GNS3 Simulator

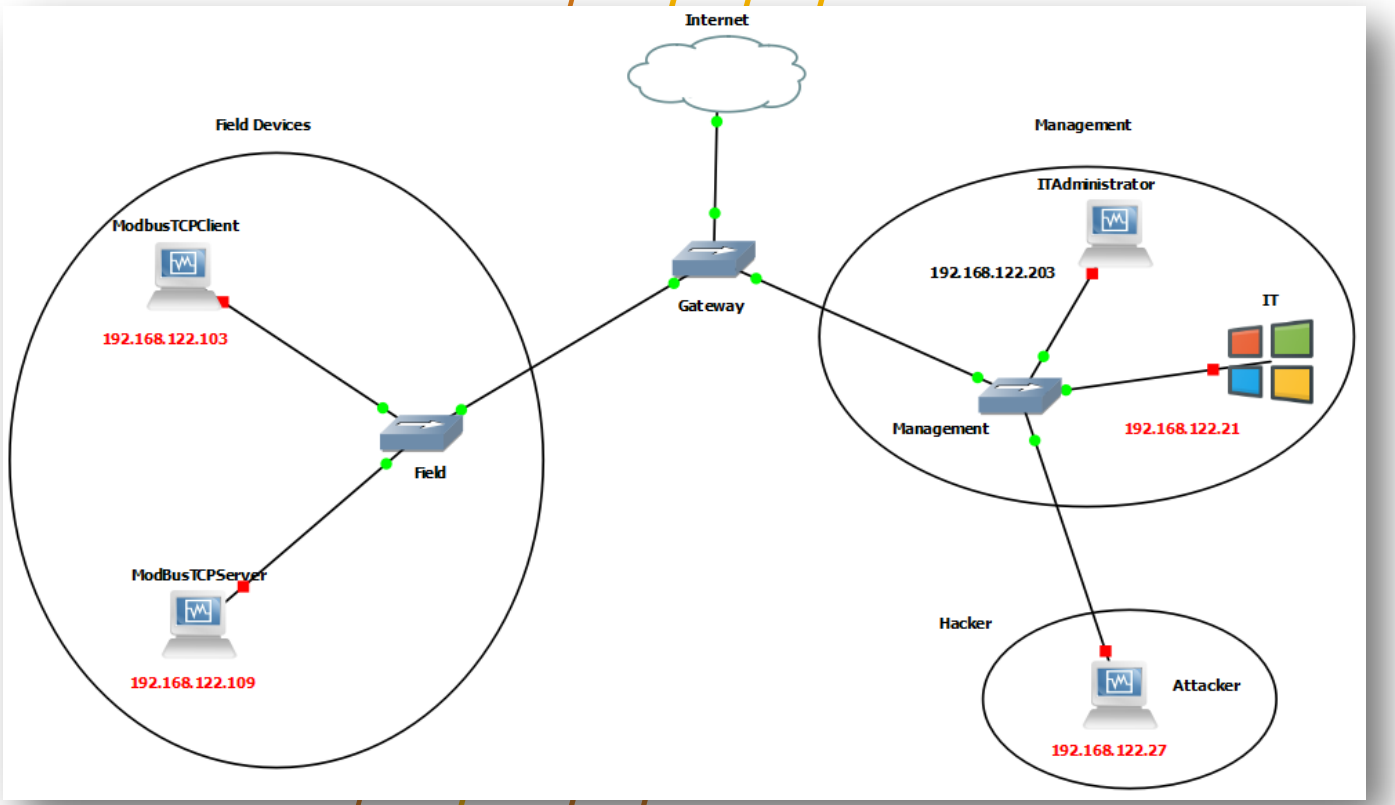
GNS3 Simulator

- GNS3, is open-source and free software.
- It allows network engineers to virtualize real hardware devices.
- GNS3 consists of two main software components:
  - the **GNS3-all-in-one software** (**GUI**) and
  - the **GNS3** virtual machine (**VM**).
- The **GNS3-all-in-one software** (**GUI**) serves as the client interface, installed on local PCs (Windows, MAC, Linux) for creating network topologies.
- The local GNS3 server runs on the same PC as the GUI, along with additional processes like Dynamips.
- The **GNS3 VM** (recommended) can be run locally using virtualization software (e.g., VMware Workstation, Virtualbox) or remotely on a server (e.g., VMware ESXi, cloud).
- GNS3 allows us to create a network topology and an environment for an ideal platform for simulating victims and attackers' machines.

