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.

Cybersecurity Lab

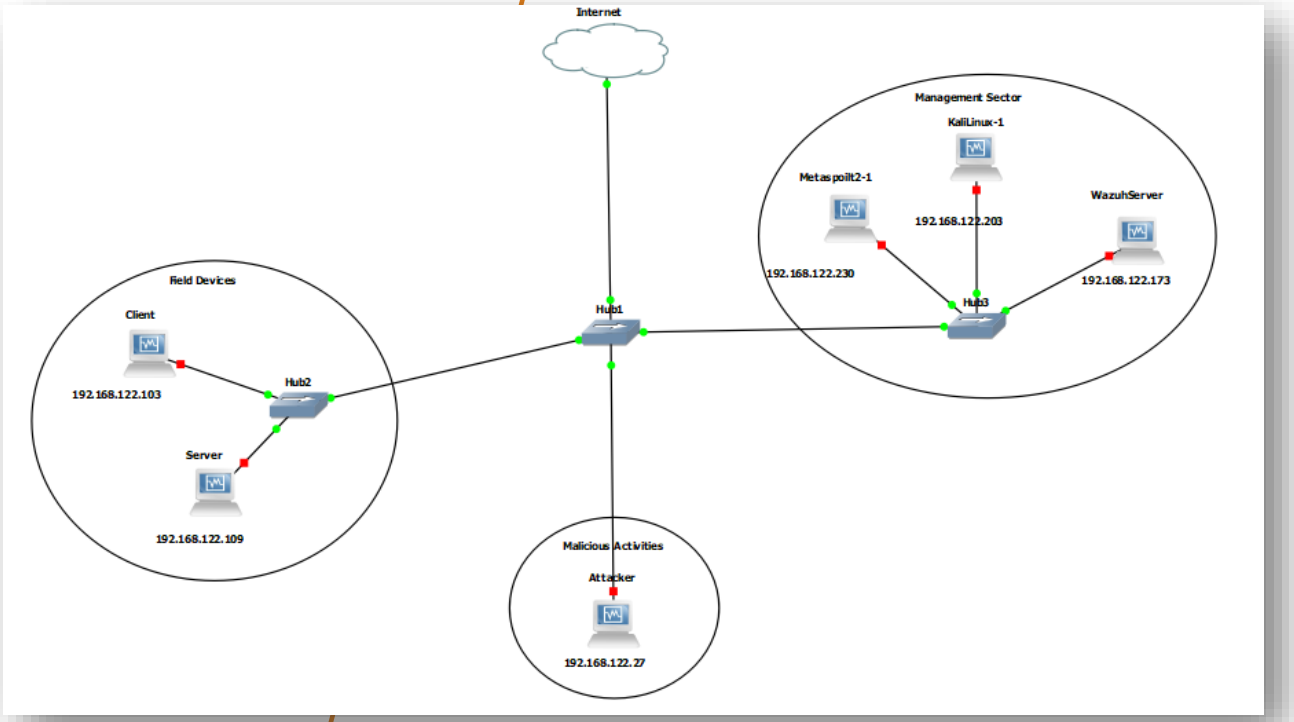
In this **lecture** we aim to **build** a **cybersecurity** lab **consisting** of a set of **virtual machines**, each playing a specific **role**.

As shown in the right-hand screenshot, we plan to include the following machines:

Victim machines: Client and Server

Management machines: Metasploit, Kali-Admin, and Wazuh Server

Attacker machine: Kali-Attacker



If you have technical issues due to limited storage on your computer, please be sure to install at least one victim machine, one attacker machine, and the Wazuh Server for our technical activities during the lecture.

Cybersecurity Lab

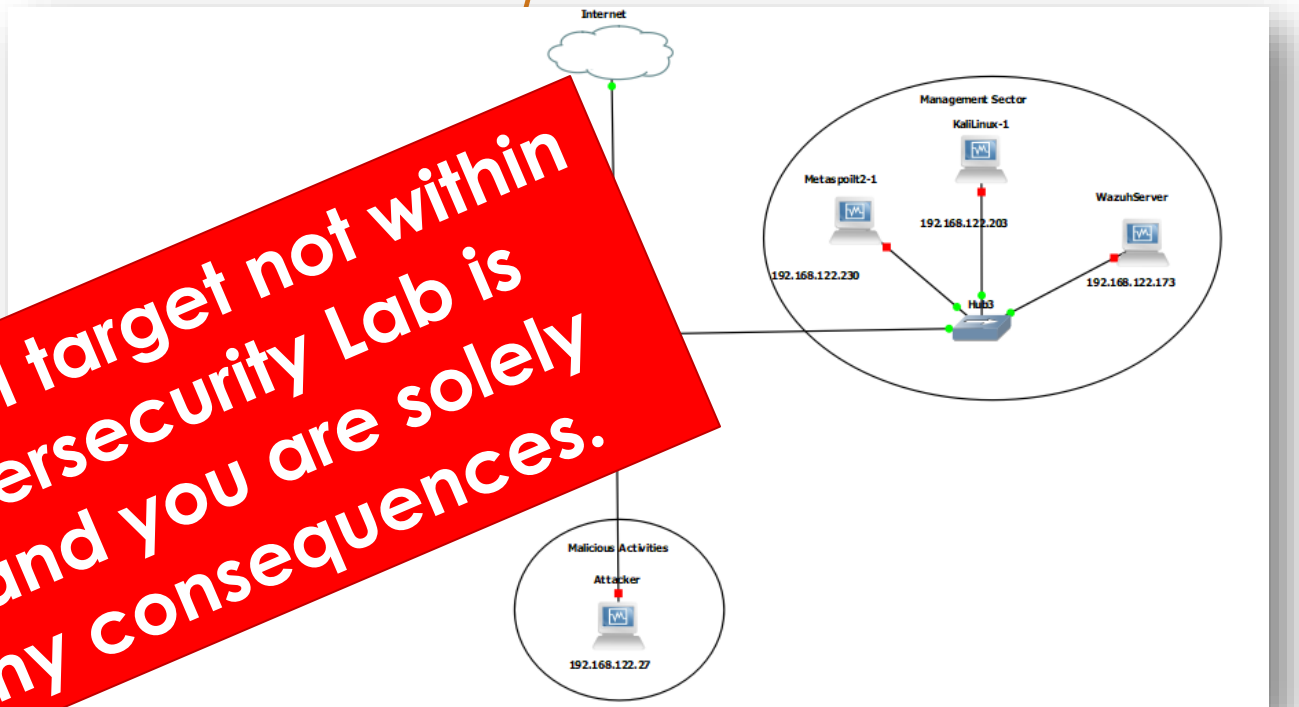
In this **lecture** we aim to **build** a **cybersecurity** lab **consisting** of a set of **virtual machines**, each playing a specific **role**.

As shown in the right-hand screenshot, we plan to include the following machines:

Victim machines: Client and Server

Management machines: Mete
and Wazuh Server

Attacker machi



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

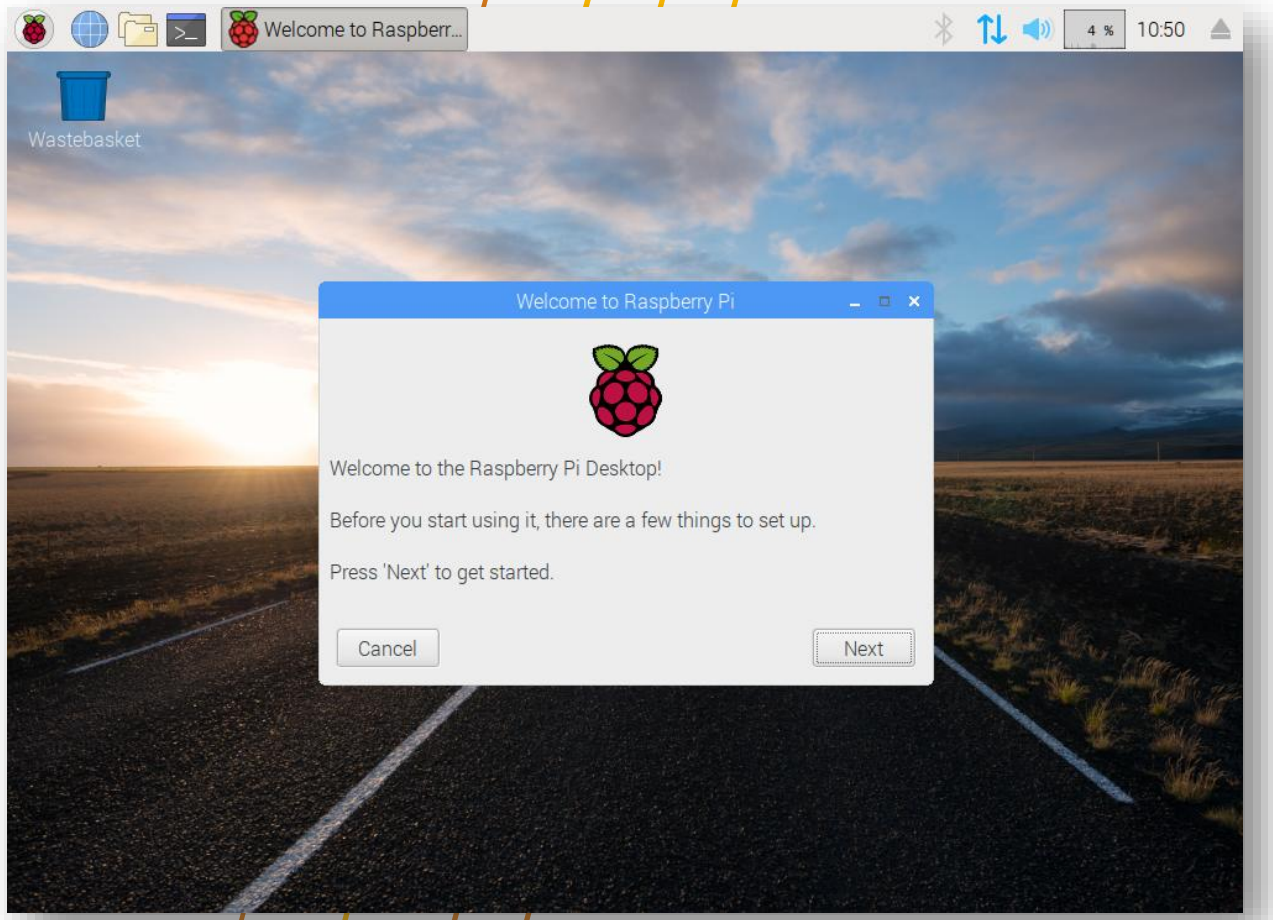
If you have techn ed storage on your computer, please be sure to install at least one victim machine machine, and the Wazuh Server for our technical activities during the lecture.

Client/Server Machines

Victim Machines: Client-Server

- Install **two lightweight Linux distributions** to serve as the **client** and **server**, such as Raspberry Pi Desktop. You can download the ISO image from HERE.

- If you already have two Linux virtual machines installed on your computer, you can use them. In that case, you may skip this slide and proceed directly with installing **Python** and the **ModbusTCP protocol**.



Python and ModbusTCP

Python and ModbusTCP

- Please make sure to install Python on your Linux **Client** and **Server** VMs before the session.

- You can follow the step-by-step installation guide here: How to Install Python on Linux

- After that, install pyModbusTCP on your Raspberry Pi Desktop (Client-Server Machines).

- A useful example for a server and client using the pyModbusTCP can be found on Python Modbus Communication.

