BlueTech
we create new talents

Advanced Cybersecurity and Penetration Testing

In this program, you will dive deep into the world of cybersecurity, learning advanced techniques to protect networks, systems, and applications. Discover the latest vulnerabilities and exploits as you explore network security, web application security, wireless network security, malware analysis, social engineering, cryptography, incident response, and more. Develop the skills needed to identify and mitigate cyber threats through hands-on exercises and real-world scenarios. Get ready to become a proficient cybersecurity professional and skilled penetration tester.

Target audience

Basic programming capabilities (in any language).
Basic background in cyber is required, including familiarity with the following topics:

- Computer networks key concepts (Router, IP and MAC addresses, proxy)
- Basic communication protocols (DNS, ARP, ICMP, TCP, UDP, HTTP)
- Basic cyber concepts (DoS, MITM, bufferoverflow, XSS, SQLi)
- Basic defense concepts (Firewall, IDS/IPS, WAF, Anti-Virus)

Course Duration: 40 hours

Module 1: Introduction to Cybersecurity

- Overview of cybersecurity fundamentals
- Understanding the threat landscape
- Security frameworks and compliance standards
- Security policies and incident response
- Introduction to ethical hacking and penetration testing

Module 2: Network Security

- Network architecture and protocols
- Network vulnerabilities and attacks
- Network scanning and enumeration
- Intrusion detection and prevention systems
- Network hardening and security best practices

Module 3: Web Application Security

- Web application architecture and components
- Common web application vulnerabilities (OWASP Top 10)
- Web application penetration testing methodologies
- Secure coding practices and input validation
- Web application firewall (WAF) and secure configuration

Module 4: Wireless Network Security

- Wireless network fundamentals (Wi-Fi, Bluetooth)
- Wireless encryption and authentication
- Wireless network attacks (e.g., rogue access points)
- Wireless penetration testing techniques
- Wireless network security best practices

Module 5: Vulnerability Assessment and Management

- Vulnerability assessment methodologies and tools
- Vulnerability scanning and penetration testing
- Vulnerability exploitation and proof of concept
- Vulnerability reporting and remediation
- Patch management and vulnerability management frameworks

Module 6: Malware Analysis and Reverse Engineering

- Malware types and characteristics
- Malware analysis techniques and tools
- Static and dynamic malware analysis
- Code obfuscation and anti-reverse engineering techniques
- Reverse engineering malware samples

Module 7: Social Engineering and Physical Security

- Social engineering techniques and methodologies
- Phishing attacks and email security
- Physical security assessments and controls
- Social engineering prevention and awareness
- Security awareness training for employees

Module 8: Cryptography and PKI

- Cryptographic concepts and algorithms
- Symmetric and asymmetric encryption
- Hash functions and digital signatures
- Public Key Infrastructure (PKI) and certificates
- Secure key management and cryptographic protocols

Module 9: Incident Response and Forensics

- Incident response lifecycle and procedures
- Incident detection, containment, and recovery
- Digital forensics principles and methodologies
- Forensic analysis of systems and network logs
- Chain of custody and evidence handling

Module 10: Advanced Topics in Cybersecurity

- Cloud security and virtualization
- Internet of Things (IoT) security
- Red teaming and adversary simulation
- Threat intelligence and security monitoring
- Emerging trends and challenges in cybersecurity

***Note**: The course structure and topics can be customized according to the specific needs and requirements of the participants.*