What is **Penetration** Testing and how can you start in the **Cyber Security** Field?

21.03.2025

AGENDA

01

Introduction

Introducing Ourselves to the New Era of Cyber Security & Collaboration

02

Penetration Testing

- What is Penetration Testing
- the Importance of Cyber Security

03

Start your Career

- How can you start
- What Resources can you use

04

Questions

Feel free to ask any question please

Eng. Ahmed Hassan

Cyber Security Engineer & Penetration Tester

Qualifications & professional certification

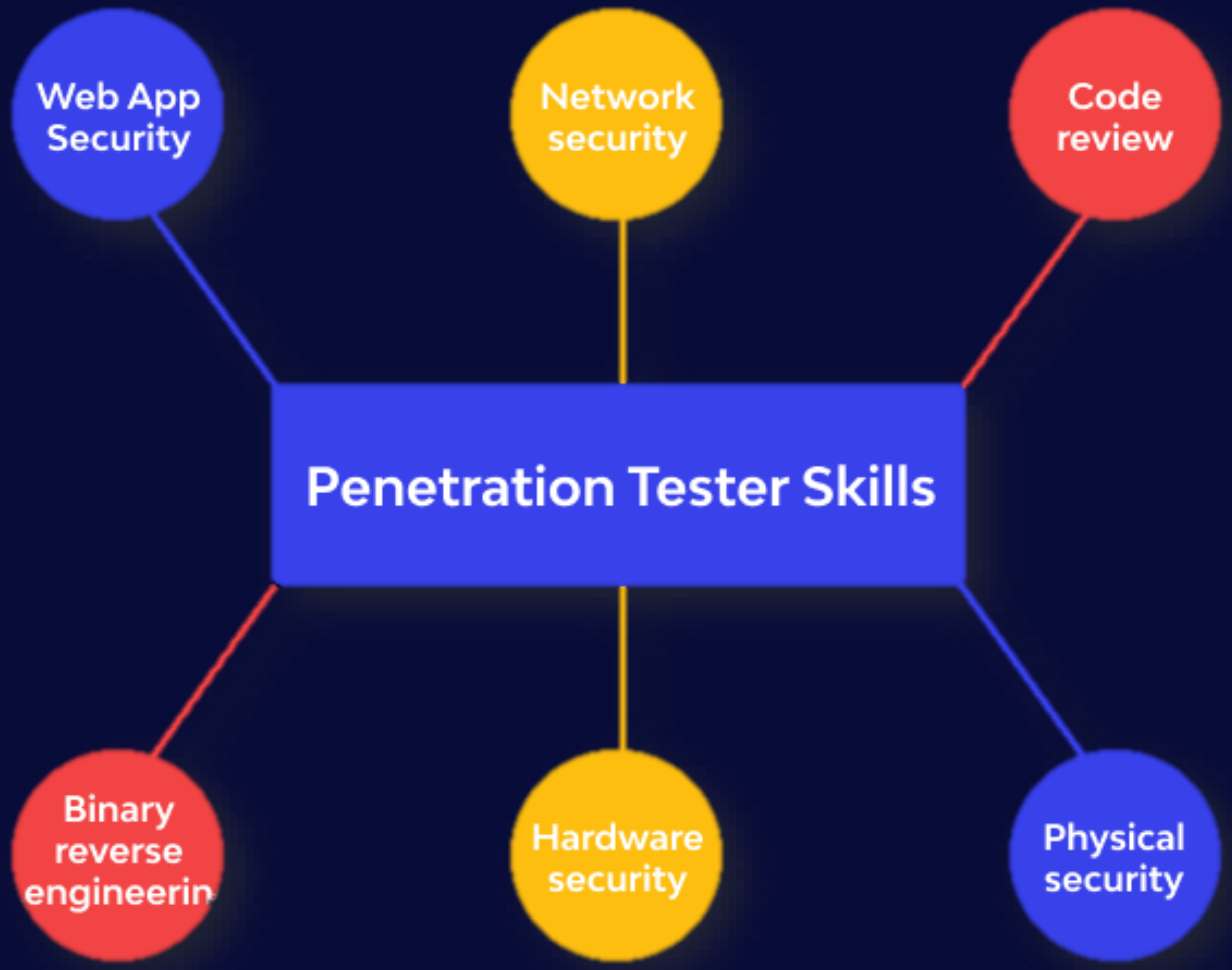
certification for advanced IT professionals

Certified EC-council Instructor

Certified Ethical Hacker

Offensive Security Certified Professional

Penetration Testing Paths



What is Pentesting?

