Ethical Hacking/ Cyber Security

Course Duration: 1.5 Months • Class Time: 1.5 Hrs

Module 1: Introduction to Ethical Hacking and an Overview of EH v13

- Introduction to Ethical Hacking
- Importance of ethical hacking in modern cybersecurity
- Ethical hacking concepts, methodologies, and frameworks
- Overview of EH v13 syllabus and objectives
- Current Trends in Cybersecurity
- Evolution of threats (from traditional to AI-enhanced)
- Role of AI in modern cybersecurity practices

Module 2: An Introduction to AI and Machine Learning in Cybersecurity

- Fundamentals of AI and Machine Learning
- Basics of Machine Learning and AI - and their usage in cybersecurity
- Key ML algorithms (supervised, unsupervised, and reinforcement learning)
- Introduction to neural networks, deep learning, and natural language processing (NLP)
- AI-Powered Cyber Threat Landscape
- Understanding how cyber attackers leverage AI
- Examples of AI-driven threats (e.g., automated phishing, AI-based malware)
- Challenges in defending against AI-enhanced attacks

Module 3: Reconnaissance and Footprinting with AI

- Reconnaissance Techniques
- Traditional reconnaissance techniques: open-source intelligence (OSINT), social engineering, network scanning
- How AI enhances reconnaissance (data mining, automated OSINT tools)
- AI for Footprinting and Threat Intelligence
- Introduction to threat intelligence with machine learning models
- Hands-on labs with AI-enhanced footprinting tools
- Tools: Maltego, Shodan, SpiderFoot, and AI-based OSINT frameworks

Module 4: Scanning Networks with AI-Based Tools

- Network Scanning Techniques
- Basics of network scanning: port scanning, vulnerability assessment, and network mapping
- AI-Driven Network Scanning
- Using AI for dynamic network vulnerability scanning
- Demonstrating automated threat detection using AI-enabled network scanning tools (e.g., Darktrace, ExtraHop)
- Hands-on lab: AI-based vulnerability scanning with Nessus and OpenVAS

Module 5: System Hacking and AI for Threat Detection

- System Hacking Phases
- Classic techniques for gaining access, increasing privileges, staying in control, and track covering
- Using AI in systems for detection like Intrusion Detection Systems (IDS) and prevent intrusion like Intrusion Prevention Systems (IPS)
- AI-driven anomaly detection and pattern recognition
- Introduction to AI-powered IDS/IPS systems
- Tools: Splunk, QRadar, and other AI-enabled threat detection tools
- Hands-on Lab: Detecting Intrusions with AI
- Practicing anomaly detection and incident response with AI-enabled IDS/IPS

Module 6: Malware Analysis with Machine Learning

- Introduction to Malware and Reverse Engineering
- Types of malware, attack vectors, and traditional detection techniques
- Machine Learning in Malware Detection
- Usage of supervised and unsupervised machine learning in order to identify and classify malware
- AI techniques in behavior-based malware detection (e.g., file and process anomaly detection)
- Hands-on lab: Using ML to classify and detect malware (e.g., by training models on labeled malware datasets)

Module 7: Social Engineering and AI-based Defense Mechanisms

- Social Engineering Techniques
- Overview of social engineering attacks like phishing, pretexting, baiting, and tailgating
- Using AI for Phishing Detection
- NLP for detecting phishing emails
- AI-based user behavior analytics to recognize anomalous actions
- Hands-on Lab: Building an NLP model to detect phishing emails

Module 8: Web Application Security with AI

- Web Application Attacks
- Common vulnerabilities: SQL injection, XSS, CSRF, and others
- AI in Web Application Security
- AI-based web application firewalls (WAF)
- Real-time detection and prevention with AI-powered security tools
- Hands-on Lab: Using AI tools for real-time web application threat detection (e.g., ModSecurity with ML add-ons)

Module 9: Wireless Network Security and AI

- Wireless Network Attacks
- WPA/WPA2 cracking, Evil Twin, and other wireless attacks
- AI for Wireless Intrusion Detection
- Using AI to monitor and detect wireless network anomalies
- AI-enabled tools for wireless security (e.g., Aircrack-ng with machine learning enhancements)

Module 10: Mobile Platform Security and AI

- Mobile Threats
- Mobile vulnerabilities and attack vectors
- Reverse engineering and exploitation of mobile applications
- Machine Learning for Mobile Threat Detection
- Using ML models to detect mobile malware and anomalies
- Hands-on lab: Analyzing mobile applications using AI-based malware detection frameworks

Module 11: Cloud Security and AI-driven Defense

- Overview of Cloud Security Threats
- Common threats in cloud environments: data breaches, misconfigurations, account hijacking
- AI for Cloud Security
- Leveraging AI for cloud-native security solutions
- Incident detection and response in cloud environments with AI-powered SIEM tools
- Hands-on lab: Setting up an AI-driven monitoring and incident response system in a cloud environment

Module 12: AI-Driven Incident Response and Forensics

- Introduction to Digital Forensics
- Incident response steps: prepare, detect, contain, eradicate, and recover
- AI for Incident Response and Forensic Analysis
- Using AI for analysis of logs, sending automated alerts, and analysing root cause
- Forensic tools with AI capabilities
- Hands-on lab: Forensic investigation using AI-enabled tools (e.g., CrowdStrike, Sumo Logic)

Module 13: Ethical Hacking using AI for Automation and Scripting

- Automating Ethical Hacking with AI
- Overview of AI-powered automation tools and frameworks
- Integrating AI and Python for hacking automation
- Hands-on lab: Automating common hacking tasks using AI and Python scripts

Module 14: Ethical Hacking Ethics, Legal, and Career Development

- Ethics and Legal Implications of AI in Cybersecurity
- Considerations (Privacy and Ethical) with AI applications in cybersecurity
- Legal implications, GDPR, and compliance standards
- Career Path in AI and Cybersecurity
- AI-powered cybersecurity: certifications, career options, and growth opportunities
- Additional learning resources and labs for continued skill development

Final Project: Implementing AI in a Cybersecurity Framework

- Project Outline
- Apply skills learned throughout the course to design and implement an AI-enhanced security framework for a simulated enterprise network.
- Deliverables: Project report and presentation showcasing solutions, tools used, and findings.

BROADWAY INFOSYS
Since 2008
An ISO 9001:2015 Certified IT Learning Center

Building Global IT Professionals since 2008

+977-1-4117578 / 4111849
+977-9841002000 / 9808724535

info@broadwayinfosys.com
www.broadwayinfosys.com

Shree Ganesh Marg, Subidhanagar,
Tinkune, Kathamandu, Nepal