ICT ACADEMY OF KERALA

CELEBRATING EXCELLENCE
10 YEARS
ICT ACADEMY OF KERALA

INDUSTRY READINESS PROGRAM

CERTIFIED CYBER SECURITY ANALYST

REGISTER NOW!

https://ictkerala.org/registration

\ictkerala

ictkerala.org

About the Program

This program is designed to acquaint students with the fundamentals of cyber security and the diverse career opportunities within the field, enabling them to grasp the real-world hurdles organizations encounter today. Through practical application and skill development, participants will learn how to effectively tackle these challenges. Emphasizing hands-on engagement, this course actively involves students in various public and industry cyber security challenges, fostering a proactive learning environment.

OFFLINE	INTERNSHIP DURATION	ONLINE
3 Months	**125 Hrs.**	**6 Months**
(375 Hrs.)	(With Mentor Support)	(500 Hrs.)

- ✓ **Physical sessions tailored for graduates and professionals**
- ✓ **Scholarships and cashbacks for meritorious candidates**
- ✓ **Comprehensive employability skills training offered**
- ✓ **3-months FREE LinkedIn Learning access**
- ✓ **100% placement assistance guarantee for the eligible candidates**

The ICT Academy of Kerala (ICTAK) offers hands-on training sessions aimed at bridging the skill gap in the information and communication technology (ICT) domain. These online or offline sessions provide job-oriented courses in information technology (IT), furnishing participants with the essential skills and certifications required for various IT job roles. This proactive approach has proven instrumental in assisting numerous individuals in securing employment within the ICT sector.

Job Roles

Candidates participating in this program can anticipate a wide range of potential career paths upon completion.

Cyber Security Analyst	~4 L	Penetration Tester	~5 L
Network Security Engineer	~5L	Information Security Analyst	~5 L

Learning Outcome

Upon completion of the program, participants will be equipped with:

- **Comprehensive Cyber Security knowledge:** A thorough understanding of fundamental and advanced cyber security concepts, including network security, cryptography, cyber attack life cycles, and cybersecurity standards and frameworks.
- **Practical Skills:** Proficiency in using cyber security tools and techniques for network and web application penetration testing, WiFi security assessments, and malware analysis, along with hands-on experience in social engineering and OSINT.
- **Critical Thinking and Problem-Solving:** Enhanced ability to identify, analyze, and mitigate various cyber security threats, employing critical thinking and problem-solving skills to address complex security challenges.
- **Career Readiness:** Preparedness to enter the cyber security field with a competitive edge, equipped to handle real-world security issues and contribute effectively to organizational security measures and projects.

Agenda

- Cyber Security Fundamentals
- Cyber Security Standards
- Types of Cyber Security Framework
- Introduction to Careers in Cyber Security
- Cyber Attack Life cycle
- Building a secure Hacking Lab
- Types of Attacks
- Network Security Attacks
- Web Application Attacks
- Zero-Day Exploit

About ICTAK

The ICT Academy of Kerala (ICTAK) is a not-for-profit organization formed by the Government of India, the Government of Kerala, and leading IT industry players like TCS, UST, IBS, and Quest Global. ICTAK offers various ICT and life skills programs such as Microsoft, Java, DevOps, Cyber Security, Artificial Intelligence/Machine Learning, and so on. Recognized by the Government of Kerala's Department of Electronics & IT, ICTAK provides comprehensive training with capstone projects and internships to prepare the next generation of ICT professionals. In the 2023-24 period, it expanded its partner network to 282 academic institutions, impacting over 12,000 students and 600 faculties. With 182 corporate partners, ICTAK organizes events, hackathons, and conferences to develop new ICT courses and promote digital literacy. Through partnerships with the government, it focuses on capacity building and project execution. Over the last decade, ICTAK has trained 1,20,000 participants and received national recognition for its innovative training practices from the Indian Society for Training & Development (ISTD).

Eligibility

- Engineering or science graduates / three-year diploma in any engineering branches, having a foundation level knowledge (plus two equivalent) in Mathematics and Computer fundamental skills.
- Students who have completed their graduation but are awaiting the final results can also apply.

**Please note that the ICT Academy of Kerala will have the right to cancel the candidature at any point if found ineligible.*

