Amro Esseroukh

amroesseroukh012@gmail.com +33 7 45 42 66 54
Paris, France
amroes.github.io @amroes @amro-esseroukh

PROFIL PROFESSIONNEL

Étudiant en 3ème année à ESISAR en cybersécurité, certifié OSEP, OSCP et CRTO. Particulièrement intéressé par la recherche de vulnérabilités, les techniques d'évasion avancées et l'ingénierie inverse.

FORMATIONS

Cycle d'ingénieur — Informatique, Réseaux et Cybersécurité (IRC) **Depuis sept. 2025**
ESISAR Grenoble-INP

Cycle d'ingénieur — Sécurité des Systèmes d'Information (SSI) **2023 - 2025**
École Nationale Supérieure d'Informatique et d'Analyse des Systèmes

Classes préparatoires — MPSI et MP (Mathématiques, Physique, Sciences de l'ingénieur) **2021 - 2023**
CPGE Lycée Moulay Hassan

EXPÉRIENCES PROFESSIONNELLES

Stagiaire en Tests d'Intrusion (Pentest) chez Orange Cyberdéfense **Juin 2025 - Août 2025**
Casablanca, Maroc

- 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 **Juillet 2024 - Septembre 2024**
Mohammadia, Maroc

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

CERTIFICATIONS

OffSec Advanced Evasion Techniques and Breaching Defenses (OSEP) **Juillet 2025 - Août 2025**
OffSec *Obtenu*

OffSec Certified Professional (OSCP) **Août 2024 - Octobre 2024**
OffSec *Obtenu*

Certified Red Team Operator (CRTO) **Décembre 2024 - Janvier 2025**
Zero-Point Security *Obtenu*

PROJETS

AmroSilencer (en cours) — Générateur de payloads C++ multi-format avec techniques d'évasion avancées et contournement des solutions de sécurité.
Contribution NetExec (nxc) — Fonctionnalité KEYWORDS du module spider_plus pour détecter des fichiers sensibles sur partages réseau.
LogMyBrowser — Outil avancé de hooking pour surveiller les interactions du navigateur sur des pages sensibles, conçu pour aider les professionnels de la sécurité et les équipes rouges à découvrir des informations sensibles, des identifiants aux informations de cartes de crédit.
byebyeAV — Outil avancé d'évasion d'antivirus utilisant le process hollowing sur dllhost.exe et le chiffrement XOR pour contourner la détection. A contourné les dernières versions de Kaspersky, Sophos et Windows Defender.
FlexSheller — Générateur de shellcodes avec support multi-protocoles et chiffrement intégré.

COMPÉTENCES TECHNIQUES

Langages de Programmation
Python (Très bien), C/C++ (Très bien), SQL (Très bien), Bash (Bien)

Compétences Spécialisées
Exploitation Active Directory; Évasion de détection (AV/EDR bypass); Développement de malware; Tests d'intrusion applicatifs; Campagnes de phishing simulées; Rédaction de rapports techniques et exécutifs

Outils
Bloodhound, Netexec, Cobalt Strike, Nmap, Burpsuite, Metasploit, Nessus, SQLMAP, Hashcat

Langues
Français (Niveau avancé); Anglais (Niveau avancé); Arabe (Langue maternelle)

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