Getting Started with GNS3 | GNS3 Documentation

Why GNS3?

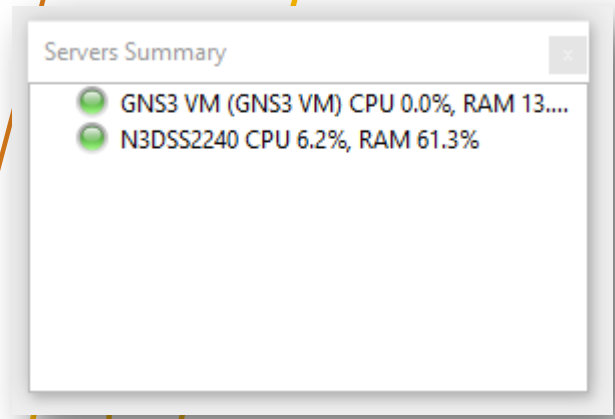
- GNS3 facilitates the building of a complete lab environment by integrating multiple VMs (installed individually).
- This will help create a fully isolated environment consisting of multiple VMs with victim machines and an attacker, allowing you to perform your practical tasks within this course in a safer way.
- Here is an example of how the virtual lab could be designed on GNS3.

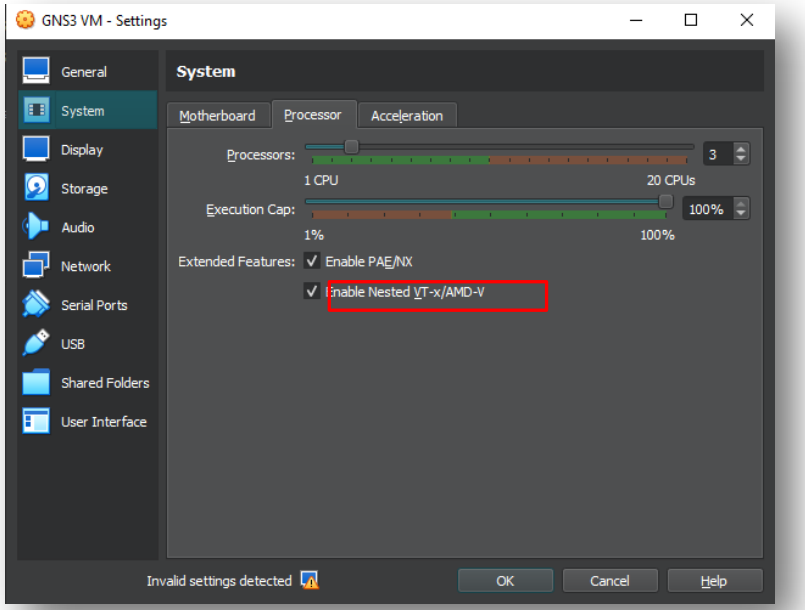


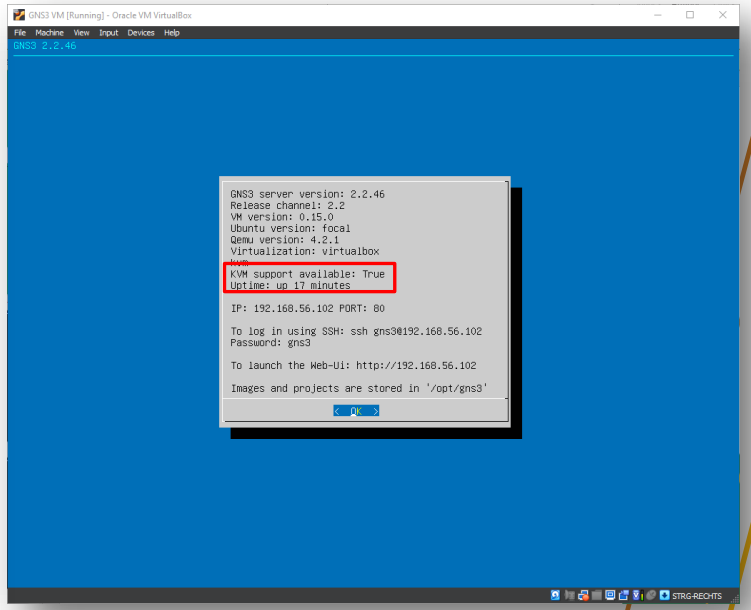
Targeting any external target not within this proposed virtual lab environment is strictly forbidden, and you are solely responsible for any consequences.

