



Clément BOUDER  
Passionné de cybersécurité offensive

📍 112 Rue du chemin vert,  
75011 Paris

📅 Né le 12/12/1995

☎ 06 58 01 42 07

✉ clement.bouder@outlook.com

🔗 <https://clement-bouder.fr>

👤 Permis B

## A Langues

### Anglais

Niveau professionnel

### Italien

Notions

## 📁 Compétences

### Sécurité informatique

Kali Linux, Metasploit, Nmap,  
Wireshark, Beef, Radare2

### Développement d'applications

C++, C#, C, Java, Python

### Gestion des systèmes d'exploitation

Debian, Ubuntu, CentOS

### Développement Web

HTML5, CSS, JavaScript, PHP,  
SQL

## 👥 Centres d'intérêt

### Hacking éthique

- Conférences (AMUSec, GreHack 2018, SecSea, Spying Challenge 2019, leHack 2019)
- CTF (pseudo CLeBeR) : Hack The Box (600ème Global Ranking) & Root-Me (4085ème sur 170 844)

**Musculation** Pratique depuis plus  
de 4 ans.

**VTT** Pratique depuis plus de 12  
ans.

**Aéromodélisme / Airsoft / Tir  
Sportif** Pratique pendant  
4 ans.

## Diplômes et Formations

De septembre 2016 à  
septembre 2019 **Licence & Master Méthodes informatiques appliquées à la gestion des  
entreprises (MIAGE)**  
[Faculté d'Economie Appliquée, Aix-Marseille Université](#) Marseille, France  
Parcours Ingénierie des données et décision (I2D)

De 2014 à 2016 **Diplôme Universitaire de Technologie Informatique**  
[Institut Universitaire de Technologie Informatique, Aix-Marseille  
Université](#) Aix-en-Provence, France

## Expériences professionnelles

Depuis novembre  
2020 **Réserviste - Sous-lieutenant**  
[Commandement Cyberdéfense](#) Paris, France  
Réserviste au Commandement de la Cyberdéfense affecté à la section  
Centre d'audits de la sécurité des systèmes d'information (CASSI), j'ai pu  
participer au Bug Bounty 2021 pour le Ministère des Armées.

Depuis novembre  
2019 **Auditeur Pentester**  
[Wavestone](#) Paris, France  
J'effectue des tests d'intrusion sur plusieurs types de systèmes dans tous  
les domaines d'activité. Je suis également affecté à des missions de type  
simulation de Phishing. Je réalise également des cartographies de réseau  
pour des missions de simulation de Red Team.

De septembre 2017 à  
septembre 2019 **Ingénieur en étude et développement en alternance**  
[SOPRA STERIA GROUP](#) Six-Fours-les-Plages, France  
Développement d'un logiciel destiné à représenter la cuve d'un réacteur  
nucléaire en Python. Sécurisation de systèmes CentOS.  
Intégration d'un SIEM (Splunk) au sein du SoC d'Airbus Helicopters et  
réalisation de tests d'intrusion.

D'avril 2017 à juin  
2017 **Développement d'application, stage**  
[SOPRA STERIA GROUP](#) Six-Fours-les-Plages, France  
Développement d'un simulateur pour les centrales nucléaires en C++ et  
C#. Utilisation de MySQL pour la base de données.

D'avril 2016 à juin  
2016 **Développement d'application web, stage**  
[SOPRA STERIA GROUP](#) Aix-en-Provence, France  
Développement d'une application web, utilisation d'AngularJS, NodeJS et  
du framework Electron pour Airbus Helicopters.

## Projets réalisés

**HiddenXploit packer C++** : Développement de mon propre packer (C++) pour injecter du code  
compilé directement en mémoire afin d'outrepasser l'analyse statique/dynamique des antivirus.

**Reverse Shell HTTP** : Développement d'un reverse shell basé sur un protocole HTTP pour  
récupérer les commandes au sein du C&C.

**Rainbow 2014 contrôle parental** : Développement d'un contrôle parental (Rainbow 2014 Contrôle  
Parental) en VisualBasic.NET.

**Blog personnel** : Création de mon blog personnel pour rédiger quelques billets de sécurité  
(<https://www.clement-bouder.fr/blog>)

**Campagne de Spear Phishing** : Mail contenant un faux sondage au format Word exécutant une  
macro téléchargeant un Reverse Shell en C++.

**USB piégée** : Création de mon Rubber Ducky à l'aide d'une carte Digispark ATtiny85.

**BugBounty** : Découverte d'une vulnérabilité de CVSS 5.4 sur le site d'une entreprise ferroviaire  
publique française.

**Découverte CVE** : CVE-2021-28674 publiée en juin 2021 sur le logiciel Orion SolarWinds.

## Certifications

- ITIL Foundation (2011) Information Technology Infrastructure Library
- Prince 2