BQ-005

CYBER SECURITY

2nd EDITION

TURN CYBER THREATS INTO CAREER OPPORTUNITIES

Duration: 3 Months

- on-campus classes

www.banoqabil.org

Table of Contents

Course Title:	Cyber Security Fundamentals
Course Code:	BQ-005
Duration:	12 Weeks
Class Structure:	
Total Hours:	48 Hours
Total Sessions:	24 Sessions (Two sessions per week or as per convenience)
Session Duration:	2 Hours

1. Course Overview

The Cyber Security course is structured to equip learners with the fundamental and intermediate knowledge and practical skills essential to protect digital assets and networks against cyber threats. Over 12 weeks, students will explore topics ranging from basic security concepts and attack types to network defense, ethical hacking, and incident response, using real-world case studies and hands-on tools like Kali Linux, Wireshark, and Nmap.

The course combines theoretical lessons with lab sessions, assignments, and quizzes to simulate real-world cybersecurity challenges. By course end, students will be prepared for entry-level roles and have the foundational skills to pursue advanced certifications.

2. Course Objectives

By the end of the course, students will be able to:

- Introduce learners to the fundamental principles, importance, and scope of cybersecurity in protecting digital assets and systems.
- Equip students with knowledge of common cyber threats, attack techniques, and effective defense mechanisms.
- Develop hands-on abilities in network security, malware defense, ethical hacking, and incident response using industry-relevant tools.
- Familiarize learners with cybersecurity laws, ethical frameworks, and career pathways to prepare them for entry-level roles in the field.

3. Learning Outcomes

By the end of the course, students will be able to:

- Recognize common cyber-attacks, their techniques, and potential impacts on individuals and organizations.
- Implement network security controls, encryption, password management, and email security practices to protect digital systems.
- Conduct basic penetration testing, utilize cybersecurity tools, and develop effective incident response and disaster recovery plans.

- Understand relevant laws, regulations, and ethical responsibilities—particularly within the context of Pakistan—while building a foundational cybersecurity portfolio.

4. Course Breakdown:

4.1.	**Theory Work**	**20%**
4.2.	**Practical Work**	**80%**

5. Assessment Criteria

5.1.	Attendance & Participation:	15%
5.2.	Quiz:	20%
5.3.	Assignments & Projects:	25%
5.4.	Final Portfolio + Presentation:	40%

6. Course Outline - Weekly Breakdown

A. Session Focus:

a. Mission, Vision & Values Alkhidmat Foundation Pakistan & Bano Qabil Pakistan

b. Course Structure, Rules, Regulations

c. Success Stories & Project Impact

d. Expectations from Students

Week-1: Introduction

A. Session-1: Introduction to Cyber Security

i. What is Cyber Security?
ii. Importance of Cyber Security Today
iii. Cyber Security Domains Overview
iv. Career Paths & Job Roles in Cyber Security
v. Real-world examples from Pakistan and global markets

B. Session-2: Cyber Threat Landscape & Common Attacks

i. Types of Cyber Threats: Malware, Phishing, Ransomware
ii. Real-World Cyber Attacks
iii. Introduction to Cyber Defense Mechanisms

C. Assignment: Research and summarize 3 recent cyber-attacks.

D. Quiz: Cyber Security Basics

E. Trainer Resource Links:

i. Cybersecurity Fundamentals - Cybrary
ii. Introduction to Cyber Security - Coursera

Week-2: Hackers Attack

A. Session-3: Understanding Hackers and Attack Techniques

i. Types of Hackers: Black Hat, White Hat, Grey Hat
ii. Common Attack Techniques: Social Engineering, DDoS, SQL Injection