Admin and Attacker Machines

Kali Machines

- Kali It is the most advanced Penetration Testing Linux Distribution.
- It 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.
- Kali Linux will be used to **simulate an attacker using multiple offensive tools against the victim machines** within the network.
- Additionally, you need to install another one to serve as an **administrator machine** for monitoring and managing network activity.

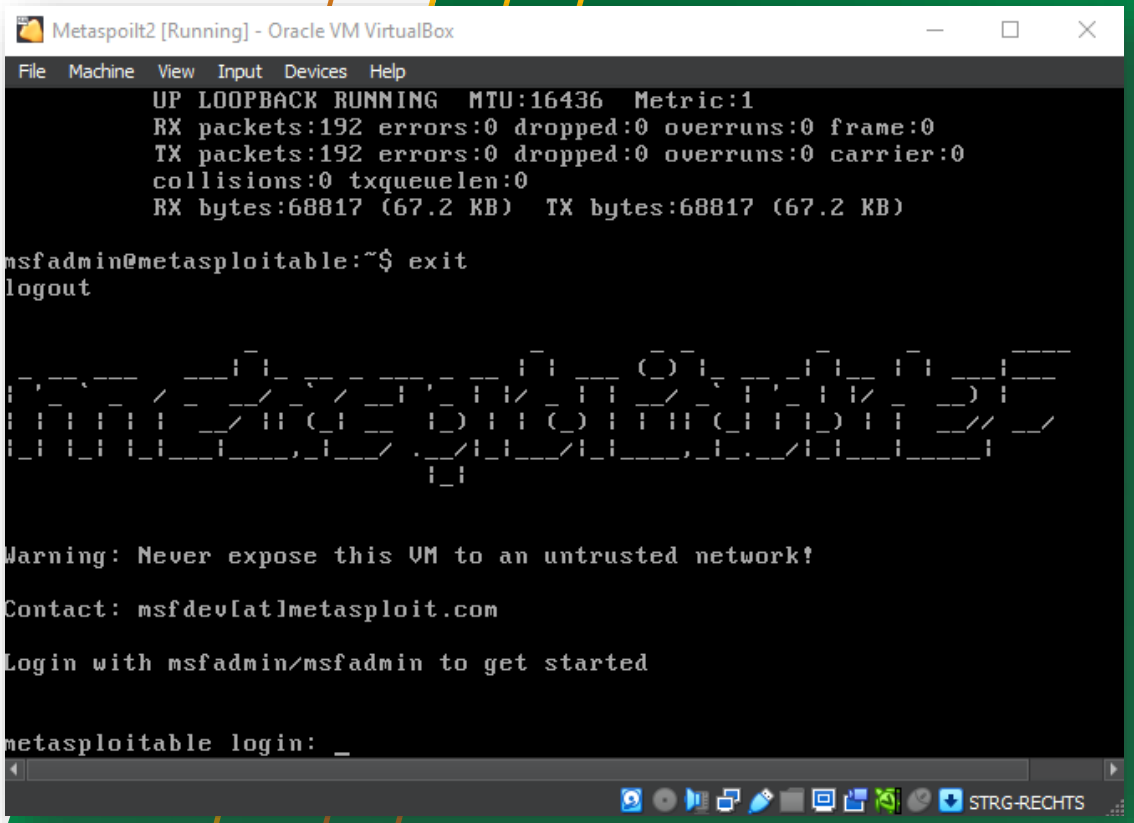
Metasploitable

What is Metasploitable?

The world's most widely used penetration testing framework.

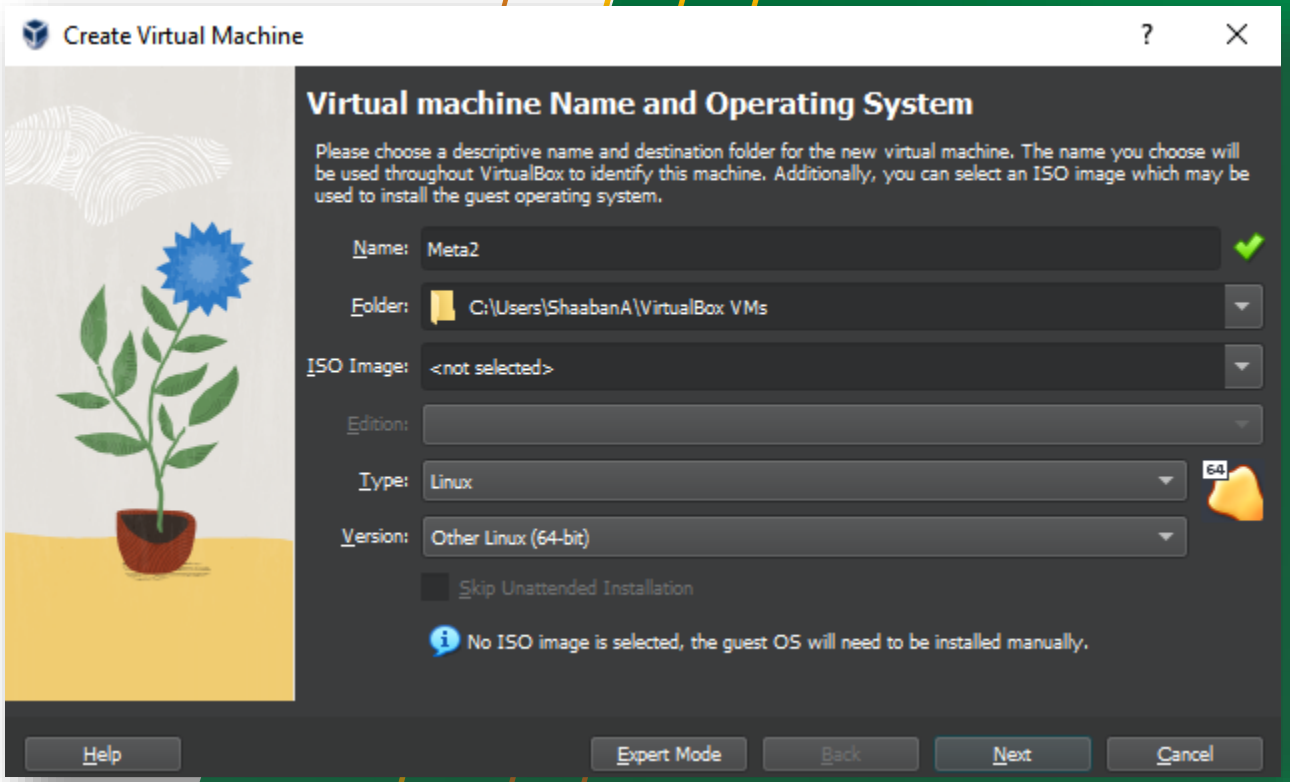
You can download it from the following link.

Metasploitable 2 | Metasploit Documentation (rapid7.com)

