INTRODUCTION TO ETHICAL HACKING

CYBERSECURITY FUNDAMENTALS TRAINING GUIDE

Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

2026 Edition

1. WHAT IS ETHICAL HACKING?

Ethical hacking is the authorized practice of bypassing system security to identify potential data breaches and threats in a network. Organizations hire ethical hackers to test their defenses and find vulnerabilities before malicious attackers do.

Definition

An ethical hacker (white hat hacker) is a security professional who systematically attempts to penetrate computer systems, networks, and applications on behalf of their owners—with explicit permission—to discover security vulnerabilities that malicious hackers could exploit.

Why Organizations Need Ethical Hackers

- Identify vulnerabilities before malicious attackers discover them
- Test the effectiveness of security controls and policies
- Ensure compliance with regulations (PCI DSS, HIPAA, GDPR, SOX)
- Protect customer data and maintain organizational trust
- Avoid costly data breaches (Average cost: $4.88 million in 2024)

2. THE FIVE PHASES OF ETHICAL HACKING

Every ethical hacking engagement follows a structured methodology consisting of five phases:

PHASE 1: RECONNAISSANCE

The preparatory phase where information is gathered about the target. This is the most critical phase as it forms the foundation for all subsequent activities.

- Passive: OSINT, social media, public records, WHOIS
- Active: DNS queries, network probing, social engineering

PHASE 2: SCANNING

Using reconnaissance data to examine the network more deeply. Identifies live hosts, open ports, services, and vulnerabilities.

- Port scanning (Nmap, Masscan)
- Vulnerability scanning (Nessus, OpenVAS, Qualys)

PHASE 3: GAINING ACCESS

Exploiting discovered vulnerabilities to gain unauthorized access to target systems.

- Exploitation frameworks (Metasploit)
- Password attacks, web application attacks, social engineering

PHASE 4: MAINTAINING ACCESS

Establishing persistent access to continue operations. Simulates advanced persistent threats (APTs).

- Backdoors, rootkits, trojans
- Privilege escalation, lateral movement

PHASE 5: COVERING TRACKS

Removing evidence of the intrusion. In ethical hacking, this teaches how attackers evade detection.

- Log manipulation, timestomping, clearing history

3. INFORMATION SECURITY FUNDAMENTALS

The CIA Triad

The foundational model for information security:

CONFIDENTIALITY
Ensuring information is accessible only to authorized parties. Implemented through encryption, access controls, and authentication mechanisms.

INTEGRITY
Maintaining accuracy and trustworthiness of data. Ensured through hashing, digital signatures, and checksums.

AVAILABILITY
Ensuring systems and data are accessible when needed. Achieved through redundancy, backups, and DDoS protection.

Additional Security Principles

- Authenticity – Verifying users and data are genuine
- Non-repudiation – Actions cannot be denied after the fact
- Defense in Depth – Multiple layers of security controls
- Least Privilege – Minimum access necessary for duties

4. SECURITY CONTROLS AND FRAMEWORKS

Types of Security Controls

ADMINISTRATIVE CONTROLS
Policies, procedures, and guidelines. Examples: Security policies, awareness training, background checks, incident response plans.

TECHNICAL CONTROLS
Hardware and software mechanisms. Examples: Firewalls, encryption, IDS/IPS, antivirus, MFA, access control lists.

PHYSICAL CONTROLS
Protect physical assets. Examples: Security guards, locks, CCTV, biometric access, mantraps, fencing.

Major Security Frameworks

NIST CYBERSECURITY FRAMEWORK (CSF)
Five core functions: Identify, Protect, Detect, Respond, Recover. Widely adopted voluntary framework for managing cybersecurity risk.

ISO/IEC 27001:2022
International standard for information security management systems (ISMS). Contains 93 controls in Annex A. Certification valid for 3 years.

MITRE ATT&CK
Knowledge base of adversary tactics and techniques based on real-world observations. Used for threat modeling and security assessments.

5. CYBERSECURITY LAWS AND REGULATIONS

Ethical hackers must understand the legal landscape governing cybersecurity:

GDPR (General Data Protection Regulation)
EU regulation protecting personal data. Penalties up to €20 million or 4% of global annual revenue. Requires 72-hour breach notification.

