



Cracking the Code My Path to Becoming a Penetration Tester

11th October 2024

Razvan-Costin Ionescu

GSE #298, Head of Professional Services





Life as a Penetration Tester



What my friends think I do



What my mom thinks I do



What society thinks I do



What hackers think I do



What I think I do



What I actually do



#whoami

Razvan-Costin IONESCU, GSE #298

- 12+ years of experience
- Head of Penetration Testing Services @Pentest-Tools.com
- worked for Dell (Services + Secureworks), Intel, Fitbit, EY
- Collaborated with: Probitas, Cobalt.io, OneLeet
- Hundreds of Penetration Tests for companies across the globe
- 3 things I love about my job: freedom, challenging, rewarding





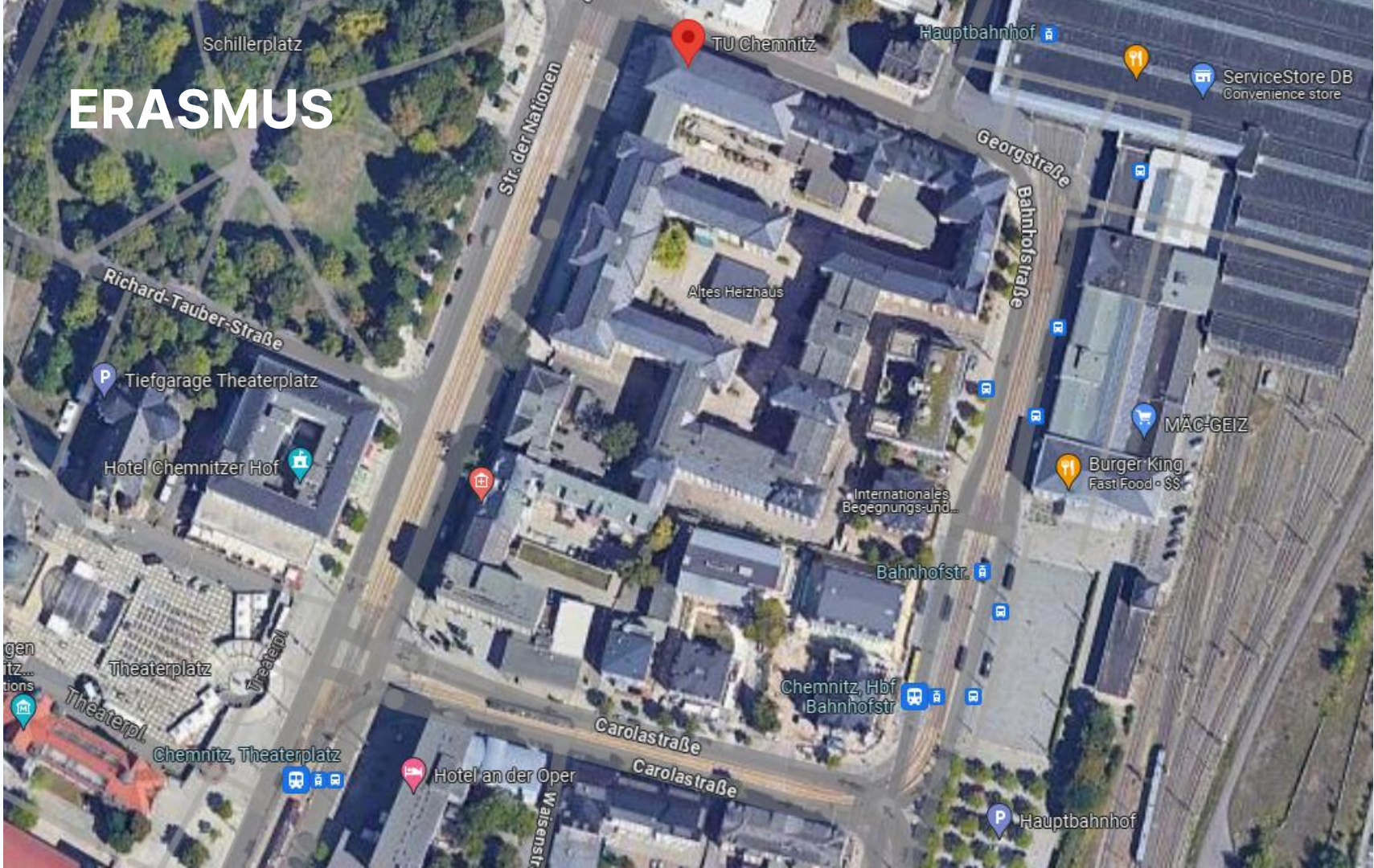
Agenda

- Learning “paths”
- Practicing
- Certifications (?)
- Events (conferences)
- Resources
- Sample of cool projects





ERASMUS



Schillerplatz

TU Chemnitz

Hauptbahnhof

ServiceStore DB
Convenience store

Str. der Nationen

Georgstraße

Bahnhofstraße

Altes Heizhaus

Richard-Tauber-Straße

Tiefgarage Theaterplatz

Hotel Chemnitzer Hof

M&C-GEIZ

Burger King
Fast Food • \$\$

Internationales
Begegnungs- und...

Bahnhofstr.

Chemnitz, Hbf
Bahnhofstr.

Theaterplatz

Chemnitz, Theaterplatz

Hotel an der Oper

Carolastraße

Carolas traße

Hauptbahnhof

Waisenstr.



The “long” road to success

Learning / experiencing

- **Say yes to ERASMUS Scholarships**
 - One of the best experiences in my life student
- **Say yes to challenges**
 - Learn a new language out of your comfort zone 😊
- **Learn at least one programming language**
 - Python would be a great start





The “long” road to success

