**About the Course**

The **Certified Ethical Hacker (CEH)** program is a globally recognized certification designed to train students in identifying, understanding, and mitigating potential cyber threats. This intensive full-time program offered by Shaheed Sukhdev College of Business Studies (SSCBS) combines theoretical learning with hands-on practice. It delves into the world of ethical hacking, enabling participants to adopt the mindset of hackers to strengthen organizational cybersecurity systems.

Key highlights include:

* Comprehensive training in 20 core modules, including system hacking, malware threats, and social engineering.
* Hands-on labs with over 4,000 tools and simulated attack scenarios.
* Industry-relevant methodologies to enhance the cybersecurity posture of businesses.

**Rationale**

In today’s hyper-connected world, cybersecurity breaches are among the most significant risks faced by organizations. The growing dependency on digital systems has created a critical need for skilled ethical hackers who can proactively protect assets. This course aligns with SSCBS’s commitment to delivering industry-driven programs that address pressing global challenges while fostering innovation and career growth.

**Aim**

To empower participants with cutting-edge ethical hacking skills and knowledge, enabling them to secure digital environments, mitigate risks, and drive proactive cybersecurity initiatives.

**Learning Outcomes**

By the end of the program, participants will:

* Demonstrate mastery of ethical hacking techniques and tools.
* Assess and enhance the cybersecurity posture of organizations.
* Perform vulnerability assessments and penetration testing effectively.
* Understand compliance requirements and develop security policies.
* Apply countermeasures to prevent potential threats and breaches.

**Objectives**

* To build a strong foundation in ethical hacking methodologies.
* To enable hands-on experience with real-world cyber-attack scenarios.
* To foster problem-solving skills for tackling emerging cybersecurity challenges.
* To prepare participants for the globally recognized CEH certification examination.

**Target Audience**

* Final-year undergraduates or postgraduates in IT, Computer Science, or related disciplines.
* Professionals in IT, network administration, or software development aiming to upskill in cybersecurity.
* Entrepreneurs and startups looking to secure their digital assets.

**Future Prospects**

Graduates of the CEH program can pursue a wide range of career opportunities, including:

* Ethical Hacker
* Cybersecurity Analyst
* Security Consultant
* Penetration Tester
* Risk Assessment Specialist
* Security Operations Center (SOC) Analyst
This program also positions participants for leadership roles in the rapidly growing cybersecurity domain, ensuring long-term career stability and growth.

**Resource Persons**

The program will be led by industry-certified professionals and academic experts with extensive experience in cybersecurity, ethical hacking, and IT governance.

Key profiles include:

* EC-Council-certified instructors.
* Practitioners from leading cybersecurity firms.
* Experts in ethical hacking and digital forensics.

**Brief Profile of Participating Institute**

Shaheed Sukhdev College of Business Studies (SSCBS), a premier institute under the University of Delhi, is renowned for its commitment to excellence in education and industry-oriented programs. Recognized as one of the top colleges for business studies in India, SSCBS combines academic rigor with practical training to produce industry-ready professionals. The college is equipped with state-of-the-art facilities, fostering an environment of innovation, research, and skill development.

Syllabus:

|  |  |  |  |
| --- | --- | --- | --- |
| **Unit** | **Module** | **Hours Assigned** | **Total** |
| **Unit 1: Introduction to Ethical Hacking and Reconnaissance** |   |   |   |
|   | Module 01: Introduction to Ethical Hacking | 2 Hours | 10 |
|   | Module 02: Footprinting and Reconnaissance | 8 Hours |
| **Unit 2: Network Scanning, Enumeration, and Vulnerability Analysis** |   |   |   |
|   | Module 03: Scanning Networks | 4 Hours | 10 |
|   | Module 04: Enumeration | 3 Hours |
|   | Module 05: Vulnerability Analysis | 3 Hours |
| **Unit 3: System Hacking, Malware, and Sniffing** |   |   |   |
|   | Module 06: System Hacking | 4 Hours | 10 |
|   | Module 07: Malware Threats | 3 Hours |
|   | Module 08: Sniffing | 3 Hours |
| **Unit 4: Social Engineering, Denial-of-Service, and Web Security** |   |   |   |
|   | Module 09: Social Engineering | 3 Hours | 10 |
|   | Module 10: Denial-of-Service | 4 Hours |
|   | Module 11: Session Hijacking | 3 Hours |
| **Unit 5: Web Application and Infrastructure Security** |   |   |   |
|   | Module 12: Evading IDS, Firewalls, and Honeypots | 3 Hours | 10 |
|   | Module 13: Hacking Web Servers | 2 Hours |
|   | Module 14: Hacking Web Applications | 2 Hours |
|   | Module 15: SQL Injection | 3 Hours |
| **Unit 6: Advanced Topics in Security** |   |   |   |
|   | Module 16: Hacking Wireless Networks | 3 Hours | 10 |
|   | Module 17: Hacking Mobile Platforms | 2 Hours |
|   | Module 18: IoT and OT Hacking | 2 Hours |
|   | Module 19: Cloud Computing | 2 Hours |
|   | Module 20: Cryptography | 1 Hour |
|   |   |   |   |
| **Total Hours: 60 hours (6 Units, 10 hours each).** |   |   |   |

