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

diligite

Course Outline: Cyber Security Professionals

Course by:

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

Last Updated: 31/10/2024

Course Summary

No.	Subject	Comments
1	Course Duration	60 Hours (20 Classes, 10 Weeks)
2	Pre-requisites	Basic understanding of computers and networking concepts.
3	Lab Facilities	ITBI, CUET will provide.

Schedule (Phase - 02)

Batch - 01 (Offline): Friday & Saturday 10 am to 1 pm
Batch - 02 (Online): Friday & Saturday 6 pm to 9 pm

Coordinator

Professor Dr. M. Moshiul Hoque
Professor, Dept of CSE, CUET
Director, IT Business Incubator, CUET
Chair, IEEE Bangladesh Section

Master Trainer

Professor Dr. Shamsul Arefin
Professor, Dept of CSE, CUET
Dean, Faculty of ECE, CUET
President, Bangladesh Computer Society

Trainers

Amit Chakraborty
Associate Professor, Daffodil International University

Ariful Islam
Network & DevOps Engineer
Trainer (Adjunct), ITBI CUET

Md. Iftakharul Islam
Cyber Security Engineer
Trainer (Adjunct), ITBI CUET

Learning Outcomes

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

- Understand the fundamentals of cybersecurity, threats, vulnerabilities, and risk management.
- Configure secure network environments, analyze potential attacks, and utilize firewalls and VPNs effectively.
- Identify and analyze malware, perform penetration testing, and respond effectively to cybersecurity incidents.
- Apply cryptographic principles and secure cloud and web applications.
- Gain hands-on experience with cybersecurity tools and techniques in simulated environments.

Course Summary

No.	Subject	Comments
1	Course Duration	60 Hours (20 Classes, 10 Weeks)
2	Pre-requisites	Basic understanding of computers and networking concepts.
3	Lab Facilities	ITBI, CUET will provide.

Course Modules	Lab Work
1. Introduction to Cybersecurity 2. Network Security Basics 3. Malware Types and Attack Vectors 4. Vulnerability and Risk Assessment 5. Security Policies and Compliance 6. Cryptography Fundamentals 7. Public Key Infrastructure (PKI) 8. Incident Response and Management 9. Web Application Security 10. Penetration Testing Fundamentals 11. Security Operations and Monitoring 12. Ethical Hacking Concepts 13. Cyber Threat Intelligence 14. Advanced Threats and APTs 15. Security in Cloud Computing 16. Capstone Project and Real-World Case Studies	1. Setting Up a Secure Environment 2. Network Scanning and Mapping 3. Firewall and VPN Configuration 4. Basic Malware Analysis 5. Vulnerability Scanning 6. Password Security and Cracking 7. Practical Cryptography 8. Web Application Security Testing 9. Penetration Testing Simulation 10. SIEM and Log Analysis 11. Incident Response Simulation 12. OSINT and Threat Analysis 13. Cloud Security Hands-on 14. Final Lab Project

Course Modules

Module	Topics Covered	Duration	Intended Learning Outcomes
Module 1. Introduction to Cybersecurity	- Key Concepts of Cybersecurity - Cyber Threat Landscape - Common Attack Vectors - Importance of Cyber Hygiene	3 Hours	- Understand fundamental cybersecurity principles. - Identify various types of cyber threats and attack vectors.
Lab 1: Setting Up a Secure Environment	- Setting up Virtual Machines (VMs) - Basic Network Security Configurations - Installing Cybersecurity Tools (e.g., Wireshark, Kali Linux)	3 Hours	- Configure a secure environment for cybersecurity exercises. - Install and familiarize with essential cybersecurity tools.
Module 2. Network Security Basics	- Basic Networking Concepts - Networking Protocols (TCP/IP, HTTP, etc.) - Understanding Firewalls and VPNs - Network Access Control (NAC)	3 Hours	- Grasp foundational concepts of network security. - Understand the roles of firewalls and VPNs in network protection.

