



# Chadi Manglé

Passionné par l'informatique depuis l'enfance, je suis actuellement en première année de BUT en Réseaux et Télécommunications et à la recherche d'un contrat d'apprentissage de deux ans en Réseaux et Cybersécurité. Rythme de l'alternance deux semaines en entreprise deux semaines à l'université dès la rentrée prochaine.



chadimangled@gmail.com



+33 7 77 88 77 24



<https://chadi-mangle.github.io/Portfolio/>



92270, Bois-Colombes, France

## CURSUS SCOLAIRE

- **IUT de Villetaneuse Paris 13**  
Actuellement en première année en **Réseaux et Télécommunications**.  
Vice président et membre de l'Association Loi 1901 « ESPLab »  
Activités d'électronique, de sécurité informatique et de programmation
- **Lycée Auguste Renoir de 2019-2022**  
Obtention du Bac général spécialité **Mathématiques/Numérique et Sciences de l'Informatique** avec mention.

## LANGUES

- Anglais: B2
- Espagnol: B1

## LOISIRS

- Judo
- Montage vidéo
- Théâtre
- Modélisation 3D
- Echecs
- Graphisme

## EXPERIENCES

### Programmation

- Réalisation de backdoor, perceptron, génération de pages web en fonction de base de données et algorithme de reconnaissance de langues en **Python**.
- Réalisation d'un planificateur automatique des tâches logistiques sur Google Cloud en **JavaScript** pour l'entreprise Solvarea.
- Réalisation d'un microprocesseur réunissant la programmation d'une **carte ESP32** en **C++** avec de la génération HTML pour l'affichage dynamique des données.
- Création d'un script **Bash** permettant de générer une nouvelle commande à un terminal **Linux** pour ajouter la dernière commande exécutée dans un fichier texte.

### Réseaux et sécurité informatique

- Mise en place de serveurs **Apache**, **DHCP**, et **DNS**.
- Connaissance du modèle **OSI** et **TCP** ainsi que des protocoles **TCP/IP**, **SSH**, **DNS**, **ARP**, et **DHCP**.
- Mise en place de pare-feu avec **Iptables**.
- Connaissance des topologies logiques et physiques des réseaux.
- Mise en place de réseaux **VLANs** et de baie de brassage et **DMZ**.
- Connaissance de la fragmentation IP et réalisation d'attaques **Teardrop**.
- Utilisation du logiciel **Oracle VM VirtualBox**
- Création de réseaux virtuels avec le logiciel **Marionnet** et **GNS3**.
- Création de **pipelines** simple avec **GitLab** et **AWS**.

## OUTILS

