CYBER SECURITY TRAINING BROCHURE

IGNITE TECHNOLOGIES

Academy for Hackers

iGNITE Technologies

"We do not provide just knowledge; rather, we train you to use your knowledge to become a PROGAURD for an organization"

About Company

Our aim at the IGNITE TECHNOLOGIES Institute is to provide businesses military, organizations, and government bodies with cutting-edge information security knowledge and skills necessary to defend their people and assets.

IGNITE offers more than 15 distinct courses, all of which are aligned with the most prevalent security team roles, responsibilities, and disciplines. Our courses equip students to deal with today's risks and tomorrow's difficulties.

Background

Our students are placed in the MNC and are capable of executing fantastic jobs safeguarding the organization's and clients' networks' security posture. Ignite Certified students were able to earn Hall of Fame status from organisations such as Facebook, Twitter, Swiggy, and Uber.

OBJECTIVE

IMPROVE THE RESISTANCE OF YOUR DEFENSIVE CAPABILITY TO SOPHISTICATED CYBER-ATTACKS.

At Ignite Technologies we aim to train students in attack and defence techniques in the cyber security domain. It will allow you to obtain the knowledge and expertise to evaluate, design and build secure computer systems, processes and people that are involved in cyber security. It covers the theory and practice of designing and building secure systems and gives you a firm grounding in cryptography, network security and secure programming, as well as optional modules in topics such as hardware and cloud security, operating systems and incident management and forensics.

With increasing awareness and concern over the growing cyber threats facing organizations, governments and individuals alike, many universities and colleges have created new graduate degree programs in cybersecurity.
Companies including Microsoft, Vodafone, E&Y, KPMG, IBM and Adobe come onto campus for placement drive.

Tech giants like Google, Microsoft, Facebook, and others offer bug bounties to people who can hack their software and help them fix security flaws. In 2019, for example, Tesla offered 900,000 USD and a free car to anyone who could hack their Tesla Model 3.

CYBERSECURITY FAST FACTS

- Every minute, $17,700 is lost due to phishing attacks.
- 94% of malware is delivered via email.
- 63% of companies said their data was potentially compromised within the last year.
- 60% of data breaches involve vulnerabilities that could have been avoided if an available security update or patch had been applied.

TRANING
PROGRAM LEVELS

Ethical Hacking, Bug Bounty, Infrastructure Pentest, Wireless Hacking

LEVEL 1

API security Assessment, Android Application pentesting, Advanced Burp Suite, Capture the Flags

LEVEL 2

Privilege Escalation, MITRE Red Team, Active Directory, MSSQL Security Assessment

LEVEL 3

iGNITE Technologies

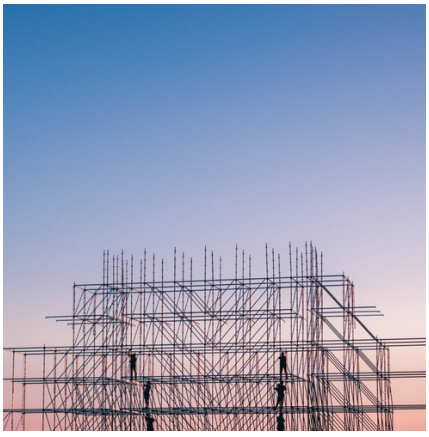
TIMEFRAME

2022 TO 2023

LEVEL 1- Beginners + Professional

At this level, the applicant will learn the fundamentals of cyber security, IT infrastructure, application and network design, and secure implementation and configuration.