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

How can you start in IT-Security?

- eJPT (eLearnSecurity Junior Penetration Tester)
- eWPT (eLearnSecurity Web Application Penetration Tester)
- eCPPT (eLearnSecurity Professional Penetration Tester)

Pentesting

- Millions of Companies got **Hacked**
  - Companies need **Pentester**
    - Improve your Skills

Uber and GTA 6 Hacked & Leaked

UK police arrest teenager suspected of Uber, GTA 6 hacks

Carly Page @carlypage_ / 4:28 PM GMT+2 • September 26, 2022 Comment

Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?

A major data breach has given the world an early look at Grand Theft Auto 6. Why is this such bad news for the developer?

[redacted] Uber staff posted a comment. Sep 15th (5 mins ago)

UBER HAS BEEN HACKED (domain admin, aws admin, vsphere admin, gsuite SA) AND THIS HACKERONE ACCOUNT HAS BEEN ALSO

Uber

How Uber was hacked in 2022

Other Resources

HacktheBox

TCM Security Academy

Tryhackme

Pentester Academy

https://github.com/ashutoshshah1/Ethical-hacking-Roadmap

Penetration Tester HackTheBox

HACKER | 17 MIN READ

How to become a penetration tester: (Practical) career guide

So you want to become a penetration tester but don't know where to start? This step-by-step guide is for you!

mrb3n, Nov 09 2022

CONTENTS

What does a penetration tester do on a daily basis?

How to become a penetration tester: 5 practical steps

- Step 1: Know thyself (and your suitability for a penetration testing career)
- Step 2: Level up your skills
  - Learning or becoming a penetration tester from scratch
  - How to get started in pentesting with IT experience
- Step 3: Get a hacking or penetration testing certification
- Step 4: Get your hands dirty in real-world environments
- Step 5: Start applying
- (Bonus) Step 6: Carve out a unique advantage

Average penetration tester salary (for beginners): How much do penetration testers make?

Penetration Tester Tryhackme

Learning Paths

Work your way through a structured learning path

Red Teaming

Learn the skills needed to become a Red Team Operator

- Use diverse techniques for initial access
- Enumerate and persist on targets`
- Evade security solutions
- Exploit Active Directory

Intermediate 48 hours

Introduction to Cyber Security

Learn the core skills required to start a career in cyber security

- Learn about different careers in cyber
- Hack your first application
- Defend against a live cyber attack
- Explore security topics in the industry

Easy 24 hours

Jr Penetration Tester

Learn the necessary skills to start a career as a penetration tester

- Pentesting methodologies and tactics
- Enumeration, exploitation and reporting
- Realistic hands-on hacking exercises
- Learn security tools used in the industry

Intermediate 64 hours

Pre Security

Before hacking something, you first need to understand the basics

- Cyber security basics
- Networking basics and weaknesses
- The web and common attacks
- Learn to use the Linux operating system

Easy 40 hours

Penetration Tester

Web Penetration Testing

Network Penetration Testing

Active Directory Pentesting

Mobile Pentesting

Companies Acknowledgments

FOUND VULNERABILITIES (BUG BOUNTY PROGRAMMS)

Siemens

United Nations (UN)

Sparkasse Bank (Austria)

osd.myndr.nl

forescout.com

Government Technology Agency of Singapore (GovTech)

MTN Group

UK Ministry of Defense (Hacker Coin as Thank you received)

UK Government

U.S. Department of State 7x -> multiple Vulnerabilities submitted (Stored XSS, SQL Errors, SQL Injection etc.)