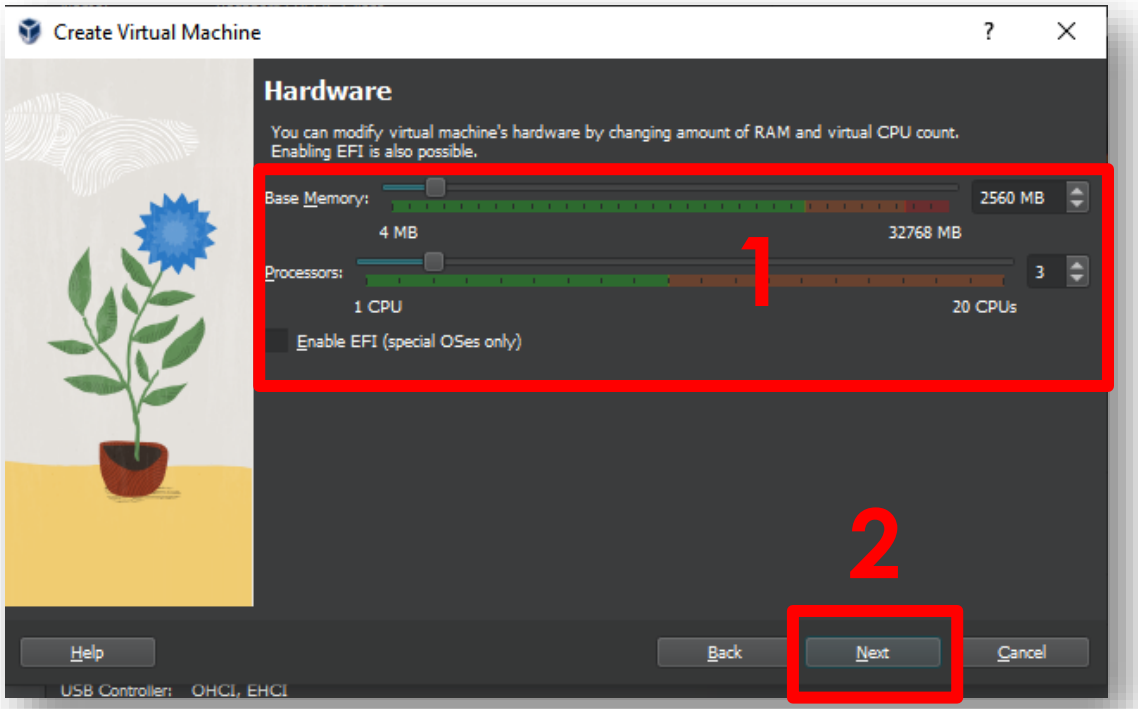


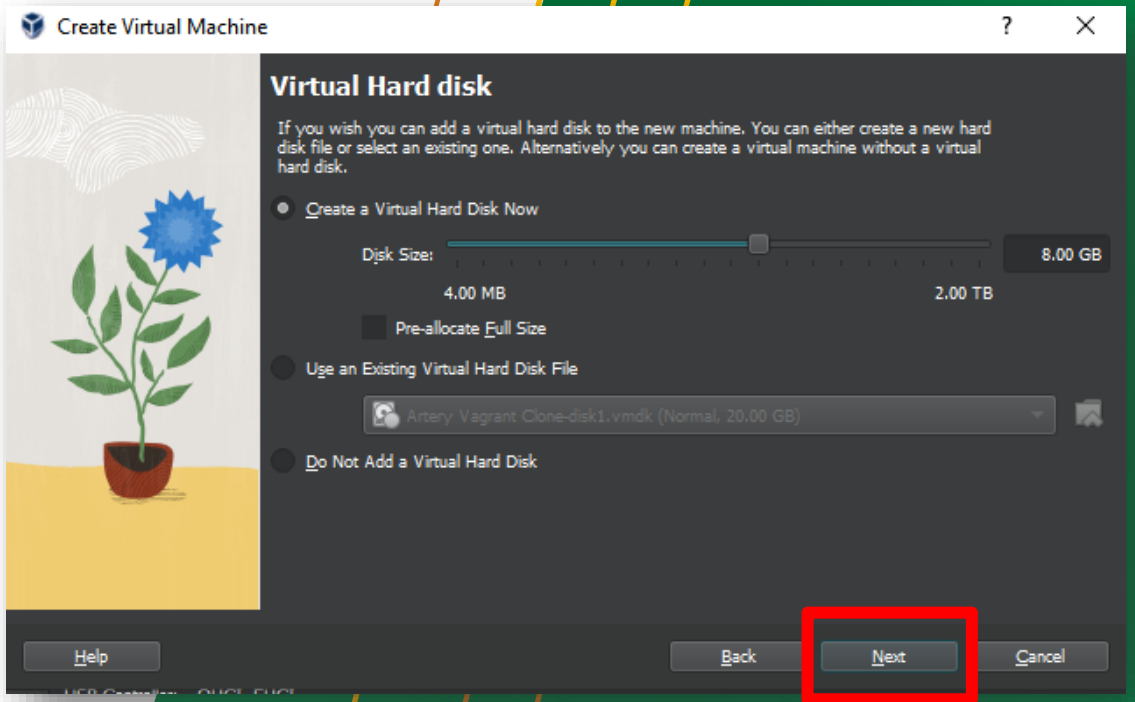
https://www.metasploit.com

Installing Metasploitable

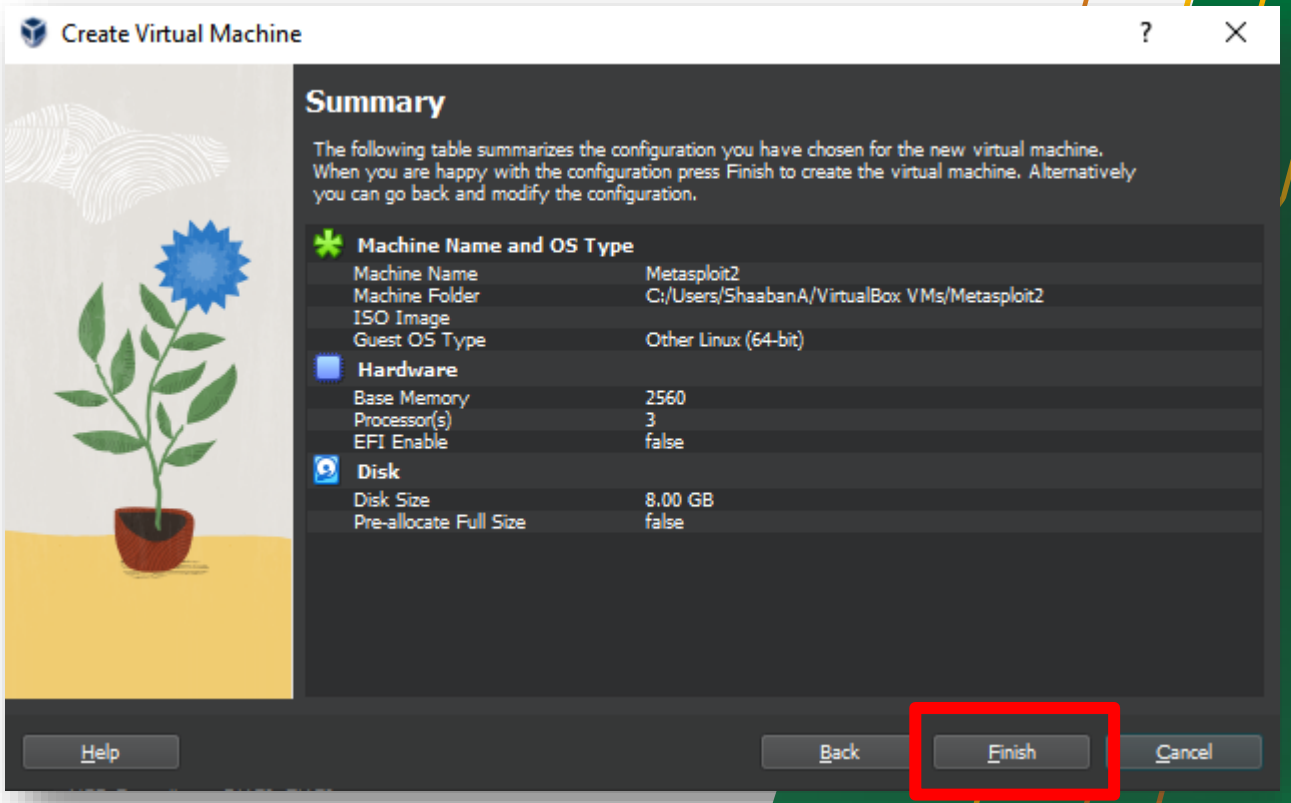


Installing Metasploitable

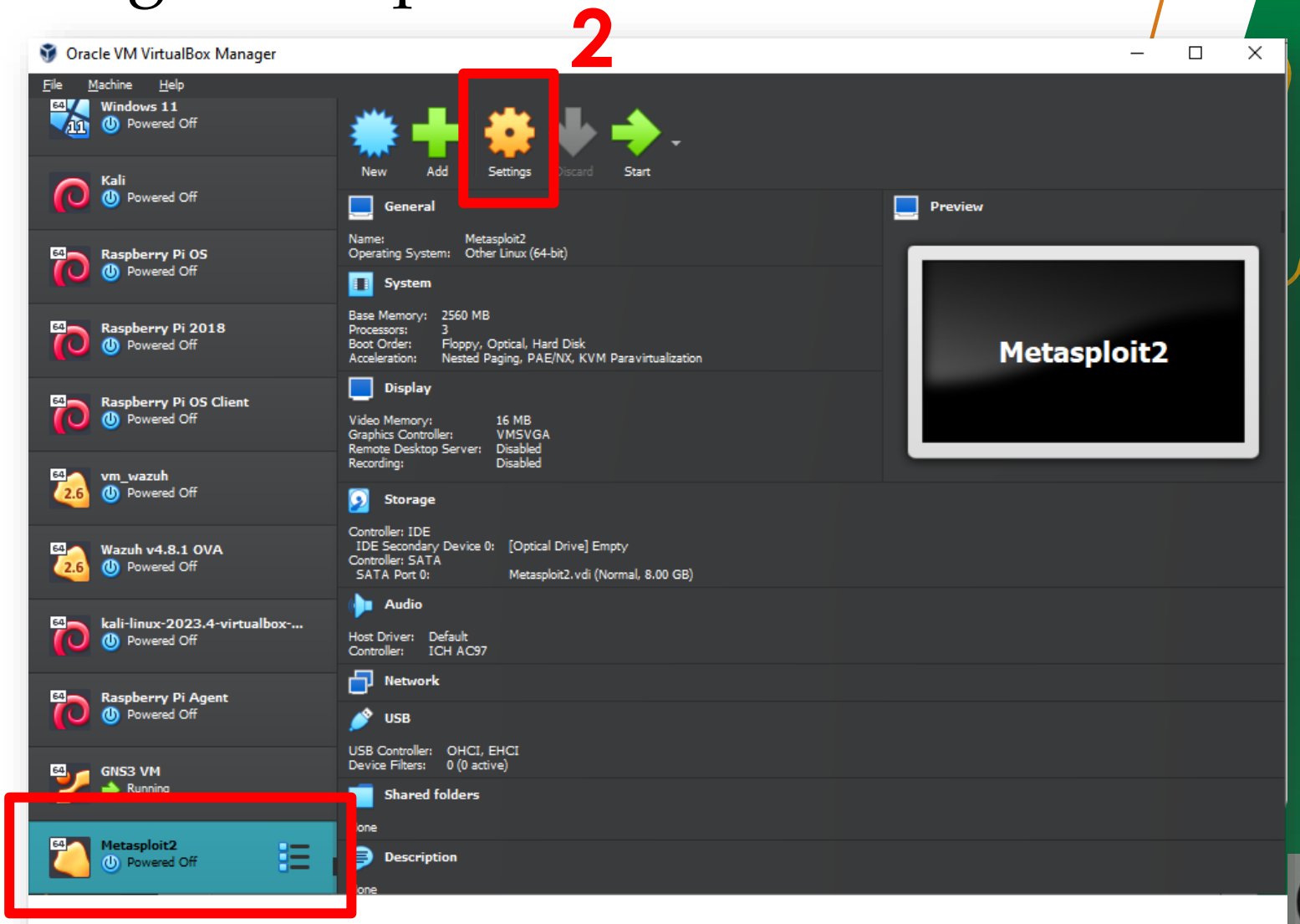




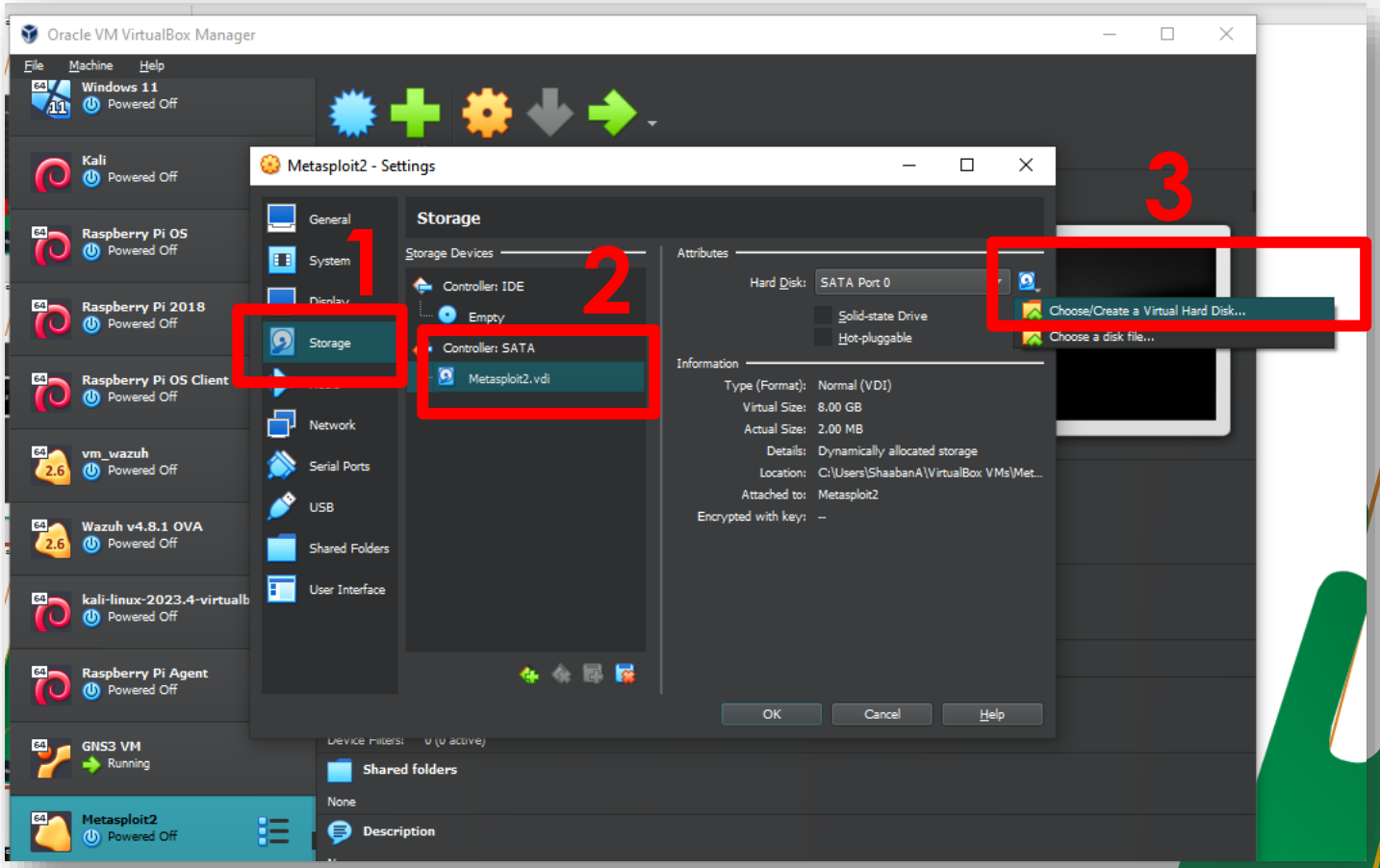
Installing Metasploitable



Installing Metasploitable