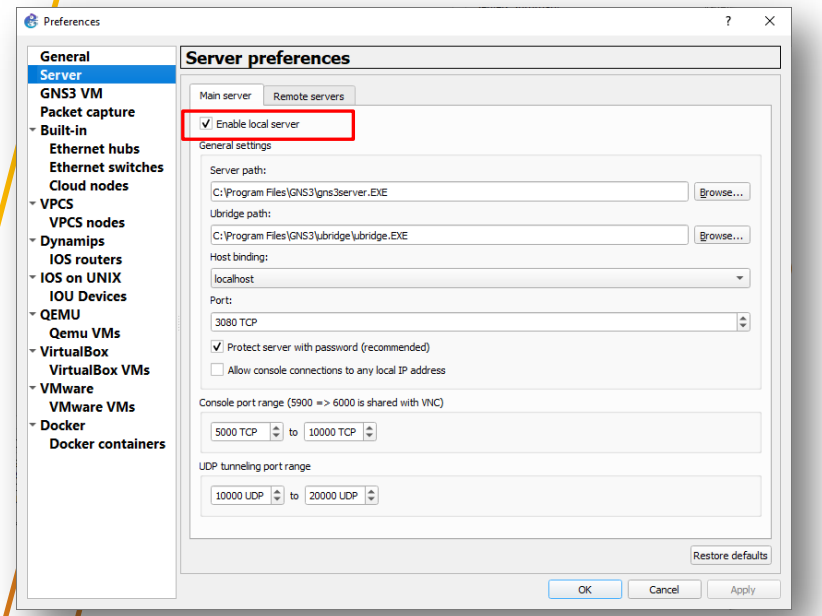
Installing GNS3

- Downlaod GNS3 from the official website: Software | GNS3, and then install it.
- **Download and install GNS3 VM based on your preferred VM: Software | GNS3**









