

No. 125

CYBERSECURITY

Ethical Hacking for Beginners

Authorized security testing explained, the legal and safe way

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 125

Ethical Hacking for Beginners

Authorized security testing explained, the legal and safe way

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Ethical Hacking for Beginners

Authorized security testing explained, the legal and safe way

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, tool and certification names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What ethical hacking is 5
2 Hats and teams 6
3 Why organizations test 7
4 Kinds of security testing 8
5 The law 9
6 Authorization and rules of engagement 11
7 Scope 12
8 Ethics 14
9 The hacker mindset 15
10 Core skills 16

PART II · THE METHODOLOGY

11 Phases of a test 18
12 Methodologies 19
13 Planning 20
14 Reconnaissance 21
15 Discovery and mapping 22
16 Vulnerability assessment 23
17 Validation 24
18 Demonstrating impact 25
19 Clean-up 26
20 Evidence and notes 27
21 Reporting 28
22 Retesting 30

PART III · AREAS OF TESTING

23 Network testing 32

FREE SAMPLE · ojayo.com

24 Web application testing 33
25 API testing 34
26 Cloud testing 35
27 Wireless testing 36
28 Social engineering tests 37
29 Physical testing 38
30 Testing AI applications 39

PART IV · GETTING STARTED

31 Building a lab 41
32 Tools 42
33 Practice platforms 43
34 Capture the flag 44
35 Certifications 45
36 Careers 46
37 AI assistants 47
38 Common mistakes 48
39 A worked example 49
40 A learning path 50
Checklists 51
Glossary 52
Further reading 53

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Ethical hacking means testing systems for security weaknesses **with permission**, so they can be fixed before criminals find them. Organizations hire ethical hackers, also called penetration testers, to see their defences through an attacker's eyes.

This book is a beginner's introduction to the field: what ethical hackers do, the legal and ethical rules that separate them from criminals, the phases of a professional test, how findings are reported and how to start learning safely. It explains concepts and process rather than step-by-step attack techniques, and every practical activity it suggests happens in your own lab or on platforms built for practice.

What this book covers

- What ethical hacking is and the kinds of security testing.
- The law, authorization, scope and rules of engagement.
- The phases and methodologies of a penetration test.
- Reporting findings and helping organizations fix them.
- Areas of testing: networks, web, APIs, cloud, people and AI applications.
- Labs, tools, practice platforms, certifications and careers.

Who this book is for

- **Students and career changers** curious about offensive security.
- **IT and development staff** who work with testers.

FREE SAMPLE · ojayo.com

- **Managers** who commission security tests.

How the book is organized

- **Part I — Foundations** (Chapters 1–10): what ethical hacking is, hats and teams, why organizations test, kinds of testing, the law, authorization, scope, ethics, the hacker mindset, and core skills.
- **Part II — The methodology** (Chapters 11–22): phases, frameworks, planning, reconnaissance, discovery, vulnerability assessment, validation, impact, clean-up, evidence, reporting and retesting.
- **Part III — Areas of testing** (Chapters 23–30): networks, web applications, APIs, cloud, wireless, social engineering, physical testing and AI applications.
- **Part IV — Getting started** (Chapters 31–40): your lab, tools, practice platforms, capture the flag, certifications, careers, AI assistants, common mistakes, a worked example and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in real testing work.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on the law

Testing systems without permission is a crime in most countries, even if you mean well. Only practise on systems you own or are explicitly authorized to test. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what ethical hacking is, why it matters, and the legal and ethical rules that define it.

FREE SAMPLE · ojayo.com

CHAPTER 1

What ethical hacking is

Ethical hacking is authorized attack simulation.

A definition

An **ethical hacker** uses the same knowledge as a criminal attacker, but with the system owner's written permission, within agreed limits, and with the goal of helping the owner fix what is found.

Three conditions

- **Permission**: the owner has authorized the test in writing.
- **Boundaries**: the tester stays within the agreed scope and methods.
- **Disclosure**: findings go to the owner, confidentially, so they can be fixed.

> **KEY IDEA**
> Skills do not make someone an ethical hacker; permission, boundaries and honest disclosure do.

FREE SAMPLE · ojayo.com

CHAPTER 2

Hats and teams

You will hear about hats and colours.

Label	Meaning
White hat	authorized, helps defenders
Black hat	unauthorized, criminal
Grey hat	unauthorized but claims good intent; still illegal
Red team	authorized adversary simulation
Blue team	defenders
Purple team	red and blue working together

Figure 2.1 The 'hats' and teams

About grey hats

Some people test systems without permission and then report the problem. Even with good intentions, this is usually still illegal, and it can cause harm. Responsible disclosure programmes and bug bounties exist to provide a legal route.

FREE SAMPLE · ojayo.com

CHAPTER 3

Why organizations test

Testing finds what defenders miss.

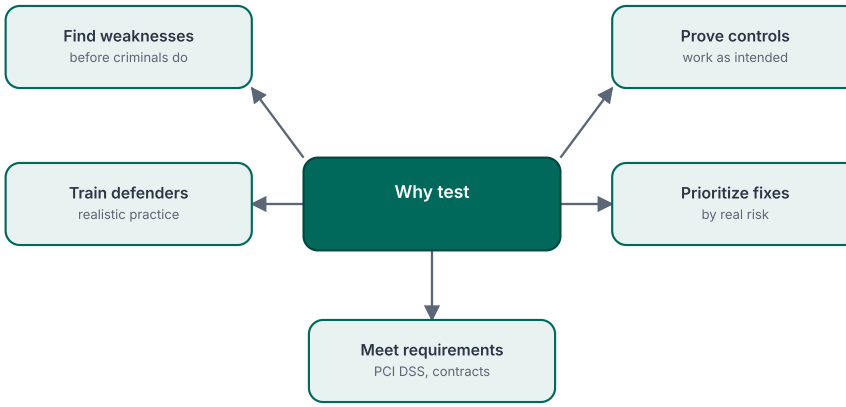


Figure 3.1 Why organizations hire ethical hackers

A different view

Defenders know how systems are supposed to work; ethical hackers look for how they actually fail. Combining both views produces stronger security.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners (you are reading…
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Ethical Hacking for Beginners

Enjoyed it? The full book has 58 pages and 40 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.