INSTALLATION OF METASPLOITABLE 2 IN UTM

Report By - Mubasshera Zaidy

INTRODUCTION

Metasploitable 2 is a purpose-built, intentionally vulnerable Linux-based virtual machine developed by Rapid7 to facilitate cybersecurity training and research. It serves as a controlled environment for testing penetration techniques, conducting vulnerability assessments, and exploring exploit development without compromising real-world systems. Its deployment is essential for simulating attack scenarios, enhancing threat detection capabilities, and reinforcing defensive strategies in a safe and legal manner.

OBJECTIVE

The primary objectives of installing Metasploitable 2 are:

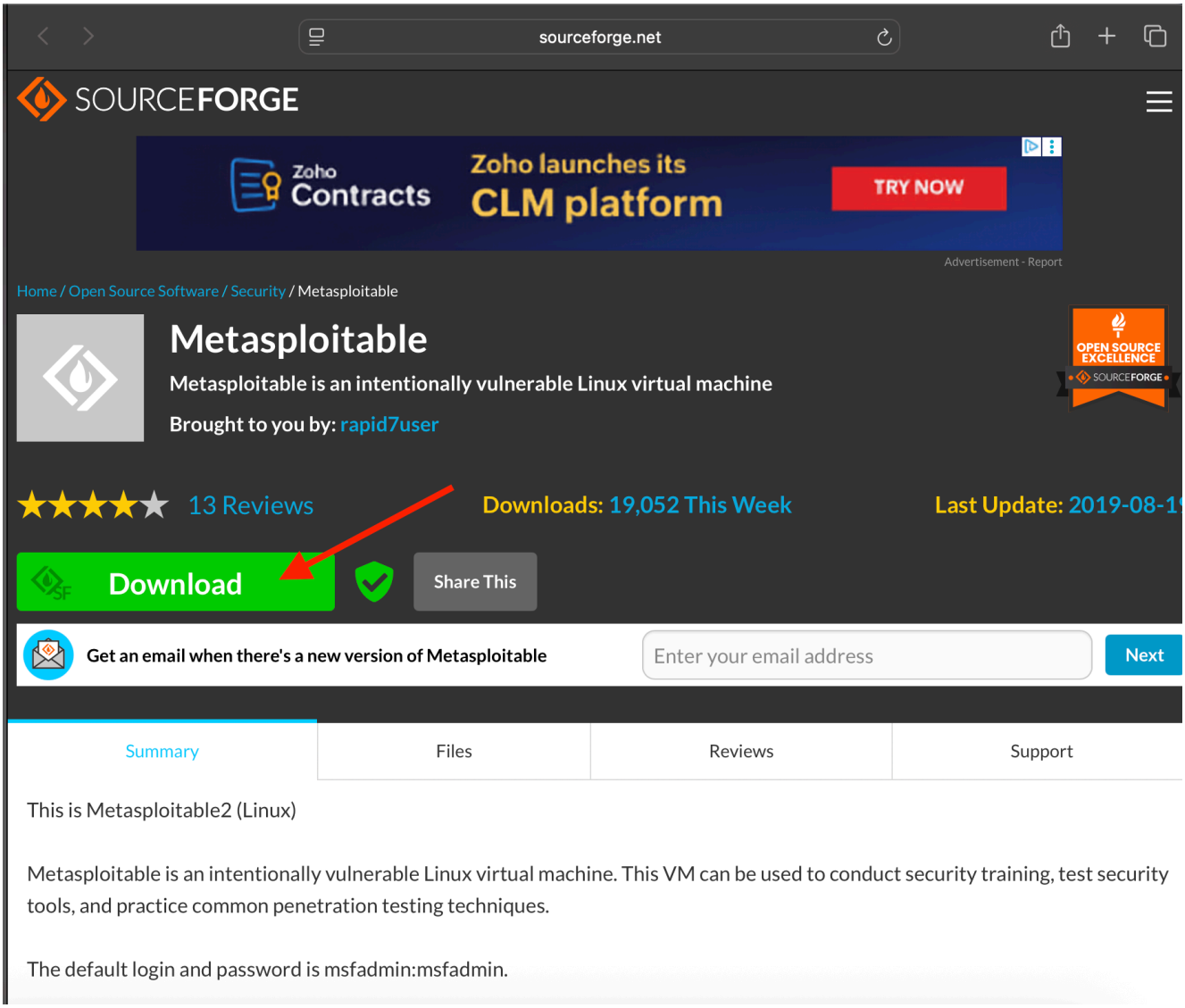
- To provide a controlled environment for learning and testing penetration techniques.
- To simulate vulnerable services and applications for exploit development.
- To support Red Team and Blue Team exercises in cybersecurity training.
- To integrate with tools like Metasploit Framework and Kali Linux for hands-on Practice.