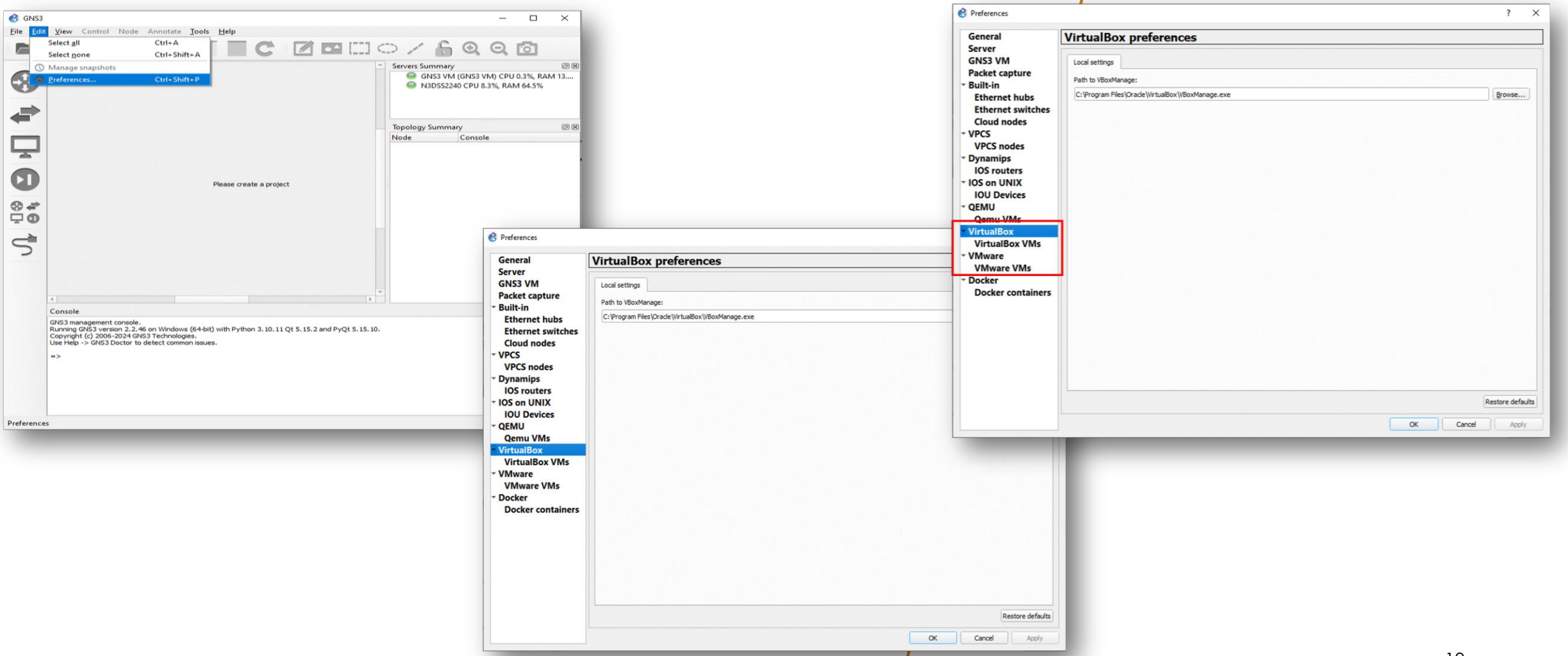
Kali Linux – Attacker and Friend

- Kali is the most advanced Penetration Testing Linux Distribution.
- Kali Linux is an open-source, Debian-based Linux distribution designed for various security tasks, including penetration testing, security research, computer forensics, and reverse engineering.
- **Download** and install the Kali Linux as a normal VM on your PC.
- Kali Linux will play a dual role in our virtual lab setup: one instance will serve as the **attacker**, simulating real-world threats, while the other, referred to as my "**admin Linux friend**," will act as a defense hub for **administrative tasks**.

