MOHAMED RACHIDI

Mobile +33 6 1281 0244 **Email** mohamedr.job@outlook.com

01 PROFIL

Professionnel de la cyber sécurité offensive avec 5 ans d'expérience progressive dans les domaines privé et public. Capable de mener des tests d'intrusion et des opérations RedTeam dans différents secteurs et environnements. Apprécié des clients et consciencieux sur les livrables.

02 QUALIFICATIONS

- Capacité à collaborer et à travailler efficacement dans une équipe ;
- Capacité à communiquer des situations complexes ;
- Capacité à rédiger des rapports et des documentations techniques claires ;
- Recherche approfondie pour trouver des recommandations et des stratégies efficaces afin de réduire les risques et améliorer la posture de sécurité ;
- Intégrité, éthique et respect de la confidentialité ;
- Maîtrise des outils de recherche et de scans de vulnérabilités ;
- >100 audits de sécurité Interne/Externe, Infrastructure, Applications Web/API, Clients lourds, Bases de données, postes de travail ;
- Plus de 100 jours dédiés à la recherche et développement de l'outillage Red Team ;
- Plusieurs exercices Red Team sur des clients matures ;

03 BACKGROUND

sept 2021 —

Consultant en sécurité informatique @[NDA]

Paris (FR)

- Réalisation des audits/contre-audit de bout en bout (réunion de lancement, coordination et préparation, audit technique, suivi et reporting, et réunion de restitution) : WebApp/API, évaluation de l'impact métier sur l'entreprise, classement par rapport au TOP 10 OWASP ;
- Réalisation d'un audit redteam afin d'améliorer la posture globale de l'entreprise à travers la rédaction de best practices : Collecte d'informations sur l'entreprise/le personnel/techniques, Spray de mot de passe, compromission de comptes VPN, Mauvaise configuration RDP, LPE local, mauvaise configuration hyperviseur backup contrôleur du domaine, impact métier) ;
- Cartographie du périmètre externe, scan de vulnérabilités, puis tests d'intrusion sélectifs ;
- Gestion des audits réalisés par des prestataires de services : sélection des prestataires selon une matrice, communication entre les prestataires et les équipes de développement/chefs de projet, vérification technique des correctifs avec les développeurs

févr 2019 — mai 2021

Consultant en sécurité informatique@Orange Cyberdefense

Paris (FR)

- Missions dans tout type de secteurs (bancaire, assurances, luxe, technologie, logistique etc.) ;

- Tests d'intrusion/Contre audits applicatifs internes, externes, en boite noire ou boite grise (nmap, metasploit, BurpSuite, OWASP, WebShells) ;
- Audit de poste : vérification de la bonne implémentation du durcissement (conformité VPN, patches, configuration bios, …), élévation des privilèges, audits clients lourds installés sur l'OS, exfiltration de données (DLP), contournement EDR/AV/Applocker) ;
- Tests d'intrusion Interne Active Directory (BloodHound, PingCastle, Masscan, CrackMapExec, Responder, Attaques Kerberoast, configuration des ACL, Credential Dumping : LSA, LSASS, SAM, Privilege Escalation) ;
- Scan de ports et de vulnérabilités (Nessus, Qualys), puis tests d'intrusion sélectifs sur le périmètre Internet externe de plusieurs grands clients (environ 1000 à 5000 IP au départ) ;
- Réalisation de missions complexes dans des environnements sensibles en production (bancaire, santé, aérospatial) : Windows Serveur et AD, Linux Red Hat, Solaris, Debian, Oracle, MSSQL et MySQL ;
- Audit sur des environnements de guichets bancaire : Jackpotting d'un GAB via le réseau (extraction d'argent), contrôle total sur le GAB via une RCE ;
- Réalisation de plusieurs missions red-team de bout en bout (CobaltStrike, MITRE ATT&CK) : Simulation de la fraude, intelligence économique, et du ransomware ;
- Membre actif de la R&D spécialisé OSINT, évasion AV/EDR, vecteurs d'infection, persistances :
  - Générateur de pages web de delivery pour les tentatives de spearphishing qui distribuent (de manière sélective) un artefact via de l'HTML smuggling,
  - Générateur de projets compilables d'artefacts permettant de loader un shellcode via direct syscalls + bypass de sandbox, avec ou sans injection de browser (bypass Windows Defender, Kaspersky, Symantec, Cynet, Trend Micro)
  - Générateur de maldocs. Execution différée (COM hijacking), ne spawn pas de sous-process Office, anti-sandboxing modulaire, VBA Purging, tracking HTTP/DNS
  - Collecte automatique OSINT : Technique (IP, domaines et sous domaines, périmètre Cloud,…) humain avec catégorisation des personnalités à des fins de Social Engineering (Facebook, Linkedin, …)

04 STAGES

févr 2018 — juil 2018

Pentester Junior @Orange Cyberdefense

Paris (FR)

- Tests d'intrusion/Contre audits applicatifs internes, externes, en boite noire ou boite grise ;
- État de l'art sur les différents frameworks de Command&Control C2 et développement d'un canal de communication DNS pour le contrôle et l'exfiltration ;
- Tests de cloisonnement, relevé de configuration, audit de code source ;

févr 2017 — mai 2017

Threat Analyst Junior @Ministère de la communication

Rabat (MA)

- Analyse des emails de Phishing remontés aux équipes de sécurité ;
- Scans de vulnérabilités ponctuels et récurrents (Qualys) ;

05 ÉDUCATION

sept 2017 — juin 2018

Université de technologie de Troyes

Troyes (FR)

Master (Sécurité des Systèmes d'Information)

sept 2014 — juin 2017

Institut National des Postes et Télécommunications

Rabat (MA)

Diplôme d'ingénieur (cybersécurité et confiance numérique)

sept 2012 — juin 2014

Classes préparatoires aux grandes écoles (MP)

Casablanca (MA)

06 LANGUES

Arabe

Anglais

Français

07 CERTIFICATIONS

nov 2018

Offensive Security Certified Expert (OSCE)

OS-CTP-014641

janv 2017

Offensive Security Certified Professional (OSCP)

OS-101-06640

mai 2016

Offensive Security Wireless Professional (OSWP)

OS-BWA-03035