Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

GNS3 Simulator

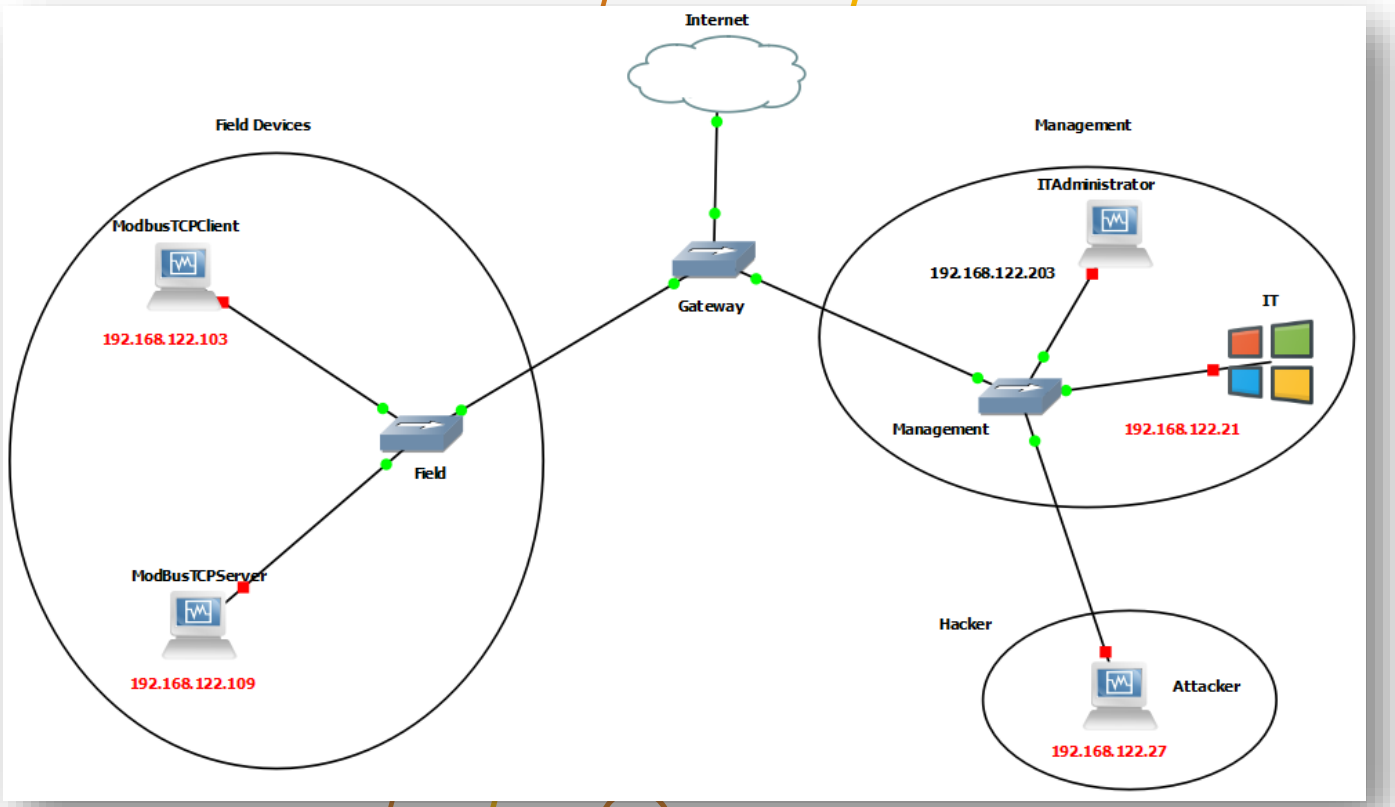
GNS3 Simulator

- 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?

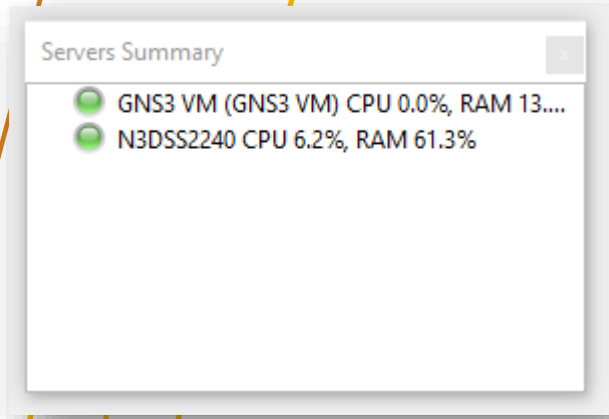
- GNS3 facilitates the building of a complete lab environment by integrating multiple VMs (installed individually).
- This will help create a fully isolated environment consisting of multiple VMs with victim machines and an attacker, allowing you to perform your practical tasks within this course in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

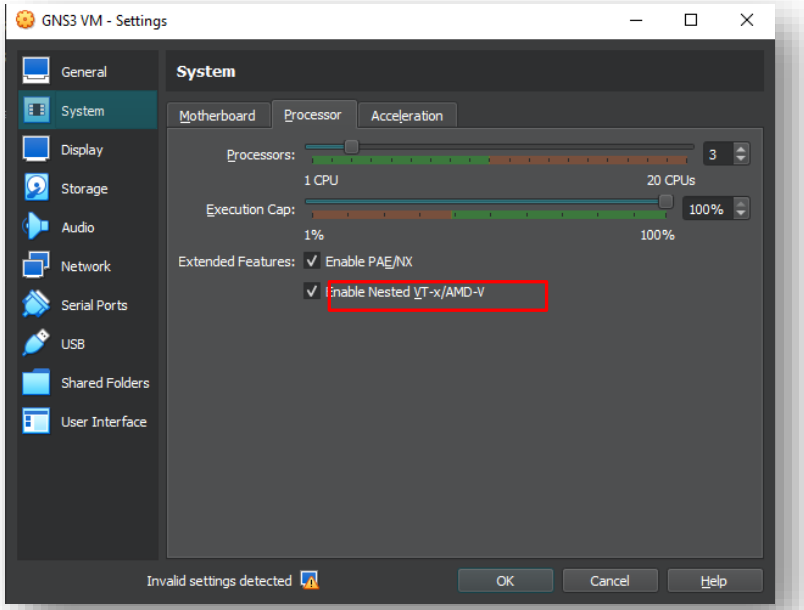


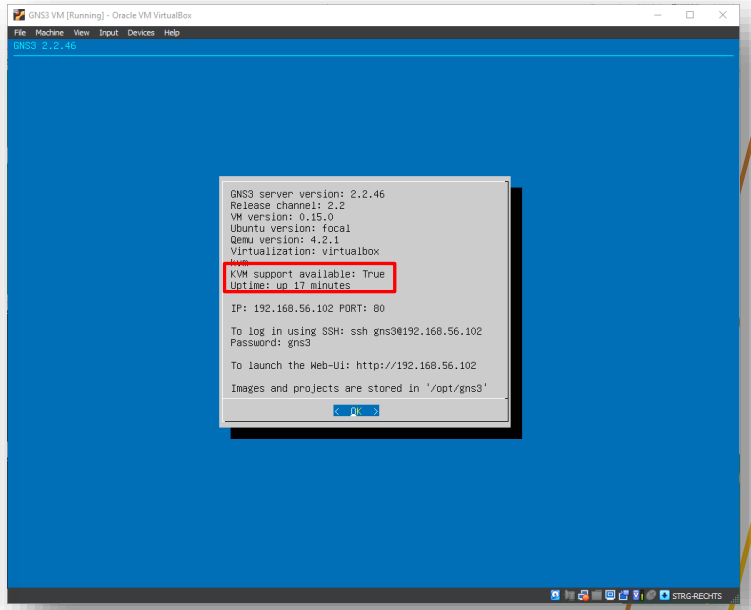
Targeting any external target not within this proposed virtual lab environment is strictly forbidden, and you are solely responsible for any consequences.

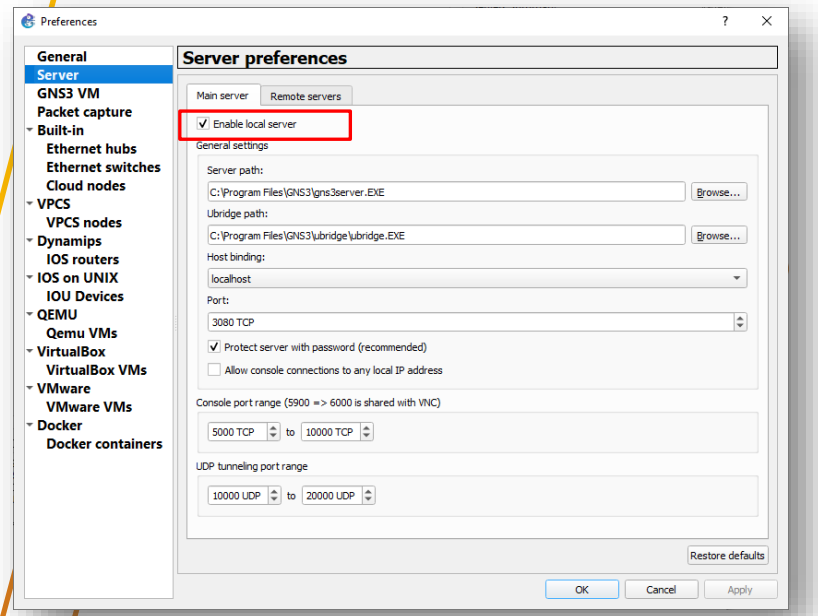
Installing GNS3

- 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

- It is the most advanced Penetration Testing Linux Distribution.

- Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics, and Reverse Engineering.

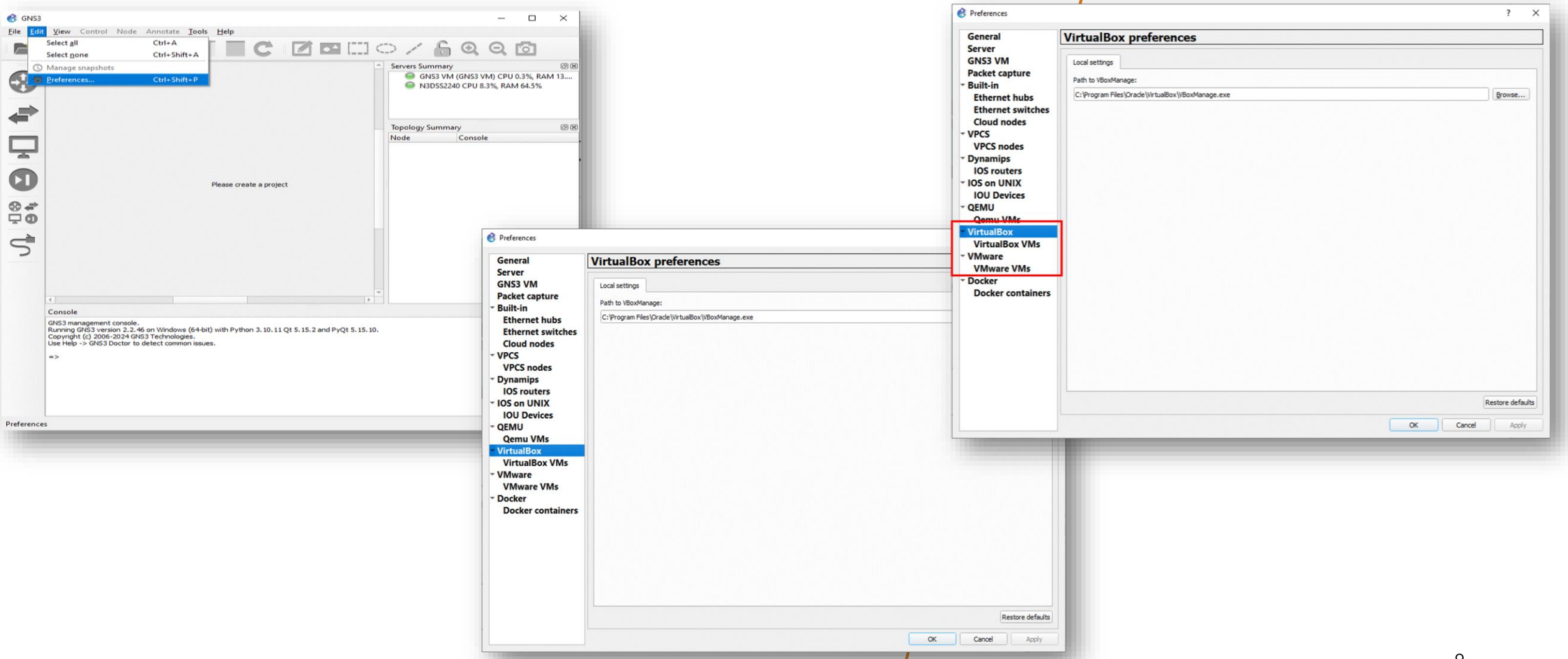
- Download and install the Kali Linux as a normal VM on your PC.