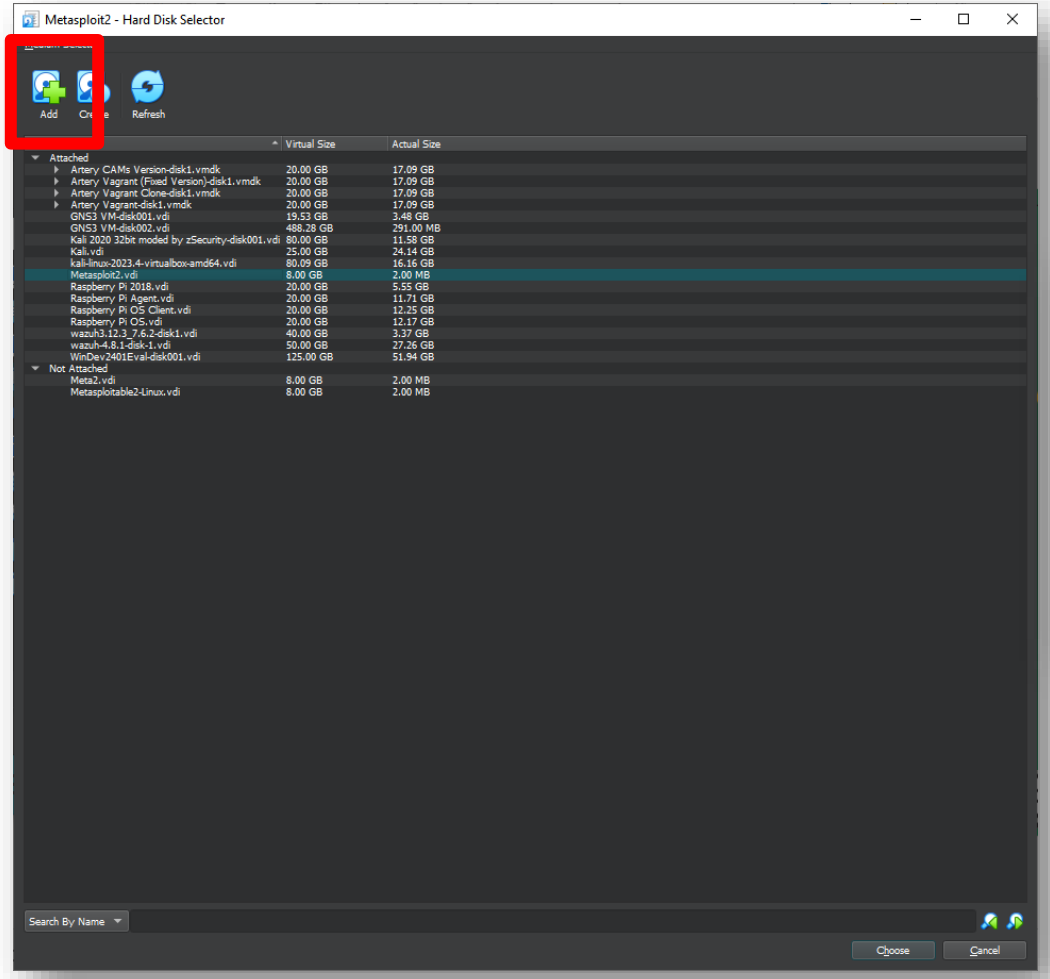


Installing Metasploitable



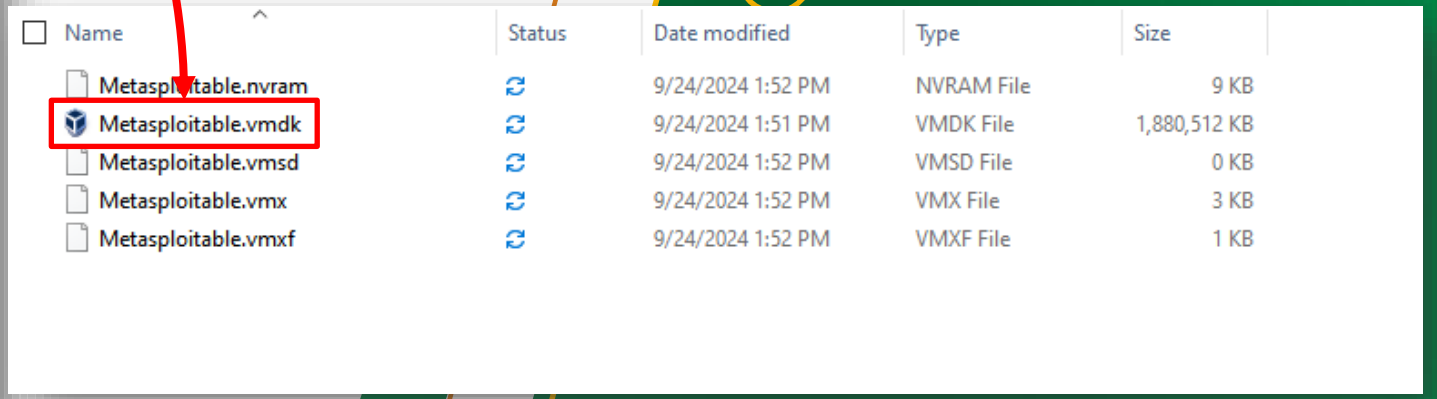
Installing Metasploitable

Add the Metasploitable VM file that you downloaded.

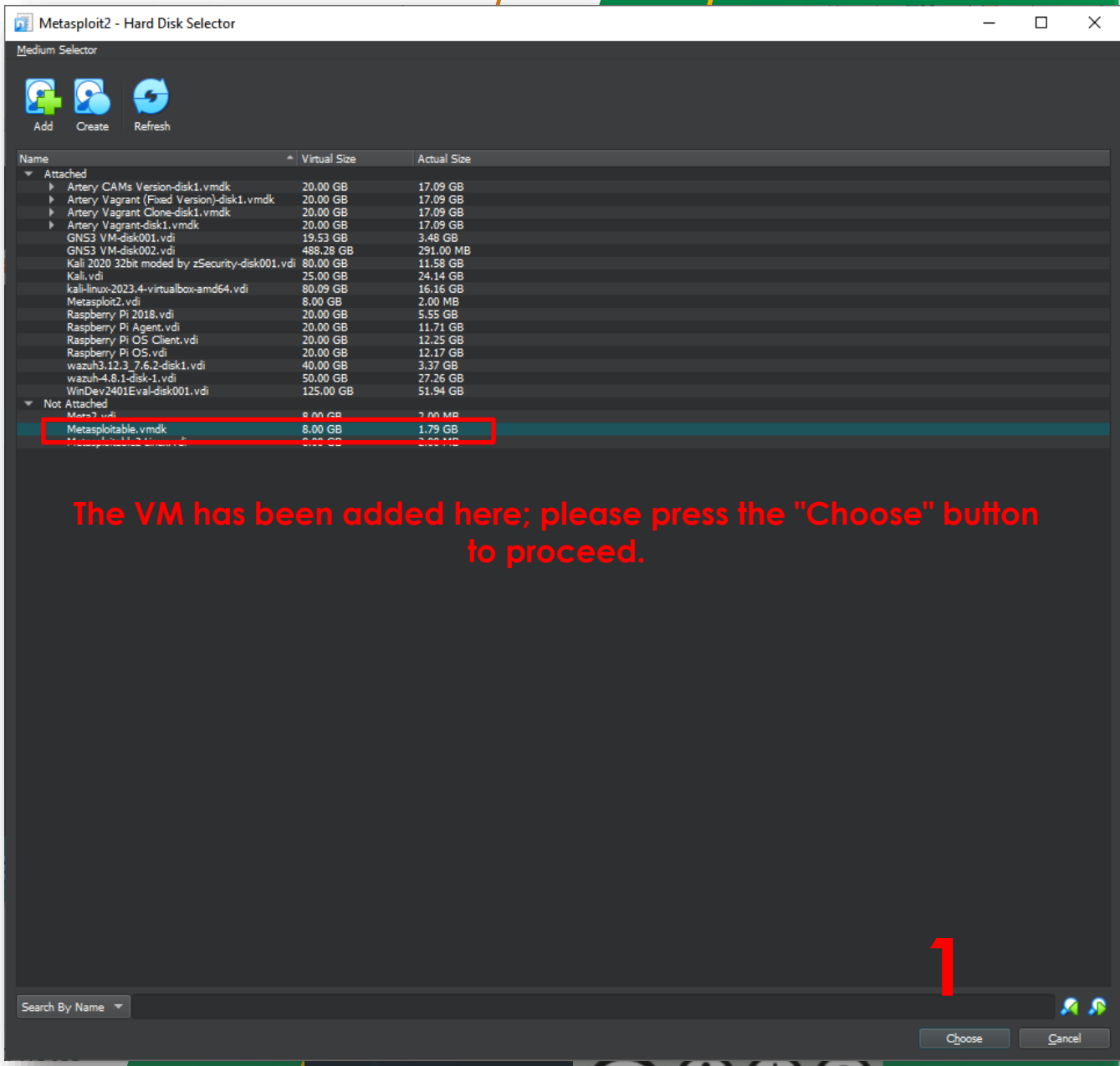


Select this file

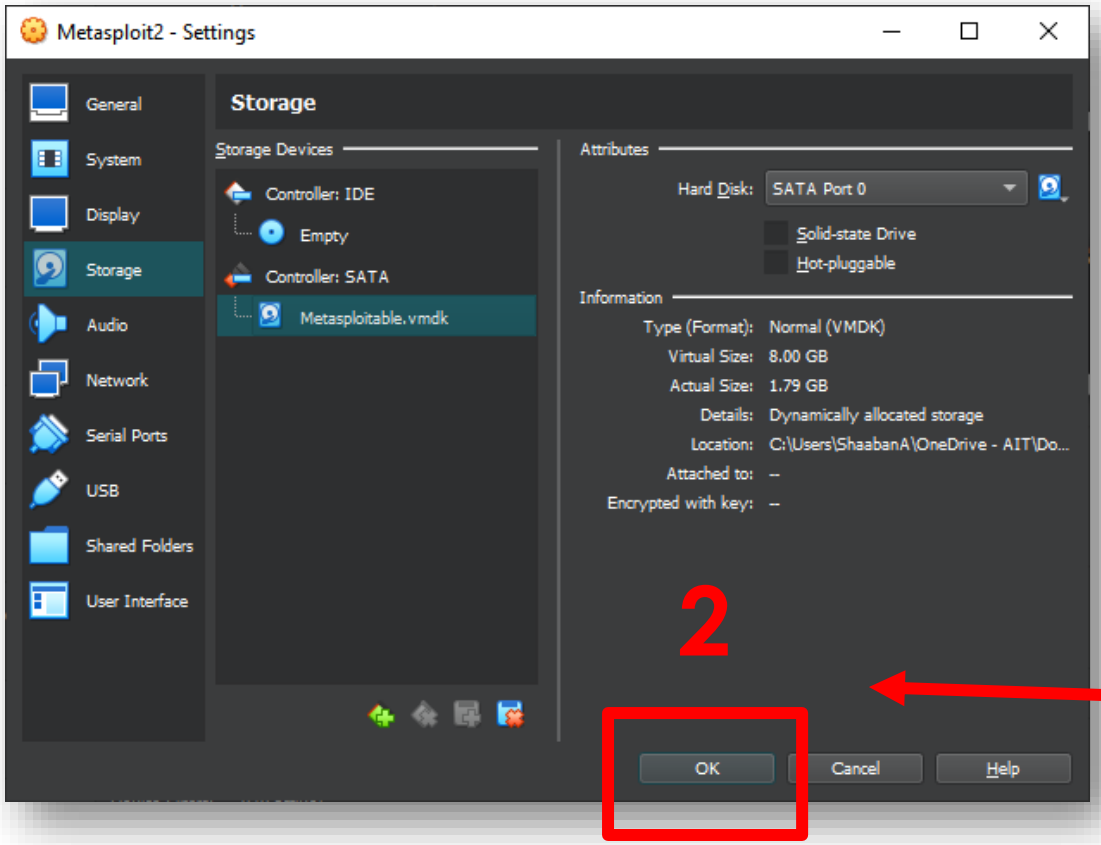
Here are the contents of the Metasploit ZIP file.

