What Is Ethical Hacking?

Ethical hackers find weak points before criminals do — learn the five legal stages, from recon to covering tracks.

Introduction

A bank hires someone to try to break into its own systems. A university pays a student to find holes in its website — before a criminal finds them. That person is an **ethical hacker**: someone who hacks with permission, to make things safer.

Ethical hacking is legal hacking. The difference between an ethical hacker and a criminal is not skill — it is permission, purpose, and reporting. The ethical hacker has written permission, works only inside the agreed limits, and reports every weak point so it can be fixed. The criminal has none of that.

Ethical hackers follow five stages: **reconnaissance** (learn about the target), **scanning** (find open doors), **gaining access** (prove a weak point can be used), **maintaining access** (show how long an attacker could stay hidden), and **covering tracks** (clean up — and in the ethical case, leave a full report, not a hidden backdoor).

In this lesson you will walk through all five stages, learn the rules that keep hacking legal, and see how a beginner can start learning ethically — without ever touching a real system without permission.

(Roman Urdu: Ethical hacking ka matlab hai ijazat se hacking — kamzori dhoondho, taake mujrim se pehle usay band kiya ja sake. Ijazat, had (scope), aur report — yehi cheez ethical hacker ko mujrim se alag karti hai.)

This lesson teaches the ideas only. Do not test these stages on any real website, network, or account without written permission — that is illegal, even if your intention is good.

Key points

- **Ethical hacking = hacking with written permission, inside an agreed scope, to improve security.** No permission means it is a crime, whatever the intention.
- **White hat hackers defend; black hat hackers attack for harm or money; grey hat hackers act without permission but claim good intentions — grey hat is still illegal.**
- **Stage 1 — Reconnaissance (recon): gather public information.** What does the target publish? Which technologies does the website use? What do employees post publicly? No touching the system yet — just looking at what is already public.
- **Stage 2 — Scanning: find the open doors.** Which ports are open? Which services are running? Which software versions are old and known to be weak?
- **Stage 3 — Gaining access: prove the weak point works.** Use the weak point to get in — in a test system, inside the agreed scope — and show what an attacker could reach.

- **Stage 4 — Maintaining access: show how an attacker could stay.** Could a criminal hide and return tomorrow? The ethical hacker proves it, then removes everything.
- **Stage 5 — Covering tracks and reporting: clean up and write it all down.** The criminal covers tracks to hide. The ethical hacker cleans up the test traces and hands over a full report: what was found, how serious it is, and how to fix it.
- **A penetration test (pentest) is a planned, time-limited ethical hack with a report at the end.** Companies order pentests before launching a product.
- **Bug bounties pay ethical hackers for real bugs.** Big companies publish a scope and pay for each reported weakness — a legal way to earn from hacking skills.

Examples

Example 1 — The five stages on a test website

```
Target: a practice website the company owns (written permission given)

Stage 1 Recon:   the site runs WordPress 6.1, hosted in Lahore,
                 admin page is /wp-admin, staff emails are public.
Stage 2 Scan:    port 80 open, port 443 open; WordPress 6.1 has a
                 known weak plugin, version 2.3.
Stage 3 Access:  the weak plugin lets the tester upload a file
                 and read one private file — proof it works.
Stage 4 Maintain: the tester shows the file could be reached
                 again tomorrow if the plugin stays.
Stage 5 Report:  tester removes the file, writes the report:
                 "Update plugin 2.3 to 2.5, block uploads."
```

Nothing was stolen, nothing was broken, and the company now knows exactly what to fix.

Example 2 — White hat, black hat, grey hat

```
White hat:  hired by the bank, written permission, reports everything.
Black hat:  breaks into the bank, steals money, hides.
Grey hat:   breaks into the bank without permission, then emails
            the bank "you had a hole, pay me to tell you where."
            Good intention or not — no permission means illegal.
```

The hat is decided by permission and law, not by how nice the person seems.

Example 3 — What a pentest report looks like

```
Finding 1 (HIGH):  Admin login has no limit on wrong tries.
                   Fix: lock the account after 5 wrong tries.

Finding 2 (MEDIUM): Old plugin version 2.3 is installed.
                   Fix: update to 2.5 this week.

Finding 3 (LOW):   Server shows its version number publicly.
                   Fix: hide the version in the settings.
```

Each finding has a severity and a fix. That report — not the break-in — is the product the company paid for.

Example 4 — Learning ethically, step by step

```
Step 1: Learn networking and Linux basics.
Step 2: Practise on YOUR OWN lab — a virtual machine you own.
Step 3: Use legal practice sites (Hack The Box, TryHackMe,
        PortSwigger Web Security Academy) — built for learning.
Step 4: Study for a certificate like CEH or CompTIA Security+.
Step 5: Join a bug bounty program and report real bugs legally.
```

Never practise on a real website, a school network, or a friend's account without written permission. Your own lab is free and legal.

Quick recap

- Ethical hacking is hacking with written permission, inside a scope, to make things safer.
- The five stages: recon, scanning, gaining access, maintaining access, covering tracks (+ reporting).
- White hat defends, black hat attacks, grey hat acts without permission and is still illegal.
- The report is the real product — findings, severity, and fixes.
- Learn on your own lab and legal practice sites, never on real systems without permission.

Common mistakes

1. **Hacking "just to test" without permission** — even with good intentions, unauthorised access is illegal in Pakistan and almost everywhere. Fix: written permission first, always.
2. **Skipping the report** — finding a hole and telling nobody leaves it open for criminals. Fix: every test ends with a written report.
3. **Going outside the scope** — permission to test the website is not permission to test the email server. Fix: stay inside the agreed limits, exactly.

4. **Leaving test files behind** — a forgotten test backdoor becomes a real attacker's door. Fix: clean up every trace, then verify it is gone.
5. **Learning on live targets** — practising scanning on a real company teaches you nothing extra and risks a police case. Fix: your own lab and legal practice platforms.

Practice

1. Write the five stages in order, with one line each, from memory. Check yourself against this lesson.
2. A friend says "I hacked my school website to show it was weak, and I told the principal after." Which hat is that, and why is it still wrong? Write two lines.
3. Make a learning plan: list three things you will learn first (for example, networking basics, Linux commands, how the web works) and one legal practice site you will use.
4. Read a public bug bounty scope (for example, on HackerOne) and write down: what is allowed to test, and what is forbidden? Notice how exact the limits are.
5. Imagine you found a weak point in a shop's website. Write the three lines you would put in a report: what is wrong, how serious it is, and how to fix it.

Practice quiz

1. What makes hacking ethical?

- Good intentions only
- Written permission, an agreed scope, and reporting what was found
- Being good at computers
- Telling nobody afterwards

Answer: Written permission, an agreed scope, and reporting what was found

2. What are the five stages of ethical hacking, in order?

- Scan, hack, hide, report, repeat
- Reconnaissance, scanning, gaining access, maintaining access, covering tracks
- Access, recon, scan, maintain, report
- Report, recon, scan, access, hide

Answer: Reconnaissance, scanning, gaining access, maintaining access, covering tracks

3. What is the real product a company pays for in a penetration test?

- The break-in itself
- The report: findings, severity, and how to fix them
- A new firewall
- A list of employee passwords

Answer: The report: findings, severity, and how to fix them

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-ethical-hacking · More free tools and notes at https://scopetreasure.com