- I will discuss later how to integrate it with GNS3

Client/Server/IT – Victim Machines

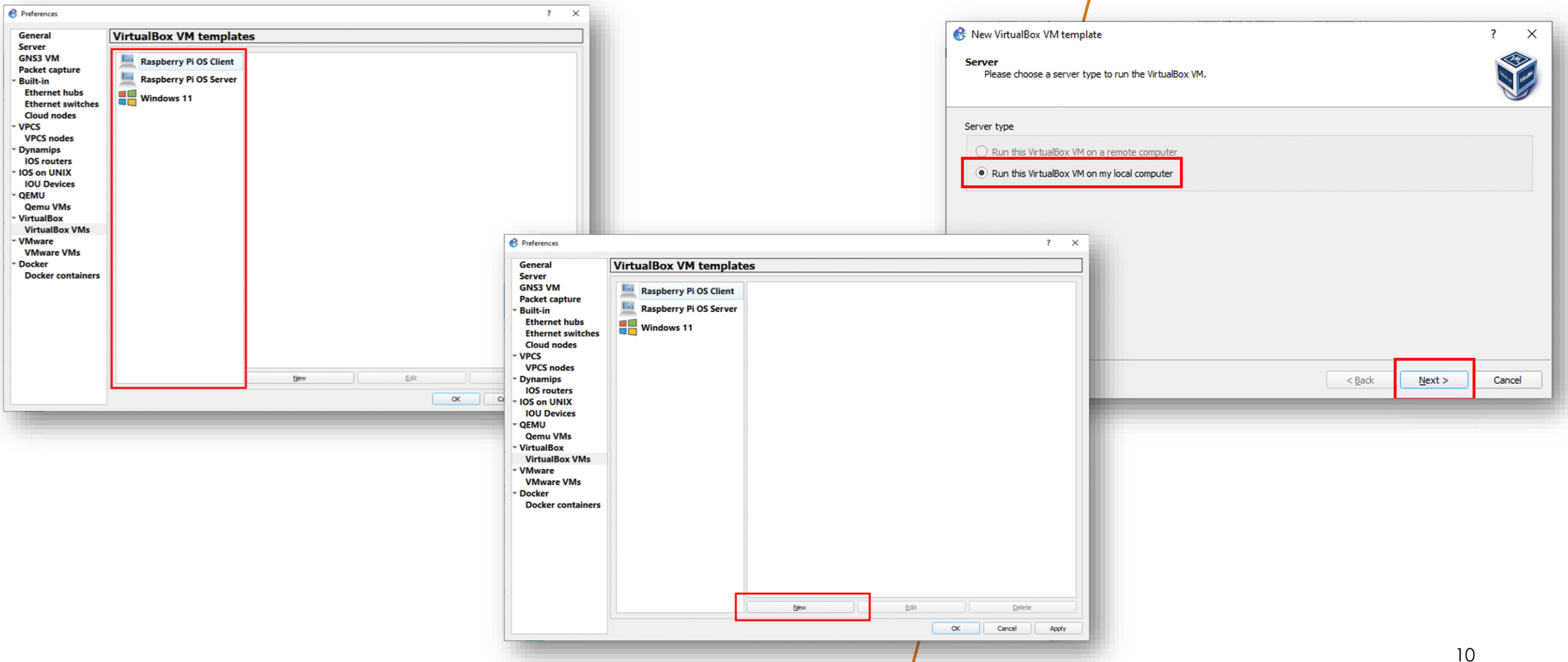
- Set up two VMs as a client and server to transmit values through the Modbus protocol.
- Therefore, install Raspberry Pi Desktop on your computer. You can download the ISO image from HERE.
- After that, install pyModbusTCP on your Raspberry Pi Desktop. A useful example for a server and client can be found on Python Modbus Communication.
- Additionally, you can install a Windows VM/ or another Klai Linux as an IT management device for monitoring the network.

Integrating VMs to GNS3



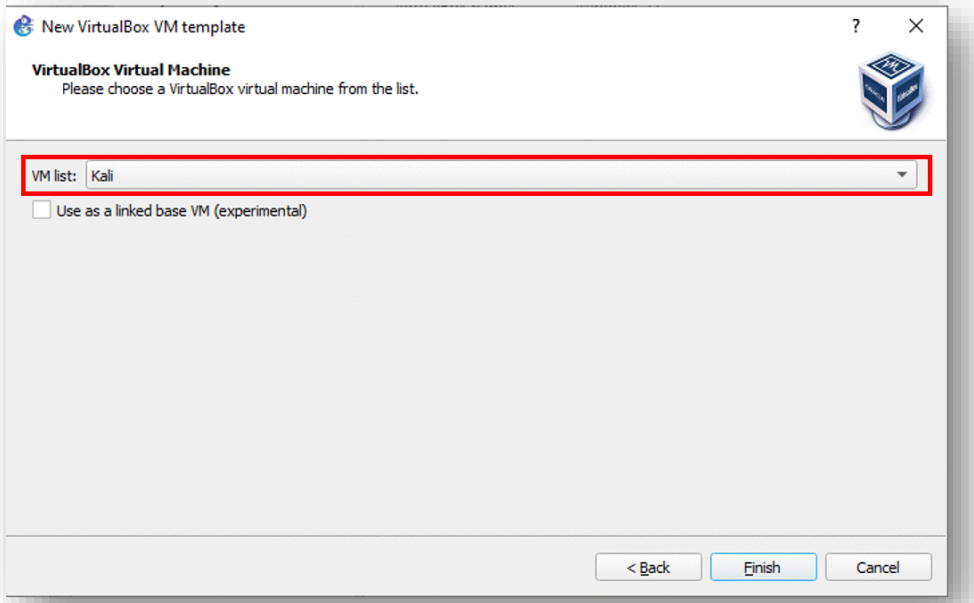
- Do the same for any VM you want to integrate with GNS3