More Learning

- University of Politehnica, MSc in Security of Complex Networks (SRIC)
 - My first failed exam ☹️
 - My first “real-world” certification – LPIC-1
- Learn to build, break and fix
 - Coursera



By <http://www.backtrack-linux.org/wp-content/gallery/backtrack-5/bt5-g0.png>, GPL, <https://commons.wikimedia.org/w/index.php?curid=16164718>



Practicing

- <https://pentest-ground.com/>
- <https://www.vulnhub.com/> - VMs – Get Root style
- <https://hackthebox.com/>
- <https://www.pentesteracademy.com/topics>
- <https://www.pentesterlab.com/>
- <https://tryhackme.com/>
- <https://portswigger.net/web-security/dashboard>
- <https://academy.tcm-sec.com/>





Vulnerable apps to benchmark your scanners and your skills

Pentest Ground is a free playground with deliberately vulnerable web applications and network services. You can use them to test how effective vulnerability scanning tools are or for educational purposes.



Vulnerable systems

NAME	URL	TECHNOLOGIES	VULNERABILITIES
Damn Vulnerable Web Application	https://pentest-ground.com:4280	Classic Web App	CSRF , XSS , SQLi
Damn Vulnerable GraphQL Application	https://pentest-ground.com:5013	GraphQL	CMDi , XSS , SQLi
RestFlaw	https://pentest-ground.com:9000	REST API	SQLi , Code Injection , XXE
CipherHeart	pentest-ground.com:6379	Redis	CVE-2022-0543 (RCE)
GuardianLeaks	https://pentest-ground.com:81	Web App	XSS , SSRF , Code Injection



What you need to get started

- Curious mind
- Thinking outside the box
- Very well-structured





Training-on-the-job

- Internship
- Practice
- Start a career – from Jr. to Infinity and beyond
- <https://pentest-tools.com/jobs>



