FUTURE PATH
INFOCAMPUS

www.teaminfocampus.com

Ethical Hacker

Beginner

About Infocampus

Infocampus is a community of learners, educators, and industry professionals dedicated to creating a supportive and dynamic learning environment. Since 2009, we have specialized in IT and networking courses for both beginners and professionals, bridging the gap between theory and practice. Our mission is to prepare students for the evolving tech industry, making us a trusted choice for career advancement in technology.

15+ Years of Expertise

5K+ Successful Graduates

Key Features

- Hands on training for real world application
- Highly experienced and skilled faculties
- State-of-the-Art Infrastructure
- Course completion certificate
- Job Assistance

Duration 2 Months

Ethical Hacker
Beginner

Infocampus introduces a structured 2-month Ethical Hacking Beginner Course, designed to build a strong foundation in cybersecurity and ethical hacking practices. This hands-on program is ideal for aspiring cybersecurity professionals, students, and IT enthusiasts who are looking to explore the world of ethical hacking in a practical and systematic manner.

The course is divided into eight focused training blocks, covering essential topics such as cybersecurity principles, information gathering, system exploitation, web application vulnerabilities, wireless network testing, and key tools like Kali Linux, Metasploit, Burp Suite, and Wireshark. Learners will gain real-world experience through interactive labs, practical demonstrations, and a capstone mini-project that reinforces end-to-end penetration testing workflows.

Whether you're starting your cybersecurity journey or planning to pursue advanced certifications, this beginner-level course provides the foundational knowledge and practical skills needed to step confidently into the ethical hacking domain.

Get started with ethical hacking—learn, practice, and protect with Infocampus.

Syllabus

01

Introduction to Cybersecurity (Foundational Unit)

- Cybersecurity Principles & Concepts
- Critical Terminologies in Cybersecurity
- Phases of Hacking & Penetration Testing
- Introduction to Operating Systems
- Networking Fundamentals
- Kali Linux: Installation & Setup
- Basic Linux Command-Line Operations

02

Information Gathering Techniques (Recon Unit)

- OSINT Framework Overview
- Active & Passive Reconnaissance Tactics
- Social Engineering & Phishing Attacks
- Google Dorking for Targeted Discovery

03

Scanning & Enumeration (Intel Unit)

- Network Scanning with NMAP
- NMAP Scripting Engine (NSE)
- Port Scanning Strategies
- Enumeration of Network Services

04

System Exploitation (Assault Unit)

- Metasploit Framework Operations
- Brute Force Attack Techniques
- Manual Exploitation Procedures
- Payloads and Shellcode Shellcode

05

Post Exploitation (Persistence Unit)

- Credential Harvesting Techniques
- Kernel-Level Exploitation
- Exploiting Misconfigured Systems & Files
- Advanced Post-Exploitation with Mimikatz & Meterpreter

06

Web Application Vulnerabilities (WebOps Unit)

- Web Application Architecture & Mechanics
- OWASP Top 10 Exploits in Action
- SQL Injection (SQLi) Techniques
- Cross-Site Scripting (XSS) Exploitation
- Web Application Interception with Burp Suite

07

WiFi Pentesting (AirOps Unit)

- Wireless Recon with Airmon-ng
- Cracking WiFi Keys using Aircrack-ng
- Wireless Traffic Capture via Airodump-ng
- Automated Attacks with Wifite & Fluxion

08

Miscellaneous (Tactical Tools Unit)

- Maintaining Anonymity with VPNs & Proxies
- Network Analysis using Wireshark
- Denial-of-Service (DoS) & Distributed DoS Attacks
- Capstone: Mini-Project Deployment & Reporting

Syllabus

FUTURE PATH
INFOCAMPUS

www.teaminfocampus.com

CALL

+91 9037555777
+91 62821 25456

Email:
hello@teaminfocampus.com

KERALA

6th Floor, Markaz Complex,
Mavoor Road,
Opp.Private Bus Stand,
Kozhikode, Kerala – 673004

BENGALURU

No.50, 1st Floor, JKN Arcade,
1st Cross Road, 27th Main,
Old Madiwala, BTM 1st stage,
Bengaluru-560068