Lab 2: Network Scanning and Mapping	- Using Nmap for Network Scanning - Host Discovery Techniques- Port Scanning Methodologies	3 Hours	- Conduct network scanning to identify open ports and services. - Analyze the network layout for security assessment.
Module 3. Malware Types and Attack Vectors	- Types of Malware (Viruses, Worms, Ransomware) - Common Attack Vectors Used by Malware - Recognizing Indicators of Compromise (IoCs) - Malware Prevention Strategies	3 Hours	- Differentiate between various types of malware and their attack methods. - Recognize the signs of a malware infection.
Lab 3: Firewall and VPN Configuration	- Configuring Firewalls (Software and Hardware) - Creating Access Control Rules - Setting Up and Testing VPNs	3 Hours	- Implement firewall rules to enhance network security. - Configure and test VPNs for secure communication.
Module 4. Vulnerability and Risk Assessment	- Risk Assessment Techniques - Vulnerability Scanning Tools (e.g., Nessus) - Analyzing and Reporting Vulnerabilities	3 Hours	- Conduct a vulnerability assessment. - Analyze and report on vulnerabilities effectively.

Lab 4: Basic Malware Analysis	- Malware Analysis in Sandbox Environments - Identifying Malicious Files - Behavior Analysis of Malware	3 Hours	- Analyze malware behaviors in a controlled environment. - Identify and report on malicious files.
Module 5. Security Policies and Compliance	- Creating Security Policies - Understanding Standards (ISO, NIST) - Data Protection Laws and Governance	3 Hours	- Develop and implement security policies. - Understand compliance and regulatory requirements.
Lab 5: Vulnerability Scanning	- Using Nessus/OpenVAS for Scanning - Vulnerability Report Analysis - Risk Prioritization Techniques	3 Hours	- Conduct vulnerability scans and interpret the results. - Prioritize remediation efforts based on risk.
Module 6. Cryptography Fundamentals	- Symmetric vs. Asymmetric Encryption - Hashing Techniques - Digital Signatures and Certificates - SSL/TLS Basics	3 Hours	- Understand key cryptographic principles. - Apply encryption methods to protect data.

Lab 6: Password Security and Cracking	- Password Hashing Techniques - Using Cracking Tools (e.g., John the Ripper) - Implementing Multi-Factor Authentication	3 Hours	- Test password security and explore cracking techniques. - Apply multifactor authentication for enhanced security.
Module 7. Public Key Infrastructure (PKI)	- Key Management Principles - Digital Certificates - Understanding Certificate Authorities - Secure Communication Techniques	3 Hours	- Implement PKI concepts to secure communications. - Manage digital certificates effectively.
Lab 7: Practical Cryptography	- Applying Encryption Techniques - Hashing Data - Setting Up SSL/TLS Certificates	3 Hours	- Practice encryption and decryption methods. - Set up secure SSL/TLS connections.
Module 8. Incident Response and Management	- Incident Response Phases - Real-World Case Studies - Detection and Response Techniques	3 Hours	- Understand the steps in the incident response process. - Apply techniques for detecting and managing incidents.

Lab 8: Web Application Security Testing	- OWASP ZAP Tool Overview - Identifying Web Vulnerabilities (XSS, SQL Injection) - Securing User Inputs	6 Hours	- Identify vulnerabilities in web applications. - Apply security measures to protect against common attacks.
Module 9. Web Application Security	- Understanding OWASP Top 10 - Techniques for Preventing XSS and SQL Injection - Secure Coding Practices	3 Hours	- Implement secure coding practices in web development. - Protect web applications from common vulnerabilities.
Module 10. Penetration Testing Fundamentals	- Penetration Testing Methodologies - Reconnaissance Techniques - Vulnerability Exploitation - Ethical Reporting	6 Hours	- Conduct basic penetration testing and document findings. - Understand the ethical implications of hacking.
Lab 9: Penetration Testing Simulation	- Performing Reconnaissance - Scanning for Vulnerabilities- Exploiting Vulnerabilities and Reporting	6 Hours	- Execute a simulated penetration test. - Document vulnerabilities and propose remediation.

Module 11. Security Operations and Monitoring	- Understanding Security Operations Centers (SOC) - Log Analysis Techniques - Threat Detection Methods - Security Information and Event Management (SIEM)	3 Hours	- Monitor and manage security operations effectively. - Respond to threats using logs and SIEM tools.
Lab 10: SIEM and Log Analysis	- Configuring a SIEM Tool - Analyzing Security Logs - Setting Up Alerts for Threat Detection	3 Hours	- Use SIEM for log analysis and threat detection. - Configure alerts for suspicious activities.
Module 12. Ethical Hacking Concepts	- Legal and Ethical Guidelines in Hacking - Penetration Testing Best Practices	3 Hours	- Learn about the ethics of hacking and legal considerations. - Understand best practices in penetration testing.
Lab 11: Incident Response Simulation	- Simulating Cyber Attacks - Documenting Incident Responses - Analyzing Security Logs	3 Hours	- Practice incident response in a simulated environment. - Analyze logs to identify incident details.