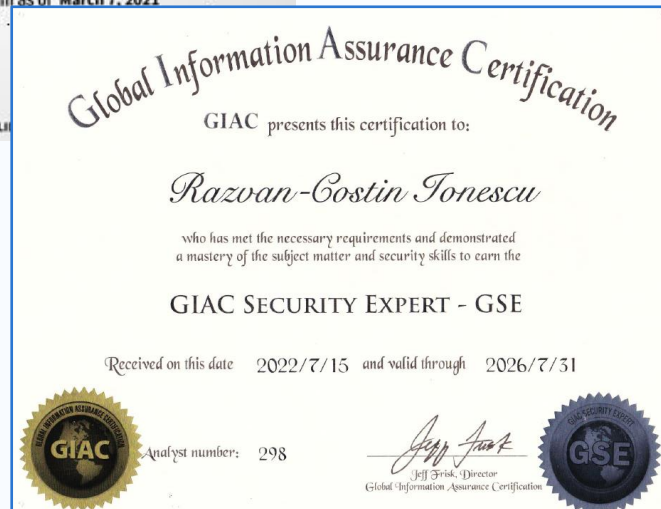
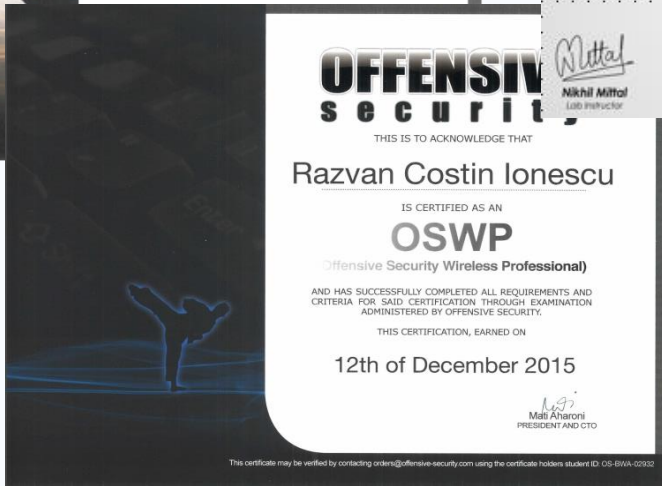


How certifications helped me get where I am today





Certifications everywhere





Have I told you about certifications ?