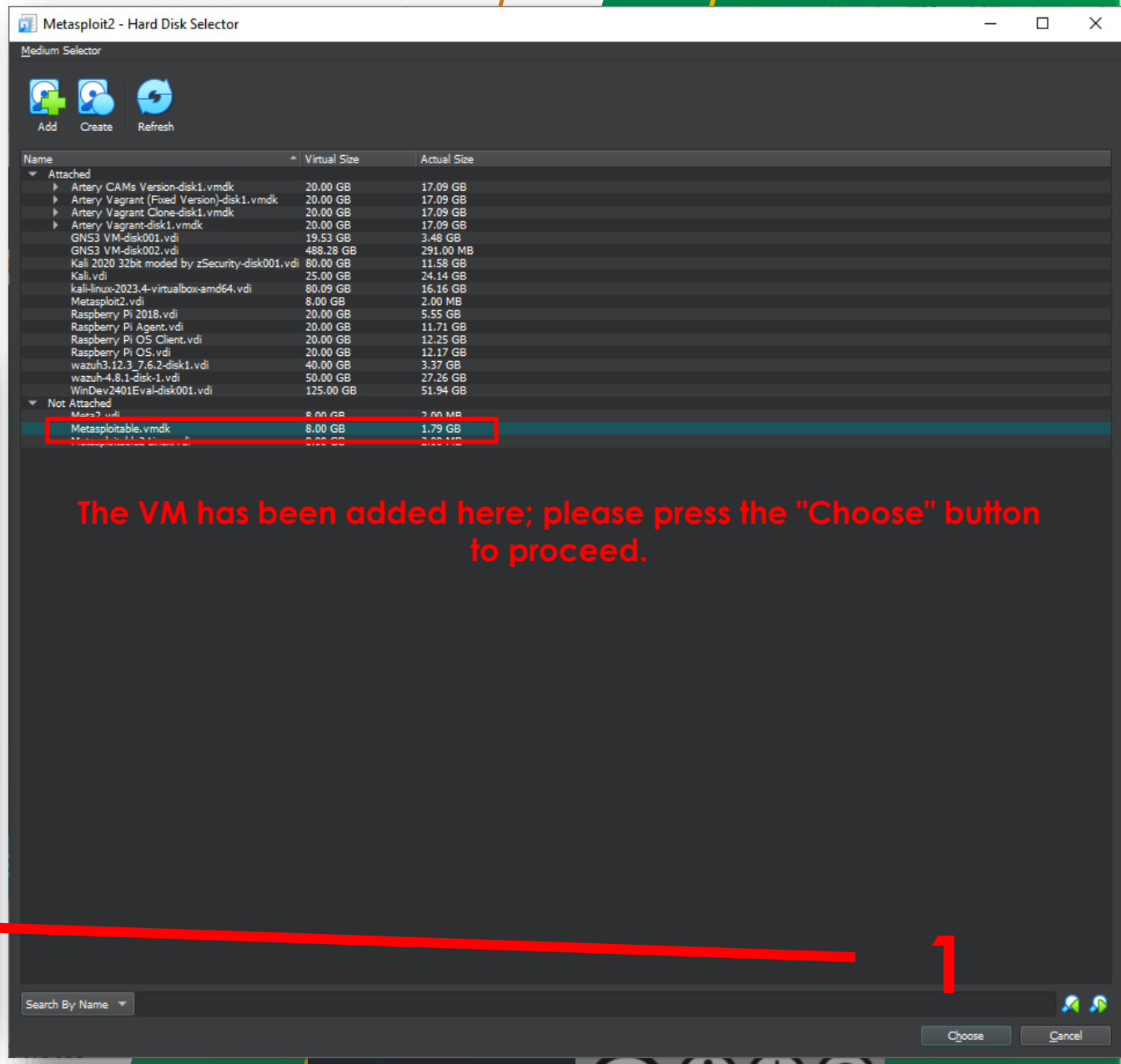


Installing Metasploitable



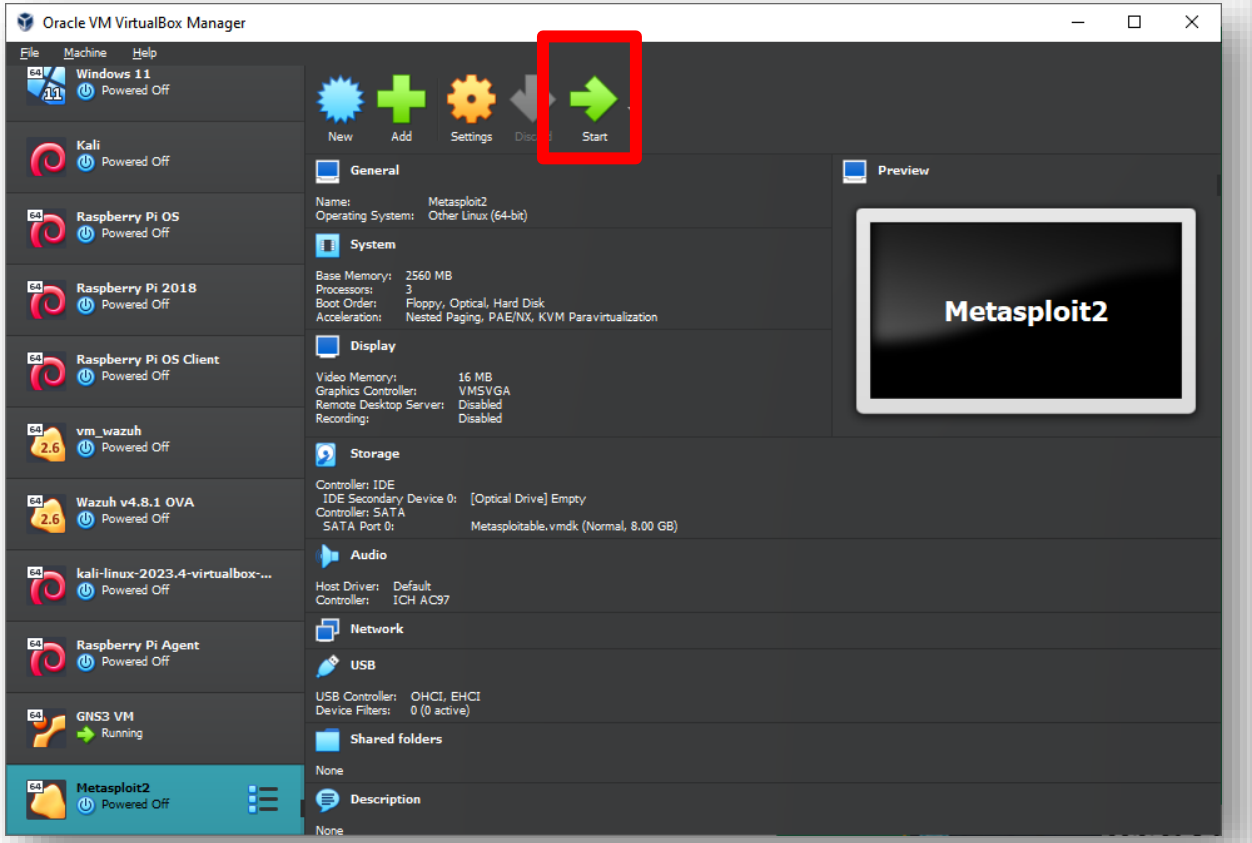
Installing Metasploitable



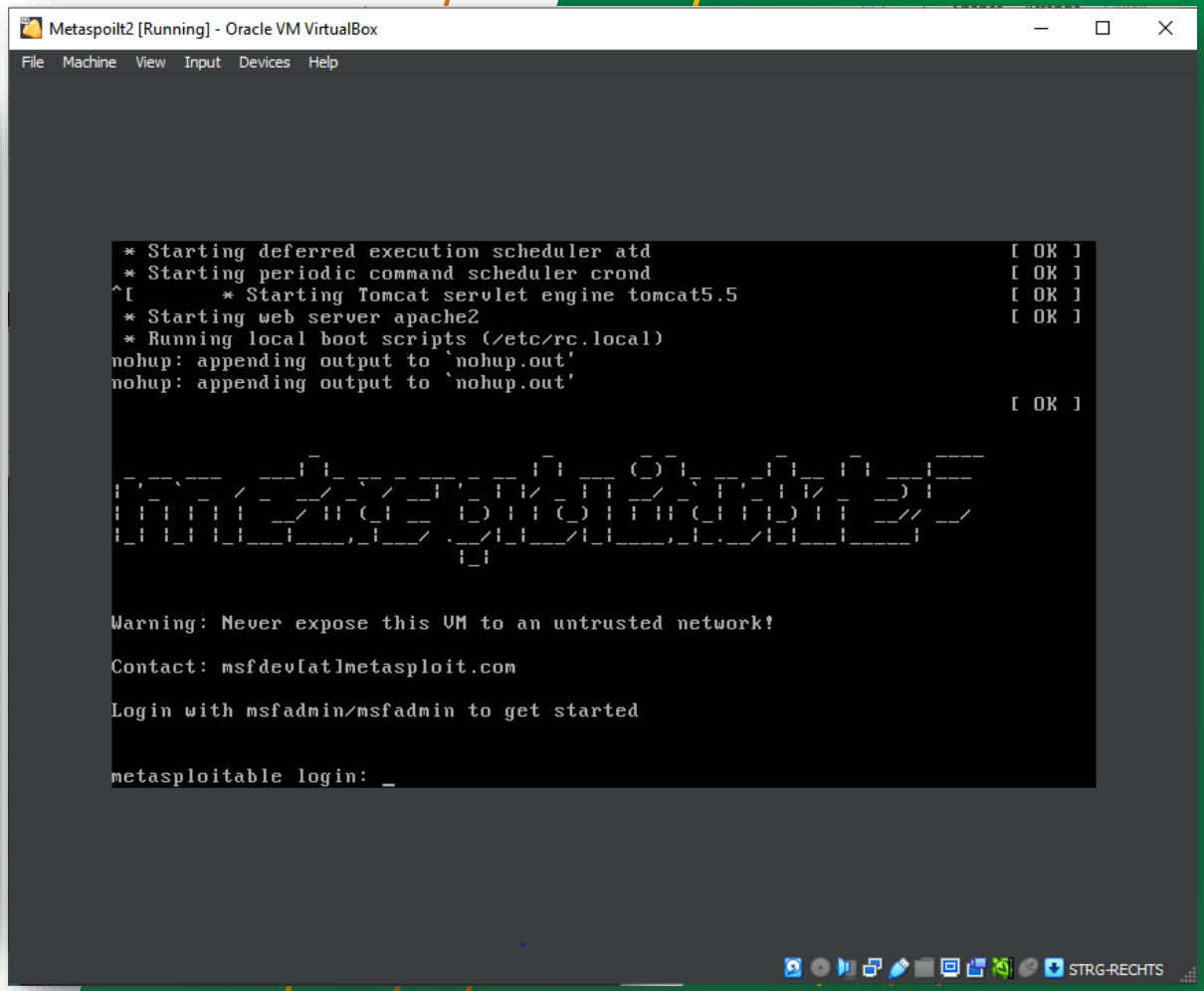


Starting the Metasploitable VM

Start the Metasploit VM

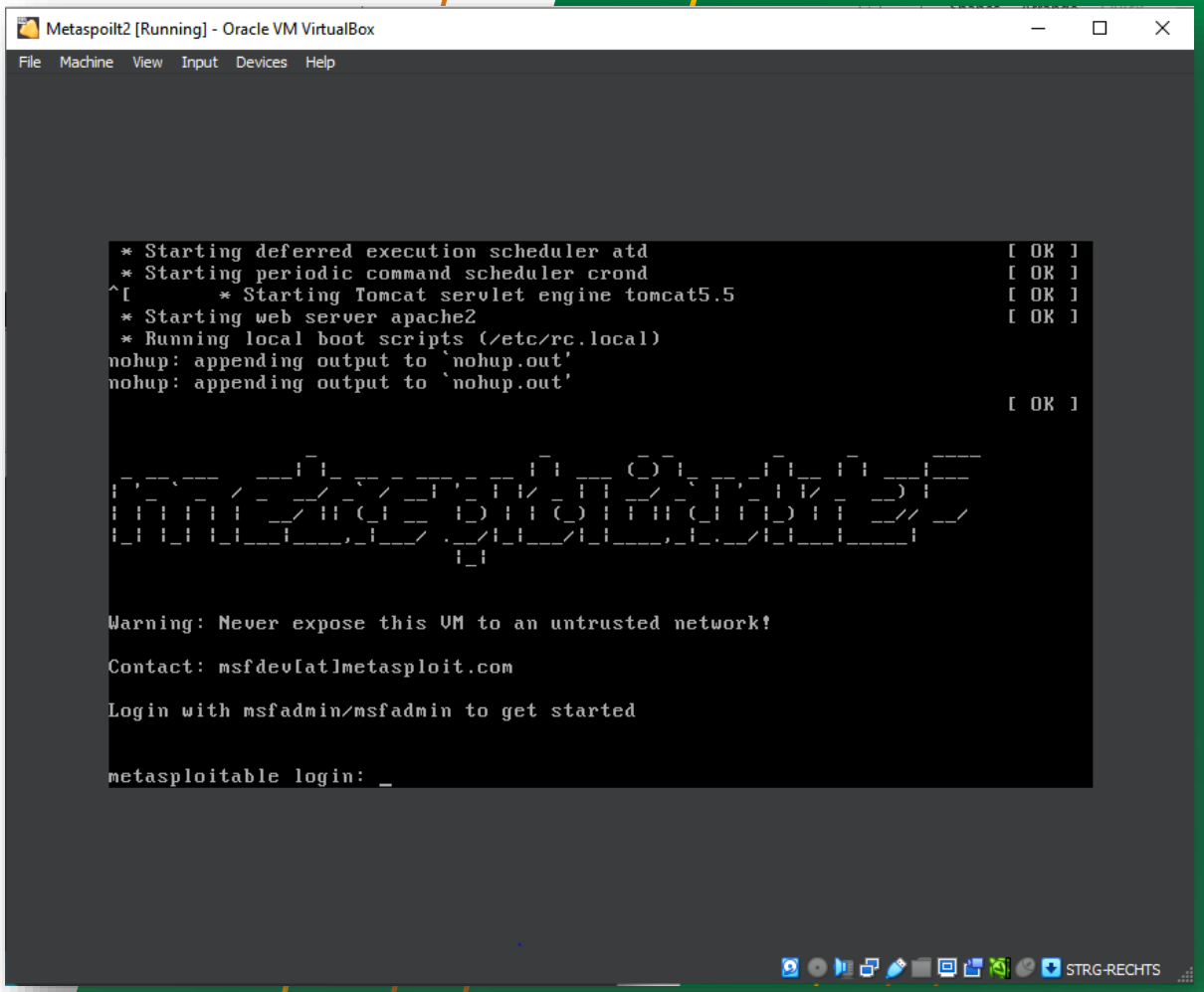


The Metasploit VM is now running successfully on your computer.



Starting the Metasploitable VM

Login: msfadmin
Password: msfadmin



Wazuh

Installing Wazuh Server

- Wazuh **provides** a pre-built **virtual machine image** in **Open Virtual Appliance** (**OVA**) format. This can be directly **imported** to **VirtualBox** or other **OVA-compatible virtualization systems**. Take into account that this **VM** only runs on **64-bit systems**. It does **not provide high availability** and **scalability** out of the box. However, these can be **implemented** by using **distributed** deployment.

