ZERODAYLAB®

Penetration Testing Course

ZERODAYLAB®

Penetration Testing Course

The objective from this three day course will be to have an understanding of:

- A background to penetration testing
- Methods and processes used
- Commonly used tools and their uses
- Infrastructure Hacking
- Web Services Hacking

ZERODAYLAB®

Itinerary

Day One

- Background
- Methods and processes
- Infrastructure Hacking Tools
- Interactive Labs
  - Reconnaissance
  - Vulnerability Analysis
  - Exploitation

Day Two

- Web Application Hacking
- Methods and processes
- Web Application Hacking Tools
- Interactive Labs
  - Using an Intercepting Proxy
  - OWASP Top 10

Day Three

- Interactive Labs
  - Client Side Exploitation
  - Kiosk Hacking
- Recap
- Further Reading

ZERODAYLAB®

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. Testing the security of a system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them for their own gain.

Ethical hacking is also known as penetration testing, intrusion testing and red teaming. An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the “good guy” wore a white hat and the “bad guy” wore a black hat.

About ZeroDayLab

At ZeroDayLab, every day is spent helping make our client's infrastructure, applications, and data more secure through the intelligent combination of services from highly trained consultants and leading edge, complimentary security technologies.

At ZeroDayLab we take a holistic approach to Total Security Management. Our skilled and experienced consultants can provide help, advice, training and support on a whole range of IT security solutions such as:

- Vulnerability Assessment of Desktop, Servers and Infrastructure
- Penetration Testing of all Internal/ External Web Applications and Infrastructure
- Broad Security Review (Architecture and Infrastructure)
- Source Code Reviews
- Firewall Audits
- Desktop and Server Build Reviews
- Blockchain Application Security Audits
- Digital Forensic Analysis
- Security Awareness Programmes
- Security Training for Developers - Secure Coding School, CBT, Online Assessment
- Pre-Breach Incident Response & Runbook Training
- Phishing Resilience Programmes
- Bespoke Senior Executive Security Training
- Red Team Testing
- PCI DSS Remediation Support
- Gap Analysis to ISO, PCI DSS, SSAE16(18), GDPR
- 360° Reviews (Cyber Risk Assessment)
- Virtual Data Protection Officer
- Virtual Information Security Manager
- ISO/NIST/EU GDPR Standards Alignment
- Internal Audits
- SERM - Supplier Evaluation Risk
- Management Cyber Threat Intelligence -
- Deep & Dark Web
- Protective Monitoring (Managed SOC)
- Security Risk Training for Agile Developers
- ZeroDayResponse - Incident Response Review & Digital Forensics Training

Our team looks forward to sharing our vision with you and helping you to defend against the malicious attacks that come from both inside and outside of your environment.

ZERODAYLAB®

Passionate About Total Security Management

Europe Headquarters:

ZeroDayLab Ltd
Suite 303, 150 Minories,
London,
EC3N 1LS, UK
Phone: +44 (0)207 979 2067

North America Headquarters:

ZeroDayLab LLC
3524 Silverside Road, Suite 35B
Wilmington, DE
19810-4929, USA
Phone: 1-302-498-8322

Amsterdam | Manchester | Edinburgh | Dublin | Brighton & Hove | Bangalore

www.zerodaylab.com | www.zerodaylab.nl | info@zerodaylab.com