HIPAA (Health Insurance Portability and Accountability Act)
US healthcare data protection. Penalties range from $100 to $50,000 per violation. Protects Protected Health Information (PHI).

PCI DSS (Payment Card Industry Data Security Standard)
Payment card data protection. Version 4.0 mandatory as of March 2024. 12 requirements across 6 control objectives.

SOX (Sarbanes-Oxley Act)
US financial reporting and internal controls for public companies. Section 404 requires internal control assessment.

CCPA (California Consumer Privacy Act)
California data privacy law. Penalties up to $7,500 per intentional violation. Grants consumers rights over their personal data.

CFAA (Computer Fraud and Abuse Act)
US federal law criminalizing unauthorized computer access. Key reason why written authorization is required before any penetration testing.

6. TYPES OF HACKERS

WHITE HAT HACKERS
Ethical hackers who use their skills for defensive purposes with authorization. Work for organizations to improve security posture.

BLACK HAT HACKERS
Malicious hackers who exploit systems for personal gain, financial profit, or to cause damage. Their activities are illegal.

GRAY HAT HACKERS
Operate between ethical and malicious. May find vulnerabilities without permission but report them rather than exploit them.

SCRIPT KIDDIES
Inexperienced individuals who use pre-written tools and scripts without understanding the underlying techniques.

HACKTIVISTS
Hackers motivated by political or social causes. Use hacking to promote ideological agenda (e.g., Anonymous).

STATE-SPONSORED HACKERS
Government-backed groups conducting cyber espionage or warfare. Often target critical infrastructure and other nations.

INSIDER THREATS
Employees or contractors who misuse legitimate access. Can be malicious or negligent. Often the most damaging threat vector.

7. PENETRATION TESTING METHODOLOGIES

OWASP Testing Guide
Comprehensive methodology for web application security testing. Covers information gathering, configuration management, authentication, session management, and more.

PTES (Penetration Testing Execution Standard)
Seven-phase methodology: Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting.

OSSTMM (Open Source Security Testing Methodology Manual)
Peer-reviewed methodology for security testing. Focuses on operational security across physical, human, wireless, telecommunications, and data networks.

NIST SP 800-115
Technical Guide to Information Security Testing and Assessment. Covers review techniques, target identification, vulnerability analysis, and planning.

Testing Types
- Black Box – No prior knowledge of target systems
- White Box – Full knowledge of systems, source code access
- Gray Box – Partial knowledge, simulating insider threat

8. PRACTICE LABS AND RESOURCES

Practice your skills legally with these platforms:

Free Online Hacking Labs

- Hack The Box – Gamified penetration testing labs
- TryHackMe – Beginner-friendly guided learning paths
- OverTheWire – War games for learning security concepts
- VulnHub – Downloadable vulnerable virtual machines
- PentesterLab – Web application security exercises
- CTFlearn – Capture The Flag challenges

Recommended Certifications

- CEH (Certified Ethical Hacker) – EC-Council
- OSCP (Offensive Security Certified Professional)
- CompTIA Security+ – Entry-level security certification
- CompTIA PenTest+ – Penetration testing certification
- GPEN (GIAC Penetration Tester)

Essential Tools

- Kali Linux – Penetration testing distribution
- Nmap – Network scanner and enumeration
- Metasploit – Exploitation framework
- Burp Suite – Web application testing
- Wireshark – Network protocol analyzer

9. QUICK REFERENCE CHECKLIST

Before Any Engagement

- ☐ Obtain written authorization (Rules of Engagement)
- ☐ Define scope clearly (IP ranges, domains, systems)
- ☐ Establish communication protocols and emergency contacts
- ☐ Set testing timeline and notify stakeholders
- ☐ Verify insurance and liability coverage

During Testing

- ☐ Document all activities thoroughly
- ☐ Stay within authorized scope
- ☐ Report critical vulnerabilities immediately
- ☐ Take screenshots and save evidence
- ☐ Avoid causing unnecessary damage or disruption

After Testing

- ☐ Remove all tools and backdoors installed
- ☐ Prepare comprehensive report with findings
- ☐ Provide remediation recommendations
- ☐ Present findings to stakeholders
- ☐ Securely dispose of sensitive data collected