120 + Hours



90+ Hours

LEVEL 2- ADVANCED

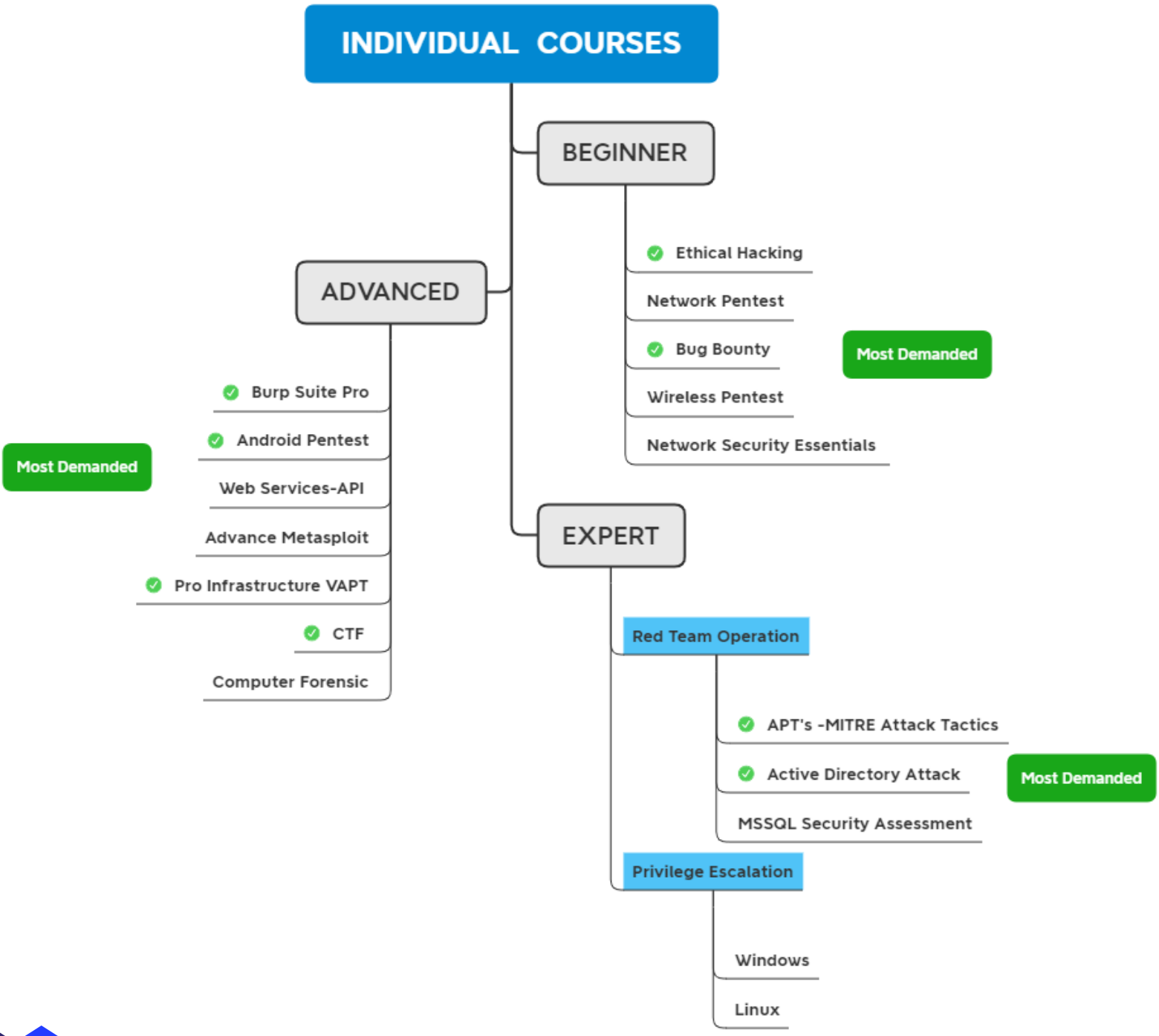
At this level, the applicant will acquire additional hands-on approaches based on industry requirements for identifying key vulnerabilities and bugs in IT networks and applications.

LEVEL 3- EXPERT

At this level, the candidate will develop an expert understanding of how to evaluate business risk consequences produced by a threat following exploitations, threat modelling, and hunting for indicators of compromised systems.

100+ Hours

ALL COURSES


INDIVIDUAL COURSES
BEGINNER
Ethical Hacking
Network Pentest
Bug Bounty
Most Demanded
Wireless Pentest
Network Security Essentials
ADVANCED
Burp Suite Pro
Android Pentest
Most Demanded
Web Services-API
Advance Metasploit
Pro Infrastructure VAPT
CTF
Computer Forensic
EXPERT
Red Team Operation
APT's -MITRE Attack Tactics
Active Directory Attack
Most Demanded
MSSQL Security Assessment
Privilege Escalation
Windows
Linux

TRAINING FRAMEWORK

OWASP

The Open Web Application Security Project (OWASP) is a "best practice" penetration testing framework that users can implement in their own organizations and a "low level" penetration testing guide that describes techniques for testing most common web application and web service security issues

NIST

NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, A 2016 study found that 70% of organizations surveyed see the NIST Cybersecurity Framework as a popular best practice for computer security.

