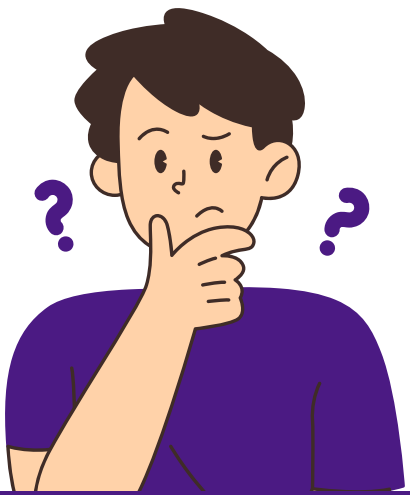
NEXTECH SKILLS

Ethical Hacking Course.

6 Months

Are you ready to dive into the world of Ethical Hacking and learn how to defend against cyber threats?

At NexTech Skills, our Ethical Hacking Course is tailored to empower you with the tools and knowledge to protect digital systems effectively. Learn how to identify vulnerabilities, safeguard data, and mitigate threats using practical, real-world strategies. Whether you're a beginner or seeking to advance your skills, this course will equip you with the expertise to excel in the cybersecurity field. Join us today and start your journey to becoming a certified Ethical Hacker and a protector of the digital world!



Month 1: Cybersecurity Foundations

Week 1: Introduction to Ethical Hacking and Cybersecurity

- Ethical hacking vs. cracking: Overview and distinctions
- Legal and ethical considerations in cybersecurity
- Career paths in cybersecurity

Week 2: Networking Fundamentals

- TCP/IP protocols: Understanding the basics
- Network topologies: Types and their applications
- Subnetting: Basic concepts and examples
- Network devices: Roles and configurations of routers, switches, and firewalls

Week 3: Operating Systems

- Linux fundamentals: Overview and command-line interface basics
- Windows fundamentals: Overview and command-line interface basics
- File systems: Structure and navigation in Linux and Windows
- Permissions: Managing and configuring access controls

Week 4: Security Concepts

- Threat modeling: Identifying and prioritizing threats
- Risk assessment: Evaluating and managing risks
- Vulnerability management: Tools and processes for finding and addressing vulnerabilities
- Security policies: Developing and implementing procedures

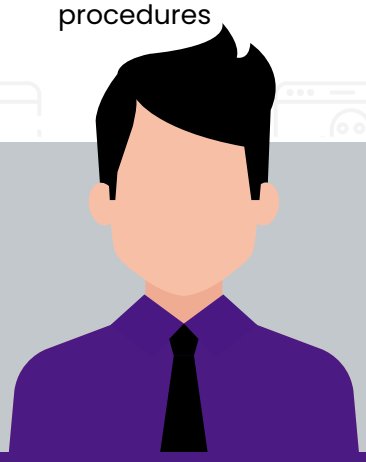
Month 2: Network Security and Scanning

Week 1: Introduction to Network Security

- Network security basics: Importance and principles
- Firewalls: Types and configurations
- Intrusion detection and prevention systems (IDPS): Overview and practical usage
- Virtual private networks (VPNs): Secure remote access setup

Week 2: Network Scanning

- Port scanning: Introduction to Nmap and practical usage
- Vulnerability scanning: Tools and techniques
- Network mapping: Understanding and visualizing network structures
- Service enumeration: Identifying running services on networked systems



As an experienced instructor, I am passionate about helping students understand how to safeguard computers and networks from cyber threats. My teaching emphasizes protecting data, mitigating online risks, and understanding the principles of cybersecurity. In class, we explore ethical hacking, methods to prevent cyberattacks, and the laws that ensure online safety. Through engaging activities and real-world examples, I aim to prepare students for successful careers in cybersecurity.