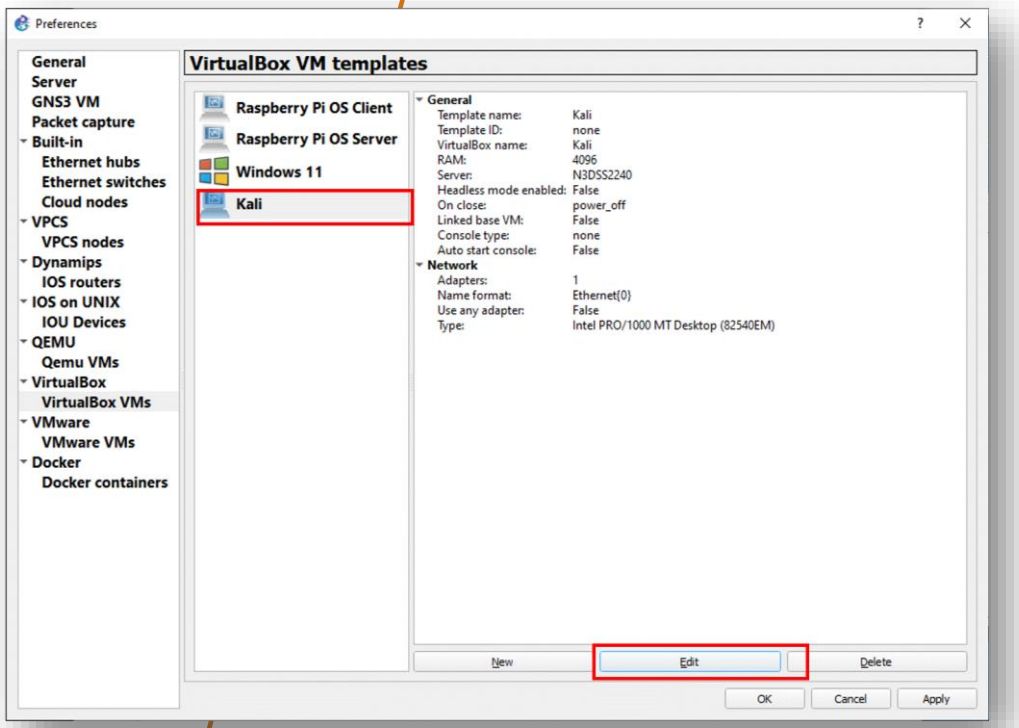
Integrating VMs to GNS3



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

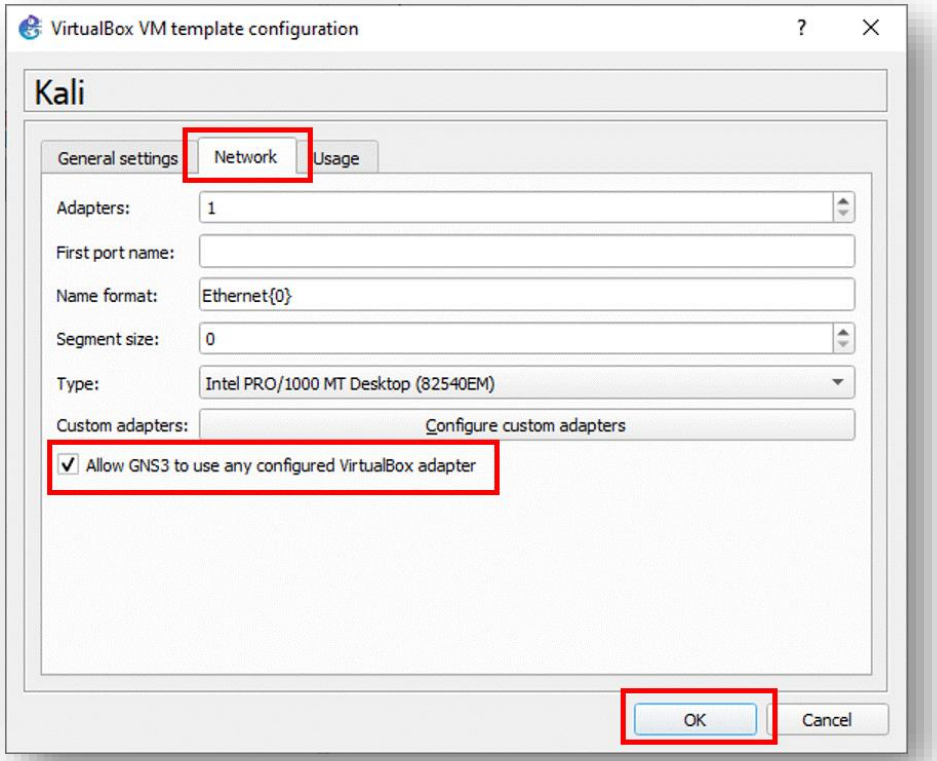
Integrating VMs to GNS3

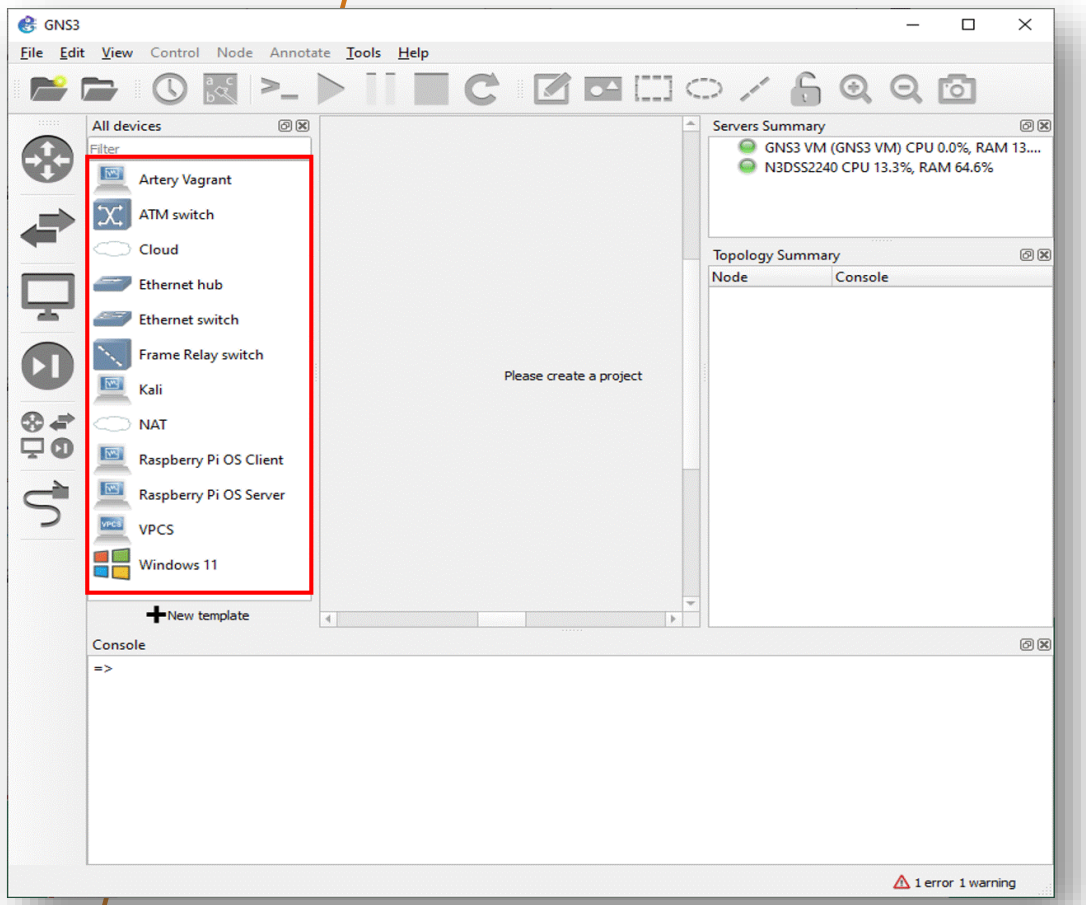




- Do the same for any VM you want to integrate with GNS3

Integrating VMs to GNS3

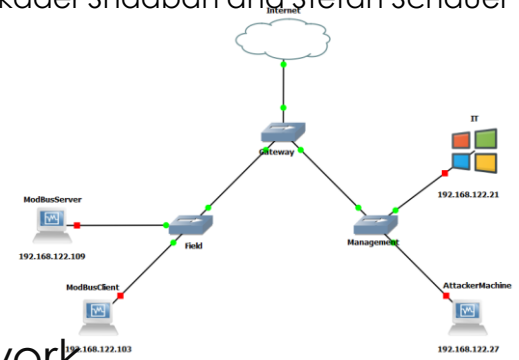




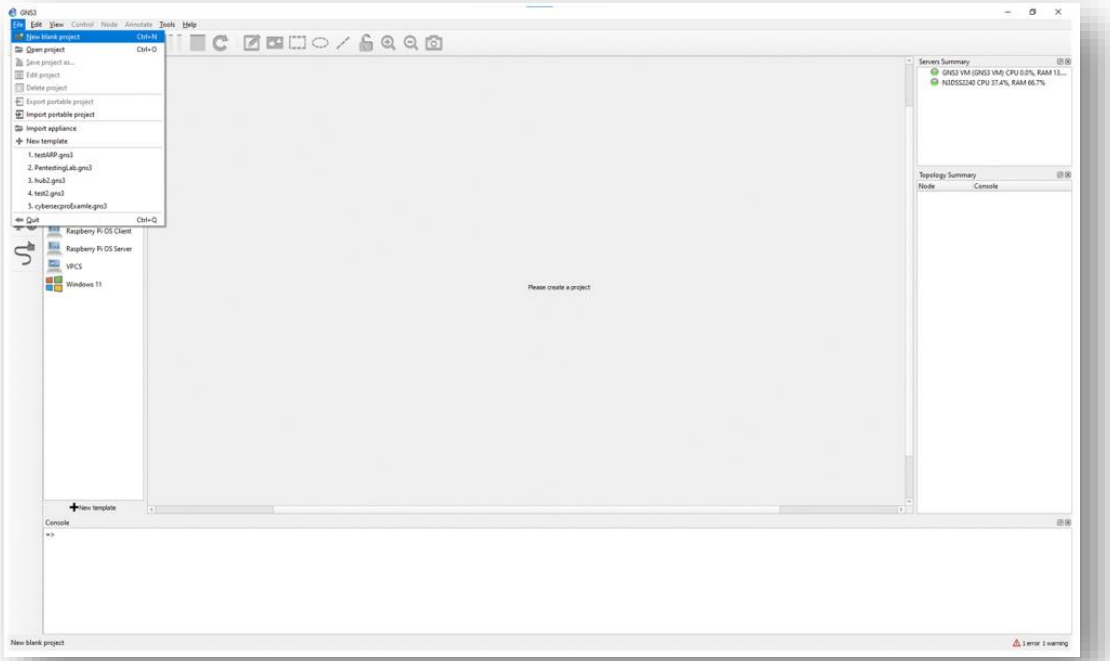
- Do the same for any VM you want to integrate with GNS3

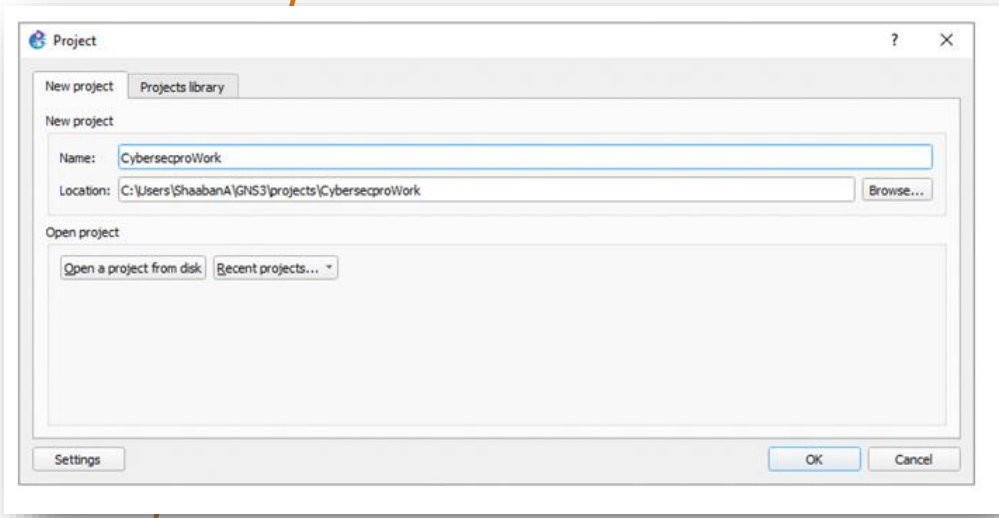
Network Topology Modeling

GNS3 Client for Network Modeling

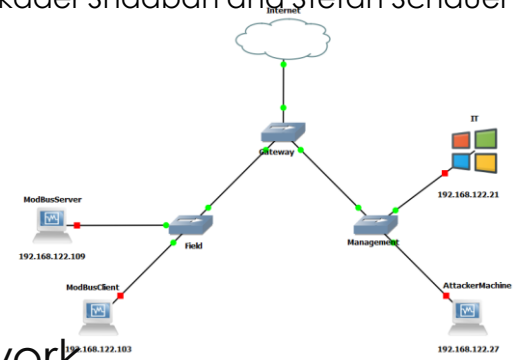


- You now have a list of all integrated VMs, and you can begin modeling your network.

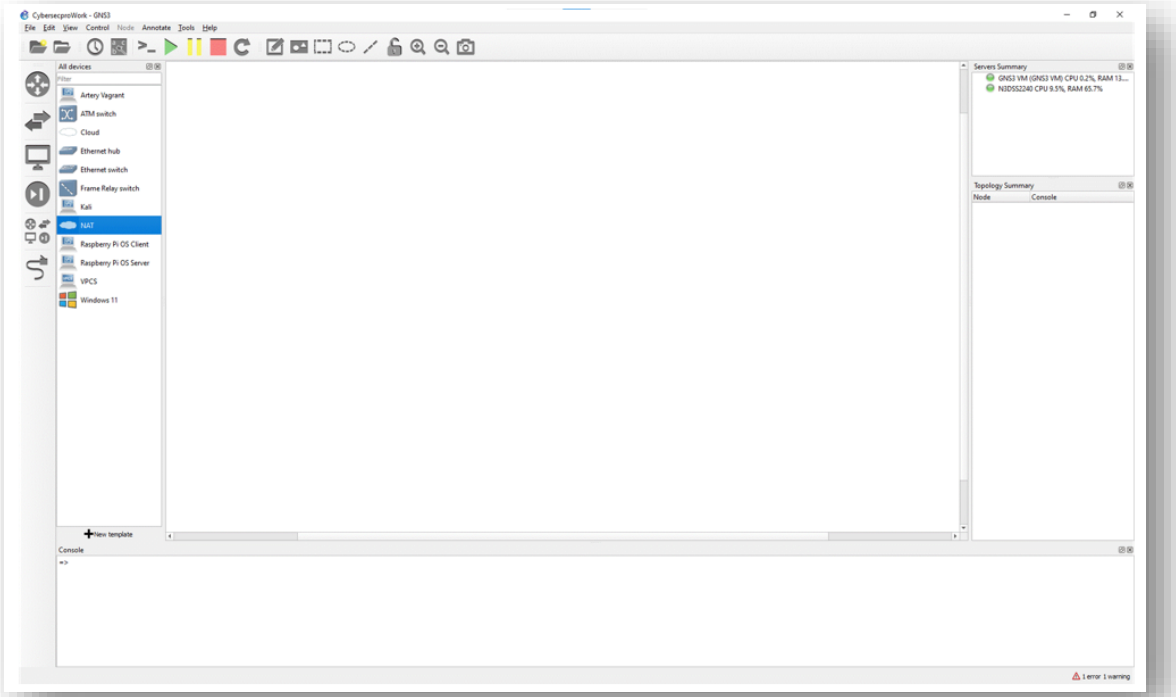


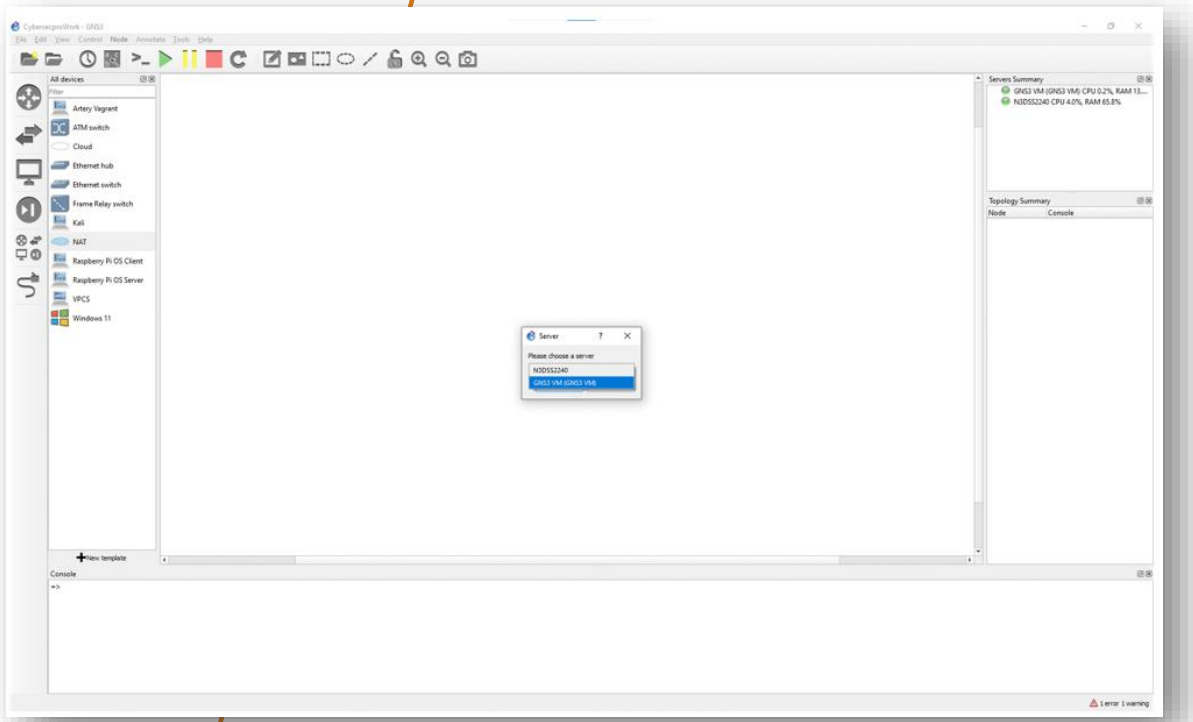


GNS3 Client for Network Modeling

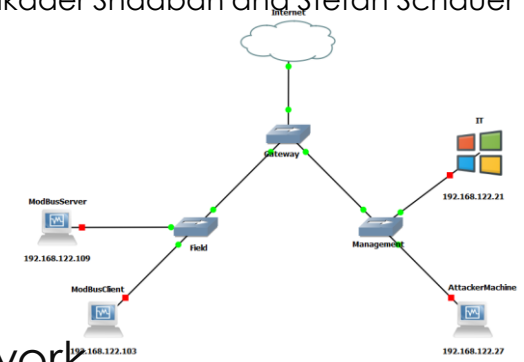


- You now have a list of all integrated VMs, and you can begin modeling your network.