Victim Machine

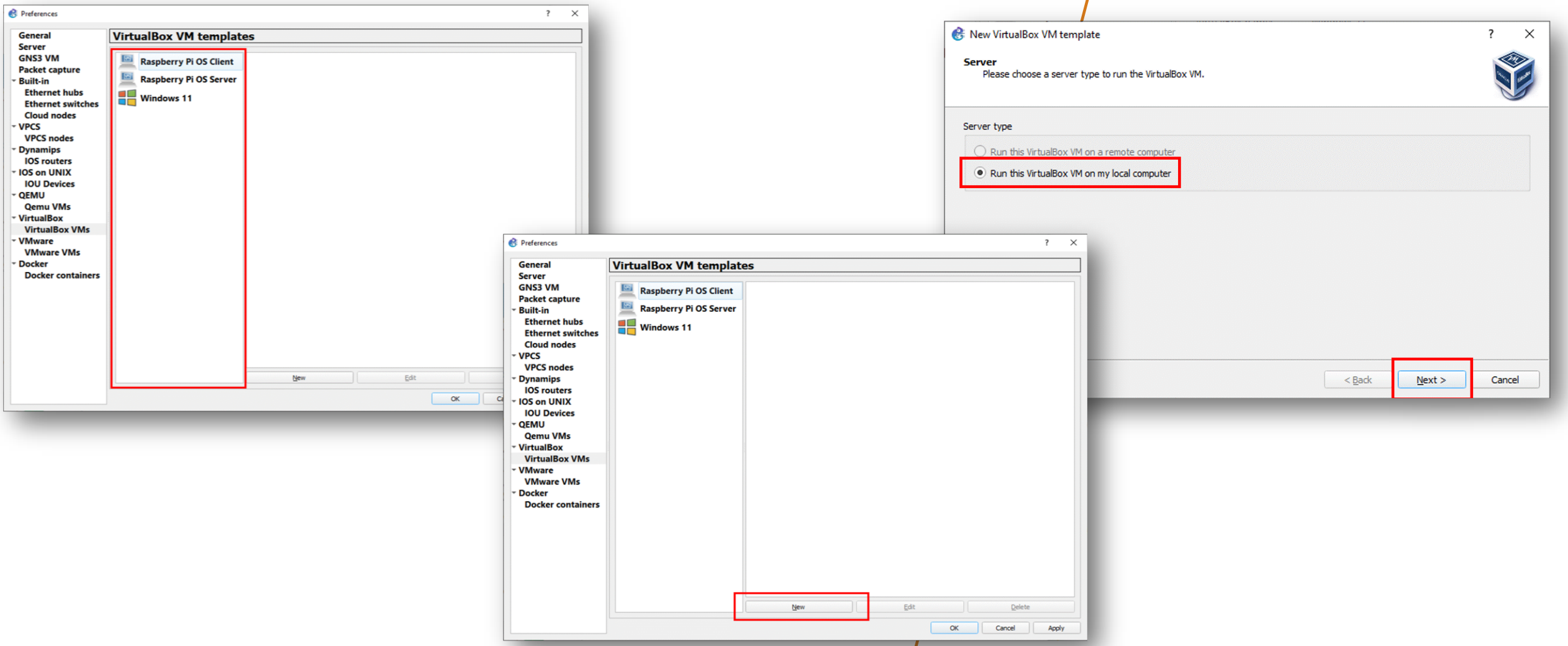
- Configure one virtual machine as the victim device in our dynamic lab environment.
- For this task, you have the flexibility to choose any Linux distribution you prefer.
- However, for a streamlined experience, we recommend installing the Raspberry Pi Desktop on your computer.
- The ISO image can be conveniently downloaded from **HERE**.

Integrating VMs to GNS3



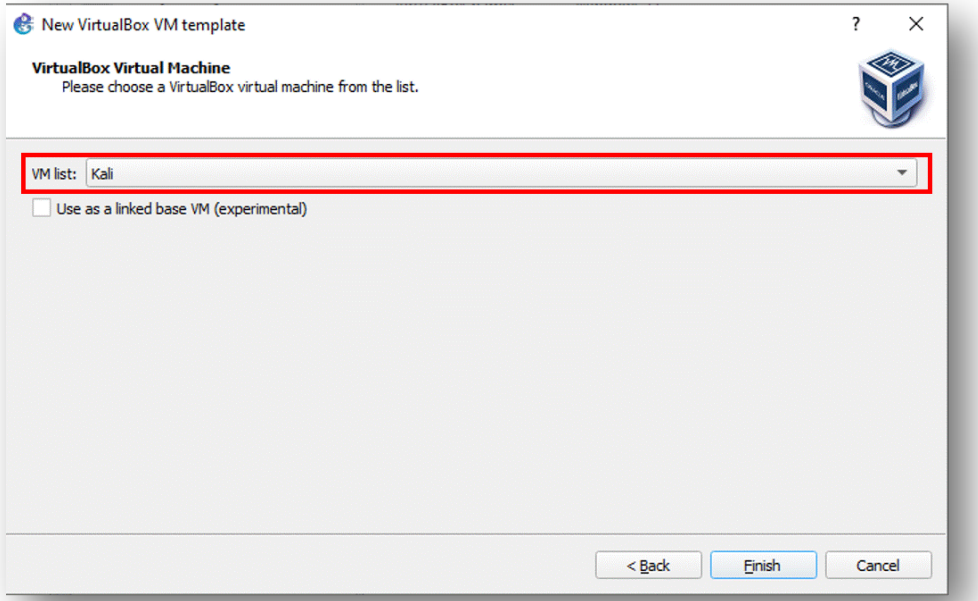
- Do the same for any VM you want to integrate with GNS3