- Select the **Wazuh version** from the **top-right part** of the page.

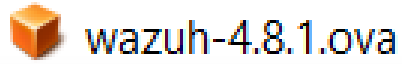
- Then **download** the virtual appliance (OVA), which **contains** the following **components**:
  - Amazon Linux 2
  - Wazuh manager 4.8.1
  - Wazuh indexer 4.8.1
  - Filebeat-OSS 7.10.2
  - Wazuh dashboard 4.8.1

- More details about the **installation** can be found on the Wazuh documentation page.

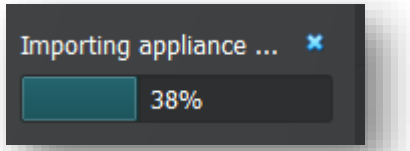
Virtual Machine (OVA) - Installation alternatives (wazuh.com)

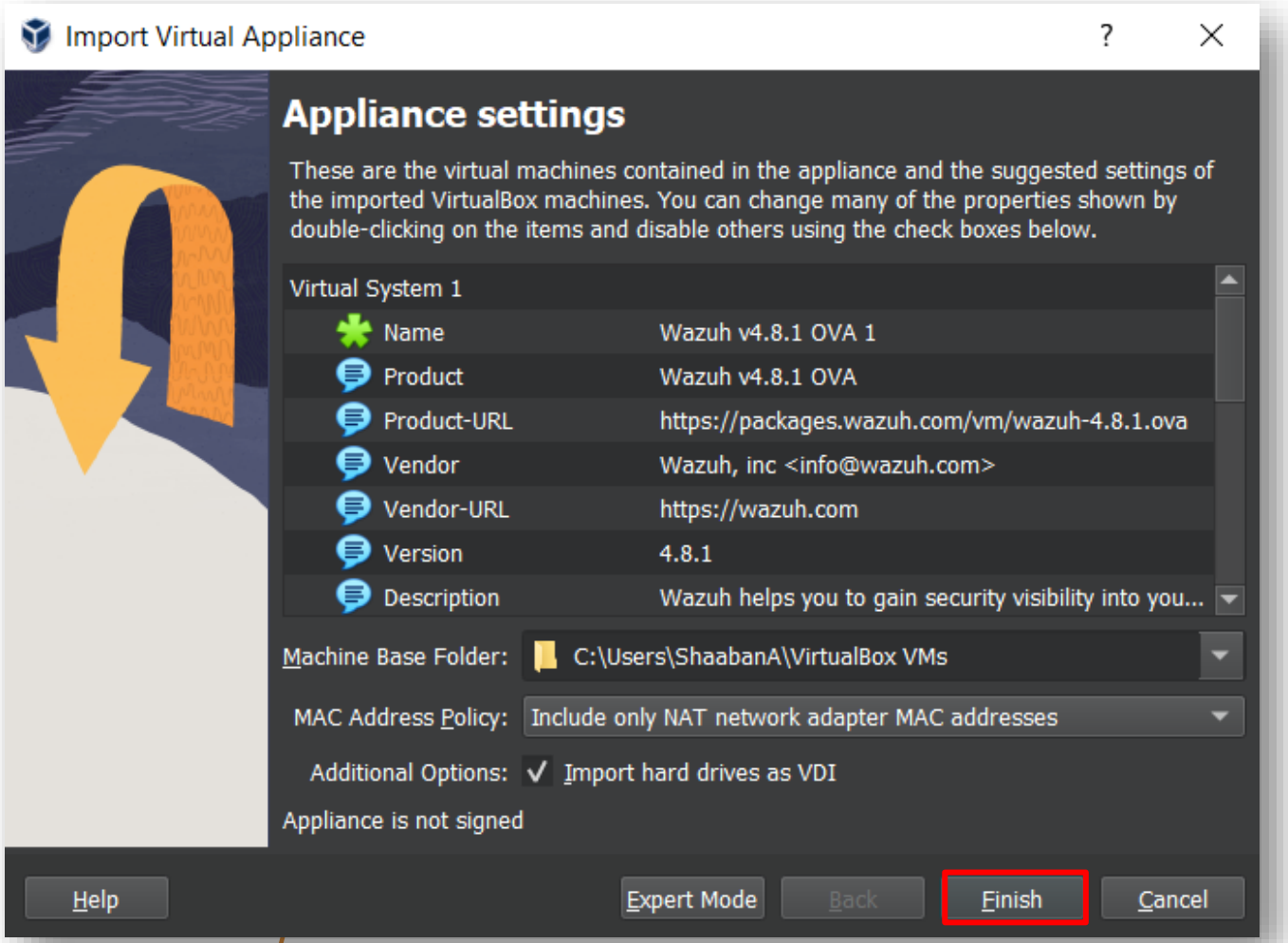
Installing Wazuh Server

- Navigate to the **downloaded .ova** file and **double-click** on it.



- Press **Finish** and then **wait** until the **VM** is **successfully** imported.



