FUTURE PATH
INFOCAMPUS

www.teaminfocampus.com

CYBER SECURITY

100% JOB GUARANTEE

ICAP- Infocampus Cyber Security Assurance Programme

About Infocampus

15+

Years of Expertise

5K+

Successful Graduates

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.

Expert Instructors

Learn from certified professionals with 20+ years of experience.

Career Advancement Assistance

Receive personalized guidance to secure your dream job.

Global Certification

Unlock global career opportunities with our internationally recognized certificate, accepted by top employers and educational institutions world wide.

Infocampus Cyber Security Assurance Programme (ICAP)

Launch Your Cybersecurity Career — With a 100% Job Guarantee Step into one of the most in-demand industries with ICAP — a premier, one-year cybersecurity training and placement program designed to turn passionate learners into high-performing cybersecurity professionals.

Whether you're starting fresh or making a career pivot, ICAP offers the perfect blend of expert instruction, real-world training, and job-focused development to ensure your success in the cybersecurity field.

Why Choose ICAP?

Industry-Aligned Curriculum

Gain mastery in core cybersecurity domains including:

- Ethical Hacking
- Penetration Testing
- SIEM & SOC Operations
- Incident Response

Learn from Industry Veterans

Train under globally certified cybersecurity professionals (including CompTIA Security+) with 3+ years of hands-on experience in the field.

Hands-On Labs & Real-World Scenarios

Build your skills through:

- Interactive virtual labs
- Red vs. Blue Team exercises
- Realistic attack-defense simulations
- Capture the Flag (CTF) challenges

Career-Ready Development

- Personalized interview preparation
- Communication & soft skills training
- Resume building and LinkedIn optimization
- One-on-one mentorship

100% Job Guarantee

We don’t just train you — we place you.
Get guaranteed job placement upon successful course completion.

Foundational Cybersecurity

Introduction to Cybersecurity

Overview of the cybersecurity landscape

Types of Cyber Threats

Malware, Phishing, DDoS (Distributed Denial-of-Service), and more

Networking Concepts

TCP/IP stack, OSI Model, protocols, and addressing

Security Policies and Risk Management

Frameworks for enterprise security

Cybersecurity Frameworks and Standards

ISO 27001, NIST Cybersecurity Framework

Cybersecurity Tools and Utilities

Introduction to key security tools for threat detection and mitigation

Networking and System Administration

Networking Protocols

DNS, HTTP, FTP, and other fundamental protocols

Network Devices and Infrastructure

Routers, switches, firewalls, and network segmentation

System Hardening

Securing Windows and Linux systems
Applying security patches and configurations

Firewall and Policy Configuration

Network security and firewall configuration techniques

VPN and Secure Communications

VPN protocols, encryption, and tunneling

Reconnaissance and Footprinting

Information Gathering and OSINT

Open-Source Intelligence (OSINT), WHOIS, DNS, and social engineering techniques

Footprinting and Network Enumeration

Identifying open ports, services, and vulnerabilities

Vulnerability Scanning Tools

Nmap, Netcat, Nessus, OpenVAS for vulnerability discovery

Threat Intelligence Platforms

Using platforms for real-time threat data collection and analysis

Exploitation Techniques

Penetration Testing Methodology

Phases of penetration testing: Reconnaissance, exploitation, post-exploitation

Common Web Application Vulnerabilities

SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)

Exploitation Tools

Metasploit framework and custom exploits

Privilege Escalation

Techniques to escalate privileges within compromised systems

Exploiting Vulnerabilities

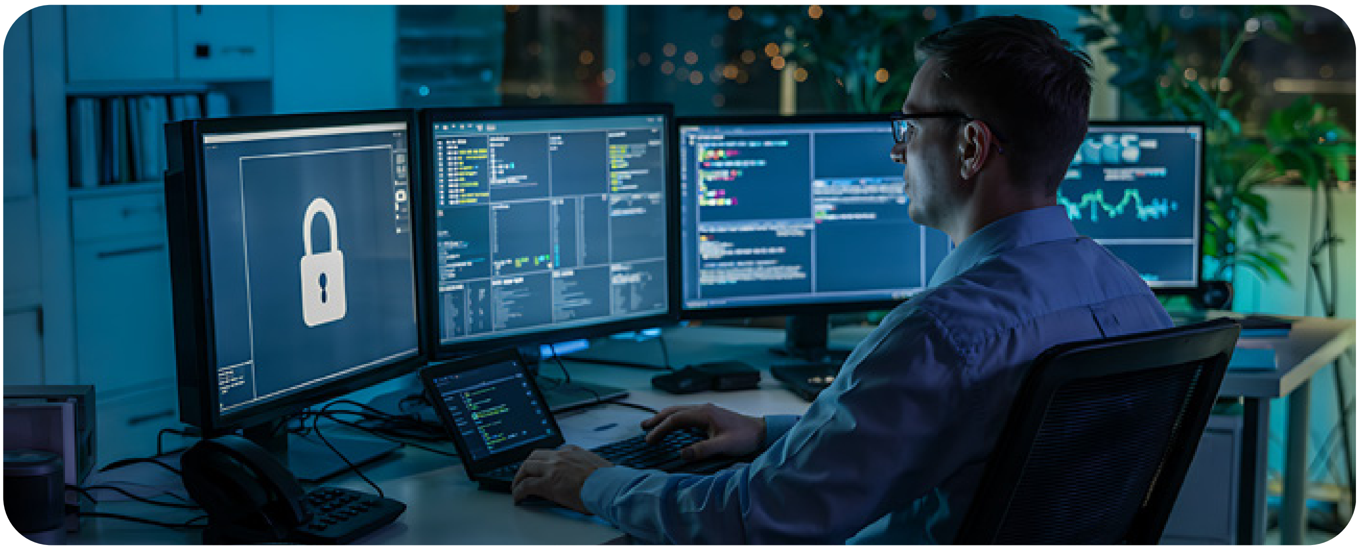
Gaining root/admin access through system flaws