Appendix: Detailed Program Carriculum

Module	Duration
Module 1 - Problem Solving & Design Thinking • Understanding the problem, Analytical thinking, Creativity and innovation, Decision-making skills, Troubleshooting skills, Logical reasoning • Design Thinking: Empathy, Defining the problem, Ideation, Prototyping, Testing and iterating, Case studies	10 Hrs.
Module 2 - Foundation Module • Introduction to Cybersecurity, Difference between Surface Web, Deep Web and Dark Web, Types of Threats, Cybersecurity Careers, Cybersecurity Certifications • Introduction to Virtual Machines & Hypervisors, Virtualbox - Basic Configuration & Usage, Introduction to Operating Systems, Operating System Principles, Comparison of various Operating Systems, Introduction to Linux, Different flavors of Linux, Installation of Kali Linux & basic usage • Command Line Interface, CLI vs GUI, Basic Linux Commands, Creation of files & directories, Navigating through the filesystem, Linux File Hierarchy Standard, Privileged and Non-privileged Users, CLI Hands On, Advanced Linux Commands - Using operators for redirection and combination, Bandit CTF Challenge • Introduction to Computer Networks, The history of human communication, How a packet travels in a modern computer network, OSI Model, TCP/IP Model, ISPs, Internet Gateway, Internet Exchange Point, Peering, Internet Backbone, Internet Protocol, IP Address & its types, MAC Address, TCP vs UDP, Ports & port numbers, Components of a URL, Domain Name System	35 Hrs.
Module 3 - Cyber Security Fundamentals • Cyber Security Objectives, CIA Triad - Confidentiality, Integrity & Availability, Authentication, Authorization, Non-Repudiation, Secure Electronic Transactions, Cyber Security Breaches • How to Address Cyber Security, Cybersecurity Principles - Defense in Depth, Principle of Least Privilege, Secure Defaults, Complete Mediation, Diverse Mechanisms etc, Cyber Terminologies, • Introduction to Cryptography, Symmetric Encryption, Asymmetric Encryption, Hashing, How HTTPS works - SSL/ TLS, Certificate Authorities, Smart Security - Three Lines of Defense, • Cyber Security Standards- HIPAA, GDPR, ISO 27001, PCI - DSS • Cyber Security Frameworks : NIST Cyber Security Framework • Cyber Attack Lifecycle, MITRE ATT&CK Framework, Ethics, Etiquettes & Consent	40 Hrs.

Module	Duration
Module 4 - Network & WiFi Pentesting • Introduction to Port Scanning, Introduction to nmap, Network Discovery using nmap, Network Enumeration using nmap, Advanced usage, Legality, Alternatives to NMap • Introduction to Wireshark, Wireshark Basics, Wireshark Filters, Hands-On, Legality, Alternatives to wireshark - tcpdump, tshark • Netcat Basics, Network enumeration using netcat, Bind shells vs Reverse shells, Vulnerability assessment using openvas, nessus etc, Web vulnerability enumeration using nikto • Metasploit basics, Exploiting a target using Metasploit, Manual Exploitation techniques, Meterpreter, Exploits vs Payloads • Privilege Escalation - Linux and Windows, Persistence, Pivoting, Covering Tracks, Hands On • Fundamentals of Wireless Communication, 802.11 specifications • Managed Mode vs Monitor Mode, Wireless Reconnaissance, WiFi Security Protocols & their weaknesses - WEP, WPA, WPA2 & WPA3, WiFi Attacks, Evil Twin Attack vs Rouge Access Point • Hands On - Cracking Vulnerable Wireless Networks	50 Hrs.
Module 5 - Web Application Pentesting -I • Basics of a website, Frontend technologies - HTML, CSS, Javascript • Website Backend - Frameworks & MVC Architecture, Database, Hosting the website • Website Enumeration, Information Gathering, Introduction to Burpsuite & ZAP Proxy • Introduction to OWASP Top 10, Directory traversal, Access control vulnerabilities, Hands On • Authentication Vulnerabilities, Server Side Request Forgery (SSRF), Hands On • OS command injection, File upload vulnerabilities, Hands On Labs	40 Hrs.
Module 6 - Web Application Pentesting -II • Introduction to SQL, SQL Hands On, SQL Injection Labs - Manual & Automated Approach, Hands On • Cross-site scripting: Reflected XSS, Stored XSS, DOM XSS, Hands On • DOM vulnerabilities, HTTP Request Smuggling, Web sockets, Hands On • Cross-site request forgery (CSRF), CORS Misconfiguration, Hands On • Insecure deserialization, Server-side template injection, Hands On • Information Disclosure, Business Logic Vulnerabilities, Host Header Attacks, OAuth Vulnerabilities, Hands On • Web cache poisoning, JWT Attacks, Web LLM Attacks Hands On	50 Hrs.

Module	Duration
Module 7 - Advanced Cyber Techniques • Introduction to Social Engineering, Introduction to OSINT, Setting up Virtual labs • OSINT Tools in detail • SET Kit, Phishing & Vishing, Advanced Phishing Tools • Incident Response, Intrusion Detection Systems, Security Information & Event Management Systems, Threat Intelligence, AI in Cybersecurity • Various MiTM Attacks, Hands On - MITM via ARP spoofing • Intro to malware, Classification of Malwares, Creating a simple Malware • Capture the Flag Competition	50 Hrs.
Module 8 - Capstone Project • Applying knowledge and skills acquired throughout the program to solve a real-world cyber security problem by conducting a penetration testing project. • Literature Survey, Reconnaissance Phase, Vulnerability Assessment Phase, Penetration Testing	100 Hrs.
Total	375 Hrs.