**Lab Hours:**

|  |  |  |
| --- | --- | --- |
| **Module** | **Lab Activities** | **Hours Assigned** |
| **Module 01: Introduction to Ethical Hacking** | N/A | 0.5 Hours |
| **Module 02: Footprinting and Reconnaissance** | Perform Footprinting Through Search Engines | 1 Hour |
|   | Perform Footprinting Through Web Services | 1 Hour |
|   | Perform Footprinting Through Social Networking Sites | 1 Hour |
|   | Perform Website Footprinting | 1 Hour |
|   | Perform Email Footprinting | 1 Hour |
|   | Perform Whois Footprinting | 1 Hour |
|   | Perform DNS Footprinting | 1 Hour |
|   | Perform Network Footprinting | 1 Hour |
|   | Perform Footprinting using Various Footprinting Tools | 1 Hour |
| **Module 03: Scanning Networks** | Perform Host Discovery | 1 Hour |
|   | Perform Port and Service Discovery | 1 Hour |
|   | Perform OS Discovery | 1 Hour |
|   | Scan beyond IDS and Firewall | 1 Hour |
|   | Perform Network Scanning using Various Scanning Tools | 1 Hour |
| **Module 04: Enumeration** | Perform NetBIOS Enumeration | 1 Hour |
|   | Perform SNMP Enumeration | 1 Hour |
|   | Perform LDAP Enumeration | 1 Hour |
|   | Perform NFS Enumeration | 1 Hour |
|   | Perform DNS Enumeration | 1 Hour |
| **Module 05: Vulnerability Analysis** | Perform Vulnerability Research with Vulnerability Scoring Systems | 1 Hour |
|   | Perform Vulnerability Assessment using Various Vulnerability Assessment Tools | 1 Hour |
| **Module 06: System Hacking** | Gain Access to the System | 1 Hour |
|   | Perform Privilege Escalation to Gain Higher Privileges | 1 Hour |
|   | Maintain Remote Access and Hide Malicious Activities | 1 Hour |
|   | Clear Logs to Hide the Evidence of Compromise | 1 Hour |
| **Module 07: Malware Threats** | Gain Access to the Target System using Trojans | 1 Hour |
|   | Infect the Target System using a Virus | 1 Hour |
|   | Perform Static Malware Analysis | 1 Hour |
|   | Perform Dynamic Malware Analysis | 1 Hour |
| **Module 08: Sniffing** | Perform Active Sniffing | 1 Hour |
|   | Perform Network Sniffing using Various Sniffing Tools | 1 Hour |
| **Module 09: Social Engineering** | Perform Social Engineering using Various Techniques | 1 Hour |
|   | Detect a Phishing Attack | 1 Hour |
| **Module 10: Denial-of-Service** | Perform DoS and DDoS Attacks using Various Techniques | 1 Hour |
|   | Detect and Protect Against DoS and DDoS Attacks | 1 Hour |
| **Module 11: Session Hijacking** | Perform Session Hijacking | 1 Hour |
|   | Detect Session Hijacking | 1 Hour |
| **Module 12: Evading IDS, Firewalls, and Honeypots** | Perform Intrusion Detection using Various Tools | 1 Hour |
| **Module 13: Hacking Web Servers** | Footprint the Web Server | 1 Hour |
|   | Perform a Web Server Attack | 1 Hour |
| **Module 14: Hacking Web Applications** | Footprint the Web Infrastructure | 1 Hour |
|   | Perform Web Application Attacks | 1 Hour |
| **Module 15: SQL Injection** | Perform SQL Injection Attacks | 1 Hour |
|   | Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools | 1 Hour |
| **Module 16: Hacking Wireless Networks** | Perform Wireless Traffic Analysis | 1 Hour |
|   | Perform Wireless Attacks | 1 Hour |
| **Module 17: Hacking Mobile Platforms** | Hack Android Devices | 1 Hour |
|   | Secure Android Devices using Various Android Security Tools | 1 Hour |
| **Module 18: IoT and OT Hacking** | Perform Footprinting using Various Footprinting Techniques | 1 Hour |
|   | Capture and Analyze IoT Device Traffic | 1 Hour |
| **Module 19: Cloud Computing** | Perform S Bucket Enumeration using Various S Bucket Enumeration Tools | 1 Hour |
|   | Exploit S Buckets | 1 Hour |
| **Module 20: Cryptography** | Encrypt the Information using Various Cryptography Tools | 1 Hour |
|   | Create a Self-signed Certificate | 1 Hour |
|   | Perform Email Encryption | 1 Hour |
|   | Perform Disk Encryption | 1 Hour |
|   | Perform Cryptanalysis using Various Cryptanalysis Tools |  1 Hour |