BQ 028

CYBER SECURITY (ADVANCE)

1ST EDITION

بنو قابل
اپنی دنیا آپ پیدا کر

DETECT FAST, DEFEND SMART

Duration 3 Months

- on-campus classes

www.banoqabil.org

Table of Contents

Course Title:	Cyber Security Advance
Course Code:	BQ-028
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:

This Advanced Cyber Security course is designed to equip learners with in-depth knowledge and hands-on expertise in protecting digital systems, networks, and applications against modern cyber threats. The program moves beyond fundamentals and focuses on advanced concepts such as penetration testing, ethical hacking, network defense, vulnerability assessment, digital forensics, and security operations.
Learners will work with real-world tools, simulate cyber-attack scenarios, and develop defensive strategies aligned with industry standards. By the end of the course, students will be capable of handling security challenges in professional environments and preparing for certifications and cybersecurity roles.

2. Course Objectives:

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

- Analyze advanced cyber threats and attack methodologies
- Perform vulnerability assessment and penetration testing
- Secure networks, web applications, and systems
- Implement incident response and disaster recovery plans
- Use industry-standard cybersecurity tools effectively
- Understand ethical, legal, and compliance frameworks

3. Learning Outcomes:

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

- Identify and mitigate complex cybersecurity threats
- Conduct penetration testing and ethical hacking activities
- Implement layered security strategies (defense-in-depth)
- Perform security audits and risk assessments
- Respond to incidents and recover compromised systems
- Build a professional cybersecurity portfolio

4. Course Breakdown

- Theory: 20%
- Practical: 80%

a) Theory Work (20%)

- **Topics:** Advanced threats, security frameworks, ethical hacking concepts, laws, and compliance

b) Practical Work (80%)

- **Tasks:** Pen testing labs, vulnerability scanning, network defense setup, security audits, final project

5. Assessment Criteria

- Attendance & Participation – ----------15%
- Quizzes – ----------20%
- Weekly Assignments – ----------25%
- Final Project + Presentation – ----------40%

6. Tools Used

a. Kali Linux
b. Wireshark
c. Nmap
d. Metasploit Framework
e. Burp Suite
f. OWASP ZAP
g. Linux Terminal
h. VirtualBox / VMware
i. GitHub (Portfolio)

7. Course Outline – Weekly Breakdown

Week-1: Advanced Cyber Security Introduction

A. Session-1: Cyber Security Landscape

I. Evolution of cyber threats
II. Advanced attack vectors
III. Security domains overview
IV. Real-world cyber incidents

B. Session-2: Writing & Running Python Code

I. ISO 27001 basics
II. NIST framework
III. CIA Triad & risk management
IV. Compliance and governance

C. Assignment: Analyze a recent cyber attack

D. Quiz: Security fundamentals

E. Trainer Reference Links:

- https://www.nist.gov/cyberframework

Week-2: Network Security & Defense

A. Session-3: Advanced Network Security

- Firewalls & IDS/IPS
- Network segmentation
- VPNs & secure communication
- Threat detection

B. Session-4: Traffic Analysis

- Packet analysis using Wireshark
- Identifying suspicious traffic
- Network monitoring techniques

C. Assignment

- Analyze network traffic

D. E-Quiz

- Network security

E. Trainer Reference Links:

- https://www.wireshark.org/docs/

Week-3: **Ethical Hacking Fundamentals**

A. Session-5: Ethical Hacking Concepts

I. Phases of hacking
II. Reconnaissance techniques
III. Foot printing tools

B. Session-6: Scanning & Enumeration

I. Nmap scanning
II. Service detection
III. Vulnerability identification

C. Assignment: Perform network scan

D. E-Quiz: Ethical hacking basics

E. Trainer Reference Links:

- https://nmap.org/book/

Week-4: Vulnerability Assessment

A. Session-7: Vulnerability Scanning

I. Types of vulnerabilities
II. Automated scanning tools
III. Risk prioritization

B. Session-8: Exploitation Basics

I. Introduction to Metasploit
II. Exploit frameworks
III. Payload execution

C. Assignment: Scan and report vulnerabilities

E. Quiz: Vulnerability assessment

F. Trainer Reference Links:

- https://docs.rapid7.com/metasploit/

Week-5: Web Application Security / Soft Skill Session

A. Session-9: Advance Web Exploitation Techniques

I. Advanced SQL Injection Techniques
II. Cross-Site Request Forgery (CSRF)
III. Remote Code Execution (RCE) Concepts
IV. Authentication & Session Hijacking Attacks

B. Session-10: API Security & Secure Application Architecture

I. REST API Security Fundamentals
II. API Authentication & Token Security
III. Broken Access Control Vulnerabilities
IV. Secure Headers & Web Hardening

C. Assignment: Perform vulnerability assessment on a demo web application and document findings.

E-Quiz: Advanced web security & API protection concepts

D. Trainer Reference Links:

- https://owasp.org/www-project-top-ten/

Week-6: Advanced Penetration Testing / Soft Skill Session

A. Session-11: Advanced Penetration Testing Methodology

I. Red Team vs Blue Team Operations
II. Advanced Reconnaissance Techniques
III. Privilege Escalation Concepts
IV. Lateral Movement & Persistence

