

iGNITE
Technologies



ETHICAL TRAINING HACKING

ABOUT



Well-Known Entity for Offensive Security

{***Training and Services***}

ABOUT US

With an outreach to over a million students and over thousand colleges, Ignite Technologies stood out to be a trusted brand in cyber security training and services

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.

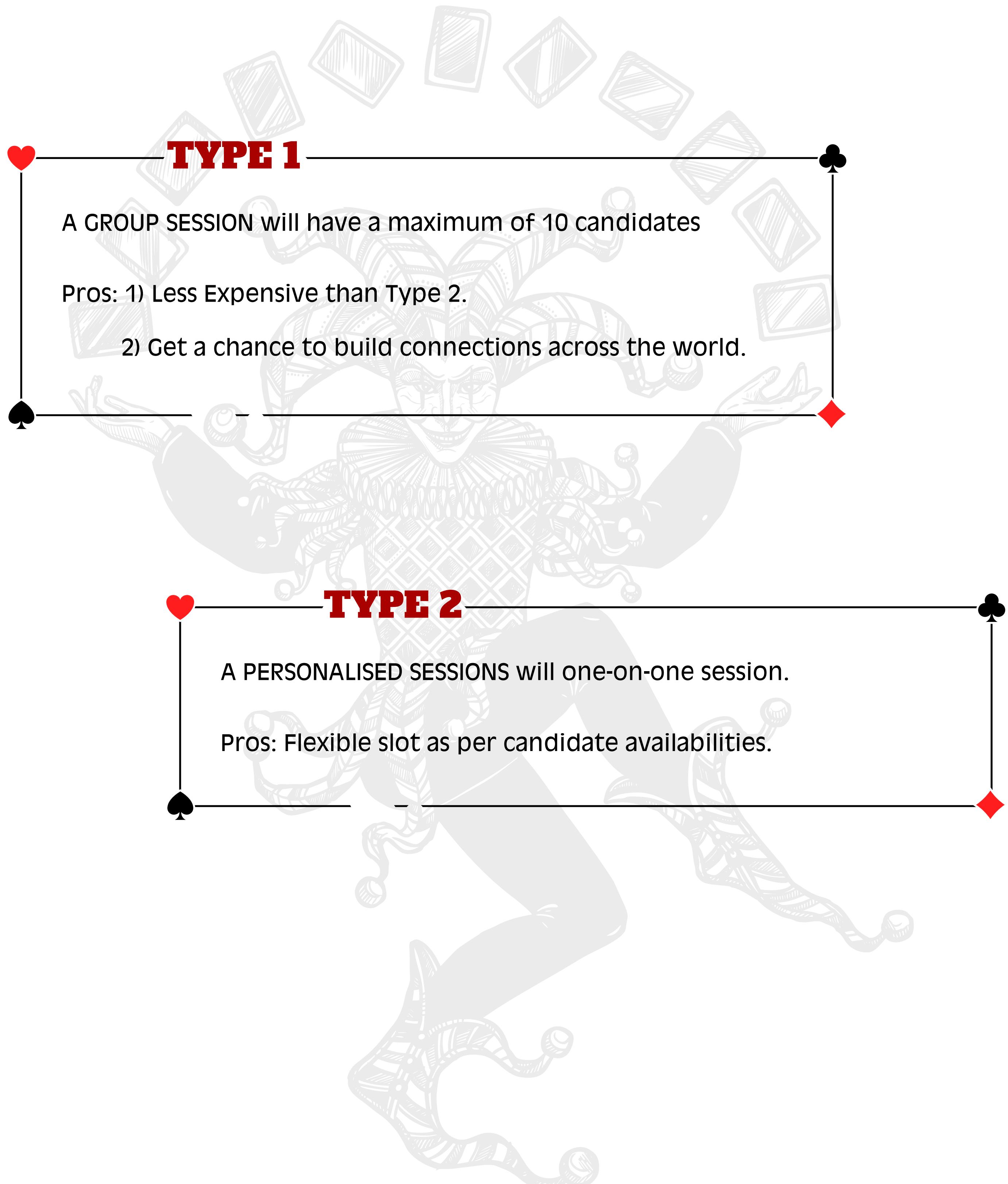
ETHICAL HACKING



People interested in learning about cyber-attacks and risks should take the course, Ethical Hacking. It offers a comprehensive understanding of realistic attackers' hacking strategies and methods.

Most businesses employ ethical hackers to do penetration tests with a hacker mindset and disclose infrastructure vulnerabilities and misconfigurations. Beginners who wish to learn about the techniques and tools used by attackers and penetration testers in cyber-attacks should take this course.