Few personal recommendations

- Offensive Security
- GIAC
- TCM Security
- Portswigger Academy





Why apply to speak at events & what that gets you





32C3





Visiting BlackHat US





Visiting DefCon - Vegas



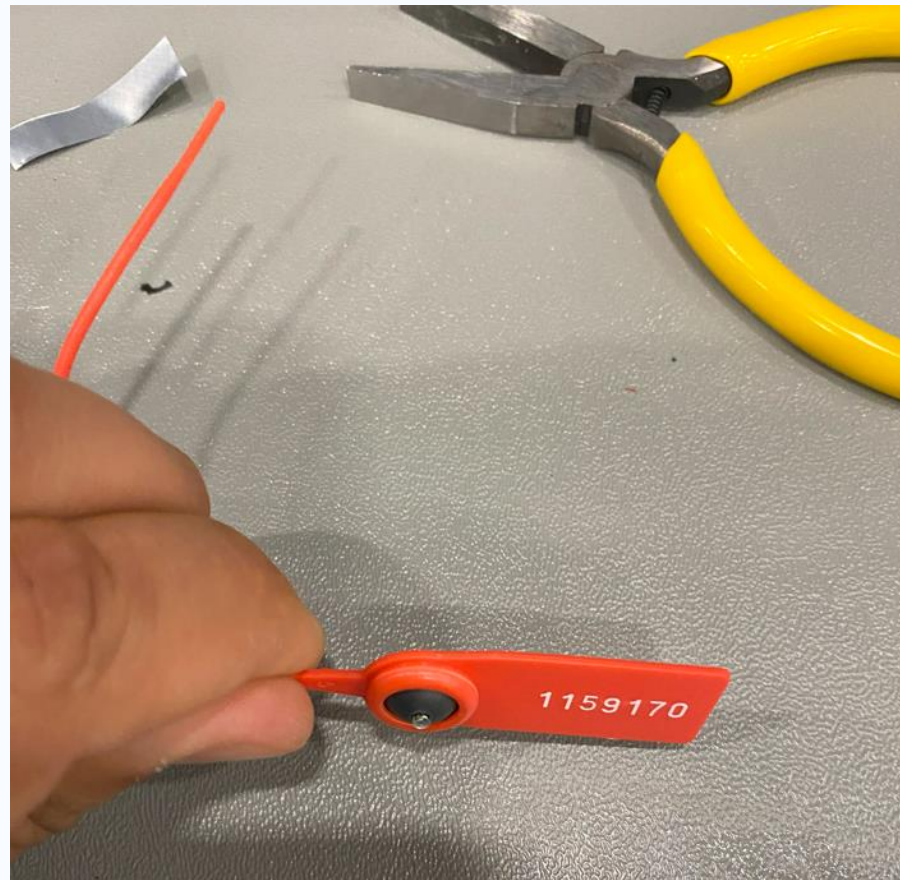


Visiting DefCon



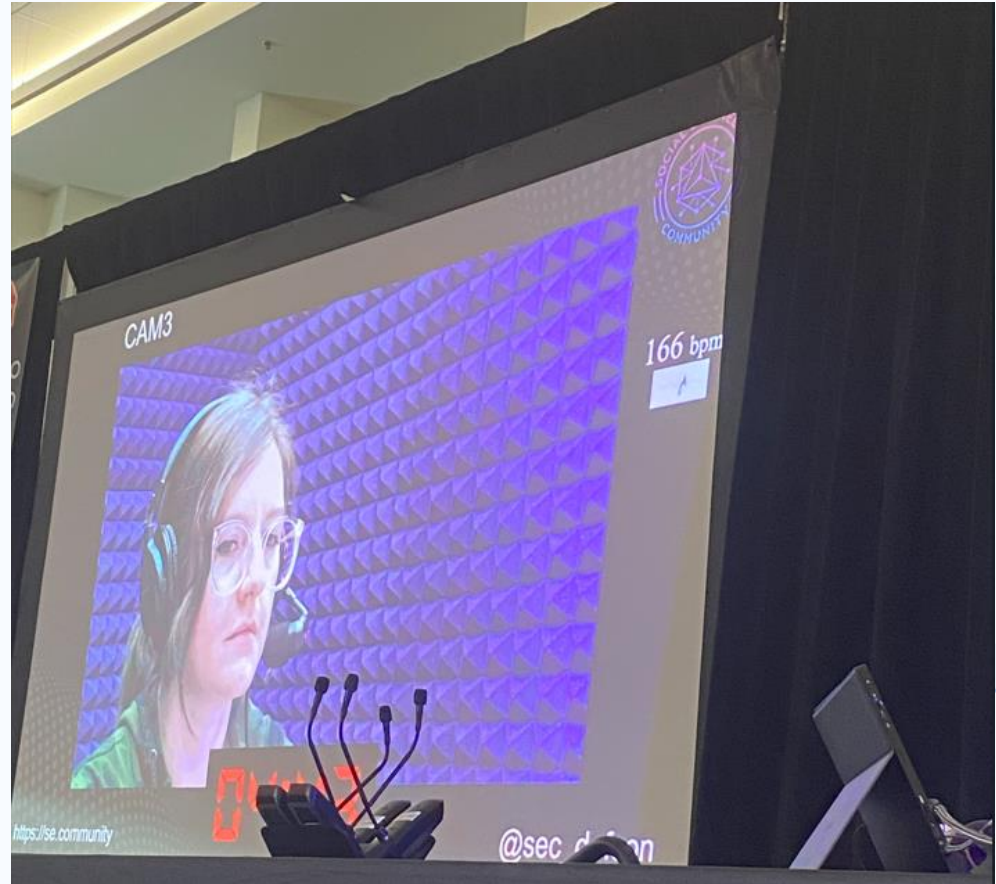


DefCon – Tamper Evident Village





DefCon – Social Engineering Village





Meeting VIPs at DefCon





Cybersecurity Community



OWASP
Open Web Application
Security Project



What are my personal recommendations to you

- Be actively involved in the Cybersecurity Community
- Find relevant learning resources and embrace them
- Never stop being curious
- Attend and speak at Cybersecurity Conferences around the world
- Say YES to your friends when they invite you to their podcasts 😊



SECRETELE SPECIALIȘTILOR

SEZONUL 1
EPISODUL 8

**RĂZVAN
IONESCU**

**penetration tester
cyber security expert**

+ head of pentesting



**viorel
mocanu**

**podcast de
carieră în IT**

We think we know Podcast by Pentest-Tools.com



IPPSEC: What makes StarCraft and Cybersecurity similar ?



CYBER EMPATHY

- **By Andra Zaharia**
- **Why we need empathy in cybersecurity ?**

WINNER - 2024

**The Conversation Starter –
Best Blog/Podcast/Vlog that
Champions Diverse Voices
and New Perspectives**

This is for the blog, vlog, podcast that
champions diverse voices and tackles
pressing, yet often underdiscussed, topics.

