IT Business Incubator
Chittagong University of Engineering & Technology (CUET)

diligite

Course Brochure: Cybersecurity Professionals

Course by:

IT Business Incubator, CUET
Chattogram-4349, Bangladesh.
Website: itbi-cuet.com

Last Updated: 15 June 2026

Summary

No.	Particulars	Information
1	Course Duration	90 Hours (30 Sessions, 15 Weeks)
2	Course Fee	BDT 12,000
3	Course Certification	Certificate awarded by IT Business Incubator, CUET
4	Vendor Certification	Certified Ethical Hacker (CEH) by EC-Council
5	CEH Preparation	24 Hours (8 Sessions, 4 Weeks)
6	Total Course Fee	BDT 30,000 (Including CEH Preparation and Exam Voucher)
7	Eligibility	Above HSC, basic computer and IT knowledge
8	Lab Facilities	Required lab facilities will be provided by ITBI, CUET

Schedule

Offline Batch: Friday & Saturday 10 am to 1 pm
Online Batch: Friday & Sunday 7 pm to 10 pm

Coordinator & Master Trainer

Professor Dr. M. Moshiul Hoque
Professor, Dept of CSE, CUET
Director, IT Business Incubator, CUET
Director, Institute of Information and Communication Technology (IICT), CUET
Former Dean, Faculty of Electrical & Computer Engineering, CUET
Former Chair, IEEE Bangladesh Section

Trainers

Professor Dr. Mahfuzulhoq Chowdhury
Professor, Dept of CSE, CUET

Md. Iftakharul Islam
IT Security Analyst, Portwest Ltd.

Ariful Islam
Network & DevOps Engineer, Diligite Ltd.

Learning Outcomes

By the end of this course, trainees will be able to:

- Build strong foundations in networking and cybersecurity concepts
- Gain hands-on skills in ethical hacking and penetration testing tools
- Learn web application security, vulnerability assessment, and exploitation techniques
- Understand SOC operations, SIEM, and incident response in real-world environments
- Prepare for cybersecurity careers and professional certifications (CEH)

Course Modules

Module No.	Module Name	Session No.	Topics	Duration (Hours)
1	Network Basics & Introduction to Cyber Security	1	Introduction to Cybersecurity , Basic Networking Concepts - Networking Protocols (TCP/IP)	3
		2	IP, HTTP, etc. - Understanding Firewalls and VPNs - Network Access Control (NAC)	3
		3	Setting up Virtual Machines (VMs) - Basic Network Security Configurations - Installing Cybersecurity Tools (e.g., Wireshark, Kali Linux)	3
		4	Malware types and their behavior	3
2	Reconnaissance & Footprinting	5	Introduction of Footprinting, Network Ports, Introduction of Nmap	3
		6	Introduction to Vulnerable Machine (Metasploitable 2), TryHackMe setup, Nmap Practical, TryHackMe room solving (Passive Reconnaissance)	3
3	Scanning & Enumeration	7	Nmap Practical continues, HPing3 Practical	3
		8	TryHackMe room solving (Passive Reconnaissance) continues	3
		9	Domain & Sub-domain Enumeration with Netcraft & Host, Wordlist making with CeWL	3
		10	Website Mirroring with HTTrack, Dir Busting with GoBuster & FFUF	3
		11	Angry IP Scanner Practical	3
4	Being Anonymous	12	Being Anonymous with Ghost-Switch, Tor, Proxychains	3

5	System Hacking & Post Exploitation	13	Hound Tool Practical, Metasploit Introduction, Uses of MSFconsole in Metasploit	3
		14	Uses of MSFConsole & MSFVenom in Metasploit, Uses of Searchexploit Command, Tool Integration in Metasploit	3
		15	MCQ Exam 1 with Answers Explanation (Offensive)	
		16	Staged & Non-Staged Payload Practical, Encoding & Encrypting Payload with Metasploit	3
		17	Manual Exploitation with Metasploit, Manually Add Exploit to Metasploit	3
		18	FTP Anonymous Login, Exploit FTP (Port-21) with Hydra, Basic Virus making with JPS Virus Maker, Compromise victim device with Thief RAT	3
6	Wireless Attacks & Network Packets Capture	19	DOS TCP SYNFlood Attack, DOS Attack using HPing3 & Raven Storm, DOS Attack using HOIC	3
		20	DOC Attack using LOIC, Anti-DDoS tool Practical with Anti-DDoS Guardian, Session Hijacking, ZAP Proxy Practical, TryHackMe room solving (Introduction to OWASP ZAP)	3
7	Vulnerability Assessment, Web Application Attacks and Penetration Testing	21	Introduction to Burp Suite, Burp Suite Fundamentals, Navigating Burp Suite Features (Target Tab, Proxy Tab, Intruder Tab & Repeater Tab)	3
		22	Attack simulations (Man In The Middle Attack & Brute Force Attack) on DVWA using Burp Suite	3
		23	CSRF Attack on DVWA using Burp Suite	3
		24	Basic SQL Injection Attack on DVWA, SQL Injection on DVWA & VulnWeb with SQLMap	3
8	Security Operations Center (SOC) & Endpoint Detection & Response (EDR)	25	Introduction to SOC, SOC Fundamentals, Tools which a SOC Analyst uses most, Introduction to EDR and CrowdStrike Falcon architecture	3
		26	Understanding Detections, Incidents, CrowdScore and Severity levels, Hands-on Investigating Alerts in Falcon Console	3

		27	Case Studies on Solving Incidents with CrowdStrike	3
9	SIEM Fundamentals & Practical Analysis	28	SIEM basics and role in SOC, Splunk Installation and Configure, Common Alert types and Correlation Logic	
		29	SPL queries in Splunk (Search, Stats, Filtering)	3
		30	Wazuh Installation and Configure, Wazuh basic Rule Sets and Alert Interpretation	3
10	Problem Solving and Career Guidelines	31	Problem Solving for all the modules, Job Hunting & Career tips, Interview Preparation	3

Enrollment Process

1. Interested candidates should apply through the online portal: www.itbi-cuet.com/training-application
2. After submission, candidates will receive the evaluation test schedule via email.
3. Candidates who pass the evaluation test will be eligible to enroll in the course. Before enrollment, they may also apply for a waiver (if applicable).
4. Finally, selected candidates can complete enrollment through: www.itbi-cuet.com/training-enrollment

Contact Information

Course Coordination Team
IT Business Incubator, CUET
Incubation Building, 7th Floor, Room No: 701
Phone: +88 01731-711434, +88 01978-464904 (Whatsapp)
Email: itbicuet@gmail.com | training@itbi-cuet.com