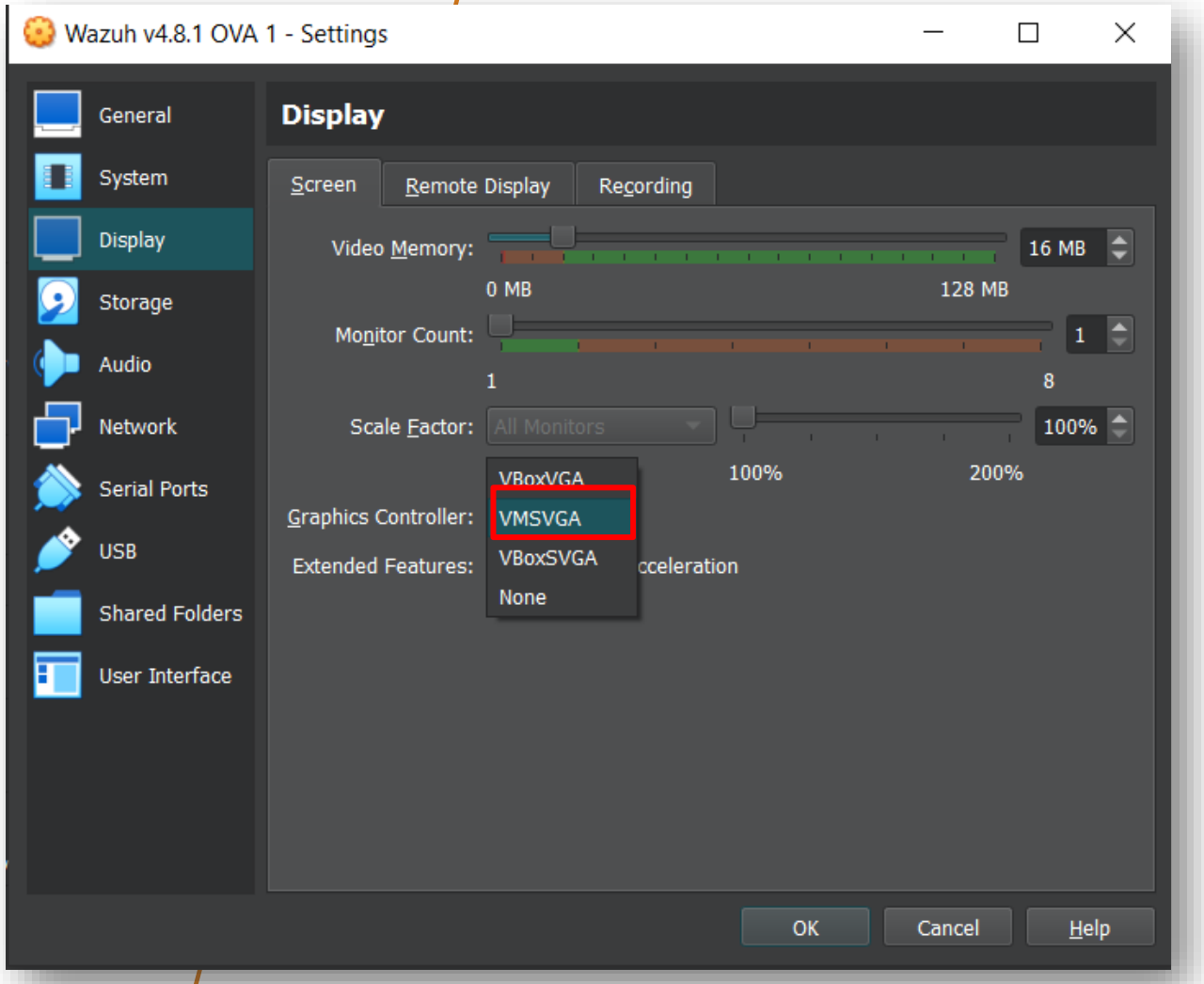


Installing Wazuh Server

- Select the **imported** VM of Wazuh, and go to **Settings** > **Display**.

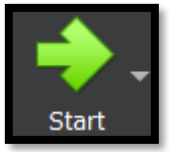
- Selct the **VMSVGA** in the **Graphics Controller.**

- Press **ok**

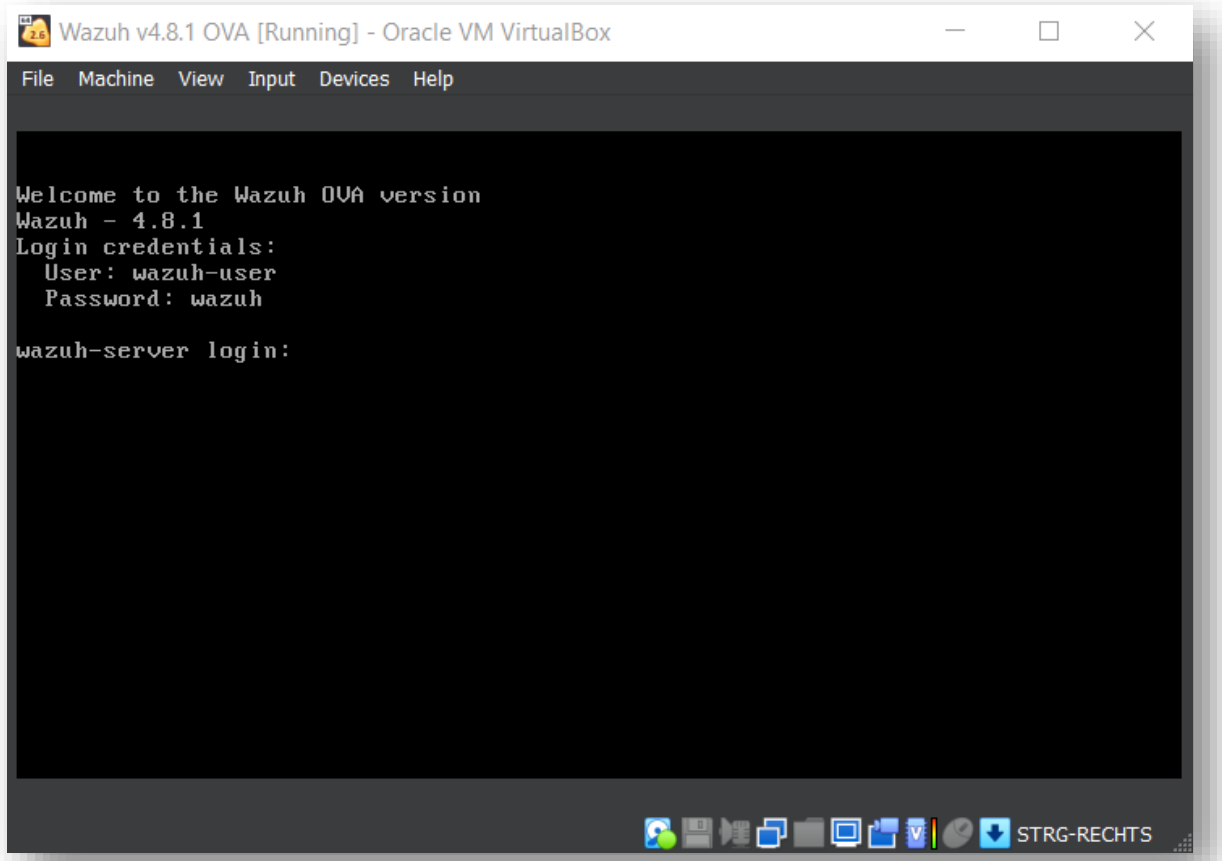


Launching Wazuh Server

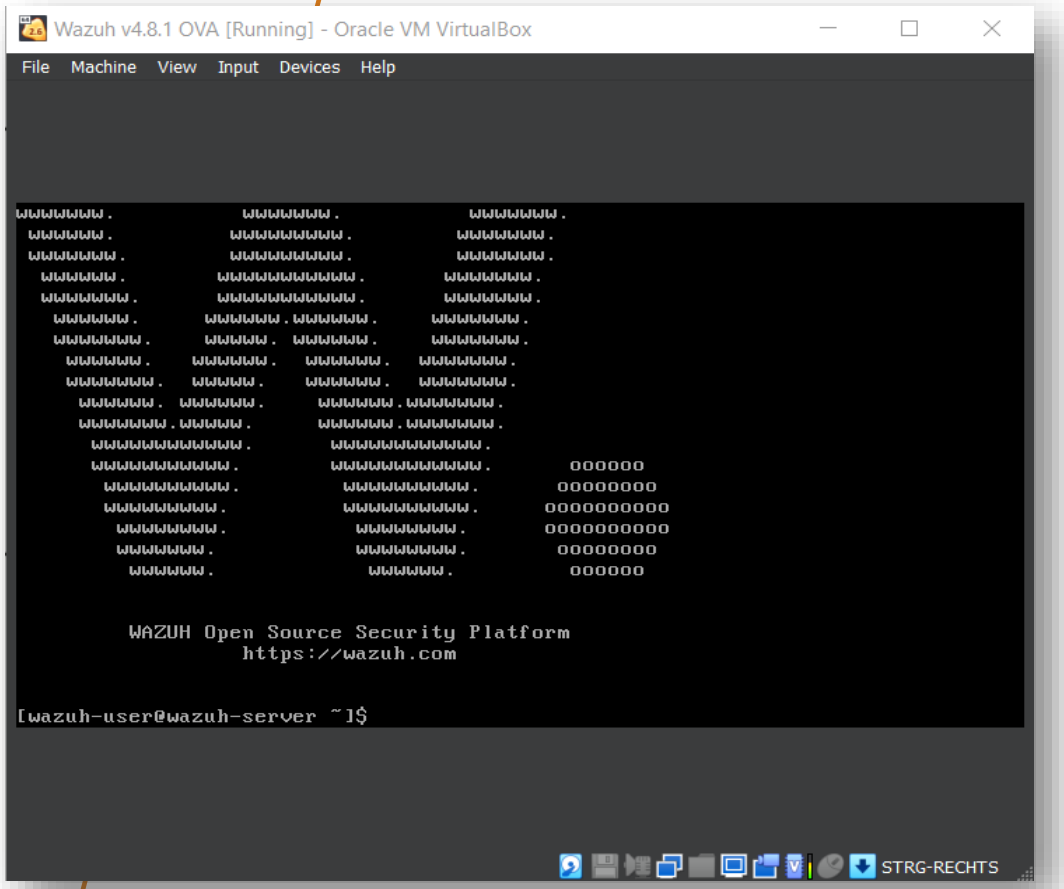
Press the **start button**.



Wait until you reach the **login** screen.



- Enter the **user** and **password**.
- **By default**:
  - **User**: wazuh-user
  - **Password**: wazuh

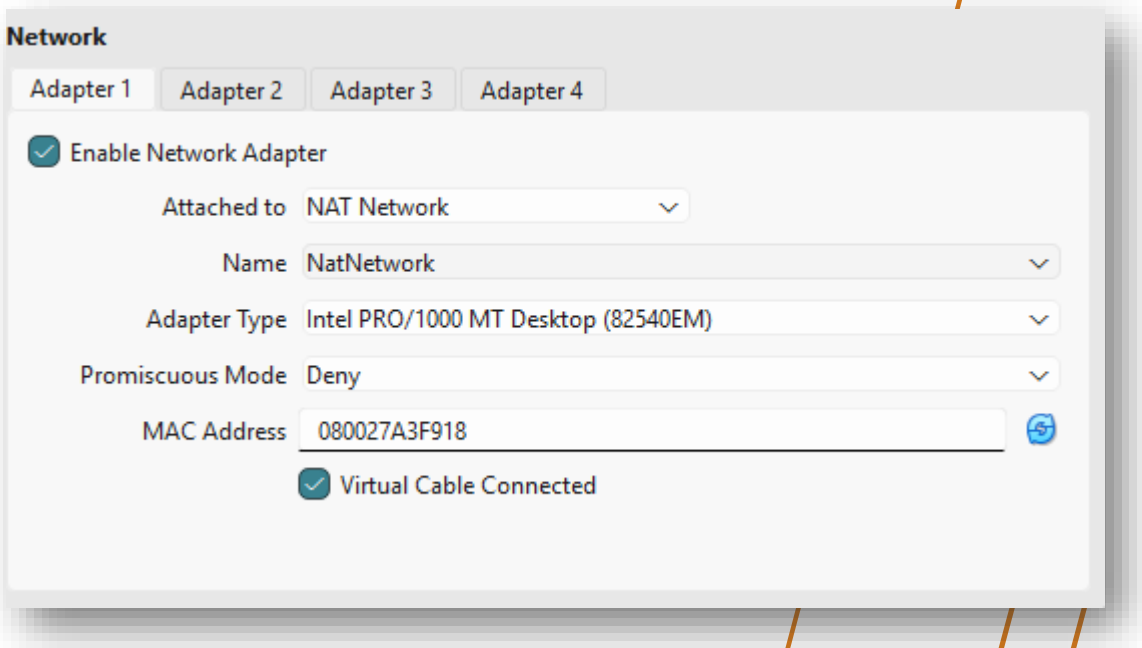


The Wazuh server has been **successfully installed** and **launched**.

