Brit College of Engineering & Technology (BCET)

High-Skill Development Programmes in Demand Worldwide

Advanced Professional Certificate in Cyber Security with R&D

Delivery Methods:

1. **First 2 months** – Gaining Practical experience on a variety of Tools/Modules/Applications. Learners are required to submit some mini-projects based on real-life applications.

2. **Following 2 months** – Internship with R&D Capstone Project Design & Implementation. Report's Length – 5000 to 7000 words. Afterwards, working on publication.

Aims

- Equip learners with advanced cybersecurity knowledge, skills, and practical expertise for real-world environments.
- Develop proficiency in both offensive and defensive security strategies.
- Foster research-oriented thinking and innovation in cybersecurity solutions.
- Prepare learners for industry-ready roles and certifications in cybersecurity.

Objectives

1. Understand comprehensive cyber defense and offense strategies.
2. Gain hands-on experience with penetration testing and vulnerability exploitation.
3. Master key cybersecurity tools and techniques for network, system, and web security.
4. Learn secure programming practices and code analysis methods.
5. Explore advanced cryptography applications for secure systems.
6. Conduct research in emerging areas like AI security, malware analysis, and IoT security.
7. Execute R&D projects with practical outcomes, including publications or innovation solutions.
8. Build career readiness for multiple cybersecurity roles with professional competencies.

Learning Outcomes (LOs)

1. LO1: Apply defensive and offensive cybersecurity strategies in real-world scenarios.

2. LO2: Conduct penetration testing and ethical hacking using industry-standard tools.
3. LO3: Analyse network traffic and detect vulnerabilities using advanced cybersecurity tools.
4. LO4: Develop and implement secure code in Python and Java, applying static and dynamic analysis.
5. LO5: Apply cryptography techniques for secure communication and data protection.
6. LO6: Investigate advanced cybersecurity challenges, including malware, AI, IoT, and blockchain security.
7. LO7: Design and execute research-driven projects demonstrating innovation in cybersecurity.
8. LO8: Demonstrate professional skills required for cybersecurity roles in industry.

Target Audience

- IT professionals seeking specialisation in cybersecurity.
- Graduates in computer science, information technology, or related fields.
- Security analysts, system administrators, and developers aiming to upskill in cybersecurity.
- Individuals preparing for cybersecurity certifications or research roles.

Programme Modules and Structure

Module	Topics / Highlights	Learning Focus / Tools	Covered LOs	Career Skills / Roles
Module 1: Comprehensive Cyber Defense & Offense	Defensive strategies, red team vs blue team, threat modelling, incident response	Firewalls, SIEM tools, Security monitoring	LO1, LO8	SOC Analyst, Cybersecurity Analyst
Module 2: Metasploitable on Kali Linux	Setting up labs on VirtualBox, exploiting vulnerabilities, practice in sandboxed environment	Kali Linux, VirtualBox, Metasploit	LO2, LO3	Ethical Hacker, Penetration Tester
Module 3: Cybersecurity Tools & Techniques	Wireshark (network analysis), Nmap (scanning), Burp Suite (web testing), John the Ripper/Hashcat (password cracking), Snort/Suricata (IDS), Aircrack-ng (WiFi security)	Hands-on labs with real-world simulations	LO2, LO3	SOC Analyst, Ethical Hacker, Network Security Engineer
Module 4: Secure Programming	Secure coding in Python & Java, Static & dynamic code analysis	SonarQube, Bandit, Fortify	LO4, LO8	Secure Software Developer, Application Security Engineer
Module 5: Hacking & Exploitation Techniques	Vulnerability assessment, ethical hacking, penetration testing, exploitation, red vs blue team exercises	Metasploit, Burp Suite, lab environments	LO1, LO2, LO8	Ethical Hacker, Pen Tester, SOC Engineer

Module	Topics / Highlights	Learning Focus / Tools	Covered LOs	Career Skills / Roles
Module 6: Applied Cryptography	Encryption algorithms, hashing, key management, digital signatures	OpenSSL, Cryptography libraries, hands-on exercises	LO5, LO4	Security Analyst, Application Security Engineer
Module 7: Research Focus in Advanced Cybersecurity	Malware analysis, digital forensics, AI security, IoT security, blockchain-based security	Sandboxed malware labs, AI/ML tools, IoT simulators	LO6, LO7	Security Researcher, Forensics Analyst
Module 8: R&D Projects & Career Readiness	Capstone projects, innovation in security solutions, professional skills development	Project management tools, collaboration platforms, presentation of findings	LO7, LO8	Cybersecurity Researcher, Security Consultant, Industry-ready professional