TS
TECH TEACH
EDUCATIONALSOLUTIO

Ethical Hacking

OUR MISSION :

"Our mission is to empower learners worldwide through innovative technology, personalized learning experiences, and accessible educational resources. We strive to cultivate a community where every individual can achieve their full potential, regardless of their background or circumstances."

OUR VALUES :

"To pioneer the future of education by leveraging cutting-edge technology to make learning more engaging, effective, and inclusive. We envision a world where education transcends boundaries, creating opportunities for lifelong learning and fostering a society enriched by knowledge and creativity."

COURSE CURRICULUM:

Week 1: Introduction to Ethical Hacking

- Day 1-2: Overview of Ethical Hacking
  - Definition, importance, and scope of ethical hacking.
  - Difference between ethical hacking, penetration testing, and malicious hacking.
- Day 3-4: Understanding Cybersecurity Fundamentals
  - Basics of cybersecurity: CIA triad (Confidentiality, Integrity, Availability).
  - Types of cyber threats and attack vectors.
- Day 5: Legal and Ethical Issues
  - Laws and regulations related to hacking and cybersecurity.
  - Ethical guidelines and responsibilities of ethical hackers.

COURSE CURRICULUM:

Week 2: Setting Up the Environment

- Day 1-2: Introduction to Linux and Command Line
  - Basic Linux commands and navigation.
  - File permissions and system administration.
- Day 3-4: Virtualization and Lab Setup
  - Setting up virtual machines using VirtualBox or VMware.
  - Installing and configuring Kali Linux.
- Day 5: Introduction to Networking
  - Understanding network architecture and protocols (TCP/IP, DNS, DHCP).
  - Basic networking commands and tools (ping, traceroute, netstat).

COURSE CURRICULUM:

Week 3: Reconnaissance and Scanning

- Day 1-2: Information Gathering Techniques
  - Passive reconnaissance: WHOIS lookup, social engineering, OSINT (Open Source Intelligence).
  - Active reconnaissance: network scanning, footprinting.
- Day 3-4: Network Scanning Tools
  - Using tools like Nmap for network discovery and port scanning.
  - Advanced Nmap usage and scripting.
- Day 5: Vulnerability Scanning
  - Introduction to vulnerability scanners (Nessus, OpenVAS).
  - Performing and analyzing vulnerability scans.

COURSE CURRICULUM:

Week 4: Enumeration and Exploitation

- Day 1-2: Enumeration Techniques
  - Identifying and gathering information about network resources.
  - Using tools like Netcat and Enum4linux.
- Day 3-4: Exploitation Basics
  - Understanding exploits and vulnerabilities.
  - Introduction to Metasploit Framework.
- Day 5: Practical Exploitation
  - Conducting basic exploitation using Metasploit.
  - Post-exploitation techniques and maintaining access.

COURSE CURRICULUM:

Week 5: Web Application Hacking

- Day 1-2: Introduction to Web Application Security
  - Understanding web architecture and common vulnerabilities (OWASP Top 10).
  - Basics of HTTP, HTTPS, and web sessions.
- Day 3-4: Attacking Web Applications
  - SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).
  - Hands-on with Burp Suite for web application testing.
- Day 5: Web Application Security Tools
  - Using tools like OWASP ZAP, Nikto, and SQLmap.
  - Analyzing and mitigating web vulnerabilities.

COURSE CURRICULUM:

Week 6: Wireless Network Hacking

- Day 1-2: Introduction to Wireless Security
    - Understanding wireless networking (Wi-Fi protocols, encryption).
    - Common wireless attacks (WEP/WPA cracking, Rogue AP).
- Day 3-4: Wireless Hacking Tools
    - Using tools like Aircrack-ng, Wireshark, and Kismet.
    - Performing wireless network penetration testing.
- Day 5: Practical Wireless Attacks
    - Conducting deauthentication attacks.
    - Capturing and cracking WPA/WPA2 handshakes.

COURSE CURRICULUM:

Week 7: Advanced Topics in Ethical Hacking

- Day 1-2: Social Engineering Attacks
    - Phishing, pretexting, baiting, and tailgating.
    - Creating and deploying phishing campaigns.
- Day 3-4: Buffer Overflow Attacks
    - Understanding buffer overflow vulnerabilities.
    - Writing and exploiting buffer overflow vulnerabilities.
- Day 5: Cryptography and Encryption
    - Basics of cryptography: symmetric vs. asymmetric encryption.
    - Common cryptographic attacks and tools.

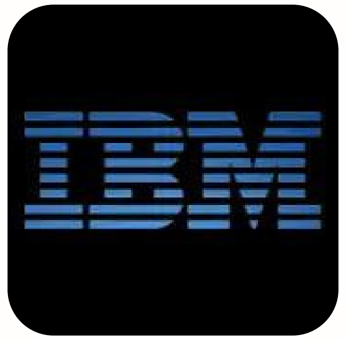
COURSE CURRICULUM:

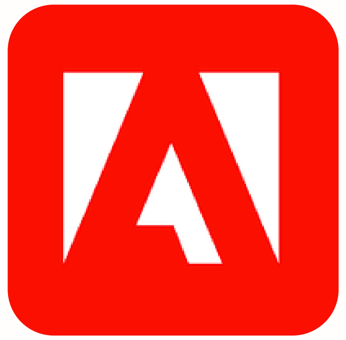
Week 8: Final Project and Presentations

- Day 1-4: Final Project Development
    - Students work on a comprehensive final project that integrates multiple aspects of the curriculum.
    - Examples: Penetration testing of a simulated environment, securing a vulnerable web application.
- Day 5: Project Presentation and Evaluation
    - Students present their projects.
    - Feedback and evaluation.

Our Partners Company's

WIPRO
Applying Thought





HCLTech | Supercharging

All India Council for Technical Education
AICTE
योगः कर्मसु कौशलम्

TATA
CONSULTANCY
SERVICES
tcs

TS

TECH TEACH

EDUCATIONALSOLUTIO

FOR SUPPORT

+91 9652379012

www.techteachedsols.com

tech.ed.sols@gmail.com

THANK YOU

www.techteachedsols.com