

Advanced Cyber Security Modules

Techcult

Module 1 : Intro to Cyber Security

- - Overview of Cybersecurity
- - Cyber Threat Landscape
- - Cybersecurity Principles
- - Legal and Ethical Considerations
- Practical: Case studies on recent cyber incidents.

Module 2 : Networking & Security Fundamentals

- - TCP/IP Protocol Suite
- - Network Design and Security Models
- - Firewalls, VPNs, and IDS/IPS
- Practical: Configure a firewall and set up a VPN.

Module 3 : Operating systems Security

- - Secure OS Configurations (Windows/Linux)
- - File System Security
- - User Account Control and Permissions
- Practical: Hardening Windows and Linux servers

Module 4 : Threats & Vulnerabilities

- - Types of Threats (Malware, Phishing, DDoS)
- - Vulnerability Assessment Techniques
- - Penetration Testing Basics
- Practical: Conduct vulnerability assessments using tools like Nessus

Module 5 : Security Monitoring & Incident Response

- - SIEM Tools and Log Management
- - Incident Response Plan Development
- - Digital Forensics Basics
- Practical: Use a SIEM tool to analyse logs and respond to incidents

Module 6 : Web & Application Security

- - OWASP Top Ten
- - Secure Software Development Life Cycle (SDLC)
- - API Security
- Practical: Perform security assessments on web applications

Module 7 : Cloud Security

- - Cloud Security Models (IaaS, PaaS, SaaS)
- - Data Protection in the Cloud
- - Cloud Compliance and Governance
- Practical: Set up and secure a cloud environment (AWS/Azure)

Module 8 : Encryption & Quantum Computing

- - Importance of Encryption: Overview and Types (Symmetric, Asymmetric)
- - Vulnerabilities of Classical Algorithms to Quantum Computing (Shor's Algorithm)
- - Post-Quantum Cryptography: Overview of promising algorithms
- - Quantum Key Distribution (QKD) Principles and Applications
- Practical: Implement a basic encryption algorithm and discuss its quantum vulnerabilities

Module 9 : Advanced Penetration Testing

- - Advanced Tools and Techniques
- - Social Engineering Tactics
- - Red Team vs. Blue Team Exercises
- Practical: Conduct a simulated penetration test on a network.

Module 10 : Cybersecurity Governance and Risk Management

- - Security Frameworks (NIST, ISO 27001)
- - Risk Assessment Methodologies
- - Policy Development and Compliance
- Practical: Create a risk management plan for a hypothetical organization

Module 11 : Emerging Technologies and Threats

- - IoT Security Challenges- Blockchain and Cybersecurity
- - AI and Machine Learning in Security
- Practical: Evaluate security implications of emerging technologies

Module 12 : Advanced Threat Detection and Mitigation

- - Threat Intelligence and Hunting
- - Anomaly Detection Techniques
- - Incident Simulation and Tabletop Exercises
- Practical: Simulate an advanced persistent threat scenario

Module 13 : Capstone Project

- Select a real-world cybersecurity problem
- Develop a comprehensive solution incorporating all learned skills.
- Presentation of findings and solutions to a panel.
- Practical: Weekly project updates and hands-on implementation of the solution

Additional Modules

Modules

○ **Network Security: Custom Proxy VPN Creation and Network Programming**

Learn network-level programming to create custom proxy VPNs and secure network traffic.

○ **Operating Systems: OS Variants and Server Technologies with Database Integration**

Study various OS variants (Windows, Linux, etc.) and their integration with database security technologies.

○ **Threat Management: Third-party Protection and Advanced Threat creation**

Explore third-party protection tools and develop advanced types of cyber threats.

Modules

○ **Advanced Monitoring: Log Formatting and AI Implementation**

Implement advanced log formatting techniques and apply AI to enhance security monitoring.

○ **Software and API Security: Strengthening or Ignoring Security Practices**

Focus on advanced techniques for strengthening software and API security, or assess when certain security measures can be deprioritized.

○ **Cloud Security: Loopholes and Socket Programming Issues**

Identify current security loopholes in cloud environments and examine problems related to socket programming.

Modules

- **Quantum Computing: Research on Impact and Solutions**

Conduct research on how quantum computing impacts classical encryption algorithms and propose solutions.

- **Advanced Penetration Testing Tools: Custom Relay Server and DNS Creation**

Develop custom relay servers and DNS solutions for advanced penetration testing scenarios.

- **Cybersecurity Modules: Custom Layers and Reverse Attack Techniques**

Design custom security layers and explore reverse attack strategies through request line analysis and session learning

Modules

○ **Current Challenges in Cybersecurity**

Examine the most pressing current challenges in cybersecurity through case studies and research. • Threat Detection and Emergency Aid

○ **Threat Detection and Emergency Aid**

Explore techniques for detecting major threats and providing emergency aid to mitigate damage.

○ **Project Types: Major and Minor**

Capstone projects may include major and minor options, with major projects extending beyond the course time line for deeper exploration