

ETHICAL HACKING

CERTIFICATION COMPARISON

GUIDE

*A practical guide to choosing the right ethical hacking certification for your career
stage*

1. Introduction

Cybersecurity certifications are everywhere, and ethical hacking is one of the most crowded corners of the market. Search for "best ethical hacking certification," and you'll find dozens of options, each claiming to be the one that will get you hired. The reality is more nuanced: no single certification is universally "best." The right choice depends on where you are in your career, how much hands-on experience you already have, and what kind of role you're aiming for.

This guide is built for three groups of readers:

- Beginners and career switchers who want a credible starting point without a steep prerequisite or price barrier.
- IT professionals who already work in networking, sysadmin, or support roles and want to move into security testing.
- Practitioners aiming for advanced, hands-on penetration testing or red-team roles.

Rather than ranking certifications against each other, this guide compares them side by side against the same criteria so you can match a certification to your goal instead of chasing whichever name is trending on social media.

2. How to Evaluate a Certification

Before comparing specific certifications, it helps to agree on what actually matters when judging one. The following six criteria apply to almost any security certification, not just the ones covered in this guide.

Foundational vs. Advanced / Hands-On

Some certifications test whether you understand ethical hacking concepts phases of an assessment, common vulnerability classes, legal and ethical boundaries. Others test whether you can actually compromise a live system under time pressure. Neither is "better" in the abstract; they answer different questions for an employer. A foundation-level credential says "I understand how this works." A hands-on practical exam says "I can do this myself, unsupervised."

Vendor-Neutral vs. Vendor-Specific

Vendor-neutral certifications (like CompTIA's) focus on concepts and tools broadly, without tying you to one platform or toolset. Vendor-specific paths may lean on a particular training provider's labs, terminology, or exam software. Neither approach is wrong, but it's worth knowing which one you're buying into, especially if you plan to stack certifications later.

Theory-Based vs. Lab/Practical Exam

Multiple-choice exams are cheaper to take, easier to schedule, and test recall and reasoning. Practical, lab-based exams (like OSCP's) test execution under realistic constraints, but they cost more, take longer to prepare for, and have a lower first-attempt pass rate. Example: a candidate who has memorized every Nmap flag may still struggle on a practical exam if they can't chain that knowledge into a working exploit path within a time limit.

Prerequisites and Experience Required

Some certifications (like the GSDC Certified Ethical Hacking Foundation) have no formal prerequisites, making them accessible to complete beginners. Others assume prior experience EC-Council's CEH, for example, expects two years of information security experience unless you complete official training instead. Always check this before you commit to a study timeline.

Cost and Renewal Requirements

Certification costs vary enormously from a few hundred dollars for a foundational exam to well over \$2,000 for an advanced practical credential once training and lab access are included.

Many certifications also require ongoing renewal: continuing education credits, an annual membership fee, or a recertification exam every few years. Factor in the full lifecycle cost, not just the sticker price of the first exam.

Industry Recognition / Employer Demand

A certification is only as useful as the doors it opens. Some credentials are explicitly recognized by government and defense frameworks (for example, U.S. DoD 8140-approved certifications), which matters if you're targeting public-sector or contractor roles. Others carry weight mainly in the private sector, where hiring managers may value a portfolio of practical work just as highly as a certification logo.

Use these six criteria as a checklist any time you're evaluating a certification not covered in this guide they hold up regardless of how the market changes.

3. Certification Comparison Table

The table below compares four certifications that sit at different points on the foundation-to-advanced spectrum: GSDC's Certified Ethical Hacking Foundation, CompTIA PenTest+, EC-Council's CEH, and OffSec's OSCP. Pricing and requirements change periodically — treat the figures below as directional and confirm current numbers on each provider's official site before enrolling.