FEATURES OF UTM

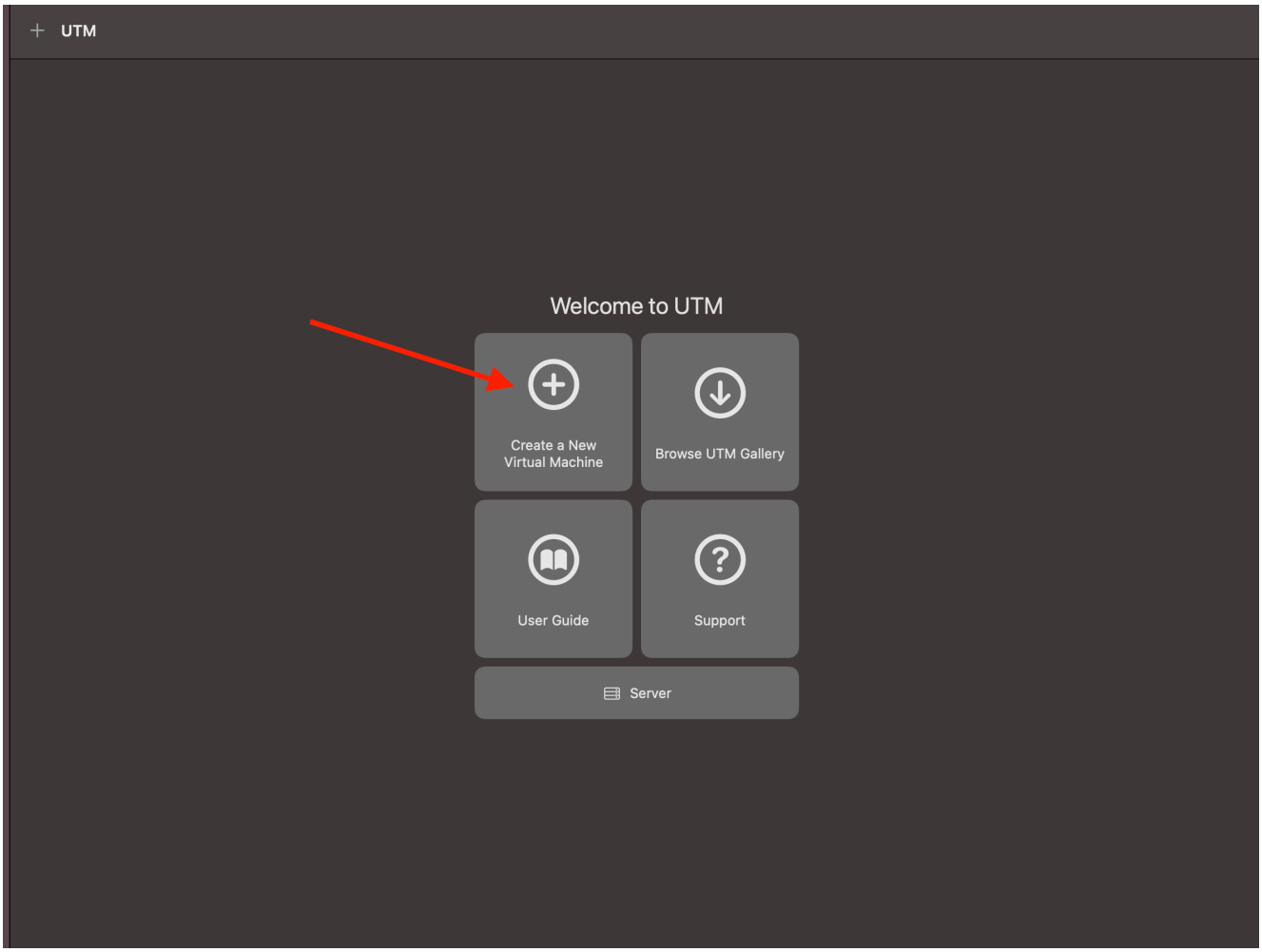
- Compatible with major hypervisors (VirtualBox, VMware Workstation/Player)
- Pre-configured virtual disk image (.vmdk) for quick deployment
- Host-only and NAT networking modes for safe, isolated testing
- Supports snapshot and rollback for repeatable exploit scenarios
- Lightweight resource footprint (512 MB RAM, 1 CPU recommended)
- Default credentials and vulnerable services pre-installed for immediate use

