • Detection of Credit Card Fraud • Security Against Credit Card Fraud • Countermeasures	3 Hours
21	**Website & Database Hacking Attacks** • Introduction of Websites & Database • Authentication Process Of Web Application • Attack on Website & Web Application • SQL Injection Attacks • PHP Injection Attacks • Java Script Injection • Scripting Attacks • RFI & LFI Attacks • Countermeasures	6 Hours

DAY	TOPICS	TIMING

22	**Web Server Hacking & Security**
	• Introduction of Webserver
	• Types of Webserver
	• Setting up a Webserver
	    • Locally
	    • Remotely
	    • Hosting C-Panel & Other Panels
	    • Database Configuration
	• Webserver Exploits
	    • Public Exploits
	    • Private Exploits
	• Shell (Control Panel) Designing & Uploading
	• Web Server Routing
	• Backdoor Installation on Server
	• Server Passwords Hacking
	• Web Server Security Against Attacks
		3 Hours

23	**Vulnerability Assessment & Penetration Testing Tools & Methodologies** • What is VA & PT • Difference between VA & PT • Need of VA & PT • Penetration Testing Methodology • Types of Penetration Testing • Scope of Pen-testing • Why Penetration Testing • Manual VA-PT • Tool Based VA-PT • Reporting a VA-PT • Available VA-PT Platforms • Closed Source Platform • Open Source Platforms • Benefits of Open Source Over Closed Source • Backtrack - VA-PT • Bugtraq - VA-PT • Some Other Recommended VA-PT Tools	**5 Hours**
24	**Wireless Hacking & Countermeasures** • Wireless Standards • Common Vulnerabilities in Wireless Devices • Encryption Standards Used in Wi-Fi • WEP Cracking • WPA/WPA2 Cracking • WPS Cracking • Countermeasures	**4 Hours**
	Exam – Theory & Practical	

ADVANCE MODULE 2 – Ethical Hacking & Cyber Security   (10 Days)

DAY	TOPICS	TIMING
25	**Linux Hacking & Security** • Introduction To Linux OS • Installation, Configuration & Maintenance • Resetting Your Linux Password • Grub Password Hacking • FTP & SSH Password Cracking • Security Against Files • Security Against Linux Systems • IP Table Configuration (Advanced) • OS Hardening • Troubleshooting	6 Hours
26	**Macintosh Hacking & Forensic** • Introduction of Mac • Architecture of Mac • Mac Password Cracking without any tool • Mac Password cracking with tool • Installing Backdoor in Mac • Data Recovery in Mac • Securing Mac System	5 Hours
27	**Switch & Router Devices Hacking** • Introduction to Switch & Router • Vulnerabilities in Switch & Router • Exploiting Switch & Router Vulnerability • Switch & Router Password Cracking With & Without Tool • Backdoor Installation • Securing Switch & Router	3 Hours
28	**Network Security & Hacking** • Introduction To Networks (LAN /WAN) • Understanding Communication Protocols • Sniffing Attacks • DOS & DDOS Attack • Mis-configuration • Firewall Configuration & Maintenance • Network Monitoring & Analysis • Logs Maintenance	3 Hours
29	**Cyber Forensics Investigations & Evidence Recovery** • Introduction to Forensics • Incidence Response and Computer Forensic • Windows Live Response • Linux Live Response • Web Browser Forensics • Network Forensic • Disk Imaging • Data Recovery Using Tools • Forensic Analysis & Chain of Custody Form	6 Hours

DAY	TOPICS	TIMING
30	**Audio, Video & Image Forensics** • Introduction to File formats • Analyzing Files • Detecting Modified Files • Extract Hidden Data from Files • Audio & Video Enhancement • Integrity Checking	**2 Hours**

31	**Cyber Crime Investigation**
	• Introduction of Cyber Crime
	• Need of Cyber Crime Investigation in Cyber World
	• Types of Cyber Crime
	    • Online Crime investigation
	    • Offline Crime Investigation
	• Solving Different Cyber Cases
	    • Email Hacking Case
	    • System Hacking Cases
	    • Credit Card Cases
	    • Privacy & Data Theft Cases
	    • Fake Profile Cases
	    • Software Piracy Cases
	    • Pornography Cases
	    • Identity Theft Cases Etc.
		4 Hours

32	**Case Study (Live Demo By i3indya Team)**	**3 Hours**
	EXAM – Theory & Practical	

Why Ethical Hacking & Cyber Security?

1. Very useful for candidates seeking career in **Information Security / Cyber Security.**

2. Important for Corporate / Working Professionals to **secure** their **cyber space.**

3. It helps you to defend against **attacks** from **Hackers & Crackers.**

4. To **catch a thief** you have to **think like a thief.**

Why Ethical Hacking & Cyber Security @ i3indya Technologies?

1. Latest and Updated Topics are covered.

2. New Topics like Hacking & Securing Linux, Android, Mac, Web Servers are taught.

3. We concentrate not only on Hacking but also on Security of all Topics.

4. Forensics on almost all platforms and devices are taught.

5. Hands on training with live demonstrations.

6. Well experienced Trainers.

7. Tied up with several government organizations for Training and Consultancy.

8. Trained more than 30000 professionals from all over India.

9. Providing training to CBI, NIA and State Police across India.

10. We limit our tool usage from third-party and we provide manual approach for each Technique.

11. We also design our own tools.

Pre-Requisites

1. Basics of Computer

2. Knowledge of how to use internet

3. Basics of Networking

Recommendation

It is strongly recommended to bring your own LAPTOP during the training so that you can easily practice the exercises at home.