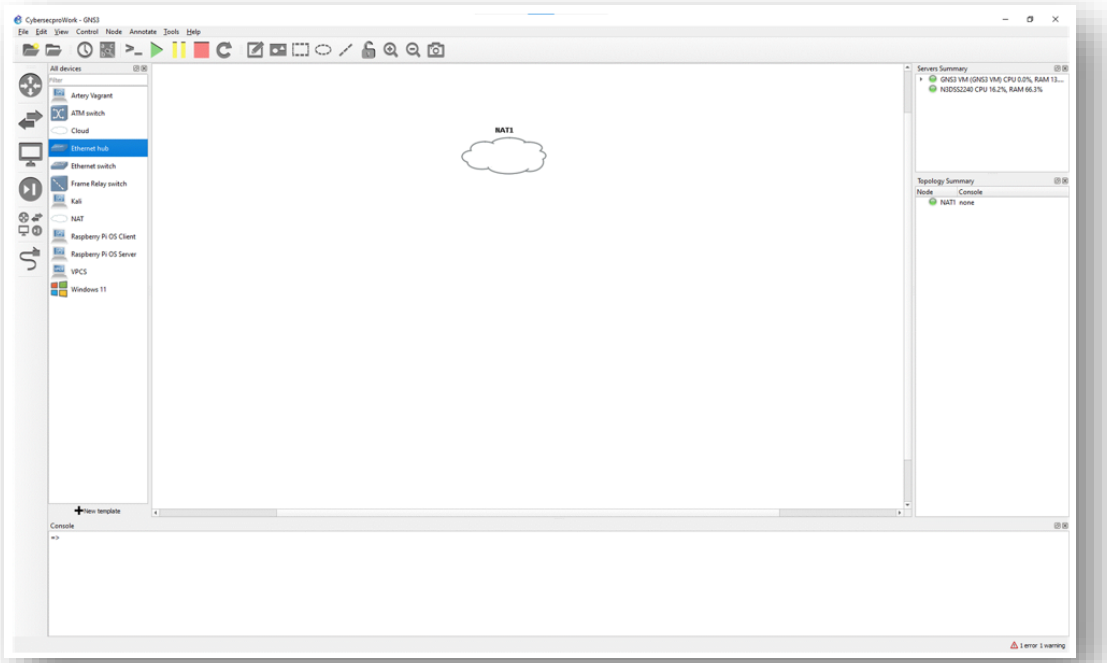


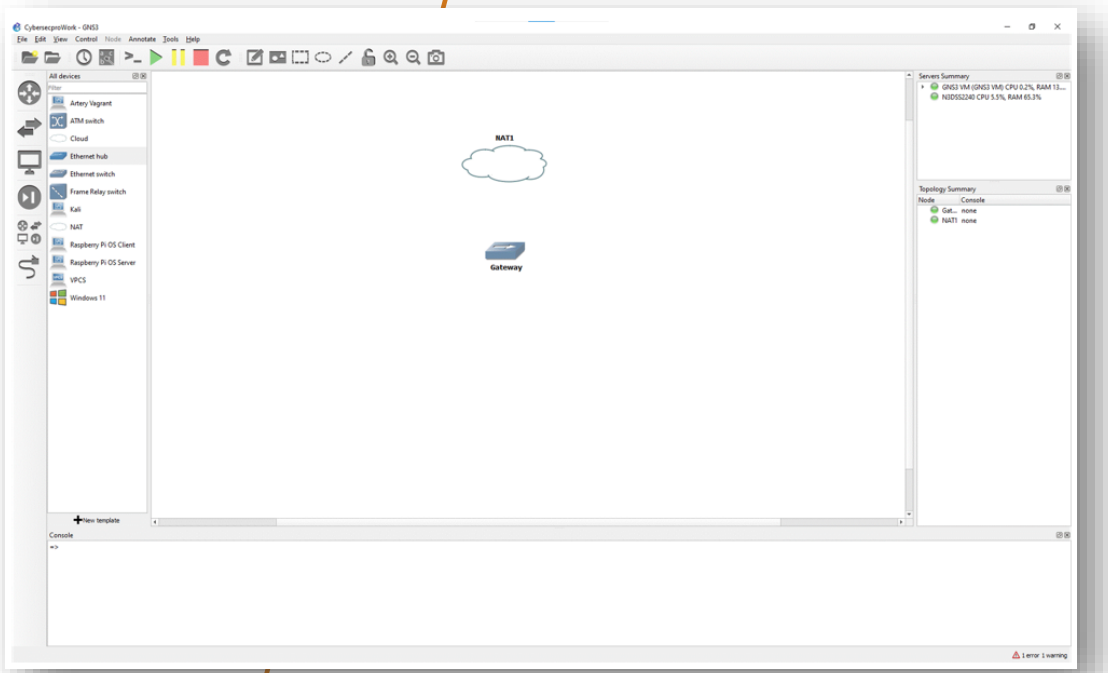


GNS3 Client for Network Modeling

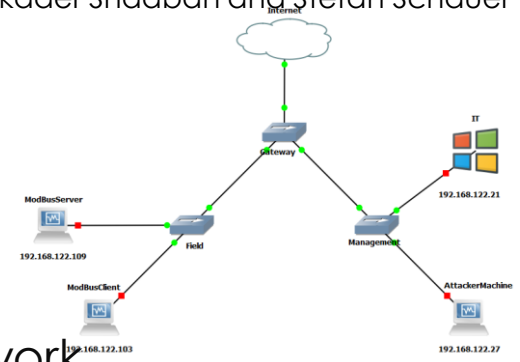


- You now have a list of all integrated VMs, and you can begin modeling your network.

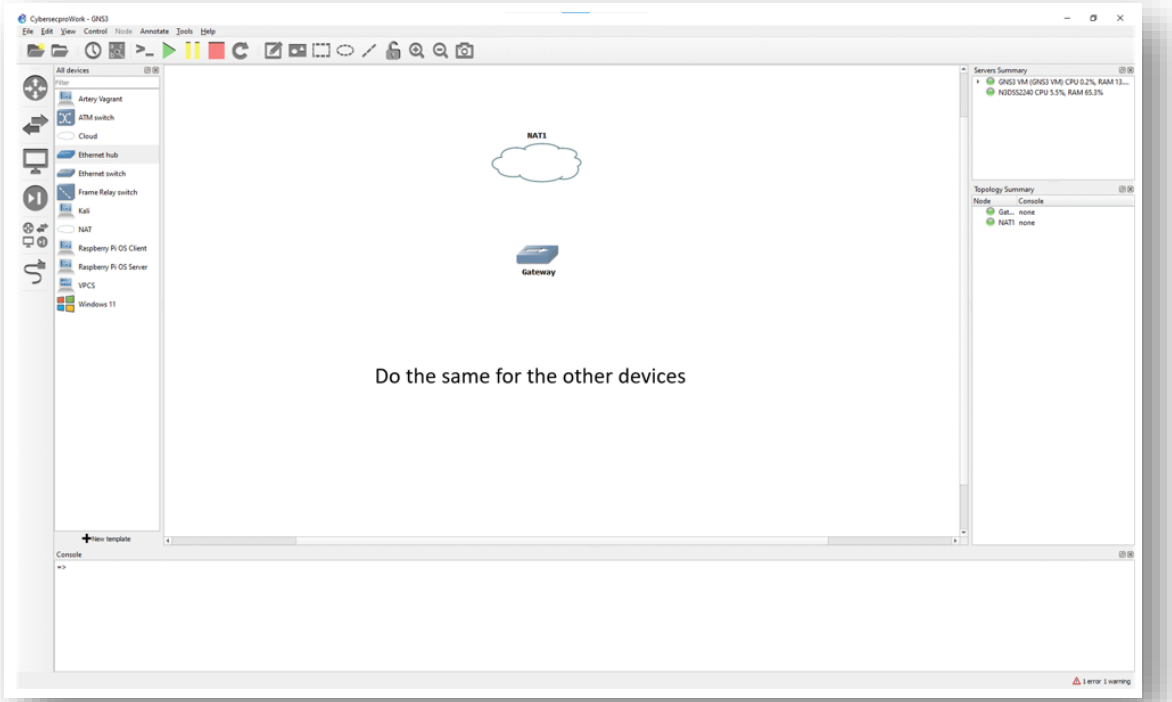


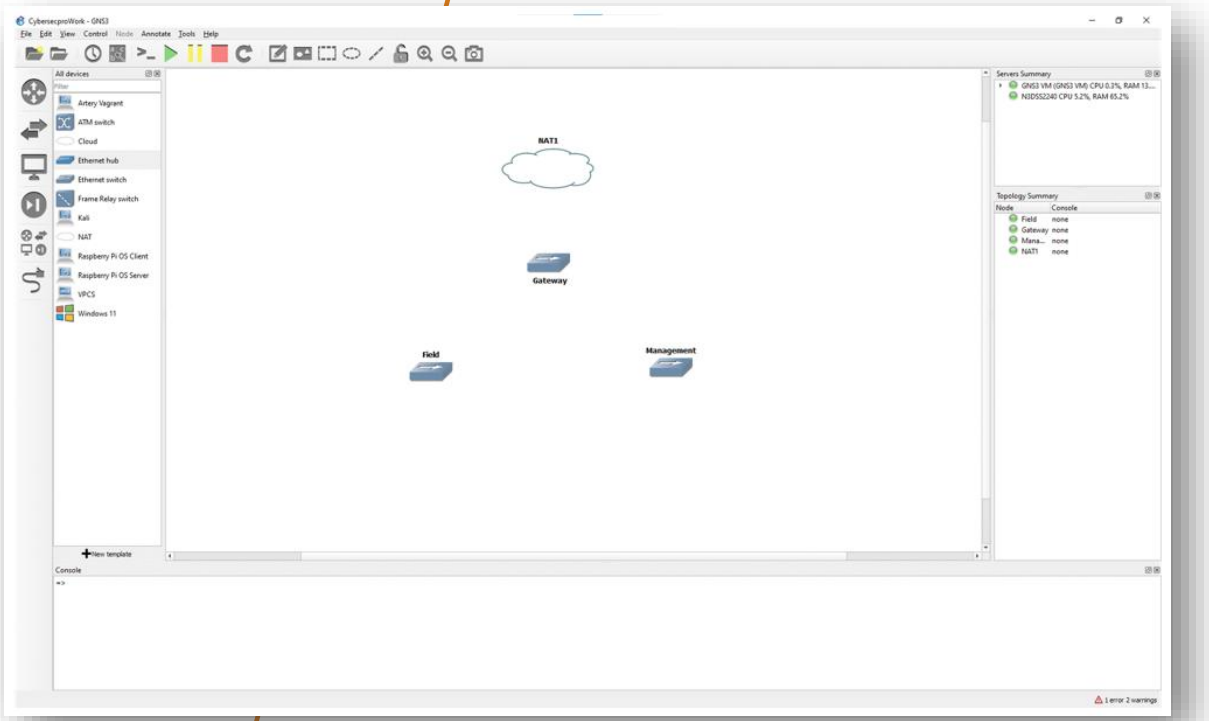


GNS3 Client for Network Modeling

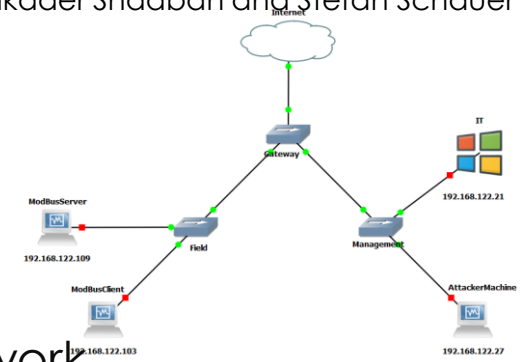


- You now have a list of all integrated VMs, and you can begin modeling your network.

