

# Avant propos

**Editeur de code préconisé pour l'UE et les TP à venir :  
Visual Studio ou Visual Studio Code**

- <https://visualstudio.microsoft.com/fr/vs/getting-started/>
  - Choisir la version Community (vs\_community.exe)
- <https://code.visualstudio.com/download>
- <https://docs.microsoft.com/fr-fr/visualstudio/install/create-an-offline-installation-of-visual-studio>

Pour visual studio

- ☐ Ouvrir une invite de commande en tant qu'administrateur
- ☐ Se positionner dans le répertoire de récupération du fichier vs\_community.exe
- ☐ Lancer la commande suivante afin créer une source locale d'installation
- ☐ `vs_community.exe --layout c:\vslayout --lang fr-FR`

*c:\vslayout étant le répertoire de récupération*

# Avant propos – Mise en place par l'auditeur

## VM Windows

Pour réaliser les certains TP, vous aurez besoin de Windows.

Vous pouvez récupérer une image de Windows conseillée par l'intervenant

Dernière version de Windows avec logiciels complémentaires

- <https://developer.microsoft.com/fr-fr/windows/downloads/virtual-machines/>

Windows 10 sans logiciels complémentaires :

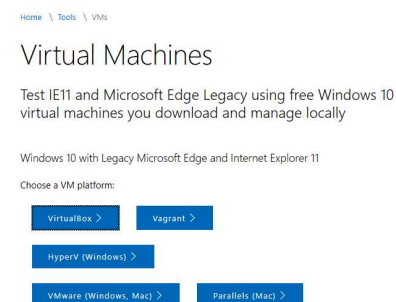
- <https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-10-enterprise>

Windows 11 sans logiciels complémentaires :

<https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-11-enterprise>

Vous pouvez récupérer VirtualBox + Extension Pack

- <https://www.virtualbox.org/wiki/Downloads>



SEC102

Menaces informatiques et codes malveillants : analyse et lutte

le cnam  
CyberSécurité

# A - Avant-propos – Logiciels à mettre sur la VM

- Téléchargez depuis votre VM
  - SysinternalsSuite <https://download.sysinternals.com/files/SysinternalsSuite.zip>
  - CFF Explorer <https://ntcore.com/files/ExplorerSuite.exe>
  - PE Studio <https://www.winitor.com/download>
  - Volatility (version 2.6 pour Windows 10) <https://www.volatilityfoundation.org/releases>
  - Volatility Workbench : <https://www.osforensics.com/tools/volatility-workbench.html>