Post-Exploitation and Maintaining Access

Pivoting and Tunneling
Lateral movement within networks to expand access

Creating Persistent Access
Maintaining access via backdoors, rootkits, and other methods

Data Exfiltration and Hiding Tracks
Exfiltrating data without detection and covering digital traces



Web Application Security

OWASP Top 10 Vulnerabilities
Understanding common web application flaws and countermeasures

Web Application Security Testing
Tools such as Burp Suite, ZAP for dynamic security testing

Bypassing Web Application Firewalls (WAF)
Techniques to evade detection by WAFs

Automated Security Testing
Integrating automated testing in development pipelines

Wireless Network Security

Wi-Fi Security Protocols

WEP, WPA, WPA2, and evolving encryption standards

Wi-Fi Penetration Testing

Tools like Aircrack-ng, Kismet for attacking wireless networks

Wireless Network Attacks

Evil Twin, Deauthentication attacks, and other wireless exploits

Secure Wi-Fi Configuration

Best practices for securing wireless networks from unauthorized access

Malware Analysis and Reverse Engineering

Malware Analysis Fundamentals

Static and dynamic malware analysis techniques

Reverse Engineering Tools

IDA Pro, OllyDbg, and other disassemblers

Creating Malware Detection Signatures

Writing signatures to detect known malware

Windows and Linux Malware Analysis

Techniques specific to both Windows and Linux malware

SOC Operations and Incident Response

Introduction to Security Operations Centers (SOC)

Key roles in a SOC, and tools used for detection and response

Incident Response Frameworks

NIST, SANS frameworks for structured incident handling

SIEM Tools and Log Analysis

Using Splunk, ELK Stack for log aggregation and analysis

Threat Hunting and Digital Forensics

Techniques for identifying hidden threats and gathering evidence for investigation

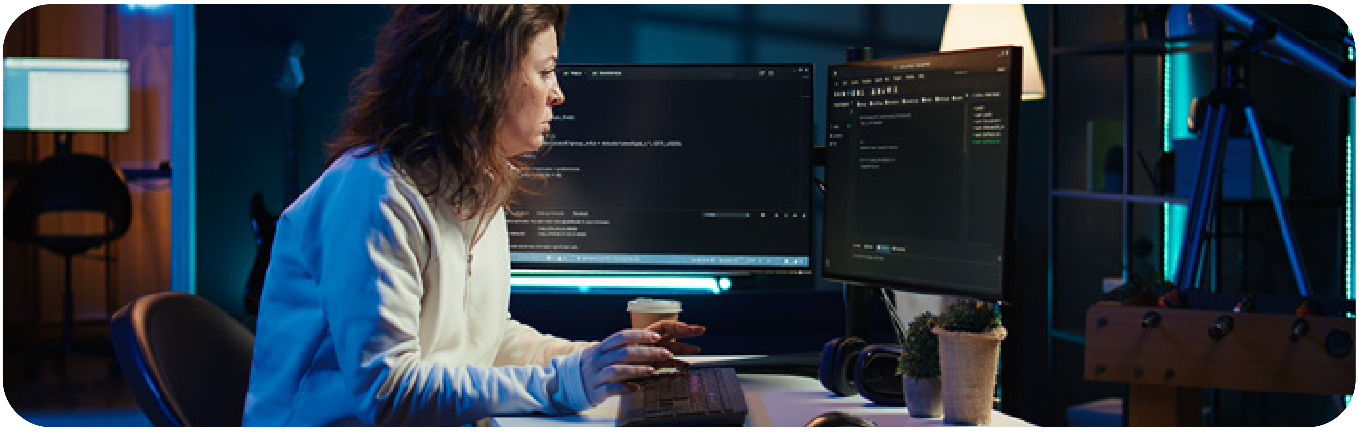
Capture The Flag (CTF) Challenges & Bug Bounty

Capture The Flag (CTF) Challenges

Real-world penetration testing scenarios and vulnerability exploitation
Hands-on experience with solving CTF challenges (network, web, cryptography)
Collaborating on problem-solving with peers

Bug Bounty Programs

Introduction to HackerOne, Bugcrowd, and other platforms
Developing strategies for identifying vulnerabilities in live web applications
Writing professional vulnerability reports and earning rewards
Building reputation as an ethical hacker in the global cybersecurity community



FUTURE PATH
INFOCAMPUS

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

Call

+91 9037555777
+91 62821 25456

Email: hello@teaminfocampus.com

www.**teaminfocampus**.com