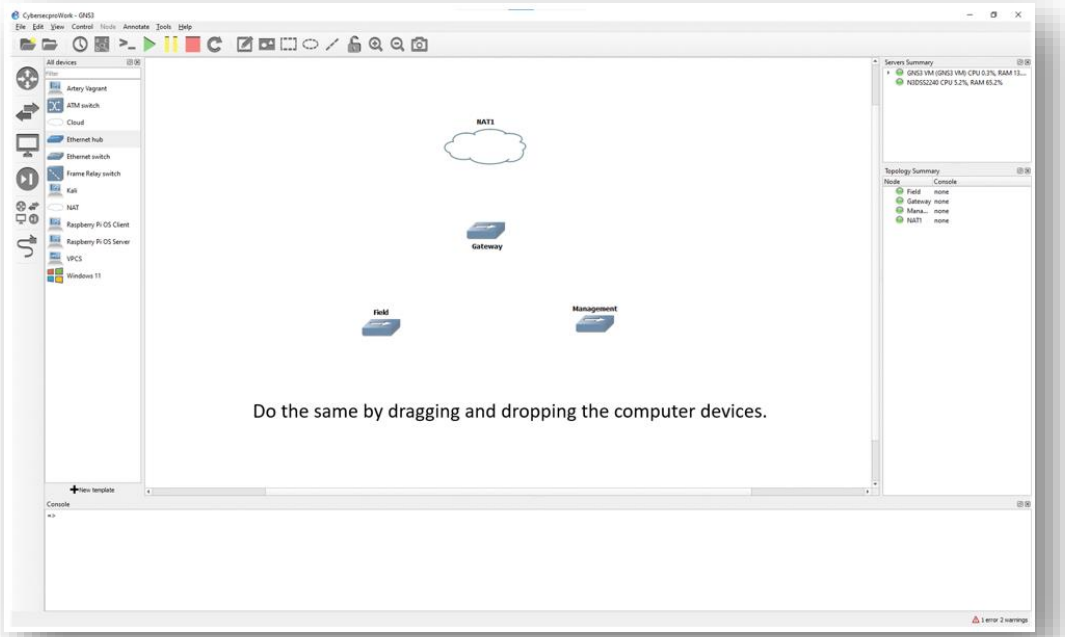


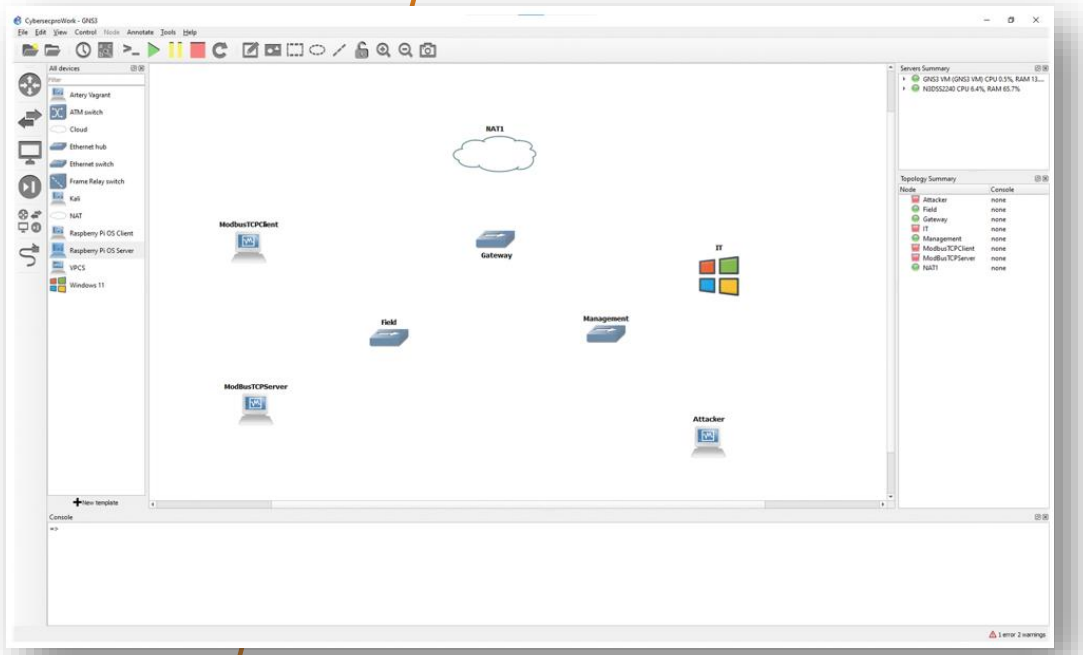


GNS3 Client for Network Modeling

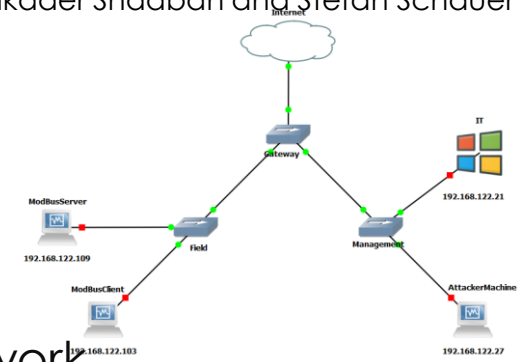


- You now have a list of all integrated VMs, and you can begin modeling your network.

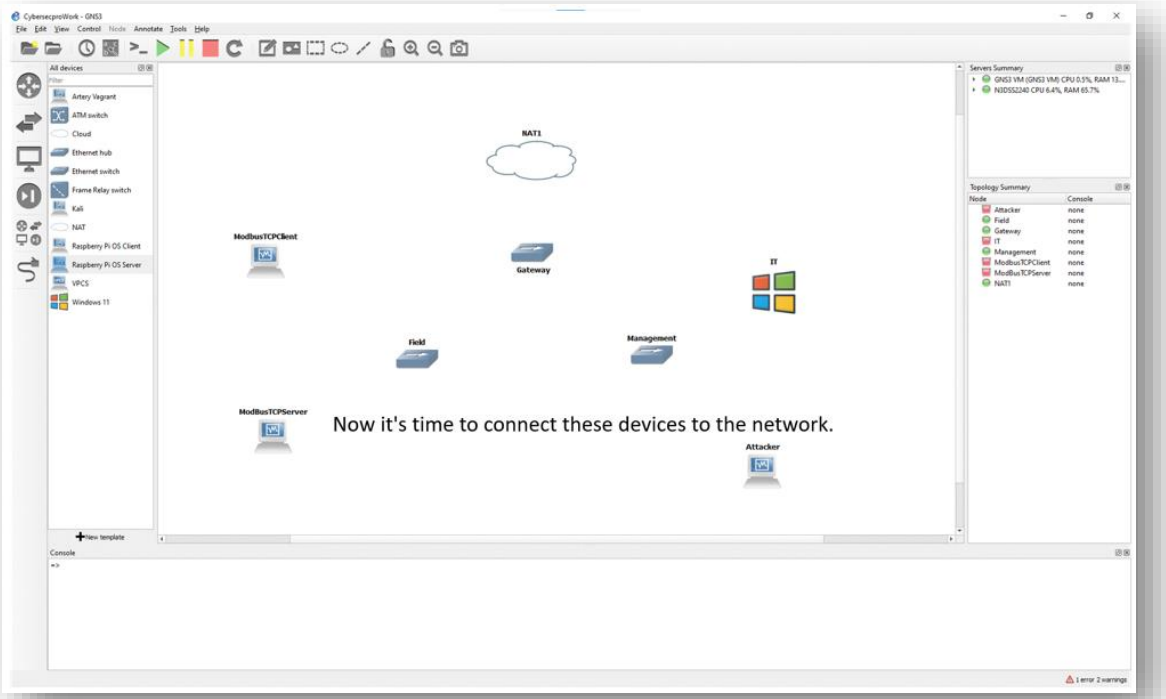


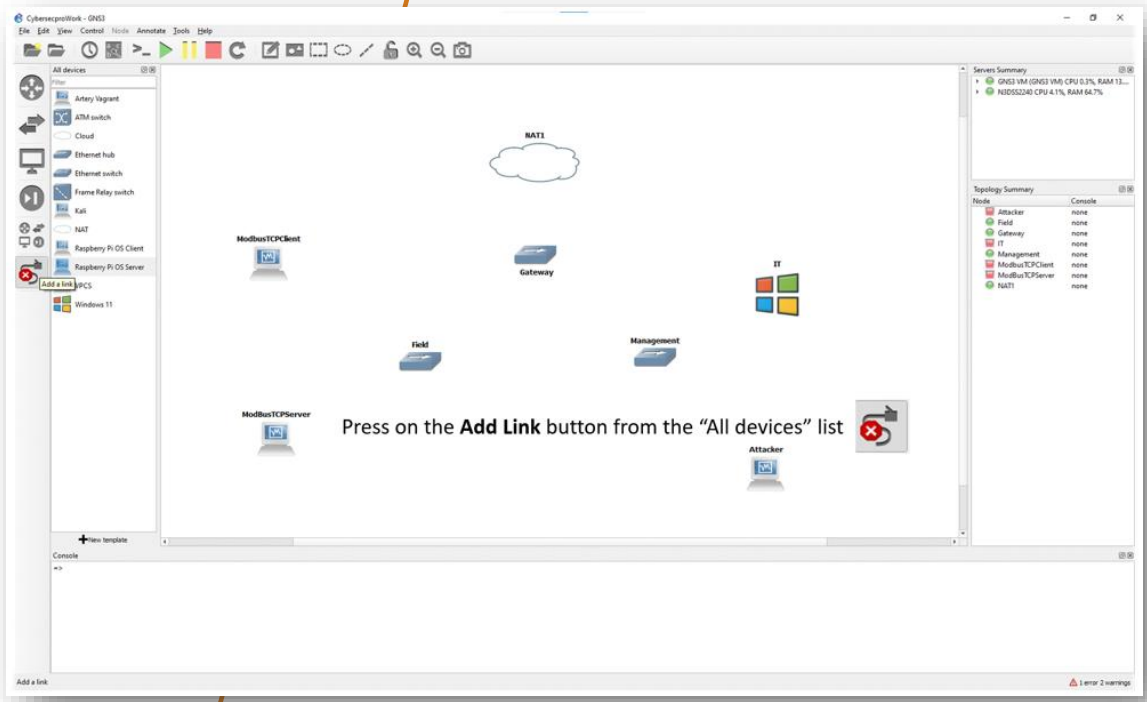


GNS3 Client for Network Modeling

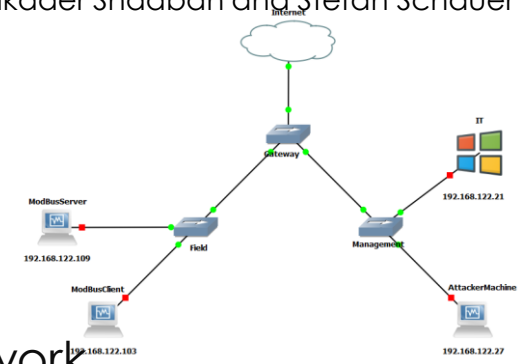


- You now have a list of all integrated VMs, and you can begin modeling your network.