Winner: Cyber Empathy Podcast

2023 / Winner

European Cybersecurity Blogger Awards

- Most Educational Blog
- Best New Cybersecurity Podcast

2023 / Shortlisted

Security Serious Unsung Heroes Awards

- Diversity Champion
- Cybersecurity Wellbeing Advocate

2023 / Recommended

The SANS LDR521 Security Culture for Leaders course lists
Cyber Empathy as a recommended resource!










How They Hacked the Prime Minister From 1 Instagram Post 📌 Darknet Diaries Ep. 84: Jet-setters



Jack Rhysider 
336K subscribers

[Subscribe](#)

-  2.1K
- 
-  Share
-  Download
-  Clip
-  Save
- 

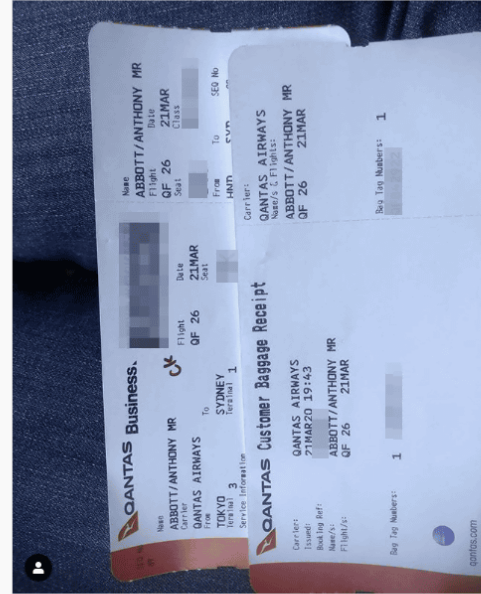


When you browse Instagram and find former Australian Prime Minister Tony Abbott's passport number

- <https://mango.pdf.zone/finding-former-australian-prime-minister-tony-abbotts-passport-number-on-instagram>

Instagram

Search



hontonyabbott • Follow

hontonyabbott • A big thank you to all the team on QF26 from Tokyo. Hope to see you flying again soon! This will pass.

33m

Stay well and safe mate
AU
21m Reply

come and jump on calderwood's truck lol
15m Reply

Liked by [redacted] and 243 others
33 MINUTES AGO

Add a comment... Post

More posts from hontonyabbott



Bank in Lebanon



Salut Razvan!

Multumesc pentru acceptarea cererii de conectare pe LinkedIn. Te contactez pentru un proiect in cybersecurity/pen testing care s-ar putea sa te intereseze.