Week 3: System Hacking and Malware Analysis

- System hacking: Techniques and countermeasures
- Malware analysis: Types, detection methods, and response strategies
- Secure remote access: Practical applications and best practices

Week 4: Footprinting and Reconnaissance

- Information gathering techniques: Basics and tools
- Open-source intelligence (OSINT): Using publicly available data for reconnaissance
- Domain name system (DNS) analysis: Understanding DNS records and their implications

Month 3: System Hacking and Malware Analysis

Week 1: Password Cracking and Privilege Escalation

- Password cracking: Techniques, tools, and countermeasures
- Privilege escalation: Methods and mitigation strategies
- Hands-on practice: Simulating password attacks and escalation scenarios

Week 2: System Exploitation and Rootkits

- System exploitation: Identifying and exploiting vulnerabilities
- Rootkits: Types, functionalities, and detection methods
- Practical exercises: Understanding rootkit behavior and removing threats

Week 3: Malware Analysis (Part 1)

- Malware types: Overview of viruses, worms, trojans, and more
- Malware lifecycle: From creation to impact
- Static analysis: Inspecting malware code without execution

Week 4: Malware Analysis (Part 2)

- Dynamic analysis: Analyzing malware behavior during execution
- Malware prevention: Tools and best practices to mitigate risks
- Malware removal: Techniques to clean infected systems

Month 4: System Hacking and Malware Analysis

Week 1: Introduction to Web Technologies

- Web technologies: HTML, CSS, and JavaScript basics
- Understanding web servers and databases: Functionality and configuration
- Building a simple web page with HTML, CSS, and JavaScript

Week 2: Web Application Security (Part 1)

- OWASP Top 10 vulnerabilities: Overview and importance
- SQL injection: Understanding, exploitation, and prevention
- Cross-site scripting (XSS): Types, attacks, and mitigation

Week 3: Web Application Security (Part 2)

- Cross-site request forgery (CSRF): Understanding attacks and prevention techniques
- Session management: Secure handling of sessions in web applications
- Practical examples: Identifying and fixing vulnerabilities

Week 4: Web Application Penetration Testing

- Manual testing: Techniques for assessing web app security
- Automated testing: Using tools to identify vulnerabilities
- Vulnerability scanning tools: Overview and hands-on practice with tools

Month 5: Wireless and Network Security

Week 1: Wireless Protocols and Network Security

- Wireless protocols: Understanding 802.11 standards
- Wireless network security: WEP, WPA, WPA2, and their vulnerabilities
- Wi-Fi Protected Setup (WPS): Functionality and common security flaws

Week 2: Wireless Hacking Techniques

- Wireless hacking techniques: Tools and methods
- WPS attacks: Exploitation and countermeasures
- Hands-on practice: Simulating attacks on wireless networks in a controlled environment

Week 3: Network Security Testing

- Penetration testing methodology: Steps and best practices
- Ethical hacking tools: Overview of Metasploit and Kali Linux
- Reporting and documentation: Writing effective security reports

Week 4: Advanced Topics and Capstone Project

- Advanced topics: Cloud security fundamentals and challenges
- IoT security: Understanding threats and mitigation strategies
- Capstone project: Applying learned techniques in a practical, real-world scenario

Month 6: Wireless and Network Security

Week 1: Cloud Security and IoT Security

- Cloud Security: Overview, challenges, and best practices
- IoT Security: Understanding vulnerabilities in IoT devices and securing them

Week 2: Mobile Security and Cryptography

- Mobile Security: Common threats and protection techniques for mobile platforms
- Cryptography: Basics of encryption, hashing, and secure communications

Week 3: Incident Response and Preparation for Capstone Project

- Incident Response: Steps for detecting, responding to, and recovering from security incidents
- Planning the Capstone Project: Defining objectives, scope, and team roles

Week 4: Capstone Project Execution and Presentation

- Real-world ethical hacking simulation: Conducting penetration tests and analyzing results
- Team-based project: Collaborative work to identify and address vulnerabilities
- Presentation: Delivering findings, providing recommendations, and discussing lessons learned