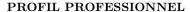
# Amro Esseroukh

amroes.github.io • @amroes

**\** +33 7 45 42 66 54

in @amro-esseroukh





Élève Ingénieur en Sécurité des Systèmes d'Information, Pentester et Red Teamer passionné, certifié OSEP, OSCP et CRTO. Particulièrement intéressé par la recherche de vulnérabilités, les techniques d'évasion avancées et l'ingénierie inverse.

#### CERTIFICATIONS

OffSec Advanced Evasion Techniques and Breaching Defenses Juillet 2025 - Août 2025

(OSEP)

OffSec

OffSec Certified Professional (OSCP)

Certified Red Team Operator (CRTO)

Zero-Point Security

Août 2024 - Octobre 2024

Obtenu

Décembre 2024 - Janvier 2025

Obtenu

DIPLÔMES ET FORMATIONS

Informatique, Réseaux et Cybersécurité (IRC) à ESISAR, Valence

Cybersécurité, Réseaux, Cryptographie, Sécurité des systèmes

Sécurité des Systèmes d'Information (SSI) à ENSIAS, Rabat

Cryptographie, Pentesting, Machine Learning, Réseaux, Bases de données, Administration systèmes

Classes préparatoires (CPGE) au Lycée Moulay Hassan, Tanger

Mathématiques, Physique, Sciences de l'ingénieur

Depuis sept. 2025

2023 - 2025

2021 - 2023

#### EXPÉRIENCES PROFESSIONNELLES

#### Stagiaire en Tests d'Intrusion (Pentest) chez Orange Cyberdéfense Casablanca, Maroc

Juin 2025 - Août 2025

- Conduite de tests d'intrusion d'infrastructures Active Directory : exploitation des trusts, attaques Kerberos (Kerberoasting, ASREPRoasting)
- Utilisation d'outils comme BloodHound et Netexec pour la découverte de chemins d'attaque et l'élévation de privilèges
- Rédaction de rapports détaillés pour des clients enterprise

## Stagiaire en Recherche Avancée sur l'Évasion d'Antivirus chez SEKERA

Juin 2025 - Août 2025

- Casablanca, Maroc (à distance en parallél)
- Contribution à des travaux de recherche sur l'évasion des solutions de sécurité
- Contournement d'EDR/antivirus (Windows Defender, Sophos, Kaspersky)
- Analyse de processus Windows et développement de PoC exploitables dans un contexte Red Team

#### Stage en Détection de Malwares par Deep Learning chez 3D SMART FACTORY Mohammadia, Maroc

Juillet 2024 - Septembre 2024

• Développement d'un système de détection de malware basé sur des modèles LSTM et Transformers avec TensorFlow

#### **PROJETS**

AmroSilencer (en cours) — Générateur de payloads multi-format en C++; contournement Defender; obfuscation et évasion des hooks utilisateur.

Contribution NetExec (nxc) — Fonctionnalité KEYWORDS du module spider\_plus pour détecter des fichiers sensibles sur partages réseau. LogMyBrowser — Outil Red Team C++: persistance, surveillance d'onglets et collecte de credentials.

Outil ayant contourné (au moment des tests) Windows Defender, Sophos et Kaspersky via process hollowing et chiffrement byebyeAV XOR, ciblant le processus non surveillé dllhost.exe

FlexSheller — Générateur polyvalent de shellcodes (MAC/IP/UUID/chiffrement)

### COMPÉTENCES TECHNIQUES

#### Langages de Programmation

Outils

Python (Très bien), C/C++ (Très bien), SQL (Très bien), Bash (Bien) Bloodhound, Netexec, Cobalt Strike, Nmap, Burpsuite, Metasploit, Nessus, SQLMAP, Hashcat

#### Compétences Spécialisées

Langues

Exploitation Active Directory; Évasion de détection (AV/EDR bypass); Français (Niveau avancé); Anglais (Niveau avancé); Arabe (Langue Développement de malware; Tests d'intrusion applicatifs; Campagnes maternelle) de phishing simulées; Rédaction de rapports techniques et exécutifs

## INFORMATIONS COMPLÉMENTAIRES

Qualités

Adaptabilité; Aptitude à résoudre les problèmes; Gestion de la sécurité; Responsabilité; Créativité et innovation Activités parascolaires Organisation et création de CTF, participation active aux compétitions, contribution aux projets techniques du club INSEC de l'ENSIAS