Hacking – How to start?

Jakub „Ziemni" Partyka

whoami

- Jakub „Ziemni" Partyka
- MSc Cyber Security Management
- Cyber Security Enthusiast

- HackTheBox Top 10
- Member of AlphaPwners
- 2 years of Professional Experience
- eJPT Certificate
- Rasta Labs Certificate

Social Media

- LinkedIn: jakub-partyka-508aa3152
- Twitter: @ziemni_
- Discord: Ziemni#2416
- HackTheBox: Ziemni (12507)

Table of Contents

How to get into Hacking?

Checklist

1. Programming languages (Python / C / JS / PHP ...)
2. Linux (Filesystem / Privileges / services ...)
3. Networking (Protocols / Ports ...)
4. Web Vulnerabilities (SQLi / XSS / LFI ...)
5. Tools (Burp Suite / nmap / MSF ...)
6. Windows (Filesystem / Privileges / services / AD ...)
7. Jeopardy Categories

Cyber Roadmap

HACK THE BOX

TryHackMe

Beginner to advanced level. Huge amount of content. One of the best hands-on learning resource.

Immersive Labs

Lots of educational content on all areas of Cyber. From risk management to labs on specific tools.

HackTheBox

Challenge based platform. Boot2root machines. CTF challenges.

VulnHub

The original boot2root machine platform. Downloadable VM images. Massive amount of content. 535+ machines.

PEH by TCM

One of the best regarded courses on penetration testing. Paid but often discounted or freely available.

eJPT

eLearnSecurity Certified Junior Penetration Tester certificate. Beginner friendly cert, very good course content (PTS).

OSCP

Offensive Security Certified Professional. Prestigious certifications. Often lands a job to its holder.

eCPPT

eLearnSecurity Certified Professional Penetration Tester. Lesser known than OSCP but has better course materials.

OSCE

High end certificate. Brutal exam. Being on this level must be nice.

CEH

The one to rule them all. The certificate of the ultimate penetration tester. (It's a joke, please avoid this thing) - Commonly required by governments.

By Tux

CTFs

CTFs

„CTF (Capture The Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks ranging from a scavenger hunt on wikipedia to basic programming exercises, to hacking your way into a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag, hence the name!"

CTFs

- Hacking Competitions
- Jeopardy / Attack & Defence

- https://ctftime.org/

Hack The Box

PEN-TESTING LABS

https://www.hackthebox.eu/

Other CTF Platforms

- Immersive Labs - Very detailed introduction to lots of areas of Cyber

- Virtual Hacking Labs - Nice pool of machines but expensive

- Cyber Sec Labs - Similar to tryhackme/hackthebox but smaller platform

- VulnHub - The original boot2root machine platform (now owned by Offsec)

By Tux

Other CTF Platforms

- [OverTheWire](#) – WarGames

- [Rop Emporium](#) - pwn & reverse engineering

- [Nightmare](#) - very good binary exploitation course

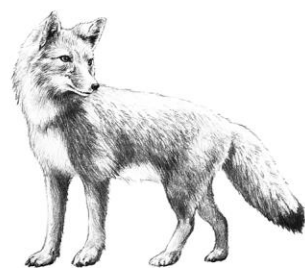- [PicoCTF](#) - Must Try CTF for beginners

By Tux

Certifications

My short story

Learning for 5h+ per day…

https://tryhackme.com/room/yotf

https://www.hackthebox.eu/

🇵🇱

Polish Cyber Security Army

My tips for everyone who wants to improve in Hacking

Be Active!

- Discord Servers
- Forums
- IRCs

- https://news.ycombinator.com/
- https://thehackernews.com/
- https://owasp.org/
- https://0x00sec.org/

Set Goals!

- Today I will learn X…
- By next week I will do this VM…
- In one year I'll be Top10 on HTB :)

Take Notes!

- Notes of things you learn
- Writeups
- Cheatsheets

- Joplin
- Notable

Q&A