B. Session-4: Malware and Spyware Fundamentals

i. Malware Types & Effects
ii. Spyware Detection & Prevention

C. Assignment: Identify and explain 3 anti-malware tools.

D. Quiz: Attack Types & Malware

E. Trainer Resource Links:

i. Malware Analysis Tools - SANS
ii. Social Engineering Explained

Week-3: Network Security **A. Session-5: Network Security Basics** **i.** IP Addressing, Firewalls, Network Segmentation **ii.** Securing Wi-Fi Networks **B. Session-6: Password Management & Authentication** **i.** Strong Password Policies **ii.** Multi-Factor Authentication (MFA) **C. Assignment:** Create a strong password policy for a small business. **D. Quiz:** Network Security & Authentication **E. Trainer Resource Links:** **i.** Cisco Network Security **ii.** Authentication Best Practices	**Week-4: Email Security** **A. Session-7: Email Security Essentials** **i.** Recognizing Phishing & Spoofing **ii.** Secure Email Practices **B. Session-8: Introduction to Cyber Laws & Ethics** **i.** Pakistan Cyber Laws Overview **ii.** Ethical Hacking Guidelines **C. Assignment:** Summarize key points of Pakistan Cyber Laws. **D. Quiz:** Email Security & Cyber Laws **E. Trainer Resource Links:** **i.** Pakistan Cyber Laws **ii.** Ethical Hacking Basics - EC-Council
Week-5: Operating System Security / Soft Skills Session: **A. Session-9: Operating System Security** **i.** Windows & Linux Security Fundamentals **ii.** User Permissions & Roles **B. Session-10: Mobile Security** **i.** Mobile OS Vulnerabilities **ii.** Secure App Usage **C. Assignment:** Analyze and report suspicious app permissions on a smartphone. **D. Quiz:** OS & Mobile Security **E. Trainer Resource Links:** **i.** OWASP Mobile Security **ii.** Mobile Security Best Practices	**Week-6: Web Security/ Soft Skills Session:** **A. Session-11: Web Security Basics** **i.** HTTPS, SSL/TLS, Cookies Security **ii.** Common Web Vulnerabilities (SQL Injection, XSS) **B. Session-12: Cloud & IoT Security** **i.** Cloud Security Risks **ii.** Securing IoT Devices **C. Assignment:** List security features of popular cloud platforms. **D. Quiz:** Web & Cloud Security **E. Trainer Resource Links:** OWASP Web Security AWS Cloud Security
Week-7: Disaster Recovery / Soft Skills Session: **A. Session-13: Incident Response and Disaster Recovery** **i.** Incident Detection & Containment **ii.** Backup Strategies **B. Session-14: Cyber Security Tools Introduction** **i.** Kali Linux, Wireshark, Nmap **C. Assignment:** Design an incident response plan for a small company. **D. Quiz:** Incident Response & Tools **E. Trainer Resource Links:** **i.** SANS Incident Response **ii.** Kali Linux Tutorial	**Week-8: Penetration Testing / Soft Skills Session:** **A. Session-15: Penetration Testing Basics** **i.** Reconnaissance and Scanning **ii.** Vulnerability Assessment **B. Session-16: Security Policies & Risk Management** **i.** Writing Security Policies **ii.** Risk Identification and Mitigation **C. Assignment:** Draft an IT security policy. **D. Quiz:** Penetration Testing & Risk Management **E. Trainer Resource Links:** Offensive Security ISACA Risk Management

Week-9: Practice / Soft Skills Session: **A. Session-17: Revision and Practice Quiz** **i.** Review of Key Topics Covered So Far **B. Session-18: Final Project Preparation** **i. Guidance on Project Presentation** **C. Assignment:** Prepare final project presentation. **D. Quiz:** Comprehensive Mid-Course Quiz	**Week-10: Final Project / Soft Skills Session:** **A. Session-19: Session-19:** Final Project Presentations (Part 1) **B. Session-20:** Final Project Presentations (Part 2)
Week-11: Freelancing in Cyber Security / Soft Skills Session: **A. Session-21: Freelancing in Cyber Security** **i.** Platforms: Fiverr, Upwork **ii.** Services in Demand: Pen Testing, Security Audits **B. Session-22: Portfolio Development** **i.** Creating Case Studies **ii.** Adding Tools & Skills Showcase **C. Assignment:** Build a portfolio with 2 security projects. **D. Quiz:** Freelancing Basics in Cyber Security **E. Trainer Resource Links:** **i.** Fiverr Cyber Security Services **ii.** Building a Cyber Security Portfolio	**Week-12: Career Planning / Soft Skills Session:** **A. Session-23: Proposal Writing & Career Planning** **i.** Crafting Security Project Proposals **ii.** Setting Weekly & Monthly Goals **B. Session-24: Final Presentation + Mock Interview** **i.** Dress Code for Interviews **ii.** Presentation Style **iii.** Confidence Building Techniques **C. Final Project:** Present portfolio + 3-month roadmap **D. Final Quiz:** Recap-based assessment **E. Trainer Resource Links:** **i.** Cyber Security Proposal Writing **ii.** Mock Interview Tips

Note: 01-hour Soft Skills Session will be conducted weekly from **Week 05 to Week 12**.

7. Guest Speaker Sessions

- **a.** Minimum 2 guest speakers required during the course:
- **b.** Topics may include: Cyber Security Careers, Industry Trends, Real-World Challenges
- **c.** Details to be submitted before Week 4
- **d.** Free Learning Platforms
- **e.** Cybrary
- **f.** Coursera Cyber Security Specializations
- **g.** edX Cyber Security Courses