NASA

[redacted] (Bounty 200 Euro) (stored XSS and HTML Injection)

INDIAN GOVERNMENT -> Stored Cross Site Scripting (XSS)

PHILIPINES GOVERNMET -> Reflected Cross Site Scripting (XSS)

CERT-EU Computer Emergency Response Team (CERT-EU) for the EU institutions

SCOTTISH GOVERNMENT -> multiple Vulnerabilities

SINGAPURE GOVERNMENT NEW ZEALAND GOVERNMENT

Huawei -> stored XSS and File Upload Restriction Bypass

Drexel University University of Texas of Austin

HP (Hewlett Packard) 2x Vulnerabilities

FOUND VULNERABILITIES (BUG BOUNTY PROGRAMMS)

stkkr.nl

Drexel University

Nokia

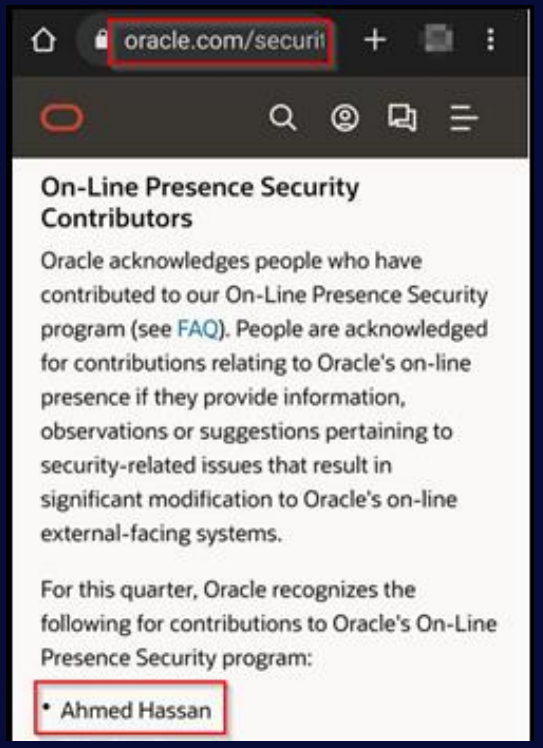
Oracle

Kuula

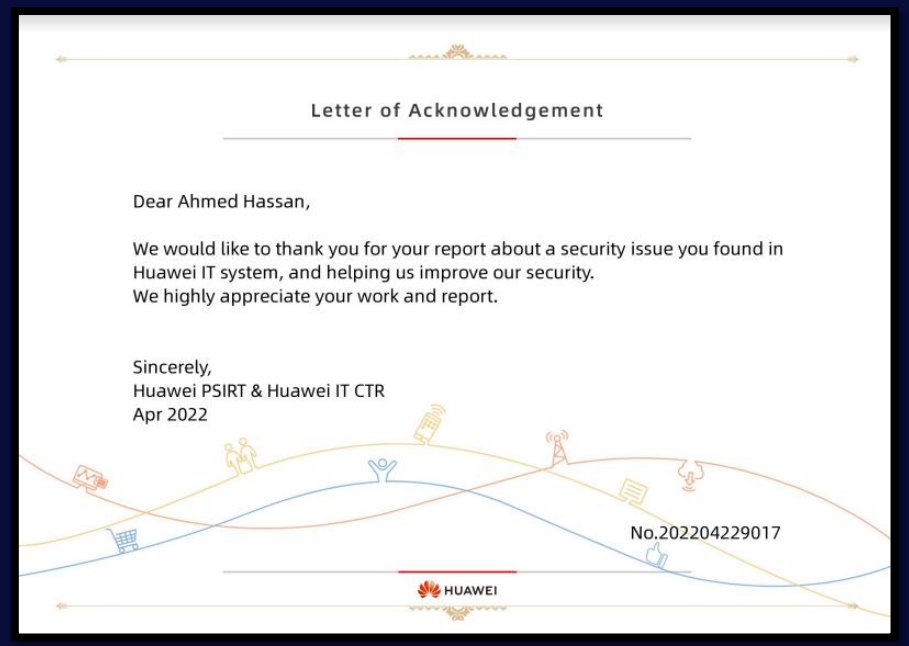
Bosch

Lenovo

Philips



Companies Acknowledgments



Letter of Acknowledgement

Dear Ahmed Hassan,

We would like to thank you for your report about a security issue you found in Huawei IT system, and helping us improve our security.
We highly appreciate your work and report.

Sincerely,
Huawei PSIRT & Huawei IT CTR
Apr 2022

No.202204229017

HUAWEI

QUESTIONS ?

THANK YOU

Follow us

LinkedIn: https://www.linkedin.com/in/ahmed-hassan-79559487/