YOUSSEF ENNACIRI

RED TEAM CONSULTANT

EXECUTIVE PROFILE

- https://c2.opsec.zone
- Experienced Red Team operator specializing in malware development, with a strong focus on evading modern EDR solutions.
- Dedicated to continuous research and development in offensive security, with a deep understanding of advanced adversary tradecraft and stealth techniques.

AREAS OF EXPERTISE

- Red Teaming
- Threat led penetration testing (TLPT)
- DORA and TIBER-EU regulations
- Programming (C++, Python, Nim)
- Malware dev
- Malware analysis
- Microsoft cloud security assessment
- Attack surface management

CONTACT AND PERSONNEL DETAILS

27 years old

+49 15207964548

ennaciri.youssef47@gmail.com

Barcelona, Spain

https://github.com/ydy4

https://www.linkedin.com/in/youssef-ennaciri-7897b6170/

https://app.hackthebox.com/profile/249618

LANGUAGES

- English (C1)
- French (C1)
- Arabic (C1)
- German (A1)

15 - Nov - 2025

PROFESSIONAL EXPERIENCE

CYBER SECURITY CONSULTANT - RED TEAM

EUROFINS Poland | from May 2023 to the Present day

Regular Engagements:

- Red Team Operations
  - Perform quarterly Red Team assessments (Cobalt Strike, PrivateC2).
  - Execute APT simulation scenarios leveraging internal threat intelligence.
- Purple Team Exercises
  - Conduct targeted Purple Team exercises.
  - Co-author a playbook for threat modeling.
  - Build and host an automated reporting system based on VECTR
- Develop tool-set for successful operations
  - Develop an in-house command and control tool PrivateC2.
  - Develop a custom shell-code loaders and beacon object files.
  - Deploy and maintain a Red Team infrastructure.
  - implement large-scale external vulnerability scans system.
  - Implement IP/domain laundering mechanisms.
- Side project
  - Co-created a dynamic dashboard to map detection capabilities to MITRE Matrix coverage based on Purple Team exercises results.

Hosted Internal Workshops;

- Hands-on PrivateC2: First Stage C2 to Back Stage
- Initial Access: Malware in Several Flavors (js, py, cpl, lnk, iso, sct, png, ts)

Attended Conferences & Trainings:

- Le Hack 2025 in Paris: The Singularity
- OffensiveCon 2024 in Berlin: Modern Malware OPSEC and Anti-reverse Techniques Implementation and Reversing
- Dark Vortex: Malware On Steroids

CYBER SECURITY CONSULTANT - PENTESTER

PwC France & Maghreb | from July 2022 to May 2023

Regular Consulting Engagements:

- Penetration testing engagements on critical applications.
- Performed pentest on financial applications (Web, Thick Client, Cloud).
- Performed attack surface management.
- Shared discovered weaknesses with both development teams and top management.

R&D projects:

- Obtained PASSI Pentest certification.
- Developed a proof of concept for deploying a micro-SOC on Azure.
- Prepared technical demos for potential clients.
- Co-authored business proposals.

Satisfied clients:

Edenred (Americas, UK, Spain, and others), Bred bank and Rexel.

MAIN INTERESTS

- History
- Learning languages
- Hiking

VOLUNTEERING

- ESC Build Sustainability Solutions
- NGO Nature Conservancy

PROFESSIONAL EXPERIENCE

CYBER SECURITY CONSULTANT - PENTESTER

DATAPROTECT Morocco | from October 2020 to June 2022

Regular Consulting Engagements:

- Collaborated with external vendors to conduct penetration tests on network infrastructures, web applications, mobile applications, and WiFi.
- Monitored and analyzed security incidents within client infrastructure.
- Provided incident response support as needed.

Satisfied clients:
Bank of Africa, Eurafric Information, Lydec and OCP group

ACADEMIC EDUCATION

ENGINEERING DEGREE

NATIONAL SCHOOL OF APPLIED SCIENCES OF SAFI

Network and Telecommunications | form 2018 to 2021

- Project 1: Performed forensics on a non-volatile memory.
- Project 2: Set up network attack scenarios in the school lab.

BACHELOR DEGREE

MULTIDISCIPLINARY FACULTY OF ERRACHIDIA

Network and Telecommunications | from 2016 to 2018

- Project 1: Created a system that transmits data over the visible light.
- Project 2: Worked on a GSM Jammer that covers 300 meters area.

HIGH SCHOOL DEGREE

HIGH SCHOOL OF MOULAY RACHID

Physics and Chemistry | from 2013 to 2015

CERTIFICATIONS

CRTL (2024) CERTIFIED RED TEAM LEAD
OSCP (2023) OFFENSIVE SECURITY CERTIFIED PROFESSIONAL
CRTO (2023) CERTIFIED RED TEAM OPERATOR
CRTP (2022) CERTIFIED RED TEAM PROFESSIONAL