mile2®
CYBERSECURITY CERTIFICATIONS

HOW TO BECOME A PENETRATION TESTER

A STEP-BY-STEP CAREER ROADMAP

By Dr. Raymond Friedman (President, Mile2)

INTRODUCTION

Penetration testing legally identifies weaknesses before attackers can exploit them. It requires technical skill, ethical judgment, methodology, communication, and a clear understanding of legal boundaries.

STRONG JOB OUTLOOK

The U.S. Bureau of Labor Statistics* projects employment for information security analysts to grow

29%

from 2024 to 2034, much faster than the average for all occupations.

~16,000 OPENINGS PER YEAR

Projected average annual openings in this field over the next decade.*

PENTESTER'S MISSION

Think like an attacker. Act ethically. Find real risk. Provide actionable recommendations. Help organizations improve their security posture.

10 STEPS TO BECOME A PENETRATION TESTER

1 BUILD A STRONG IT FOUNDATION

- Networking (TCP/IP, DNS, routing, ports)
- Operating Systems (Windows, Linux)
- Web technologies
- Cloud basics
- Security fundamentals

2 LEARN ETHICAL HACKING METHODOLOGY

- Pre-engagement planning
- Reconnaissance
- Scanning & enumeration
- Exploitation validation
- Reporting
- Retesting

3 GET HANDS-ON PRACTICE

- Use legal labs & cyber ranges
- Practice in controlled environments
- Build repeatable process
- Never test without permission

4 LEARN CORE TOOLS

- Network scanning
- Web testing tools
- Password auditing
- Exploitation frameworks
- Proxy, cloud, AD & reporting tools

5 DEVELOP REPORTING & COMMUNICATION SKILLS

- Explain what, why, impact, and evidence
- Provide remediation guidance
- Communicate to technical teams & business leaders

6 CHOOSE THE RIGHT CERTIFICATIONS

- Start with a foundation
- Advance to professional penetration testing
- Add AI-era security knowledge

7 BUILD A PORTFOLIO

- Lab write-ups
- Sample reports
- GitHub / scripts
- Blog posts
- CTF & range notes
- Home lab diagram

8 THINK LIKE A CONSULTANT

- Understand business processes & data risk
- Assess real-world exploitability
- Prioritize impactful remediation

9 APPLY FOR THE RIGHT ROLES

- Security Analyst
- SOC Analyst
- Sys/Net Admin
- Vulnerability Analyst
- Security Consultant (and more)

10 KEEP LEARNING ALWAYS

- Cloud & AD security
- Web, API & container security
- AI security
- Scripting (Python, PowerShell, Bash)
- Purple teaming

RECOMMENDED CERTIFICATION PATH (MILE2®)

C)PEH
Certified Professional Ethical Hacker

Build ethical hacking foundations and attacker mindset.

Best for:
- New cybersecurity pros
- IT admins / support pros
- Students
- Ethical hacking foundations

C)PTE
Certified Penetration Testing Engineer

Develop comprehensive penetration testing workflows and skills.

Best for:
- Aspiring pentesters
- Security analysts
- System administrators
- Hands-on test experience

CAICSO™
Certified AI Cybersecurity Officer

Understand AI-enabled cyber risk, governance, and secure AI systems.

Best for:
- Pentesters & red teamers
- Security leaders
- AI app / LLM testers
- AI governance roles

FOUNDATION → PROFESSIONAL → AI-READY FUTURE

OTHER INDUSTRY CERTIFICATIONS TO CONSIDER

Certified Ethical Hacker (CEH)
One of the most recognized ethical hacking certifications. Teaches how to think like a hacker in the age of AI.

Offensive Security Certified Professional (OSCP)
Hands-on penetration testing exam with a strong practical reputation. Best pursued after building solid fundamentals.

GIAC Penetration Tester (GPEN)
Enterprise-focused penetration testing training across cloud, on-prem, and identity environments.

Certified Penetration Testing Consultant (C)PTC
Advanced exploitation techniques, buffer overflows, DEP & ASLR bypass, and professional reporting.

COMMON ENTRY-LEVEL ROLES

- Security Analyst
- SOC Analyst
- Network Administrator
- System Administrator
- Cloud Support Engineer
- Vulnerability Management Analyst
- Application Security Analyst
- IT Support Specialist (with security responsibilities)
- Cybersecurity Consultant

NICE FRAMEWORK

The NICE Framework® provides a common language for cybersecurity workforce roles, tasks, knowledge, and skills helping employers, educators, and learners describe cybersecurity work more consistently.

HOW LONG DOES IT TAKE?

6 – 12 MONTHS
For IT professionals with focused study, labs, and certifications to reach junior pentest roles.

12 – 24 MONTHS
For beginners starting from zero to build core IT and security skills.

24+ MONTHS
For advanced pentesting, red teaming, cloud & AI exploitation, and continuous development.

WHAT MAKES A GREAT PENTESTER?

Technical Depth · Ethical Mindset · Methodical Approach · Clear Communication · Business Awareness · Lifelong Learner

LEGAL & ETHICAL PRINCIPLES

- Always obtain written authorization
- Respect scope and rules of engagement
- Protect data and sensitive information
- Document responsibly
- Stop when you should stop

IMPORTANT REMINDER

Unauthorized testing is illegal. Practice only in environments you own or have explicit written permission to assess.

REFERENCES

- Bureau of Labor Statistics. (2025). Information security analysts: Occupational Outlook Handbook.
- CISA. (2026). NICE Workforce Framework for Cybersecurity.
- EC-Council. (2026). Certified Ethical Hacker CEH AI.
- Mile2® Cybersecurity Institute. (2026). C)PEH, C)PTE, CAICSO™ Course Outlines.
- SANS Institute. (2026). SEC560: Enterprise Penetration Testing.
- SANS Institute. (2026). Penetration Tester Certifications.

VISIT mile2.ca FOR MORE INFORMATION ABOUT CAREERS IN CYBERSECURITY.