ACTIVE CLEARANCE · MISSION: CERTIFICATION

FREE PREVIEW

CLEARED GOVTECH PARTNERS

EC-Council CEH v13 312-50

Exam Preparation Booklet — Free Preview

400 scenario questions · full answer key · glossary
study plan · career roadmap · exam-day strategy · glossary quiz

Prepared for our transitioning servicemembers and veterans.
Aligned to the current 312-50 (v13) exam objectives. · This free preview contains a sample of the full 400-question booklet.

CONTENTS

What’s in this preview

In the full booklet — not in this preview

WELCOME

Learn the Attacker’s Method — Legally.

CEH is broad rather than deep. It covers the full attacker playbook — twenty modules, dozens of tools, and a lot of terminology — and it tests your judgment about method, tool selection, the attack phases, and ethics far more than it asks you to type commands. The mindset it certifies is ‘think like the adversary so you can defend like a professional.’

What carries you through this exam is the methodology spine: the five phases an engagement moves through, and the ethical and legal line that separates sanctioned testing from a federal crime. Get those reflexes solid — authorization first, scope always, document everything — and the module-by-module terminology becomes far easier to hold in your head.

It is approved under DoD 8140/8570 for several CSSP roles, which keeps it strong in the cleared market. If you carried a security mindset in uniform, CEH formalizes it into a recognized credential. Let’s learn the attacker’s method — on the right side of the law.

— The team at Cleared GovTech Partners

BEFORE YOU BEGIN

The CEH v13 (312-50) exam at a glance

Exam code	312-50 (CEH v13)
Format	125 multiple-choice questions
Time limit	4 hours (240 minutes)
Passing score	Variable cut score, ~60–85% (scaled to question difficulty)
Structure	20 modules grouped into 9 official domains
Eligibility	Official EC-Council training, OR a $100 eligibility application with 2+ yrs infosec experience
Renewal	120 ECE credits over 3 years (or re-take the current exam)
DoD value	Approved under DoD 8140/8570 for several CSSP roles — strong in the cleared market
Style	Conceptual and methodology-driven — judgment, tool selection, the attack phases, and ethics rather than operational attack recipes

A note on price. CEH pricing is genuinely confusing because EC-Council bundles the exam with training in several ways, and resellers quote very different numbers. Depending on the path, candidates report figures from roughly $650 for a standalone voucher up to about $1,199 when the exam is bundled with official training; the eligibility application adds ~$100 if you self-study. Confirm the current cost on EC-Council's site before you budget — and see the funding page near the back, because you may not have to pay it yourself.

SEE IT TO LEARN IT

The Five Phases of Ethical Hacking

CEH organizes the attacker’s method into five phases. The exam keeps returning to this spine — know the order and what happens at each step.

Authorization and scope wrap the entire process — nothing in these five phases is legal without signed permission first.

DOMAIN 1

Information Security & Ethical Hacking Overview

Scenario questions · the methodology spine

OFFICIAL EXAM OBJECTIVES FOR THIS DOMAIN

- Information security concepts, the CIA triad, and the risk equation
- Threat actors and their motivations (hacktivist, state-sponsored, insider, script kiddie)
- The legal and ethical foundation: authorization, scope, and rules of engagement
- Assessment types — vulnerability assessment vs. penetration test

Source: EC-Council CEH v13 (312-50) blueprint. These are summarized objective areas for this domain; download the complete, authoritative blueprint directly from EC-Council at eccouncil.org.

How this booklet helps you excel here

This is the methodology spine — the ethics, the legal line, the threat-actor taxonomy, and the CIA triad that the rest of the exam keeps coming back to. Get the judgment reflexes right here (authorization first, scope always) and the module terminology gets far easier to carry.

Sample of 5 questions from this domain. The full booklet contains all 400.

1. You run a small testing firm. A new client, eager to start, says over a phone call: ‘We trust you completely — just begin testing tonight, we’ll sort the paperwork later.’ Their network includes systems that process cardholder data. Your project lead asks how to proceed before any traffic is sent. What is the correct course of action?

A. Do not send a single packet until a signed authorization and scope agreement are in place

B. Limit tonight’s work to the public-facing website only, since it is already exposed to the internet

C. Run a quiet, low-impact scan tonight to show value, then formalize the authorization in the morning

D. Proceed on the verbal approval but email yourself a timestamped note describing what was agreed

2. During a threat-modeling workshop, an analyst profiles a group that repeatedly defaces a government agency’s websites and leaks documents to protest a new policy. They take no money and openly claim responsibility to draw attention to their cause. The team needs to label this actor correctly to predict its next move. Which category fits best?