Module 13. Cyber Threat Intelligence	- Sources of Threat Intelligence - Open Source Intelligence (OSINT) - Threat Analysis and Profiling Techniques	3 Hours	- Gather and analyze threat intelligence to identify risks. - Develop threat profiles based on intelligence.
Lab 12: OSINT and Threat Analysis	- Utilizing OSINT Tools for Threat Gathering - Creating Threat Profiles - Analyzing Threat Data	3 Hours	- Use OSINT tools to gather and analyze intelligence. - Develop actionable threat profiles.
Module 14. Advanced Threats and APTs	- Understanding Advanced Persistent Threats (APTs) - Modern Attack Tactics - Defensive Techniques	3 Hours	- Recognize and respond to advanced cyber threats. - Apply defensive strategies against APTs.
Module 15. Security in Cloud Computing	- Cloud Security Models (IaaS, PaaS, SaaS) - Identity and Access Management (IAM) - Data Protection Strategies - Secure Cloud Configuration	6 Hours	- Apply security best practices in cloud environments. - Manage data protection and IAM effectively.

Lab 13: Cloud Security Hands-on	- Configuring IAM in the Cloud - Securing Cloud Access - Data Protection Techniques	6 Hours	- Implement IAM and data protection measures in cloud services. - Configure secure cloud environments.
Module 16. Capstone Project and Real-World Case Studies	- Reviewing Real-Life Cybersecurity Case Studies - Final Capstone Project Development	6 Hours	- Demonstrate comprehensive skills in cybersecurity through a final project. - Analyze real-world case studies for practical insights.
Lab 14: Final Lab Project	- Securing a Simulated Network Environment - Vulnerability Remediation Techniques - Presenting Project Findings	6 Hours	- Complete a hands-on project to secure a network. - Present findings and remediation strategies

Frequently Asked Questions (FAQ)

1. **Who Can Enroll in This Course?**

Anyone with a basic understanding of computers and networking can enroll in the Cyber Security Professionals course

2. **Who are the trainers for the course?**

Our courses will be conducted by a combination of faculty from CUET and industry experts, ensuring a comprehensive and practical learning experience.

3. **Is the course offered online or offline?**

We offer the course in both formats. You can enroll in either an online or offline batch, depending on your convenience.

4. **Are there any specific qualifications required to enroll in the course?**

No specific qualifications are required to enroll. However, a basic understanding of computers and networking will be beneficial for hands-on exercises throughout the program.

5. **Will class recordings be available?**

Yes, recordings of each class along with additional educational materials will be accessible on your dashboard within 24 hours after the class concludes.

6. **What type of certificate will be awarded upon course completion?**

Upon successfully completing the course and passing the assessment, you will receive a certificate issued by CUET. This certificate will serve as proof of your skills and knowledge.

7. **Is a waiver available, and how can I apply? What percentage can I expect?**

Yes, waivers are available. To apply, accurately fill Waiver Application form and submit it. After submission, you will need to take an online assessment test. Based on your application, CV, and assessment results, waivers ranging from 20% to 30% may be granted.

8. **How can I enroll?**

You can enroll either online through our website (www.itbi-cuet.com) or by visiting the office directly. Register on our website and select your desired course by clicking the 'Add to Cart' button. If you have a waiver coupon, apply it before confirming your cart. Then, proceed to checkout and complete your payment using the SSLCommerz gateway. For detailed instructions, please refer to the file: Enrollment Process.

9. **Can I enroll in multiple courses?**

Yes, you can enroll in multiple courses. However, please ensure that the schedules of the courses do not overlap.

10. **Can I switch from online to offline batches or vice versa?**

Generally, batch changes are not permitted. However, you may contact the authorities for special circumstances to discuss your request.

11. **I live far from CUET; is there accommodation available for offline batch students?**

Yes, there is accommodation available at the IT Business Incubator's dormitory, with a cost of 600 BDT per night.