Certification	Level	Format	Prerequisites	Cost (approx., USD)	Best Suited For
GSDC Certified Ethical Hacking Foundation (CEHF)	Foundation	Knowledge-based exam	None required	Budget-friendly; check GSDC site for current pricing	Beginners, career switchers, non-technical roles wanting foundational literacy
CompTIA PenTest+	Intermediate	Multiple-choice + performance-based (live scenario) questions	No formal prerequisite; Network+/Security+ knowledge recommended	~\$404 (exam voucher)	IT professionals moving into hands-on testing roles; DoD 8140-approved
EC-Council CEH v13	Intermediate	Multiple-choice knowledge exam (practical add-on available)	2 years of infosec experience, or official EC-Council training	\$950–\$1,199 (voucher) plus \$100 application fee if self-studying	Professionals wanting a widely recognized, DoD 8570/8140-compliant credential

OffSec OSCP (PEN-200)	Advanced	24-hour hands-on practical exam (live system exploitation)	Comfort with Linux, networking, and scripting strongly recommended	\$1,699–\$1,749 (standalone/bundle); Learn One ~\$2,749/yr	Aspiring penetration testers and red-teamers who want a hands-on, employer-respected credential
----------------------------------	----------	--	--	--	---

Note: OSCP pricing reflects OffSec's 2026 PEN-200 bundle structure; CEH pricing reflects EC-Council's standard online-proctored voucher. Both providers offer additional bundles (extended lab access, multiple attempts) that change the total cost.

4. Certification Deep Dives

GSDC Certified Ethical Hacking Foundation (CEHF)

- **What it covers:** Core ethical hacking concepts — phases of an assessment, common attack types, key vulnerabilities, and the tools professionals use, taught at a conceptual rather than exploit-execution level.
- **Who it's for:** Complete beginners, students, and professionals in adjacent IT roles who want a structured entry point into cybersecurity without needing prior experience.
- **Strengths:** No prerequisites, vendor-agnostic framing, and a lower cost of entry than most competing certifications — a practical way to test interest in the field before investing in an advanced credential.

- **Limitations:** As a foundation-level, knowledge-based credential, it doesn't validate hands-on exploitation skills the way a practical exam does — most holders treat it as step one, not a career-ending destination.
- **Typical next step:** CompTIA PenTest+ or EC-Council CEH, followed by a hands-on practical certification once real-world or lab experience has been built up.

CompTIA PenTest+

- **What it covers:** Penetration testing planning and scoping, information gathering, vulnerability identification, attack and exploitation techniques, and reporting — tested through a mix of multiple-choice and performance-based questions.
- **Who it's for:** IT professionals with some networking or security background who want a mid-tier, employer-recognized credential without CEH's experience prerequisite or price tag.
- **Strengths:** No mandatory prerequisite, DoD 8140-approved for the same government work roles as CEH, and a meaningfully lower cost — the exam voucher runs close to a third of CEH's price.
- **Limitations:** Still primarily an exam-based credential rather than a fully practical one, so it doesn't replace hands-on lab experience for advanced roles.
- **Typical next step:** OSCP or another practical, lab-based certification once the candidate is ready to prove hands-on exploitation skills.

EC-Council Certified Ethical Hacker (CEH v13)

- **What it covers:** A broad curriculum spanning reconnaissance, scanning, system hacking, malware, web application attacks, wireless security, and in the current version AI-assisted attack and defense techniques, organized around 20 modules.
- **Who it's for:** Professionals who want one of the most widely recognized names in ethical hacking, particularly those targeting government, defense-contractor, or large-enterprise roles where CEH is often an HR screening requirement.
- **Strengths:** Broad name recognition, DoD 8570/8140 compliance, and an optional practical add-on exam (leading to the CEH Master designation) for candidates who want to demonstrate applied skill on top of the knowledge exam.
- **Limitations:** The standard exam is multiple-choice, so on its own it tests knowledge more than execution; it also carries an ongoing annual membership fee and continuing-education requirement to stay current, and requires either two years of experience or official training to sit for.
- **Typical next step:** The CEH Practical exam for the Master designation, or a transition into OSCP for candidates prioritizing hands-on penetration testing skills.

OffSec OSCP (PEN-200)

- **What it covers:** Real-world penetration testing methodology, tested through a lengthy hands-on exam in which candidates must actually compromise a set of live systems, including an Active Directory environment, and then produce a professional report.
- **Who it's for:** Candidates who already have foundational security knowledge and want the certification most widely respected among penetration testers and red teamers for proving practical skill rather than recall.

