ETHICAL HACKER



GENTEX®

TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

The Ethical Hacker Training Course prepares security professionals to test systems the way attackers do, but with authorisation and discipline. Weaknesses rarely announce themselves; they sit in misconfigured services, unpatched software, and overlooked credentials until someone finds them. Authorised offensive testing reveals those weaknesses before criminals exploit them. This course covers reconnaissance, scanning, exploitation, and reporting across networks, systems, and applications. Furthermore, it applies the ethical and legal boundaries that separate testing from intrusion. As a result, participants find real vulnerabilities and help fix them.

Ethical Hacker Course Objectives

- Explain ethical hacking principles, scope, and authorisation requirements.
- Apply reconnaissance and open-source intelligence gathering techniques.
- Conduct network scanning, enumeration, and service identification.
- Assess vulnerability findings and prioritise remediation.
- Apply system exploitation techniques in controlled environments.
- Test web application security including OWASP Top 10 vulnerabilities.
- Assess wireless, mobile, and cloud attack surfaces.
- Apply password, social engineering, and credential attack techniques ethically.
- Identify system weaknesses and recommend hardening measures.
- Prepare professional penetration test reports with clear findings and remedies.

Course Methodology

- Interactive lectures with real vulnerability and breach case studies.
- Hands-on reconnaissance, scanning, and enumeration exercises.
- Controlled exploitation and post-exploitation labs.

GENTEX® TRAINING CENTER

- Web application testing workshops against OWASP guidance.
- Structured peer discussion with facilitator feedback on testing decisions.

Who Should Take This Course

- Penetration testers and security consultants.
- Security analysts and security operations staff.
- Network and system administrators.
- Application developers with security responsibilities.
- IT auditors reviewing technical security controls.
- Security managers overseeing testing programmes.

Ethical Hacker Course Outlines

Day 1: Ethical Hacking Foundations and Legal Boundaries

- Ethical hacking concepts, phases, and professional standards.
- Authorisation, scope definition, and rules of engagement.
- Legal frameworks and computer misuse offences.
- Testing methodologies and penetration testing standards.
- Lab setup, isolation, and safety controls.
- Documentation, evidence, and client confidentiality.
- Case study: a penetration test that found a critical flaw.

Day 2: Reconnaissance and Scanning

- Passive reconnaissance and open-source intelligence collection.

- DNS enumeration, subdomain discovery, and footprinting.
- Active scanning, port scanning, and host discovery.
- Service and version identification with banner grabbing.
- Vulnerability scanning tools and result interpretation.
- Avoiding disruption and managing scan load.
- Workshop: performing reconnaissance and scanning safely.

Day 3: System Exploitation and Privilege Escalation

- Exploitation concepts, payloads, and delivery methods.
- Windows and Linux privilege escalation techniques.
- Credential harvesting and hash analysis concepts.
- Lateral movement and pivoting within authorised scope.
- Persistence and detection evasion awareness.
- Post-exploitation cleanup and client notification duties.
- Workshop: exploiting and escalating in a controlled lab.

Day 4: Web, Wireless, and Application Security

- Web application architecture and common attack paths.
- OWASP Top 10 vulnerabilities and testing methods.
- Injection, broken access control, and authentication flaws.
- API testing and insecure interface exposure.
- Wireless network attack surfaces and testing approaches.
- Mobile and cloud configuration weaknesses.
- Workshop: testing a web application against OWASP guidance.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Day 5: Reporting, Remediation, and Defensive Alignment

- Structuring a penetration test report.
- Rating findings by severity and business impact.
- Writing clear remediation guidance for technical teams.
- Executive summaries and risk communication.
- Retesting, validation, and closure processes.
- Aligning testing with defensive controls and threat detection.
- Course review, assessment, and action planning.

Conclusion

By successfully completing Ethical Hacker, participants will gain a thorough understanding of reconnaissance, scanning, exploitation, application testing, and penetration test reporting. They will also acquire practical skills in vulnerability assessment, controlled exploitation, web application testing, and remediation guidance. In addition, the course prepares them to test systems responsibly and improve organisational security. Gentex Training Center delivers this programme with a strong focus on applied security testing practice and measurable control improvement.

FAQs for Ethical Hacker course

Q1 What is the "Ethical Hacker" course about?

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

It is a five-day programme on authorised offensive security testing. It covers ethical hacking phases and legal boundaries, reconnaissance and scanning, system exploitation and privilege escalation, web, API, wireless and cloud testing, and penetration test reporting and remediation.

Q2 What are the key benefits of the "Ethical Hacker" course?

Participants gain the ability to find weaknesses before attackers do, which prevents costly breaches. The course improves vulnerability identification accuracy, sharpens risk prioritisation, raises remediation quality, strengthens application and network defences, improves compliance evidence, and gives security teams confidence in their control testing.

Q3 What skills will I gain from the "Ethical Hacker" course?

Participants gain reconnaissance, scanning and enumeration techniques, vulnerability assessment and system exploitation practice, web, API and wireless security testing, and penetration test reporting with remediation guidance. These four skills cover the practical core of authorised security testing work.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "Ethical Hacker" course?

The course covers ethical hacking phases and rules of engagement, authorisation and scope documentation, legal frameworks and computer misuse offences, penetration testing methodologies and standards, passive reconnaissance and open-source intelligence collection, DNS enumeration and subdomain discovery, port scanning and service identification, banner grabbing, vulnerability scanning tools, exploitation concepts and payload delivery, Windows and Linux privilege escalation, credential harvesting and hash analysis, lateral movement and pivoting, persistence and detection evasion awareness, post-exploitation cleanup, web application architecture and attack paths, the OWASP Top 10 including injection and broken access control, API testing, wireless testing approaches, mobile and cloud configuration review, severity rating methods, and remediation reporting standards.

Q5 How is the "Ethical Hacker" course applied in real-world practice?

Participants apply the methods in authorised testing engagements. They gather intelligence, scan targets, identify vulnerabilities, exploit them safely in controlled conditions, test applications against OWASP guidance, and produce reports with prioritised remediation steps. Many leave with testing checklists and a report structure ready for immediate use.