
# Lab Setup

PRESENTATION BY:
Nuno Filipe Freitas Pedrosa ( PDMFC )

# Laptop requirements for Winter School 2026

Most sessions will use a VM image to run the examples and exercises.
These require a fair ammount of resources (memory, storage, CPU).

So laptop should have at least:

- **16GB RAM**,
- **4 cores** and
- **over 100GB** of free storage space.

**Virtualization technology** (commonly referred to as **Intel VT-x or AMD-V**) must be **enabled in the system BIOS settings.** This may require intervention of your IT department to enable them.

# Software requirements

These are some general requirements:

- Virtual Machine with Kali Linux (https://www.kali.org/get-kali/#kali-installer-images):
  - 4–8 GB RAM
  - 2 or more CPU cores
  - 40 GB or more disk space (with dynamic allocation)
  - 3D acceleration enabled

- Host or Virtual machine:
  - Ollama - https://ollama.com/download
  - Python - https://www.python.org/downloads/
  - curl - https://curl.se/download.html
  - Garak - https://docs.garak.ai/garak/llm-scanning-basics/setting-up/installing-garak

# Handling models

Download some small LLMs (llama2,  llama3 and mistral) with ollama (each model is about 4-5GB large):

```
ollama pull llama2
ollama pull mistral
# optional if you don’t have storage space
ollama pull llama3
```

Check if the models are there by typing

```
ollama list
```

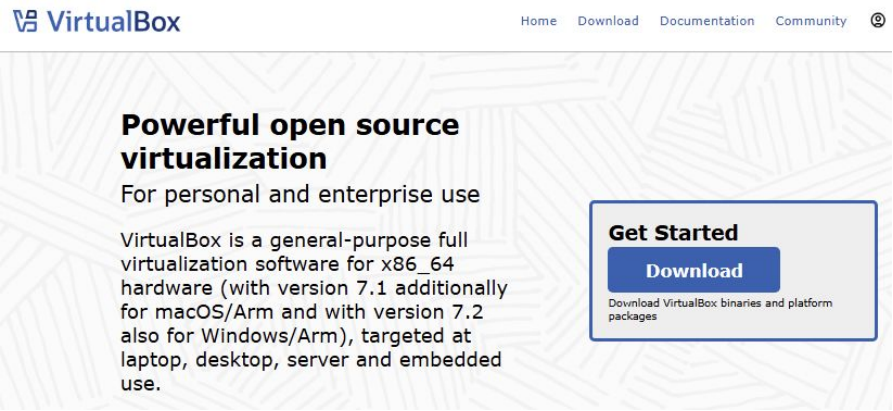
Run a model with:

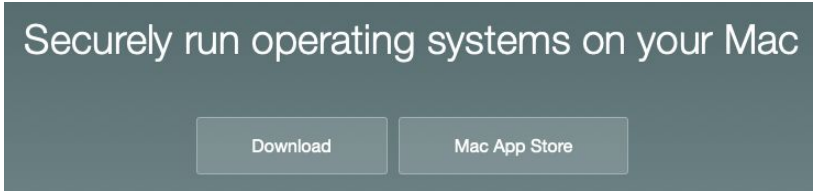
```
ollama run llama2 "<Some text>"
ollama run llama2 "What is a pastel de Belém?"
```

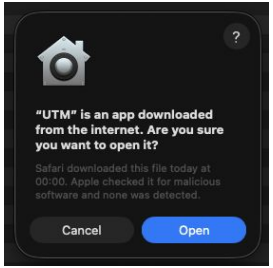
# Virtual Machines

On ARM: UTM https://mac.getutm.app

On x86: https://www.virtualbox.org



# Troubleshooting

Troubleshooting:

- In Windows, VirtualBox does not start, complaining about mismatched signatures.
  - VirtualBox requires that HyperV is disabled. If it's not, it can give some unrelated or "strange" errors.
  - To find whether Hyper-V is enabled, run in CMD:
    ```
    systeminfo | findstr /i "hyper"
    ```
  - If it shows that Hyper-V / WSL is active, you need to disable it and reboot the system. To do this, run in CMD:
    ```
    bcdedit /set hypervisorlaunchtype off
    ```

Reboot the system.

# Feedback survey

https://admin.cybersecpro-project.eu/evalsurvey/viewpublicsurvey/id/63