**Environnement Technique**

Hajar Benkhadra

5/5/2025

Cadre : stage

On présente dans ce compte rendu un environnement technique pour coder et tester une API RESTFUL et les étapes de pré-réalisation.

**I)Séparation des environnements :**

Dualboot :

Le dualboot permet d’installer deux systèmes d’exploitation sur une même machine.  
Pour le mettre en place, il faut :

* Une **clé USB bootable** contenant l’image ISO du système à installer (via des outils comme **Rufus** ou **Ventoy**) ;
* Un **disque dur externe (SSD ou HDD)** pour sauvegarder les fichiers importants, par mesure de sécurité ;
* Une **documentation complète** jointe au dossier, expliquant les étapes nécessaires.

**Les hyperviseurs** :

Il est également possible d’utiliser des hyperviseurs tels que **VirtualBox**, **VMware**, ou encore des solutions plus avancées comme **Proxmox**.  
La documentation fournie inclut également des alternatives pour l’installation des systèmes via des machines virtuelles.

**II)L’ENVIRONNEMENT TECHNIQUE LINUX :**

. Linux pour la cybersécurité

Linux est reconnu pour sa compatibilité avec les besoins en cybersécurité, notamment dans les domaines suivants :

* Pentest
* Red team / Blue team
* Ethical hacking
* Défense offensive et défensive

Les distributions recommandées :

* Kali Linux (spécialisée en pentest)
* Purple Kali (orientée blue team)
* Arch Linux (flexibilité, contrôle total pour les utilisateurs expérimentés)

2. Linux pour le développement

Selon le niveau de compétence et les besoins, on peut choisir :

* Ubuntu / Fedora : très utilisés par les développeurs (stabilité, support communautaire)
* Manjaro : bon compromis pour des développeurs intermédiaires
* Arch Linux : pour les utilisateurs avancés grâce à sa structure minimaliste et hautement personnalisable

**III)Propositions :**

On combine tous ses données et on propose les environnements (soit en dualboot ou VM) pour une réflexion dev/cyberséc :

* *Pour cybersécurité : Arch linux, kali*
* *Pour développement : Windows, manjaro*
* *Une combinaison dev/cybersec: Windows/Arch ou Windows/kali*

**IV)Outils nécessaires pour coder et tester une API RESTFUL :**

***Sur Windows****:*

1. **Développement**

*Node.js, Express.js, MySQL, Dotenv*

*our stocker le mot de passe*

1. **Sécurité**

*Helmet,express-rate-limit,cors,express validator,JWT,Bcrypt*

1. **Tests**

*Postman GUI,cURL,Morgan,Nodemon,Jest/supertest*

***sur Linux:***

*La différence entre coder sur Windows et sur Linux est dans les outils par ici les équivalents de chacun outils utilisé dans Windows au système de Linux:*

* VScode=>Code-css / Neovim
* Node.js=>Deno
* Express=>Fastify
* MySQL=>MariaDB/CockroachDB
* Postman=>Insomnia
* Morgan=>journactl (cmd)/ Winston
* Nodemon=>PM2
* Git=>gh(cmd)
* Dotenv=>.env+diren

**outils supplémentaire :**

* OpenSSl: pour le hashage et les certifications
* GnuPG:pour le chiffrement
* RestClient : pour les API Rest