Proiectul dureaza 20 zile din care 15 se lucreaza remote si 5 vor fi on site in orientul mijlociu (cu avion si toate cheltuielile decontate separat). Bugetul proiectului pentru acest rol este [REDACTED]

Cererea vine de la o companie care tocmai a semnat un contract pentru servicii de networking si securitate informatica si este urgenta. Intre timp te rog sa ma anunti cu ce intrebari sau detalii te mai pot ajuta si cand am putea sa ne auzim pe un telefon ca sa povestim despre acest proiect.

Sa ne auzim cu bine,

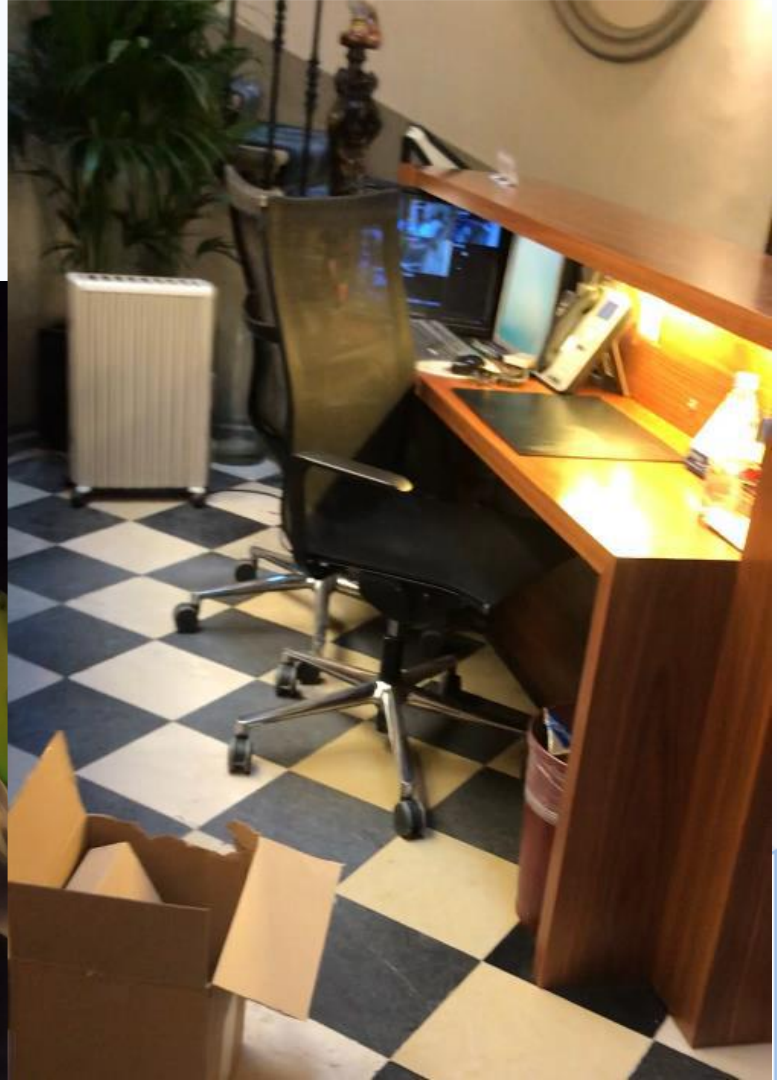


Metro station in Dubai





Swiss Private Bank





Misc

- <https://www.youtube.com/@ViorelMocanu> ->
<https://www.youtube.com/watch?v=dy8GNrGtPzs>
- <https://www.youtube.com/@PentestToolscom/podcasts>
- <https://www.youtube.com/@cyberempathy>
- <https://darknetdiaries.com/>
- <https://pentest-tools.com/jobs>



Q & A

razvan.ionescu@pentest-tools.com
<https://www.linkedin.com/in/ionescr/>