HOW WE FUNCTION: TRAINING TYPE





Target Audience

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator



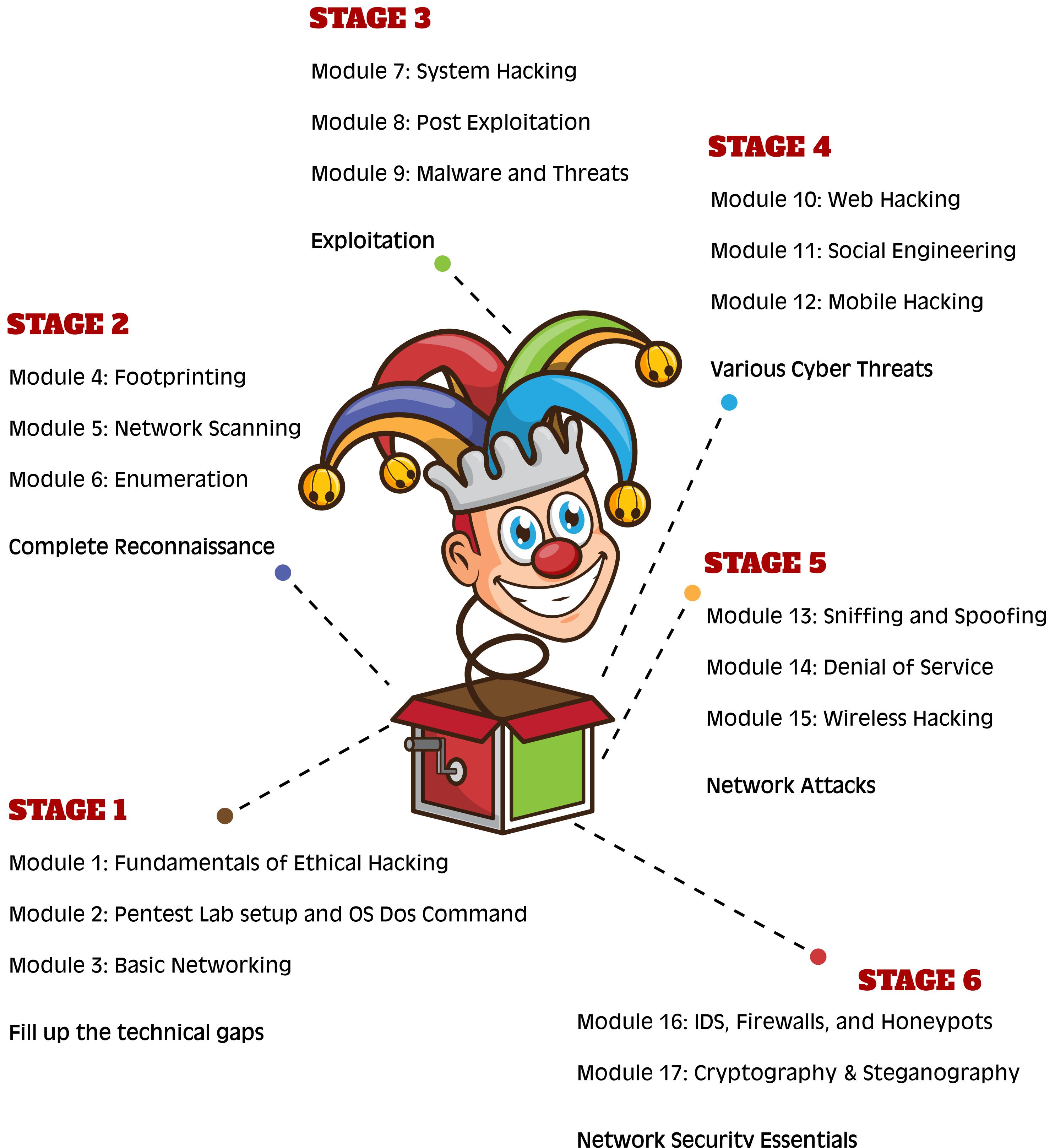
Why Ignite Technologies

- Level each candidate by providing the fundamental knowledge required to begin the Ethical Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide real-time exposure.
- Get a training certificate of participation.



COURSE DURATION: 32 HOURS

TECHNICAL ROADMAP



STAGE 1

In this Stage, the trainer will focus on the primary skills required to fulfil prerequisites for ethical hacking by providing conceptual and practical sessions on the following Modules.