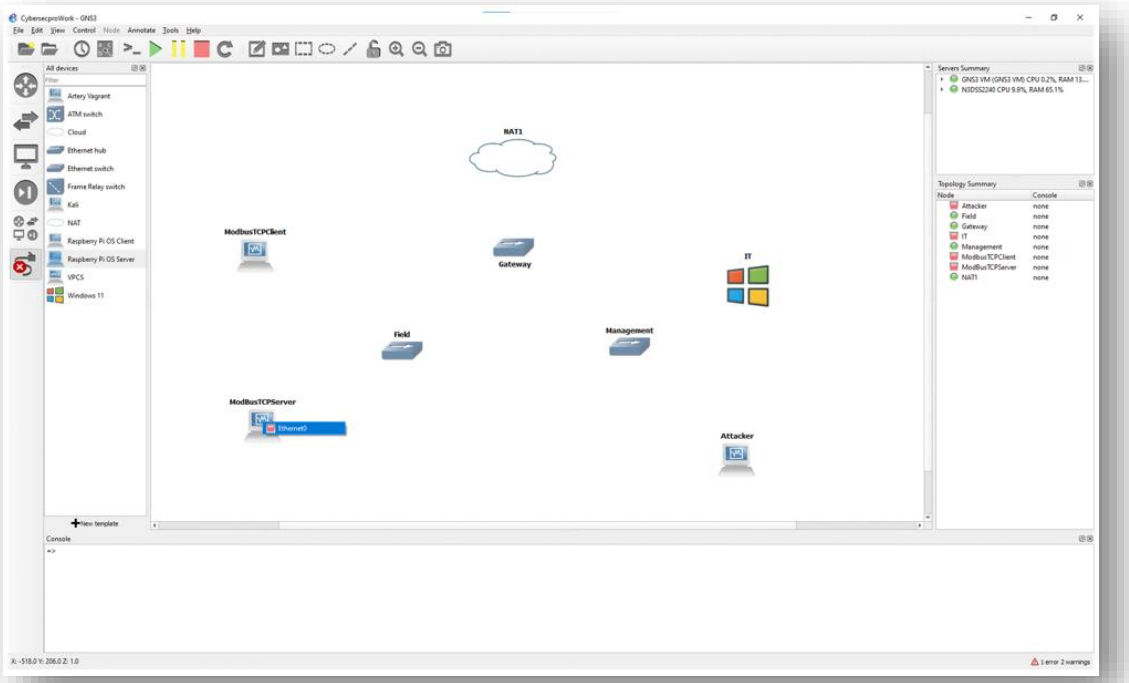


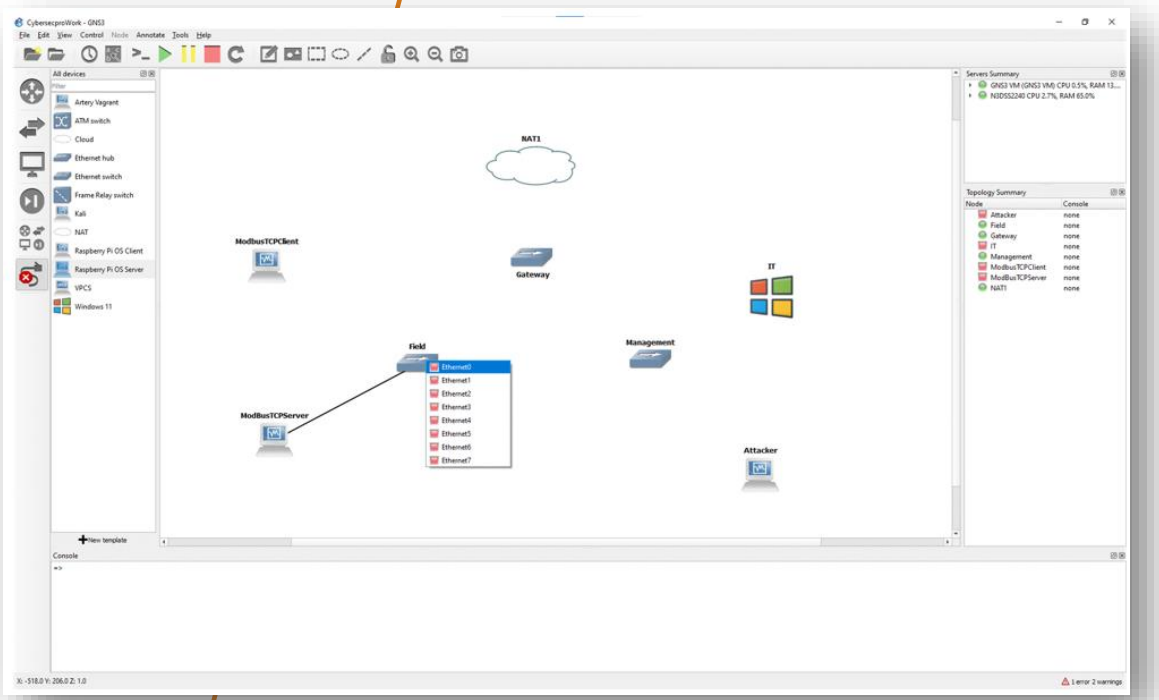


GNS3 Client for Network Modeling

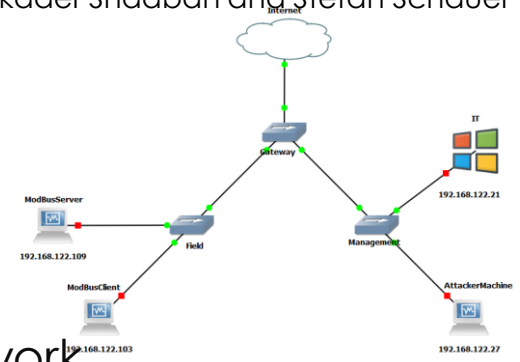


- You now have a list of all integrated VMs, and you can begin modeling your network.

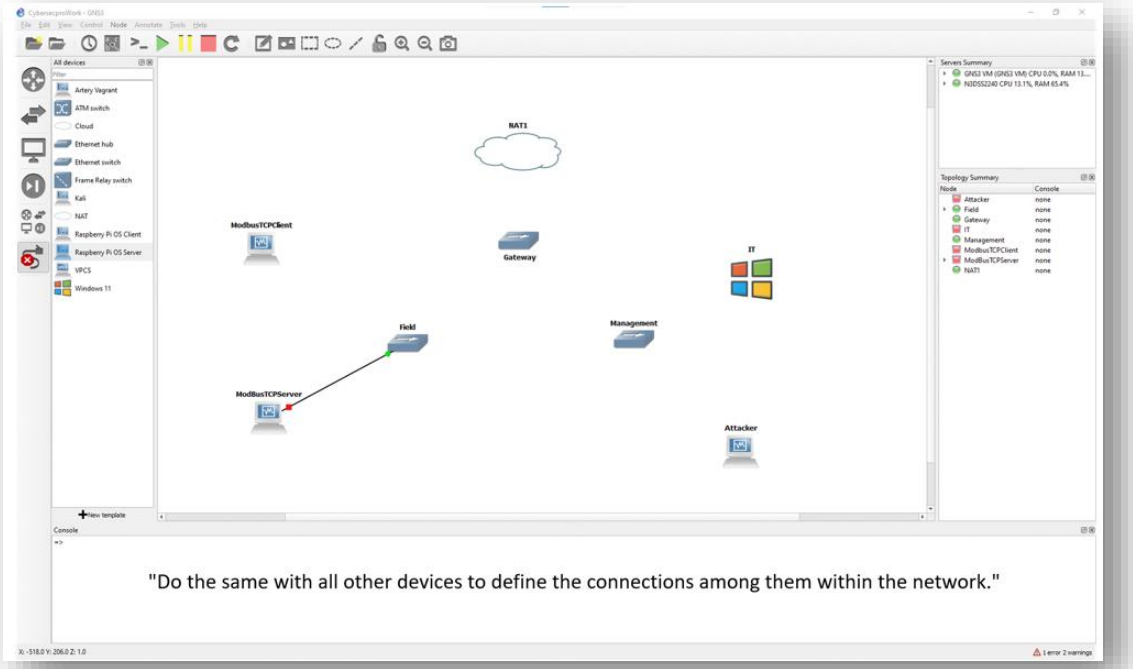


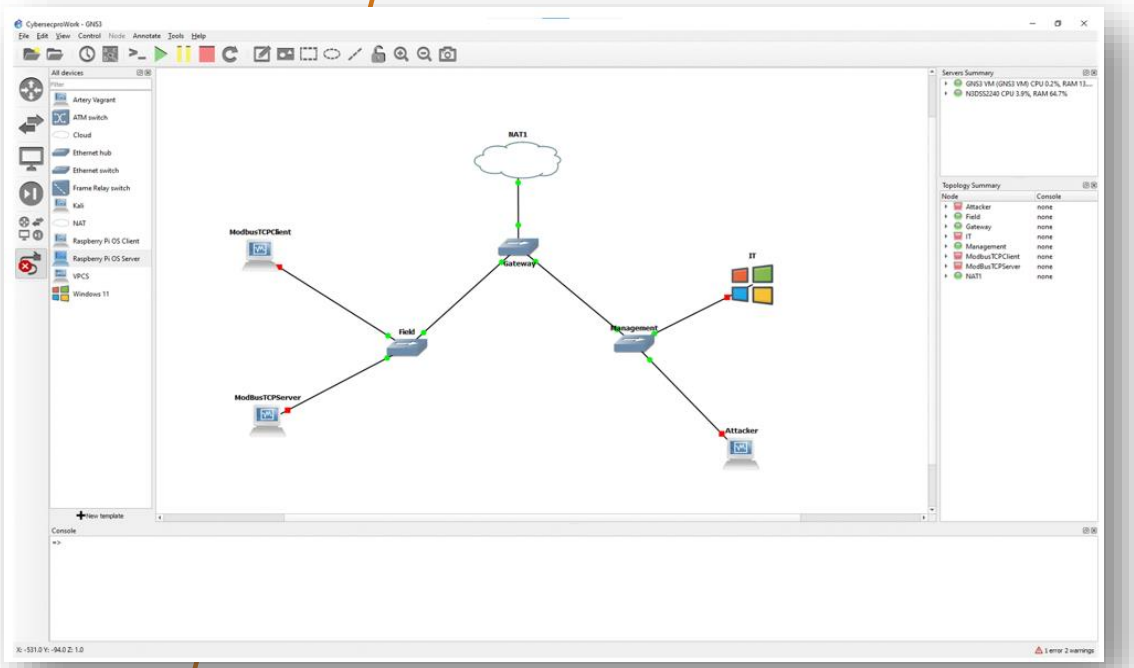


GNS3 Client for Network Modeling

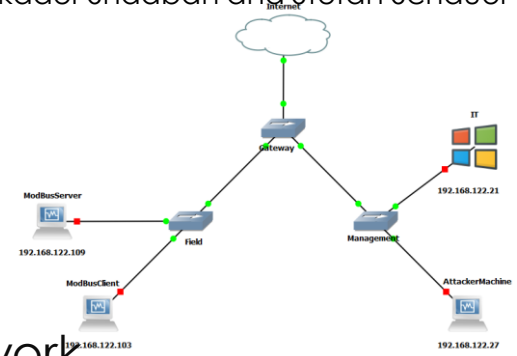


- You now have a list of all integrated VMs, and you can begin modeling your network.

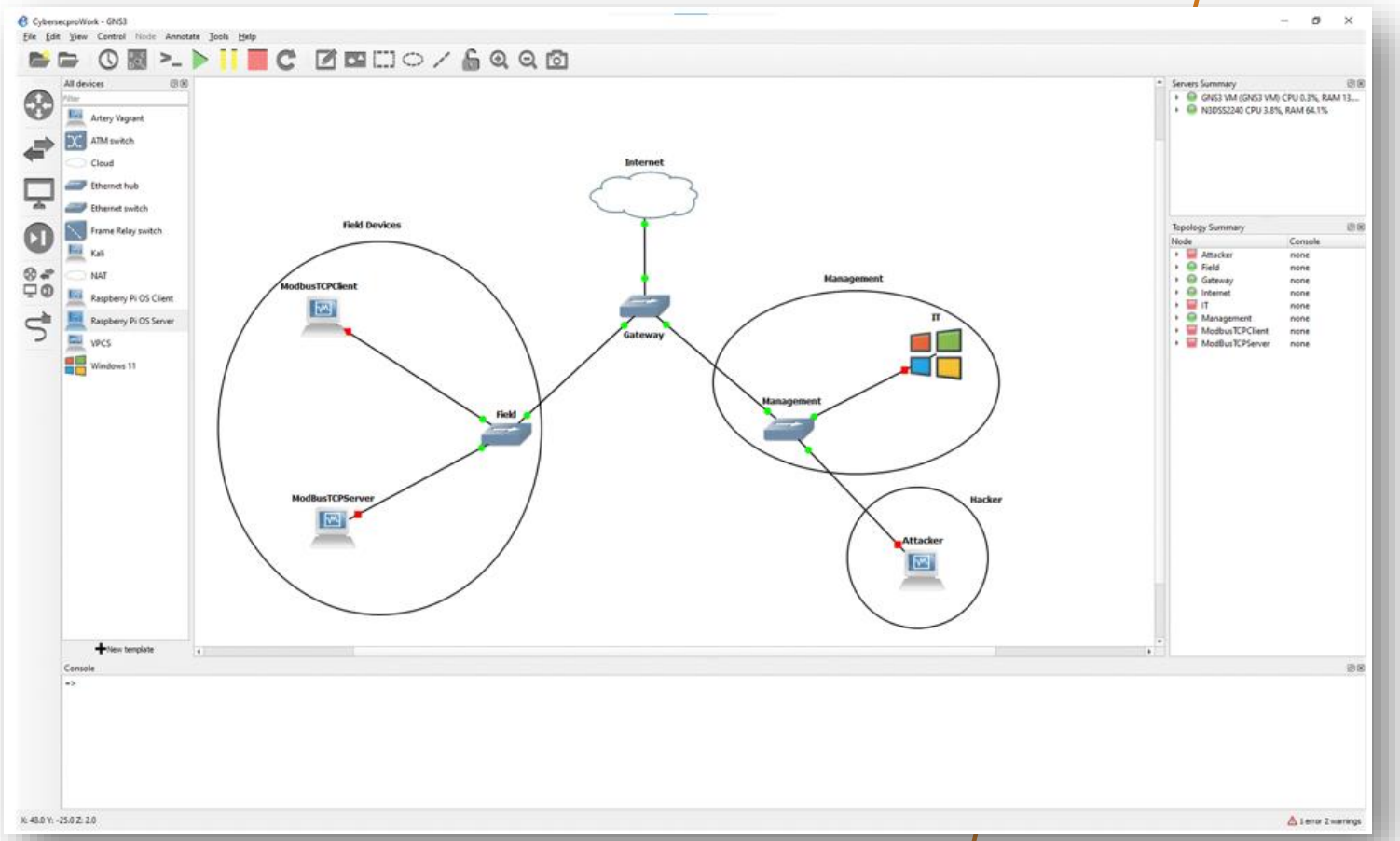




GNS3 Client for Network Modeling



- You now have a list of all integrated VMs, and you can begin modeling your network.

