

Introduction to Ethical Hacking

Introduction to Ethical Hacking

Prepared as a quick-reference guide

1. What Is Ethical Hacking?

Aspect	Description
Definition	Authorized, systematic testing of computer systems, networks, or applications to discover security weaknesses before malicious actors can exploit them.
Goal	Strengthen security posture by identifying and remediating vulnerabilities.
Key Principle	"Permission, Legality, and Transparency" – the tester must have explicit consent, operate within legal boundaries, and report findings openly.
Alternative Names	Penetration testing, white-hat hacking, security assessment.

2. Types of Hackers (Color-Coding)

Color	Typical Motivation	Typical Activities
White-Hat	Protect organizations, improve security	Conduct authorized tests, develop defensive tools
Black-Hat	Personal gain, sabotage, espionage	Exploit, sell, or weaponize vulnerabilities
Gray-Hat	Curiosity, mixed motives	May test without permission, then disclose findings (often responsibly)
Red-Team	Simulate advanced persistent threats	Full-scale, multi-vector attack simulations
Blue-Team	Defense and detection	Monitor, respond, and harden systems
Purple-Team	Collaboration between red & blue	Joint exercises to improve both attack and defense skills

Introduction to Ethical Hacking

3. Legal & Ethical Foundations

1. **Written Authorization** – A formal agreement (e.g., Rules of Engagement, Scope Document) signed by the system owner.
 2. **Compliance Standards** – Align with regulations such as GDPR, HIPAA, PCI-DSS, ISO 27001, NIST SP 800-115.
 3. **Non-Disclosure Agreements (NDAs)** – Protect sensitive data discovered during testing.
 4. **Responsible Disclosure** – If a vulnerability is found outside the scope, notify the owner promptly and give them time to remediate before public disclosure.
 5. **Professional Codes** – Follow guidelines from organizations like EC-Council (CEH), (ISC)², ISACA.
-

4. Phases of an Ethical Hacking Engagement (The “Pentest Lifecycle”)

1. Planning & Reconnaissance

- Define scope, objectives, timeline, and rules of engagement.
- Gather open-source intelligence (OSINT): domain names, IP ranges, employee info, public code repositories.

2. Scanning & Enumeration

- Network scanning (Nmap, Masscan).
- Service/version detection.
- Vulnerability scanning (Nessus, OpenVAS, Qualys).
- Enumerate users, shares, APIs, web endpoints.

3. Exploitation

- Choose appropriate exploits (Metasploit, custom scripts).
- Gain foothold: remote code execution, credential reuse, injection attacks.
- Maintain stealth to avoid detection.

4. Post-Exploitation

Introduction to Ethical Hacking

- Privilege escalation (kernel exploits, token manipulation).
- Lateral movement (Pass?the?Hash, SMB relay).
- Data exfiltration simulation, persistence mechanisms.

5. Reporting

- Executive summary (business impact).
- Technical findings (vulnerability details, proof?of?concept, CVSS scores).
- Remediation recommendations (patches, configuration changes, security controls).
- Appendices: raw data, scripts, logs.

6. Remediation Verification (Optional)

- Re?test patched systems to confirm fixes.