Module 1: Fundamentals of Ethical Hacking

This module describes all methods, techniques, approaches and standards used by attackers. Moreover, will give an overview of the Risk, threats and Vulnerabilities.

Key pointers:

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts and their Types
- Penetration Testing Concepts and their Types
- Scope of Ethical Hacking

Module 2: Pentest Lab setup and OS Dos Command

This module will help the candidate to implement the Virtual lab environment for hands-on learning including basic OS installation for Windows and Linux platforms.

Key pointers:

- Fundamental of VMware and Virtual Box
- VM Network Setting (NAT/Bridge/Host-only)
- Virtualization of Windows and Linux
- Installation of Kali Linux
- Command Kung-fu for Windows and Linux

Tools: VMware and Virtual Box

OS: Windows, Linux and Kali Linux

Module 3: Basic Networking

This module will help to understand well-known Ports and Protocols used in network concepts. Although it will focus on key areas of networking required for the Network Hacking Concept.

Key pointers:

- Fundamental IP Address & Subnet Mask
- Network Devices
- OSI Layer Model vs TCP|IP Model
- ARP, ICMP, TCP, UDP protocol
- TCP Flags
- TCP 3-way handshake
- Well known Services Port

STAGE 2

In this stage, the trainer will focus on various techniques and tools used for information gathering to perform Recon with the help of Footprinting, network Scanning and Enumeration by providing conceptual and practical sessions on the following Modules.

Module 4: Footprinting

In this module, the candidate will learn how to gather information against their target with the help of online tools available on the Internet to fetch the information available on the web.

Key pointers:

- OSINT Framework
- Email Footprinting
- DNS Footprinting
- Web FootPrinting
- Google Hacking Database

Tools: Shodan, Whois, DNS Dumpster, Exploit DB, Hunter, iplogger, OSINT, Httrack and similar alternative tools

Module 5: Network Scanning

This module will help the candidate to learn network scanning to identify live hosts, OS, ports, installed services and their versions.

Key pointers:

- Host Discovery
- OS Fingerprinting
- Subnet Scanning
- Default Scan
- Stealth Scan
- TCP Scan
- UDP Scan
- Specific port Scan
- ALL port Scan
- Version Scan
- Script Scan
- Decoy Scan
- Fast Scan
- Time Scan
- Aggressive Scan

Tools: Nmap, netdiscover, Zenmap, advanced IP scanner and similar alternative tools.

Module 6: Enumeration

This module will help the candidate to collect gather juicy information for installed services running inside a host machine.

Key pointers:

- NetBios Enumeration
- FTP Enumeration
- SMB Enumeration
- Telnet Enumeration
- SMTP Enumeration

Tools: Nmap, Rpcclient, SMBmap, SMBclient, NBTScan and similar alternative tools

STAGE 3

In this stage, the trainer will focus on various tools and techniques used by hackers to compromise the target machine by providing a conceptual and practical session on the following Modules.

Module 7: System Hacking

The module primarily focuses on techniques used by an attacker to compromise the target machine with the help of Metasploit Framework and other tools.

Key pointers:

- Scanning Vulnerability
- Exploiting Vulnerability
- Password Brute Force
- Creating Malicious File Type (eg: Exe, Elf, apk)
- Metasploit Framework – Auxiliaryes, Exploits, Payloads Post Modules and meterpreter
- Msfvenom Framework

Tools: Metasploit, Msfvenom, Netcat

Module 8: Post Exploitation

This module will help the candidate complete the objective of Hacking a system from an attacker's point of view.

Key pointers:

- Post Enumeration
- Gathering System information
- Gathering User Information
- Download and Upload operations
- Process Migrate
- Web Camera Hacking
- Collect Stored Credentials (System, Browser, Wifi)
- Privilege Escalation to gain Administrator Access
- Hashdump
- Clear Event logs
- Persistence to maintain permanent access

Tools: Metasploit Post Modules

Module 9: Malware and Threats

This Module will help candidates to understand the different behaviours of various types of malware and analysis malicious process behind their execution.

Key pointers:

- Malware Concept
- Techniques used for Spreading Malware
- Trojan Concept Vs Virus and Worm
- Payload Binders and Crypter
- Countermeasures
- Malicious Process Analysis

Tools: Trojans RAT, Virus Total, TCP View, Process Explorer, Ad blocker

STAGE 4

Module 10: Web Hacking

This module will define Standards and tools used by hackers to exploit websites by injecting malicious code or commands.