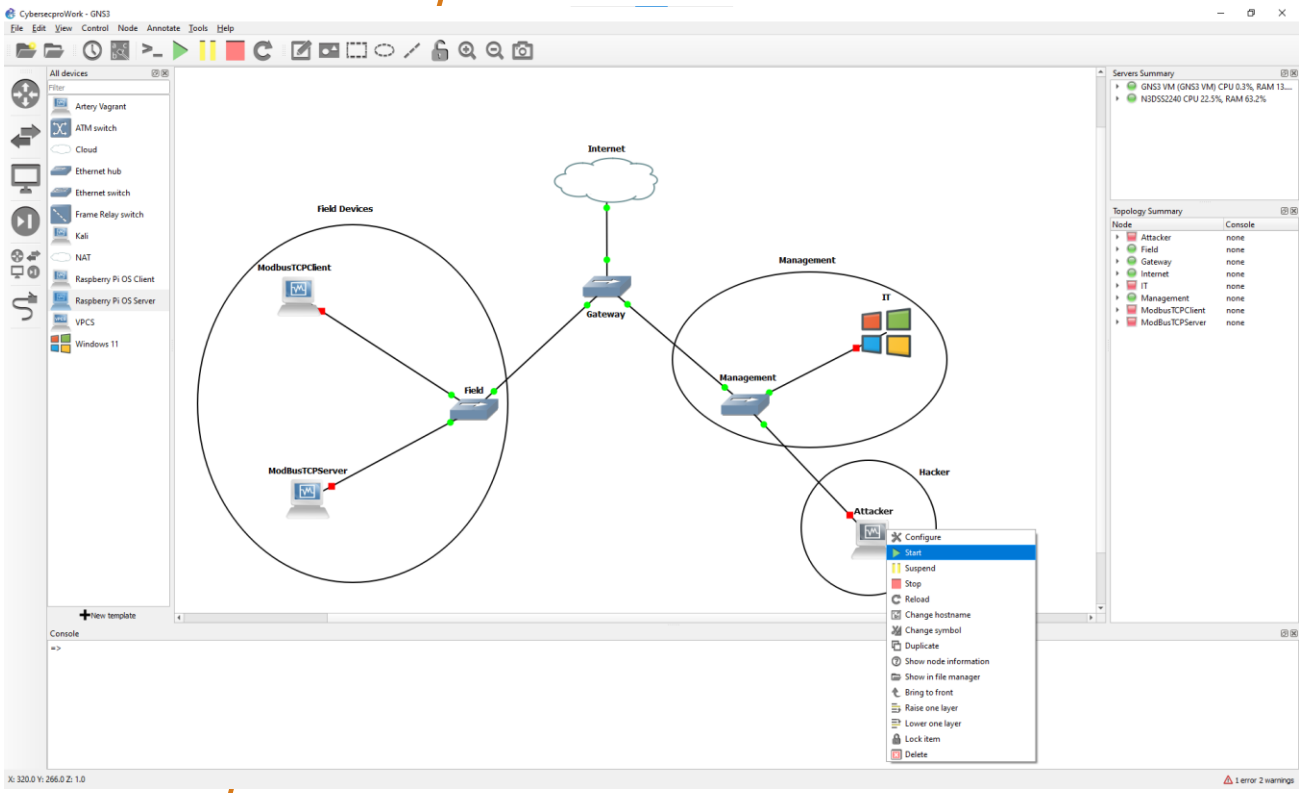


GNS3 Client for Network Modeling

- Before start performing any penetration testing activities, it is crucial to discover the IP addresses of all connected devices in the network.

- Additionally, it is important to ensure that all devices on the network can communicate with each other.

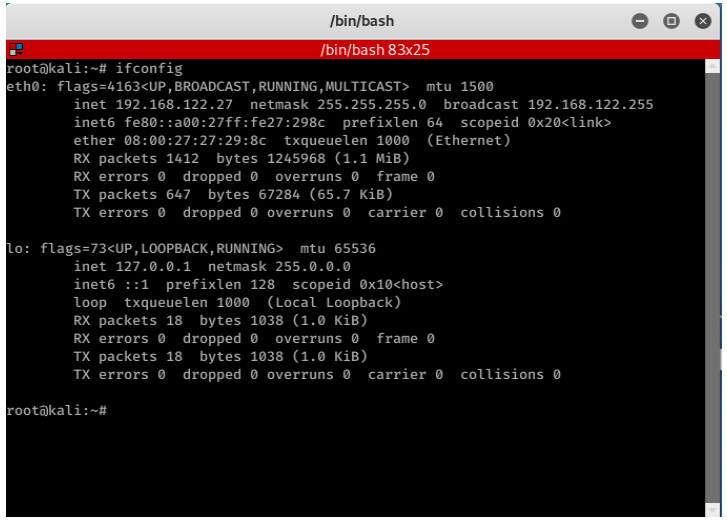
- Therefore, start all devices and verify their IPs.



GNS3 Client for Network Modeling

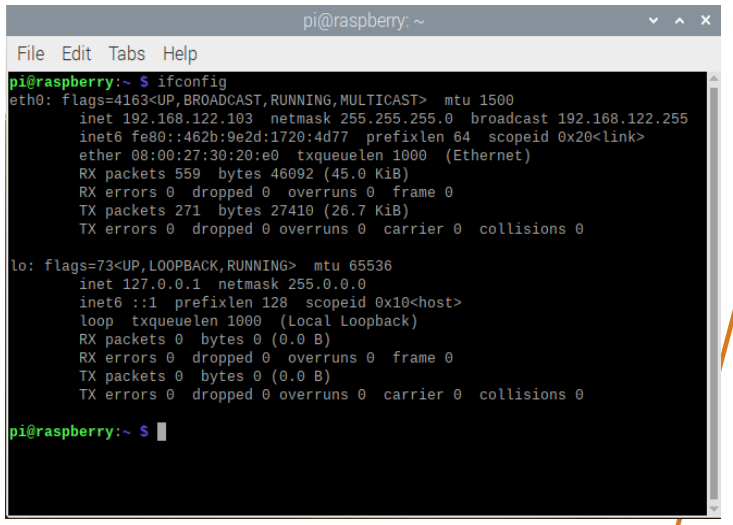
- Use the ifconfig command on the Linux devices to know more about the network configuration

Kali



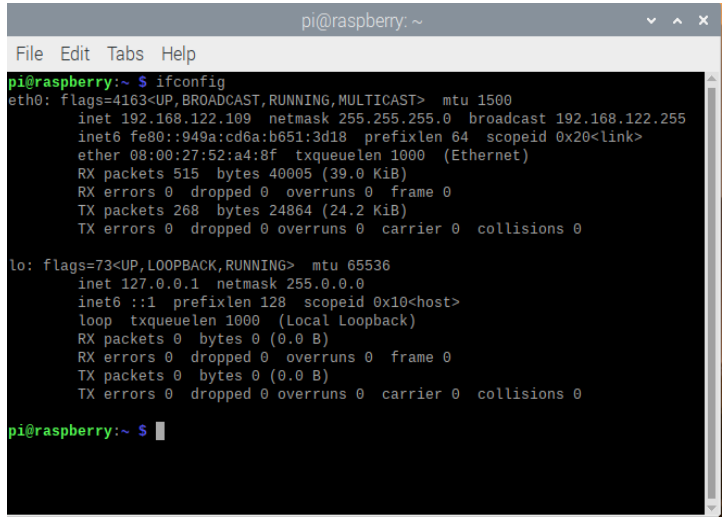
192.168.122.27

Server



192.168.122.109

Client

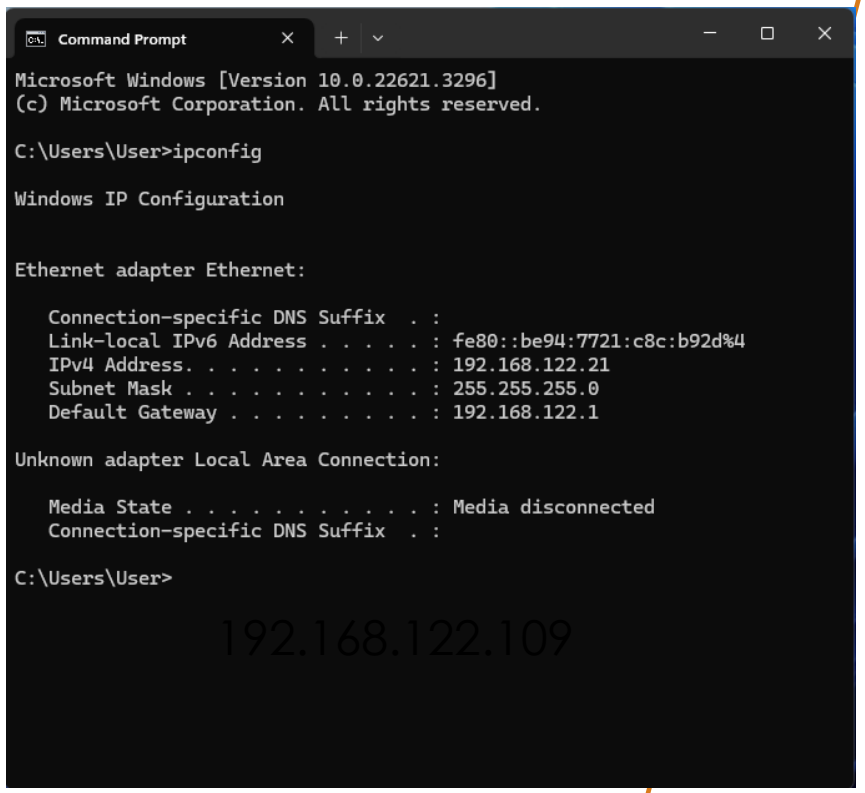


192.168.122.103

GNS3 Client for Network Modeling

•Use the ipconfig command (if you use a windows OS) to know more about the network configuration

Windows

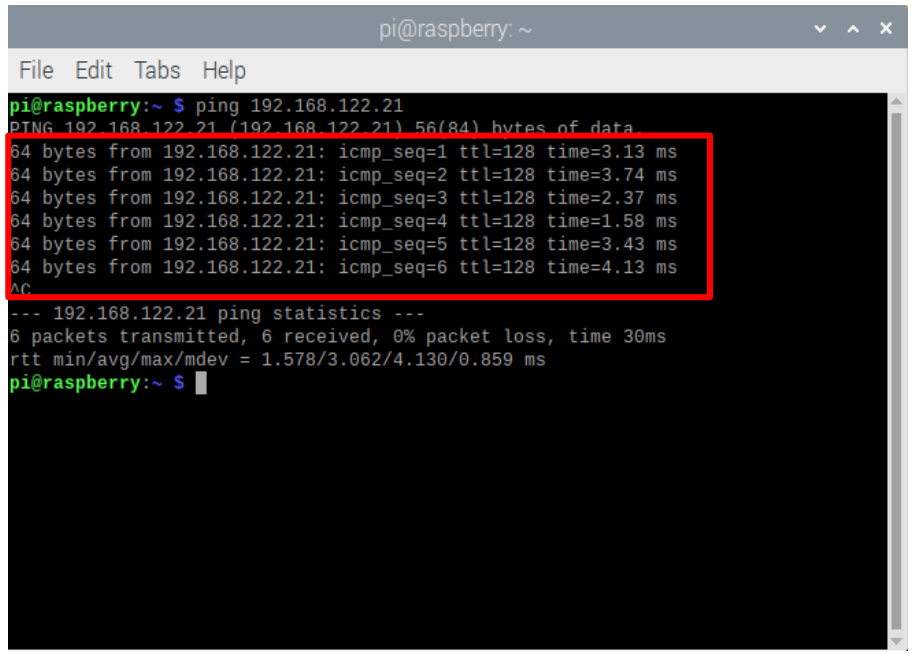


192.168.122.21

GNS3 Client for Network Modeling

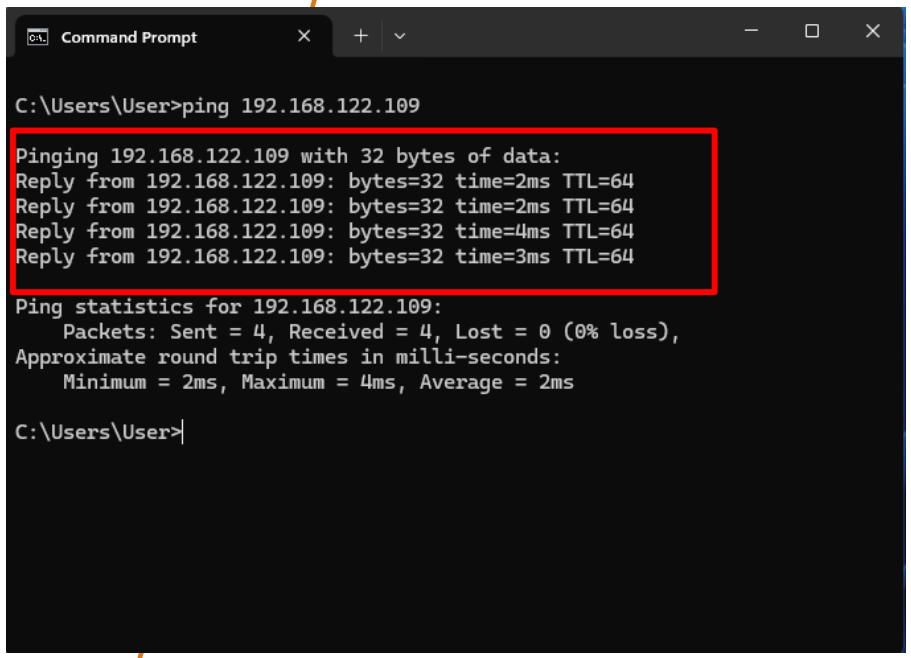
- Now we have the IPs of the network devices, be sure that all devices can reach each other.
- Use the **ping <destination IP-address>** to test the successful establishment of the network.