B. Session-12: Professional Skills for Cyber Security Experts

I. Technical Reporting Standards
II. Security Documentation & Audit Writing
III. Communication with Clients & Teams
IV. Ethical Disclosure Practices

C. Assignment: Simulate a penetration testing workflow and prepare a professional report.

D. Quiz: Penetration testing lifecycle & reporting standards

E. Trainer Reference Links:

- https://www.offensive-security.com/

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

Week-7: Advanced Malware Analysis / Soft Skill Session

A. Session-13: Malware Reverse Engineering & Threat Analysis
- I. Static vs Dynamic Malware Analysis
- II. Ransomware Behavior & Detection
- III. Trojan & Rootkit Analysis
- IV. Sandbox Environment Usage

B. Session-14: Cyber Threat Hunting & Research Skills
- I. Threat Hunting Methodologies
- II. IOC Identification Techniques
- III. Open-Source Intelligence (OSINT)
- IV. Security Research Workflow

C. Assignment: Analyze malware indicators and prepare a threat intelligence summary.

D. Quiz: Malware analysis & threat hunting concepts

E. Trainer Reference Links:
- https://malwareunicorn.org/

Week-8: Advanced Digital Forensics / Soft Skill Session

A. Session-15: Digital Forensics & Incident Investigation
- I. Memory & Disk Forensics
- II. Log Analysis & Event Correlation
- III. File Recovery Techniques
- IV. Network Forensics Fundamentals

B. Session-16: Investigation Reporting & Documentation
- I. Forensic Reporting Standards
- II. Evidence Documentation Techniques
- III. Chain of Custody Procedures
- IV. Professional Case Report Writing

C. Assignment: Conduct forensic investigation on sample evidence files.

D. Quiz: Digital forensics & evidence handling

E. Trainer Reference Links:
- https://www.sans.org/digital-forensics/

Week-9: **Cloud, IoT & Enterprise Security / Soft Skill Session**

A. Session-17: Enterprise & Cloud Security Operations
- I. Cloud Security Architecture
- II. Identity & Access Management (IAM)
- III. Container & Virtualization Security
- IV. IoT Security Challenges

B. Session-18: Security Awareness & Operational Excellence
- I. Security Governance Practices
- II. Cybersecurity Risk Awareness
- III. Security Policy Enforcement
- IV. Continuous Skill Development

C. Assignment: Prepare a cloud infrastructure risk assessment report.

D. Quiz: Enterprise cloud & IoT security concepts

E. Trainer Reference Links:
- https://cloud.google.com/security

Week-10: **Incident Response & SOC Operations / Soft Skill Session**

A. Session-19: Advanced Incident Response & SOC Workflow
- I. Security Operations Center (SOC) Fundamentals
- II. SIEM Tools & Log Correlation
- III. Incident Detection & Containment
- IV. Recovery & Post-Incident Analysis

B. Session-20: Cyber Crisis & Security Operations Management
- I. Crisis Communication in Cyber Incidents
- II. Team Coordination During Attacks
- III. Security Escalation Procedures
- IV. Decision-Making Under Pressure

C. Assignment: Design a complete incident response playbook.

D. Quiz: SOC operations & incident response lifecycle

E. Trainer Reference Links:
- https://www.sans.org/incident-response/

Week-11: **Security Operations, Compliance & Freelancing / Soft Skill Session** **A. Session 21: Advanced Security Operations & Compliance** I. Vulnerability Management Lifecycle II. Compliance Standards & Auditing III. Threat Intelligence Platforms IV. Security Monitoring & Alerting **B. Session 22: Cyber Security Career & Freelancing Development** I. Building Cybersecurity Case Studies II. Freelancing Security Services III. Portfolio & LinkedIn Optimization IV. Cybersecurity Certification Pathways **C. Assignment:** Build professional cybersecurity portfolio with practical case studies. **D. Quiz:** Security operations & freelancing concepts **E. Trainer Reference Links:** • https://www.cybrary.it/	**Week-12: Final Project & Career Development / Soft Skill Session** **A. Session-23: Advanced Cyber Security Capstone Project** I. End-to-End Security Assessment II. Vulnerability Identification & Exploitation III. Security Hardening & Defense Strategy IV. Final Technical Documentation **B. Session-24: Final Presentation & Career Preparation** I. Project Presentation & Demonstration II. Mock Technical Interview III. Cyber Security Career Roadmap IV. Professional Portfolio Review **C. Assignment:** Submit complete cyber security project with assessment report and presentation. **D. Final Quiz:** Comprehensive course assessment **E. Trainer Reference Links:** • https://www.cyberseek.org/

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

8. **Guest Session:** Cyber Security Expert / Ethical Hacker / SOC Analyst
   Topics Include:

   - Real-World Cyber Attacks & Defense Strategies
   - Ethical Hacking & Penetration Testing Industry Practices
   - SOC Operations & Threat Intelligence Workflow
   - Cyber Security Certifications & Career Roadmap
   - Freelancing & Remote Opportunities in Cyber Security
   - Industry Tools, Labs & Practical Learning Guidance