MITRE ATT&CK

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

IN 2019, THE VALUE OF THE HEALTHCARE CYBERSECURITY MARKET WAS 9.78 BILLION AND THIS IS PROJECTED TO RISE TO $33.65 BILLION BY 2027

(GLOBENEWSWIRE, 2020)

WHY TO CHOOSE US?

- Ignite Technologies trainers are experts in conducting proactive live training sessions
- Simulate a real-time scenario to mimic real-time threat and risk impact.
- Focused on personalized training as per individual skills.
- Less than 10 students in a group
- Ignite offers 1-year Diploma course that has more than 2000 practical sessions.
- Job Assurance for Diploma Holders
- Experience in training 10000+ students around the globe
- Community of more than 50,000+ individuals
- Ignite is highly adaptable in offering Online, weekend, and weekday programs according to students' available time windows.
- Ignite provides free access to the Ignite library, which contains a variety of e-books and lab manuals.
- After completing Ignite's Level 1 program, they were awarded a scholarship for Level 2.
- Ignite offered a Diploma and Postgraduate Diploma in Cyber Security to applicants who completed ALL levels of Training.
- Ignite Provided Diploma and PG Diploma Holders with 6-Month or 1-Year Training and Internship Letters.

SCHOLARSHIP PROGRAM

Ignite encourages your interest in hacking with its scholarship programme. Candidates enrolled in the Level 1 Program are eligible to participate in the Level 2 Scholarship Program.

Level 2 is comprised of Advanced Topics that enable candidates to conduct more thorough Penetration Testing on a network, web application, Web API sockets, and Android.

In addition, Level 2 focuses on Capture the Flag training in order to provide candidates seeking industry-recognized certification with hands-on training.

Scholarship Criteria for Level 2 Program

PARTICIPANTS	SCORE	DISCOUNT
Winner	100	100%
1st Runner-up	85	50%
2nd Runner-up	75	25%

BEGINNERS

ETHICAL HACKING

By opting to pursue this course, you will learn the fundamentals of hacking, penetration testing, network security, web application security, wireless security, auditing and much more.

Prerequisites: Basic in Computer and Networks (Optional)
System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 32 Hours

iGNITE Technologies

BEGINNERS

NETWORK PENTESTING

This course has been devised to upskill the security competency of an IT professional/individual by imparting knowledge on the basics as well as advanced concepts of Network Security & Organizational Infrastructure. One of the benefits of opting for this course is the flexibility of the course structure which allows even an individual with little to no technical skills to easily grasp the knowledge.

Prerequisites: Candidate should be aware of Ethical Hacking (Optional)
System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 32 Hours

iGNITE Technologies

BEGINNERS

BUG BOUNTY

Companies sponsor bug bounty programmes to allow security researchers and pentesters from all over the world to prove their abilities and uncover weaknesses in their websites. Depending on the severity of the bug reported, they are either compensated or recognised as a token of appreciation.
This course will build an understanding of application security vulnerabilities and penetration testing.

Prerequisites: Know about Ethical Hacking. Additionally, the candidate should be familiar with frontend and backend web development concepts (optional).
System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 32 Hours

iGNITE Technologies

PROFESSIONAL

ADVANCED BURP SUITE

Bug Bounty without Burp Suite? Is it even possible? That is completely out of the question!! Testing for vulnerabilities in web applications is currently regarded as one of the most important subfields within the broader domain of information security. However, within all of this, Burp Suite plays a significant part. Whether it's a basic web application scan or the exploitation of the vulnerabilities that have been uncovered, burp suite can handle it all.