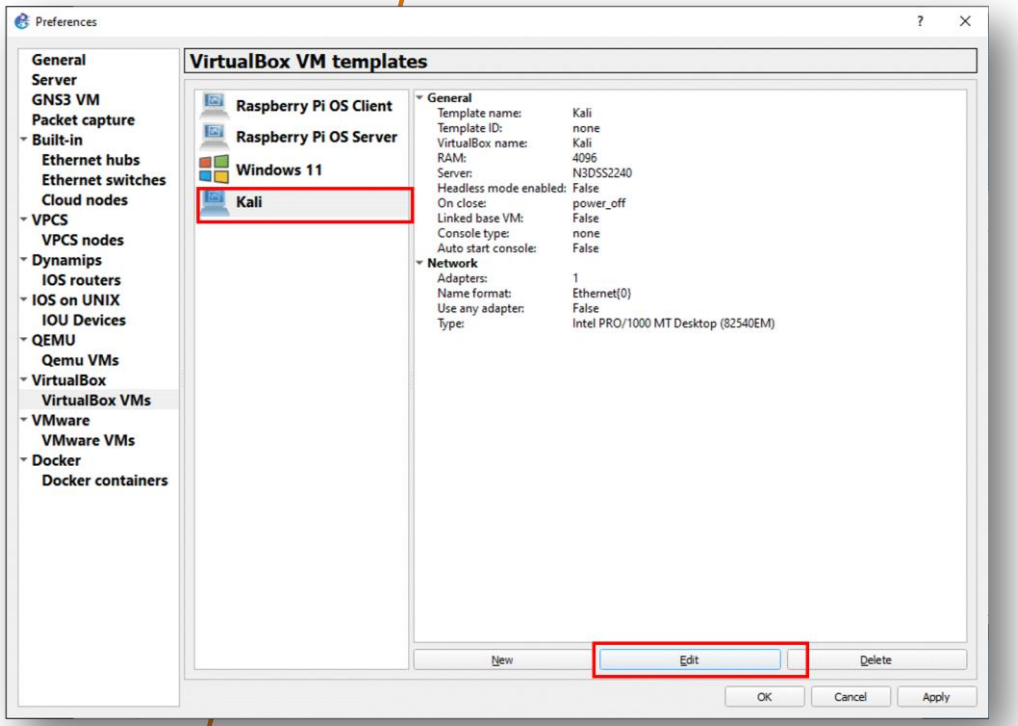
Integrating VMs to GNS3



- Do the same for any VM you want to integrate with GNS3

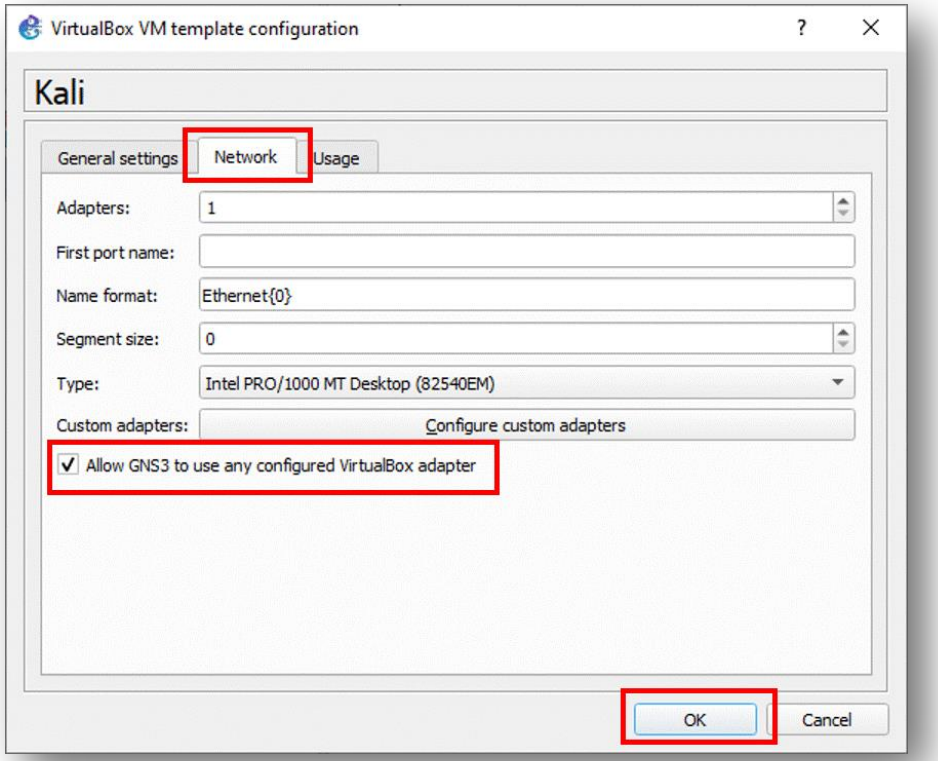
Integrating VMs to GNS3