- **Strengths:** A hands-on exam format that closely mirrors real engagement work, strong name recognition among technical hiring managers, and a credential that's difficult to earn without genuine capability.
- **Limitations:** The highest cost and steepest learning curve of the four certifications compared here; it assumes comfort with Linux, scripting, and networking fundamentals, so it's rarely a first certification.
- **Typical next step:** Specialized OffSec tracks such as OSWA (web) or OSEP (advanced evasion) for candidates deepening a specific specialization.

5. Which Certification Fits Your Goal?

If you only remember one section of this guide, make it this one. Match your current situation to the certification path that fits it you can always stack another credential later as your experience grows.

"I'm new to cybersecurity and want to see if this field is for me."

Start with a foundation-level certification such as the GSDC Certified Ethical Hacking Foundation. It has no prerequisites, introduces core concepts and tools, and lets you validate interest before committing to a more expensive, experience-gated credential.

"I want a recognized, mid-tier credential without a steep experience requirement."

CompTIA PenTest+ is a strong fit. It has no mandatory prerequisite, includes performance-based questions that go beyond rote memorization, and is recognized for the same government work roles as CEH at a fraction of the cost.

"My target employer specifically screens for CEH."

In that case, EC-Council's CEH is worth pursuing directly — name recognition and HR screening requirements are real factors, even when a candidate already has strong practical skills. Budget for the experience prerequisite (or official training) and the ongoing annual membership fee.

"I want to prove I can actually test systems, not just describe how to."

OSCP is the benchmark here. Its hands-on, timed practical exam is built specifically to separate candidates who understand penetration testing conceptually from those who can execute it under pressure. It's a demanding, expensive step best attempted once you already have foundational experience under your belt.

"I'm not sure which employer requirements matter most to me."

Pull three to five real job postings for the role you want and note which certifications they list as required versus preferred. Certification requirements vary significantly by industry, region, and whether the employer is public or private sector the job market itself is the most reliable guide.

6. Certification & Salary Snapshot

Salary figures for ethical hacking and penetration testing roles vary widely by experience, location, industry, and the specific employer — the ranges below are general market indicators, not guarantees, and are gathered from recent public salary-data reporting.

- Entry-level security analyst roles: roughly \$90,000–\$95,000 per year in the U.S., often the landing spot after a foundation or mid-tier certification plus some hands-on practice.

- CEH-holding professionals: commonly cited in the \$105,000–\$137,000 range, with some sources noting a 10–20% salary bump for professionals who add CEH to existing experience.
- Penetration testers broadly: roughly \$85,000 at entry level up to \$140,000+ for senior roles, reflecting how much weight the market puts on hands-on, practical skill.
- OSCP-holding professionals: averaging close to \$120,000 per year in recent U.S. salary data, consistent with OSCP's reputation as a practical-skills benchmark.

These figures are general indicators pulled from public salary-reporting sources in 2026 and will vary by region, employer, and individual experience. Treat certification as one input into your earning potential, not a guaranteed outcome.

7. Next Steps

Certification is a foundation, not a substitute for hands-on practice. Whichever path you choose from this guide, pair it with real practice home labs, capture-the-flag challenges, or supervised project work so the credential reflects skill you can actually demonstrate in an interview or on the job.

If you're just starting out and want a structured, no-prerequisite entry point into ethical hacking concepts, GSDC's Certified Ethical Hacking Foundation is designed for exactly that stage building a working understanding of ethical hacking methodology, vulnerabilities, and security-testing practices you can build on with more advanced certifications later.

Learn more about GSDC's Certified Ethical Hacking Foundation and see how it fits into your certification roadmap.

CERTIFIED ETHICAL HACKING FOUNDATION (CEHF)

THE CERTIFIED ETHICAL HACKING FOUNDATION BUILDS CORE SKILLS IN ETHICAL HACKING, CYBERSECURITY, AND VULNERABILITY ASSESSMENT TO COMBAT CYBER THREATS.



ABOUT GSDC CERTIFICATION



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.



LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Showcase practical ethical hacking skills for real-world organizations.
- Strengthen your cybersecurity knowledge and demonstrate your expertise.
- Build foundational understanding of machine learning.

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now



www.gsdccouncil.org