The course's holistic framework and real-world practice with Burp Suite Professional Edition's Basic to Advanced features make it a worthwhile investment. The training is meant for both beginners and professionals who wish to improve their Web-Application Penetration Testing skills.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty
System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 20 Hours

iGNITE Technologies

PROFESSIONAL

ANDROID PENTESTING

This course will focus on code-level security, which means that you will now understand the working of codes on the backend of the mobile applications and then be able to determine the type of attacks that can be performed on the application. The information gained from performing the pentests can help devise proper mitigation strategies to secure the Android applications.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty
System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 25 Hours

iGNITE Technologies

PROFESSIONAL

INFRASTRUCTURE VULNERABILITY ASSESSMENT & PENETRATION TESTING

Infrastructure penetration testing is discovering and probing vulnerabilities and faults in computer systems and devices connected to a network, cloud, or Servers. It is the process of discovering security vulnerabilities in an organization's security framework.
Typically, it is performed in conjunction with other approaches, such as External, Internal, Wireless, Cloud, and Virtualization Penetration Testing.
This course will instruct you on how to construct secure networks and systems for an organization's infrastructure.

Prerequisites: Candidate should be aware of Ethical Hacking
System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 50 Hours

iGNITE Technologies

PROFESSIONAL

CAPTURE THE FLAG (CTF)

Capture the Flag is an information security competition that is an amalgamation of various challenges that applies concepts like Reverse engineering, Web Applications, Binary, Network, Cryptography, Forensics, etc. Each challenge holds a certain number of points based on its difficulty level. The idea behind these CTFs is to provide an individual with practical knowledge of the different kinds of attacks and issues in the real world.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty
System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 45 Hours

iGNITE Technologies

EXPERT

APT'S MITRE ATTACK

RED TEAM TACTICS

To help organizations assess the scale and level of preparedness for a cyberattack, Red Team Operations simulates a meticulously orchestrated cyberattack. In-depth testing of an organization's detection and response capabilities over a long period of time

The training includes attacker simulators and attack frameworks like Cyber Kill Chain, Attack Tree, and MITRE ATT&CK Framework. Candidates can act as an adversary and use local tools to achieve corporate goals while avoiding detection. The training also focuses on using open-source tools and scripts and customizing them to meet an organization's needs.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty
System Configuration: 16 GB RAM & i7 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 50+ Hours

iGNITE Technologies

EXPERT

ACTIVE DIRECTORY ATTACK

RED TEAM TACTICS

Professionals who want to learn about the most common risks can benefit from this course. To begin, you'll do a sneak reconnaissance and enumeration of hosts, servers, services, and privileged users to identify them. To wrap things up, you will learn how to conduct red team attacks on Active Directory by targeting common misconfigurations and leveraging genuine Windows/Active Directory features.

Prerequisites: Candidate should be aware of Ethical Hacking
System Configuration: 16 GB RAM & i7 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 30+ Hours

iGNITE Technologies

EXPERT

MSSQL SECURITY ASSESSMENT

RED TEAM TACTICS

This Security Assessment will examine SQL Server instance discovery, inadequate configuration auditing, and privilege escalation at scale. Penetration testers and red teams are the primary targets of this operation. However, manual assessment supports a number of methods that administrators may utilise to inventory the SQL Servers in their ADS domain.

Additionally, a company can use this approach to define the risk factor and ensure compliance with information security policies. They can also use it to assess their level of reaction to any cyber-based threats.

Prerequisites: Candidate should be aware of Ethical Hacking
System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 20+ Hours

iGNITE Technologies

EXPERT

WINDOWS PRIVILEGE ESCALATION

The Privilege Escalation Training curriculum consists of approaches that help students comprehend how an adversary gains access to higher-level privileges on a system or network. A network's adversaries are often able to go around within the system without proper credentials.

As part of your cybersecurity strategy, this course explains how to protect user accounts in your systems and web application.

Prerequisites: Candidate should be aware of Ethical Hacking
System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 20+ Hours

iGNITE Technologies

EXPERT

LINUX PRIVILEGE ESCALATION

The Privilege Escalation Training curriculum consists of approaches that help students comprehend how an adversary gains access to higher-level privileges on a system or network. A network's adversaries are often able to go around within the system without proper credentials.

As part of your cybersecurity strategy, this course explains how to protect user accounts in your systems and web application.

Prerequisites: Candidate should be aware of Ethical Hacking
System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

DOWNLOAD

Durations: 20+ Hours

iGNITE Technologies

Contact US

PHONE

+91-9599387841 | +91 11 4510 3130

WHATSAPP

https://wa.me/message/HIOPPNENLOX6F1

OFFICE

26, Pusa Rd, Block 1, WEA
Karol Bagh, New Delhi, 110005

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

iGNITE Technologies