A. Script kiddie

B. State-sponsored actor

C. Insider threat

D. Hacktivist

3. A junior penetration tester on an authorized engagement gains access to a database and, excited by the find, copies a table of real customer credit-card numbers to a personal USB drive ‘so I can reference it while writing the report at home.’ A senior reviewer stops them. Which principle did the junior’s action most directly violate?

A. Availability of the affected database

B. Confidentiality of client data and the engagement’s data-handling rules

C. Non-repudiation of the engagement findings

D. The requirement to scan systems in parallel

4. A prospective customer asks your firm to ‘just confirm which of our systems have weaknesses and how bad they are — you don’t need to actually break in.’ Your colleague argues this is the same as a penetration test. How should you describe the difference so the client buys the right service?

A. The two are interchangeable terms for the same activity

B. A vulnerability assessment identifies and rates weaknesses; a penetration test goes further by safely exploiting them to prove real impact

C. A penetration test only scans, while a vulnerability assessment actively exploits flaws

D. A vulnerability assessment is illegal unless it includes exploitation

5. A hospital is hit by malware that encrypts patient-record files and demands payment for the decryption key. Staff can no longer open charts, and scheduled procedures stall. When you classify the impact for the incident report using the CIA triad, which element took the primary hit?

A. Confidentiality

B. Integrity

C. Non-repudiation

D. Availability

Reference

Answer Keys & Explanations

Detailed rationale for every question in the full booklet

DOMAIN 1 — ANSWER KEY

Information Security & Ethical Hacking Overview

1. Correct answer: A — Do not send a single packet until a signed authorization and scope agreement are in place.

Signed, written authorization defining scope, rules of engagement, and dates is the legal line between ethical hacking and a federal crime under laws like the CFAA. Verbal trust, self-notes, or 'just the public site' all leave you personally exposed — a single unauthorized packet can be prosecutable, and on a cardholder environment the stakes (and regulators) are even higher.

The mature move is to pause and get the paperwork signed, even if it slows the start.

2. Correct answer: D — Hacktivist.

Hacktivists are motivated by ideology or a political/social cause and often court publicity, which is exactly the pattern described. Labeling them correctly matters operationally: hacktivists favor defacement, leaks, and DDoS for visibility, so defenses and monitoring should anticipate those, not the quiet long-dwell espionage of a state actor or the privilege abuse of an insider.

A script kiddie lacks the skill and motive shown here.

3. Correct answer: B — Confidentiality of client data and the engagement's data-handling rules.

Authorization to access a system is never authorization to exfiltrate or retain sensitive data; moving real cardholder data onto personal media breaks confidentiality and almost certainly the contract's data-handling clause. In the real world this can turn a legitimate test into a reportable breach, void the engagement, and create personal and firm liability.

Proving impact rarely requires removing live data — redacted evidence is enough.

4. Correct answer: B — A vulnerability assessment identifies and rates weaknesses; a penetration test goes further by safely exploiting them to prove real impact.

What the client described — finding and rating weaknesses without breaking in — is a vulnerability assessment. A penetration test adds controlled exploitation to demonstrate which findings are truly dangerous and chainable.

Selling the right one matters: charging for a pen test but delivering a scan (or vice versa) misleads the client and leaves real risk unvalidated. Each has its place; they are not the same engagement.

5. Correct answer: D — Availability.

Encryption-for-ransom denies legitimate users access to their own data, which is squarely an availability impact — and in a hospital that can directly threaten patient care. Confidentiality is only implicated if the attacker also stole data before encrypting (increasingly common), and integrity if files were altered, but the defining, immediate harm here is loss of availability.

Classifying it correctly drives the right recovery priorities: restore access first.

YOU'VE SEEN THE SAMPLE

Unlock the full CEH v13 booklet

This preview is a taste. The complete 400-question booklet takes you through every domain with the same scenario-driven questions and plain-language explanations — built to match how the real 312-50 exam thinks.

- ✓ All 400 scenario questions across every domain
- ✓ Full answer keys with exam cues for every question
- ✓ 8-week study schedule & recommended resources
- ✓ Career roadmap, acronym glossary & glossary quiz
- ✓ Exam-day quick reference & funding guide

You may not have to pay for this yourself.

Transitioning servicemembers and veterans can often fund the exam fee and training through Credentialing Assistance (Army CA / COOL), the GI Bill, or VET TEC. The full booklet includes a step-by-step funding guide. Ask us how to get your voucher covered before you pay out of pocket.