Key pointers:

- Introduction to Web Server and Web Applications
- Well Known web servers and CMS
- Introduction to OWASP
- Website Scanning
- Introduction to burpsuite
- SQL injection
- Cross-Site Scripting
- Remote command Execution
- Brute Force

Tools: Wappalyzer, Burpsuite, Sqlmap, Nikto

Module 11: Social Engineering

This module will focus on techniques used by attackers to perform social engineering to gather target-sensitive information through phishing and impersonation.

Key pointers:

- Social Engineering Concepts
- Social Engineering Techniques
- Email Spoofing
- Geolocation
- Credential Harvesting
- Haveibeenpwned
- Detect a phishing attack

Tools: Social Engineering Toolkit, Phishtank, Mxtool box, Iphlogger

Module 12: Mobile Hacking

This Module will focus on the real-time application used to compromise the mobile device to spy on someone's activity.

Key pointers:

- Kali Linux NetHunter
- Generating Malicious APK
- Fake SMS
- Fake caller
- Key loggers
- Introduction to Rooted Devices
- Trace Phone Location
- Anonymous Chat Application
- Network Mapper
- Wi-Fi Kill

Tools: Nirsoft, Fing, Online Application, Net hunter

STAGE 5

In this stage, the trainer will focus on well-known network attacks to perform MITM and DOS attacks and countermeasures used for prevention.

Module 13: Sniffing and Spoofing

This module will help the candidate to understand network attacks executed by attackers on less secure Protocols to conduct Man-in-middle attacks.

Key Points:

- Introduction Sniffing and Its Types
- Spoofing
- Man-in-the-Middle Attack
- ARP Poisoning
- DNS Poisoning
- Password Sniffing
- HTTP Password Capture
- Telnet Password Capture
- FTP Password Capture

Tools: Ettercap, Wireshark and similar alternatives tools

Module 14: Denial of Services

This module helps candidates to understand the Dos and DDOS attacks. It also explains countermeasures followed in organizations for protecting jewel assets.

Key Points:

- Introduction of DOS Attack & Its Types
- Distributed Denial of Service DDOS
- Botnet
- DOS Attack
- SYN Flood
- ICMP Flood
- UDP Flood
- TCP Flood
- Blue Screen Death Attack

Tools: Golden-eye, Hping3, Metasploit Framework

Module 15: Wireless Hacking

This module helps the candidate to understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures

Key Points:

- Introduction to Wireless standard IEEE
- Introduction to WIFI Security & Protocols
- Detect Hidden SSID
- Monitor mode Vs promiscuous mode
- Capture WPA/WPA2 Handshake
- WPA/WPA2 Password cracking
- Evil Twin
- Dump Wifi Credentials

Tools: Alpha wifi Adapter, Airgeddon

STAGE 6

In this stage, the trainer will focus on Network Security Essential by describing the countermeasure used for network attacks by providing a conceptual and practical session on the following Modules.

Module 16: IDS, Firewalls, and Honeypots

This module helps the candidate learn various types of security tools and applications used to protect the organization from cyber-attacks.

Key Points:

- Introduction to IDS, IPS Firewall, DMZ & Honeypots
- Honey Bot, Kfsensor
- Windows Advanced Firewall Rules
- Evading Firewall
- Event Log Management
- Fundamentals of DLP

Tools: Windows ACL, Linux Iptables, Event Viewer, Kfsensor, Snort

Module 17: Cryptography & Steganography

This module helps candidates to understand how secure the entire communication is or choose the covert mode for making secret communication.

Key Points:

- Introduction to Information Security & CIA Model
- Basic Concept of Encoding
- Base64
- Binary
- Hexa Decimal
- Basic Concept of Steganography
- Image, audio and file-based Steganography
- Introduction to Cryptography
- Cesar cypher
- Rot 13
- Modern Cryptography
- AES Symmetric Encryption
- PGP Asymmetric Encryption
- Basic Concept of Hashing
- Hash Calculator
- Signature Compression

Tools: Steghide, PowerShell, Online Tools

CONTACT US

Phone No.

 +91 9599 387 41 | +91 1145 1031 30

WhatsApp

 <https://wa.me/message/HIOPPNENLOX6F1>

EMAIL ADDRESS

 info@ignitetechnologies.in

WEBSITE

 www.ignitetechnologies.in

BLOG

 www.hackingarticles.in

LINKEDIN

 <https://www.linkedin.com/company/hackingarticles/>

TWITTER

 <https://twitter.com/hackinarticles>

GITHUB

 <https://github.com/ignitetechnologies>