Server



192.168.122.109

Windows



192.168.122.21

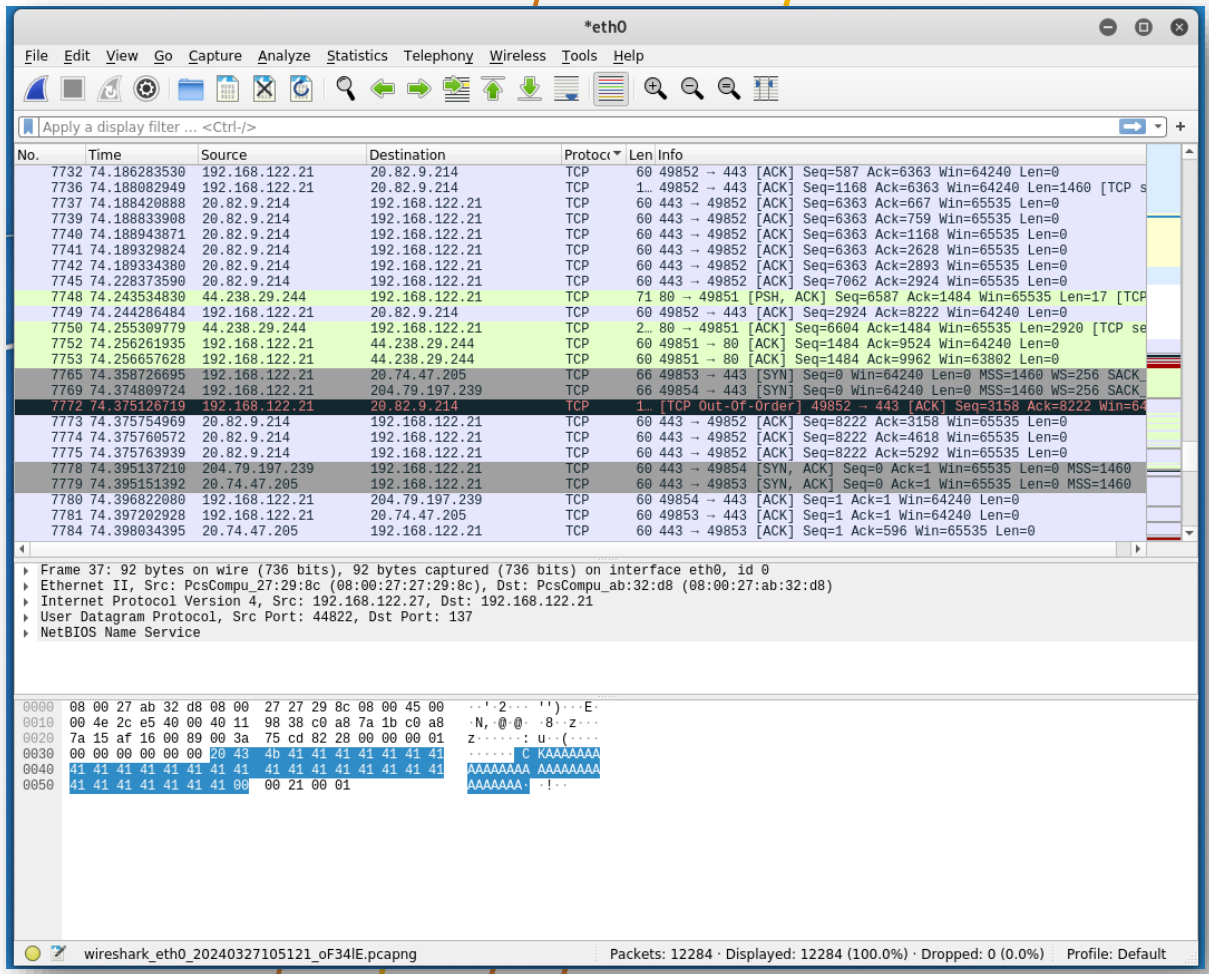
Offensive Tools

Wireshark

Wireshark Sniffing & Packets Analysis

- **Wireshark** is a network protocol **analyzer** designed to help network **administrators** keep track of what is **happening** in their network.
- When you **become** an **MITM**, the **Wireshark tool** can be used to **sniff** and **analyze** traffic **sent** and **received** by the targets.

Green – TCP packets
Dark blue - is DNS packet
Black – TCP packets that have an issue

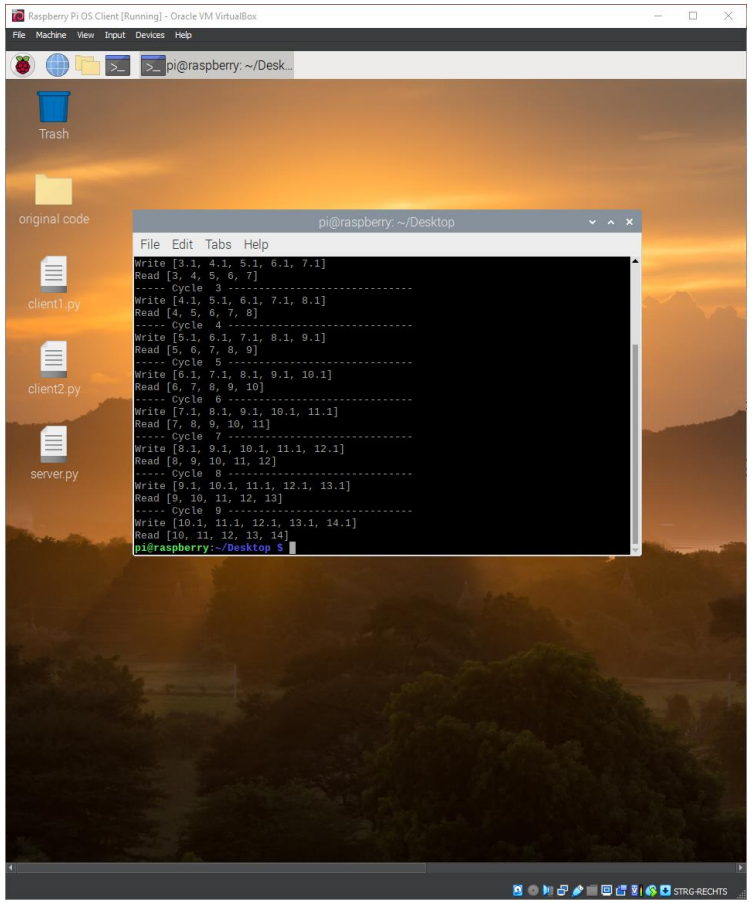


Wireshark – Client/Server Example

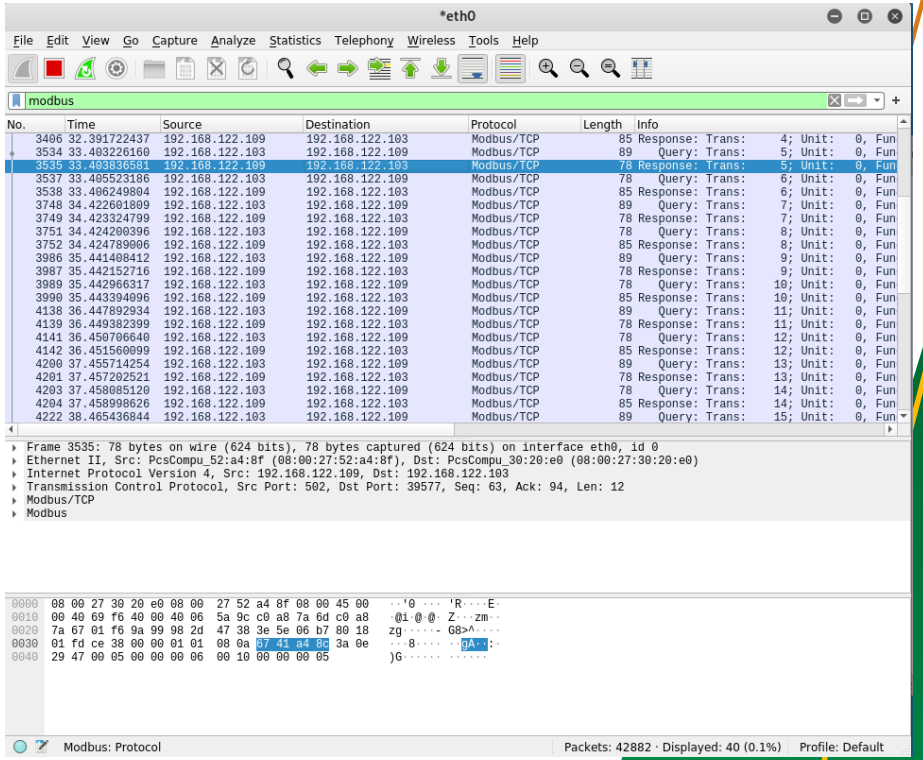
- In the Server/Client example, we have two Linux machines: the client sending data to the server through the **ModbusTCP** protocol.

- When the attacker is a **Man-in-the-Middle**, Wireshark tool can be used for capturing all data transmitting, and other actions could be applied, such as:
  - Filtering collected data (**Modbus**)
  - Analysis traffic

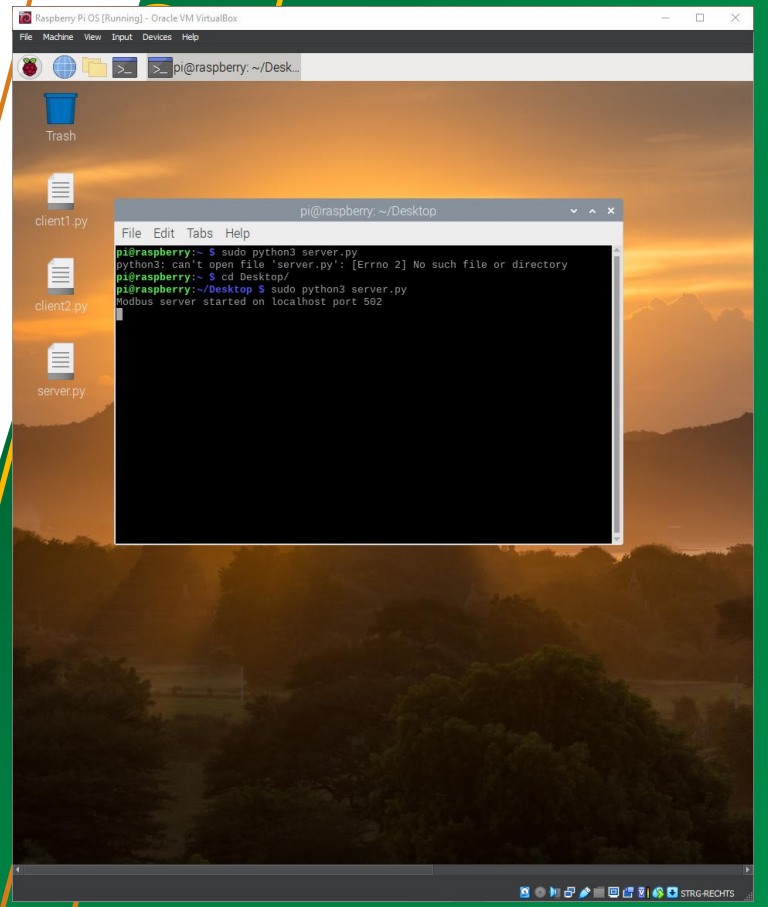
Wireshark – Client/Server Example



Client



Kali



Server

Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at