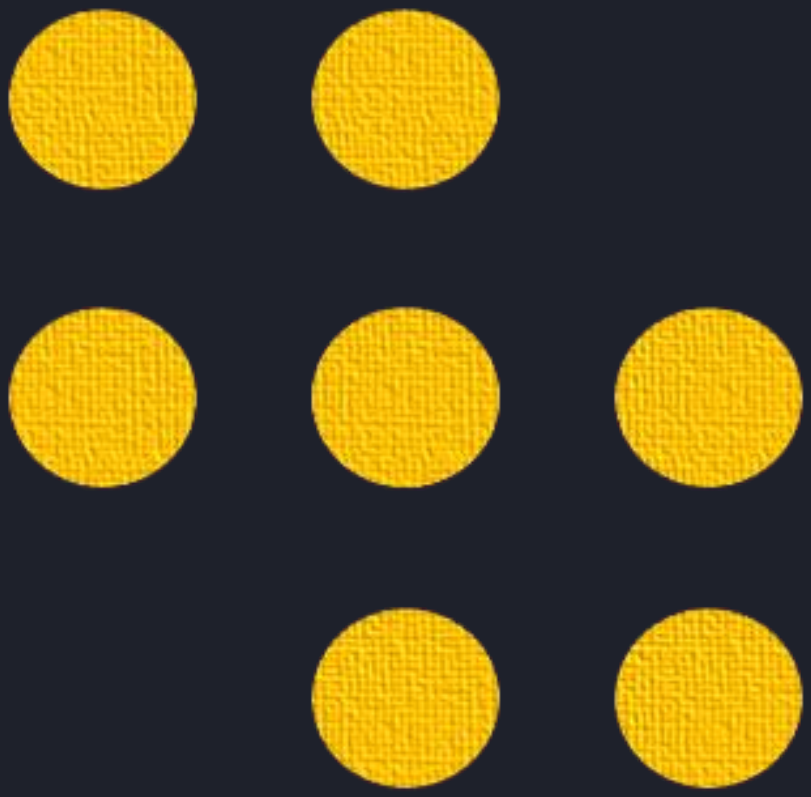
FIGURESHUB



CYBER SECURITY SYLLABUS

FIGURESHUB

Cyber Security Syllabus

COURSE OVERVIEW

The Comprehensive Cyber Security Program at FiguresHub is a 6-month intensive training designed to equip participants with the knowledge and practical skills needed to thrive in the dynamic field of cybersecurity. The program covers a wide range of topics, from foundational principles to advanced techniques, ensuring that students develop a deep understanding of cybersecurity concepts and can apply them effectively in real-world scenarios.

REQUIREMENTS

- No prior mobile development experience is required.
- A fully functional laptop that is able to access the internet.
- Minimal hardware requirements for laptop [core i7, 256 SSD, and 16Gb of RAM]

RESOURCES

VirtualBox or VMware, Kali Linux, OWASP WebGoat, Wireshark, Nmap, Burp Suite, etc.

FIGURESHUB

COURSE CURRICULUM

WEEK	CONTENT
Week 1	**Introduction to Cyber Security Fundamentals** • Understanding threats and vulnerabilities • Introduction to risk management
Week 2	**Networking Essentials for Cyber Security** • TCP/IP basics • Subnetting and addressing. • Firewalls and network security principles
Week 3	**Operating System Security** • Securing Windows and Linux systems • User authentication and access controls
Week 4	**Cryptography Basics** • Encryption and decryption • Public and private key infrastructure • Digital signatures and certificates ***Hands-on Project:*** *Set up a basic secure network with firewalls, user authentication, and encrypted communication*
Week 5	**Web Application Architecture and Security** • Understanding web application components • Common web vulnerabilities (OWASP Top Ten)
Week 6	**Secure Coding Practices** • Best practices for writing secure code. • Code review techniques
Week 7	**Web Application Firewalls (WAF)** • Implementing and configuring WAF • Web server hardening
Week 8	**Database Security** • Securing databases and SQL injections

	• Database encryption and access controls ***Hands-on Project:*** *Conduct a web application penetration testing on a simulated environment, addressing vulnerabilities and implementing secure coding practices.*
Week 9	**Introduction to Threat Intelligence** • Understanding threat feeds • Cyber threat modeling
Week 10	**Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)** • Configuring and managing IDS/IPS • Analyzing and responding to alerts
Week 11	**Incident Response Planning** • Developing incident response plans • Role of incident responders
Week 12	**Digital Forensics Basics** • Evidence collection and preservation • Disk and memory forensics ***Hands-on Project:*** *Simulate a cyber incident and guide students through the incident response process, including forensics analysis.*
Week 13	**Advanced Firewall Configuration** • Application-layer filtering • VPNs and secure communications
Week 14	**Wireless Network Security** • Securing Wi-Fi networks • WPA3 and other encryption methods

Week 15	**Virtualization and Cloud Security** • Securing virtual environments • Cloud security principles
Week 16	**IoT Security** • Risks and vulnerabilities in IoT devices • Securing IoT networks ***Hands-on Project:*** *Design and implement a secure network architecture, including firewall configurations, VPN setup, and securing IoT devices.*
Week 17	**Introduction to Penetration Testing** • Types of penetration testing • Legal and ethical considerations
Week 18	**Scanning and Enumeration** • Network and application scanning • Enumeration techniques
Week 19	**Exploitation and Post-Exploitation** • Exploiting vulnerabilities • Maintaining access and post-exploitation tactics
Week 20	**Report Writing and Documentation** • Creating comprehensive penetration testing reports • Communicating findings to stakeholders ***Hands-on Project:*** *Conduct a penetration test on a provided environment, produce a detailed report, and present findings to the class.*
Week 21	**Advanced Cryptography** • Blockchain and cryptocurrency security • Quantum computing implications

Week 22	**Security in DevOps** • Integrating security into the development process • Continuous integration and continuous deployment (CI/CD) security
Week 23	**Secure Coding Review and Best Practices** • Review of secure coding principles • Practical application in real-world scenarios
Week 24	**Capstone Project** • Design and implement a comprehensive security solution for a fictitious company. • Present the solution, addressing challenges and demonstrating key learnings. ***Hands-on Project:*** *The capstone project will serve as the culmination of the program, allowing students to apply all learned skills in a real-world scenario.*

ADDITIONAL INFORMATION

Our Cyber Security course not only provides a robust curriculum but also emphasizes mentorship and community collaboration. With dedicated instructors and a vibrant learner community, you'll benefit from personalized guidance and industry insights. Enjoy lifetime access to resources, exclusive webinars, and continuous support for a successful learning journey. Receive a completion certificate and join a digital security community that values your success.