COURSE SYLLABUS

Ethical Hacking and Offensive Security Essentials Course (Self-Paced)

Learn the foundations of ethical hacking, from authorization and methodology through reconnaissance and reporting.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/ethical-hacking-and-offensive-security-essentials-course-self-paced



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Ethical Hacking Foundations: Law, Ethics, and Authorization

- Lessons:
  - What Ethical Hacking Is and Is Not
  - Authorization, Scope, and Rules of Engagement
  - Relevant Laws and Professional Codes of Conduct
- Applied activity: Learners draft a one-page mock authorization and scope memo for a fictional engagement, using a provided template, and check it against a provided checklist of required elements.

Module 2: The Penetration Testing Lifecycle and Methodologies

- Lessons:
  - Overview of the Testing Lifecycle: Planning Through Reporting
  - Comparing Testing Methodologies and Frameworks
  - Choosing an Approach for a Given Engagement
- Applied activity: Learners map a short case study engagement description onto the lifecycle phases and identify which methodology best fits, using a provided worksheet.

Module 3: Reconnaissance and Open Source Intelligence

- Lessons:
  - Passive versus Active Reconnaissance
  - Open Source Intelligence (OSINT) Techniques and Tools
  - Documenting Reconnaissance Findings
- Applied activity: Learners perform an OSINT exercise on a provided fictional company profile using publicly available search techniques on their own machine, and record findings in a provided worksheet.

Module 4: Scanning and Enumeration Techniques

- Lessons:
  - Network and Port Scanning Fundamentals
  - Service and Vulnerability Enumeration
  - Interpreting Scan Output
- Applied activity: Learners review an annotated sample scan report and identify which findings warrant further investigation, checking their answers against a provided key.

Module 5: Vulnerability Identification and Analysis

- Lessons:
  - Vulnerability Categories and Common Weakness Types
  - Using Vulnerability Databases and Scoring
  - Prioritizing Findings for Risk
- Applied activity: Learners score three sample vulnerabilities using a public scoring reference and rank them by priority, comparing their ranking to a provided answer key.

Module 6: Exploitation Concepts and Common Attack Techniques

- Lessons:
  - How Exploitation Turns a Vulnerability Into Access
  - Common Attack Technique Categories
  - Limits of Safe, Authorized Testing
- Applied activity: Learners review a narrated, screenshot-based walkthrough of a sample exploitation scenario against a test system and answer reflection questions about what made the exploit possible.

Module 7: Web Application Attack Fundamentals

- Lessons:
  - The Web Application Attack Surface
  - Common Web Application Weaknesses
  - Recognizing Findings in a Web Application Report
- Applied activity: Learners review a sample, redacted web application finding report and match each finding to its weakness category, using a provided vendor-neutral weakness reference.

Module 8: Post-Exploitation, Reporting, and Remediation

- Lessons:
  - Post-Exploitation Goals and Boundaries
  - Writing Findings for a Non-Technical Audience
  - Remediation and Retesting
- Applied activity: Learners rewrite a technical finding excerpt into a plain-language summary for a business stakeholder, using a provided before-and-after example as a model.