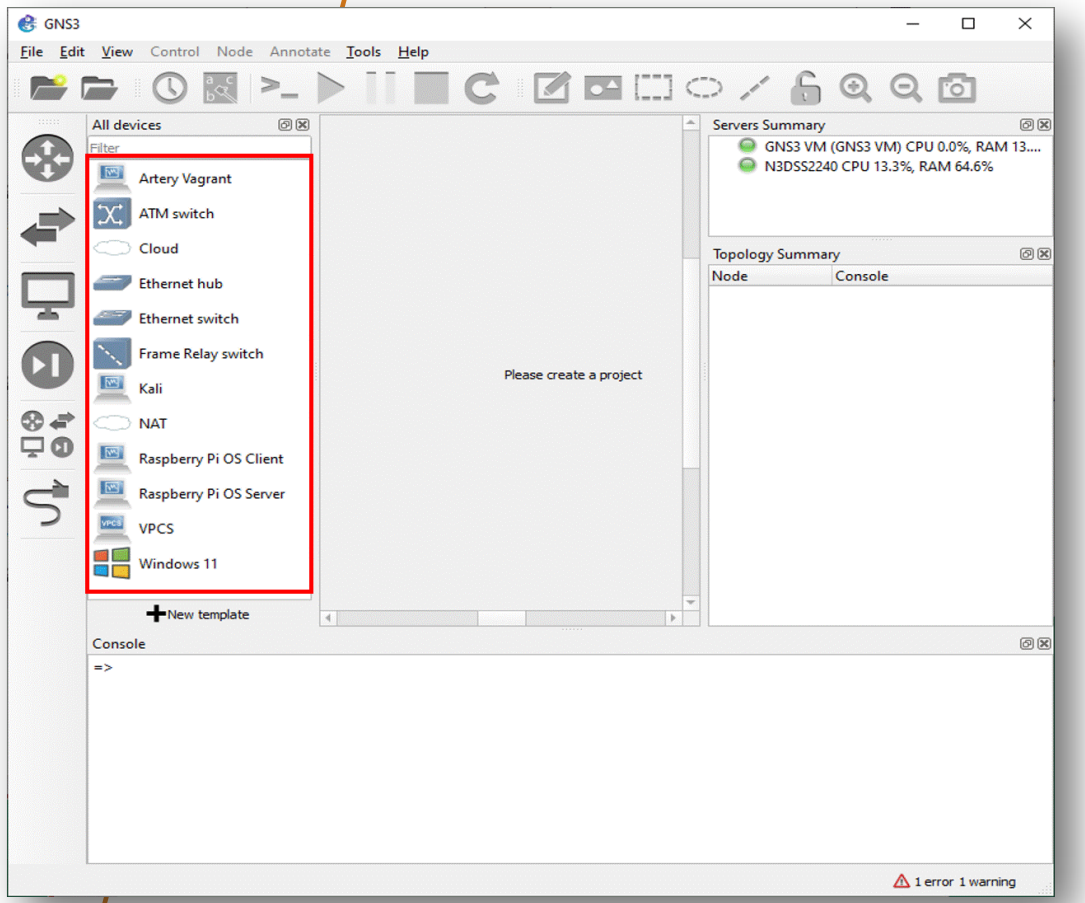




- Do the same for any VM you want to integrate with GNS3

Integrating VMs to GNS3





- Do the same for any VM you want to integrate with GNS3