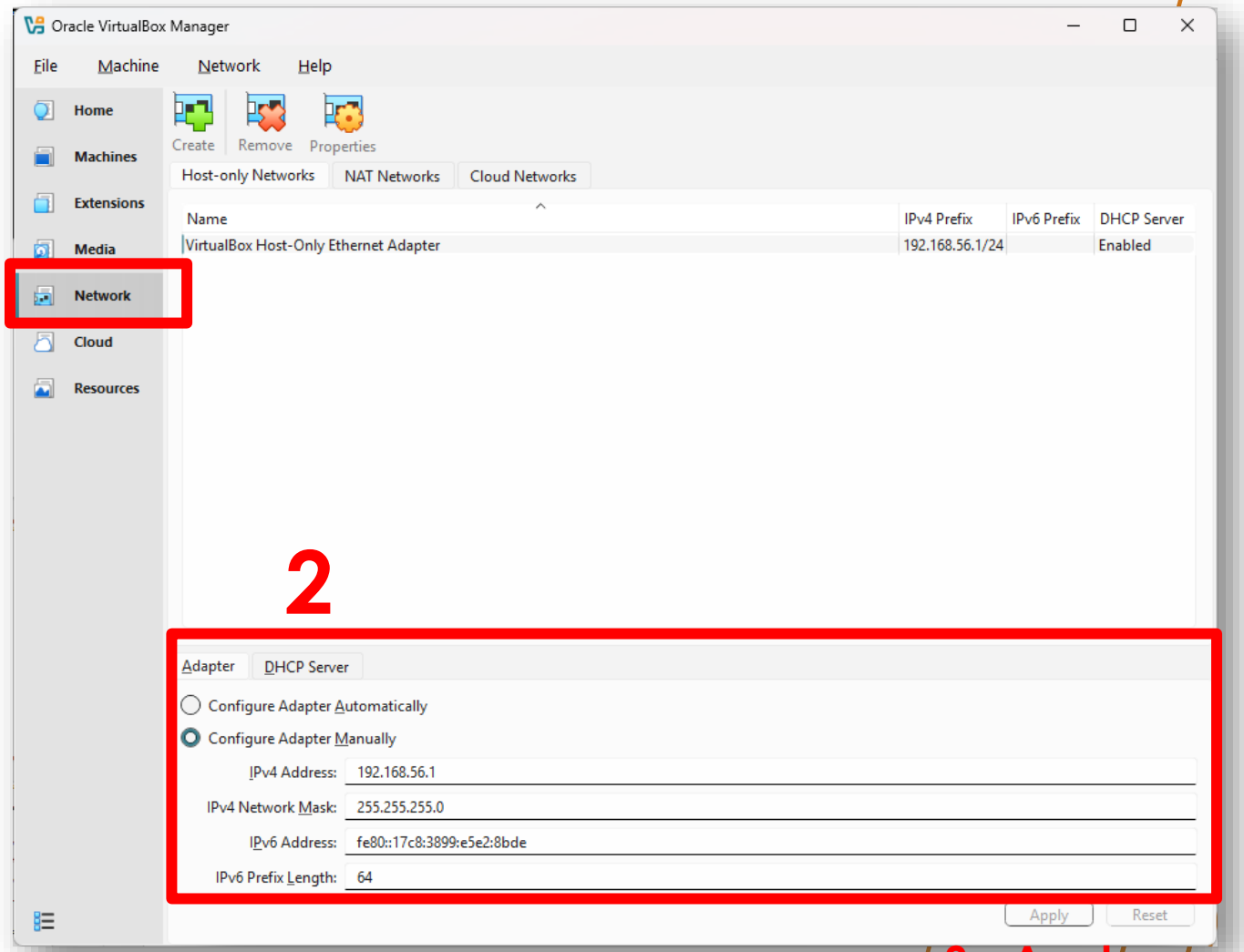
NAT Network

NAT Network Configuration

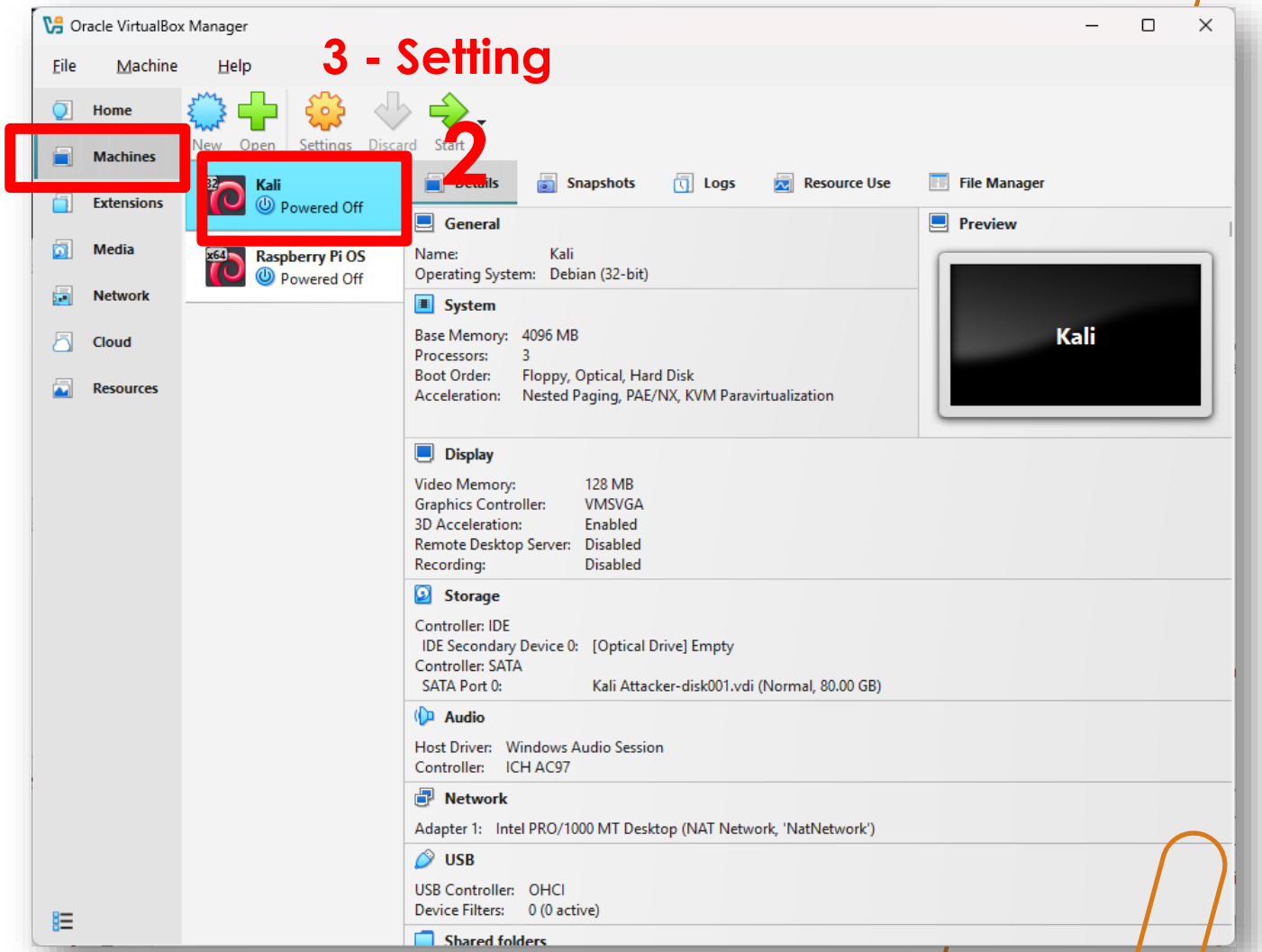
- We want to ensure that all devices in this lab are reachable.
- The network configuration for each VM in this lab should use the NAT network as follows:



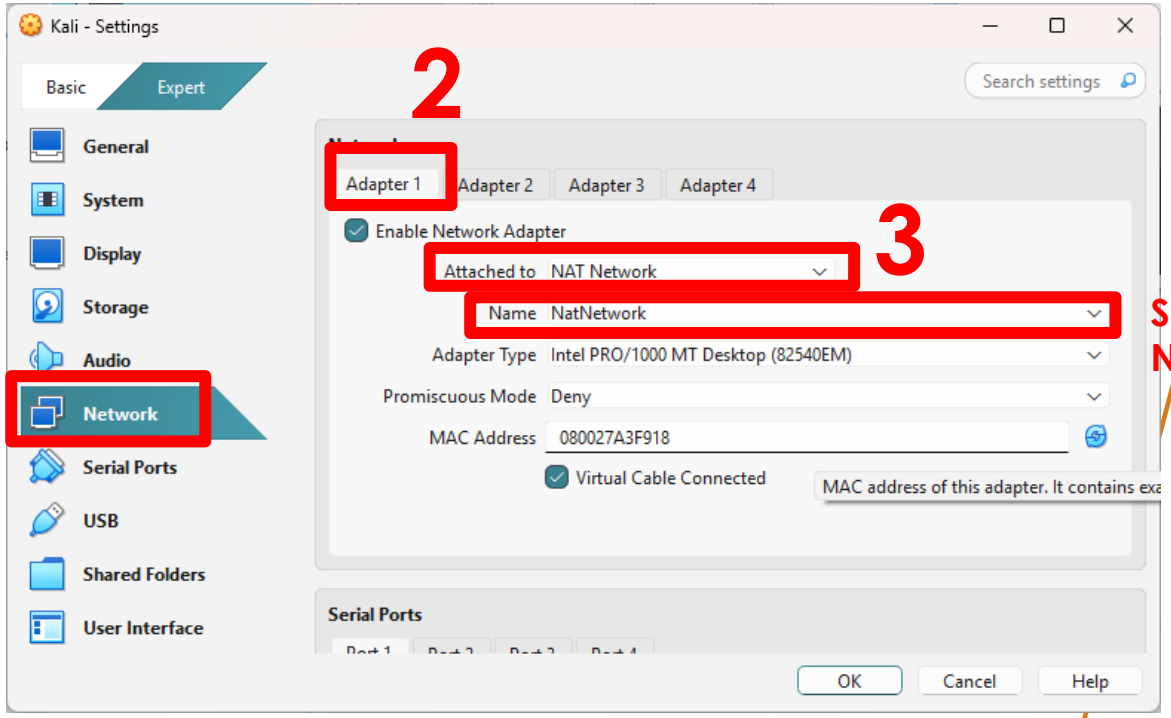
NAT Network Configuration



NAT Network Configuration



NAT Network Configuration



Select the NAT Network Name, as created before

Virtual Lab Summary

- As outlined in this guide, you will need to set up a Lab with a set of VMs.
- Please ensure that your installation is **fully completed before the lecture date, January 22nd**, our planned start date. This will help ensure a smooth beginning and prevent any delays or technical challenges during the sessions.
- To provide a comprehensive understanding of how to simulate a real-world network, we will use a diverse set of virtual machines. This includes:
  - **Client and Server VMs**: To demonstrate communication flows and observe how an attacker might intercept or compromise these systems.
  - **Metasploit Server**: To explore how known vulnerabilities can be exploited within a networked server environment.
  - **Wazuh Server**: To detect and monitor suspicious activity across the network.
  - **Kali Admin VM**: To simulate an administrator's device capable of detecting unusual behavior and performing security monitoring.
  - **Kali Attacker VM**: To carry out penetration testing and simulate various attack scenarios.
- As shown, several machines are involved in our practical activities to support both **offensive and defensive cybersecurity scenarios**.
- However, if your system has resource limitations, please ensure that you install **at a minimum**:
  - **One Kali Linux VM (attacker)**
  - **One victim/client machine**
  - **The Wazuh server**

Thank you

Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at