INSTALLATION OF METASPLOITABLE :

STEP 1 : Download metasploitable2 from sourceforge.net/projects/metasploitable

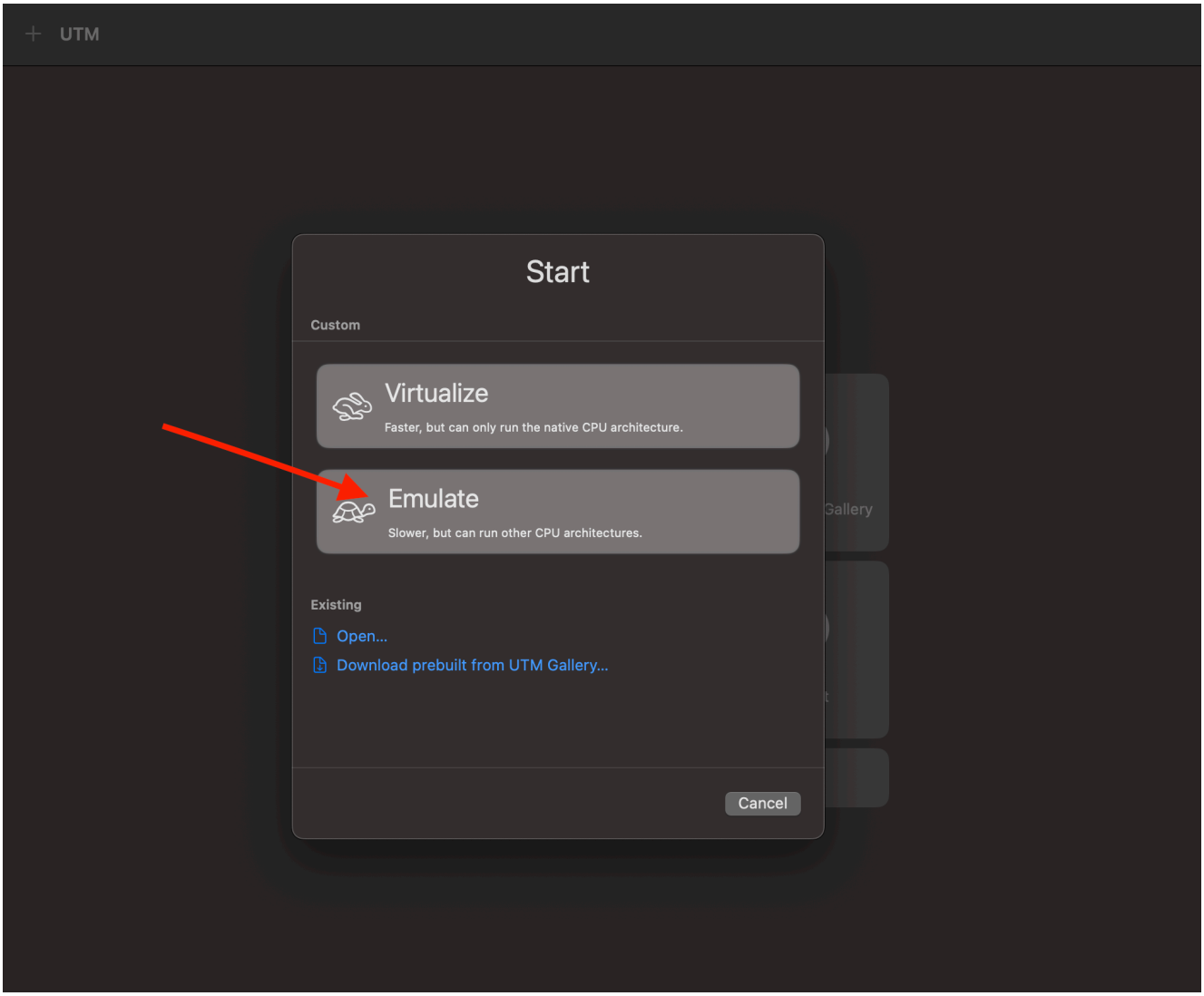


STEP 2 : Once downloaded , open UTM and click on ‘+ ’

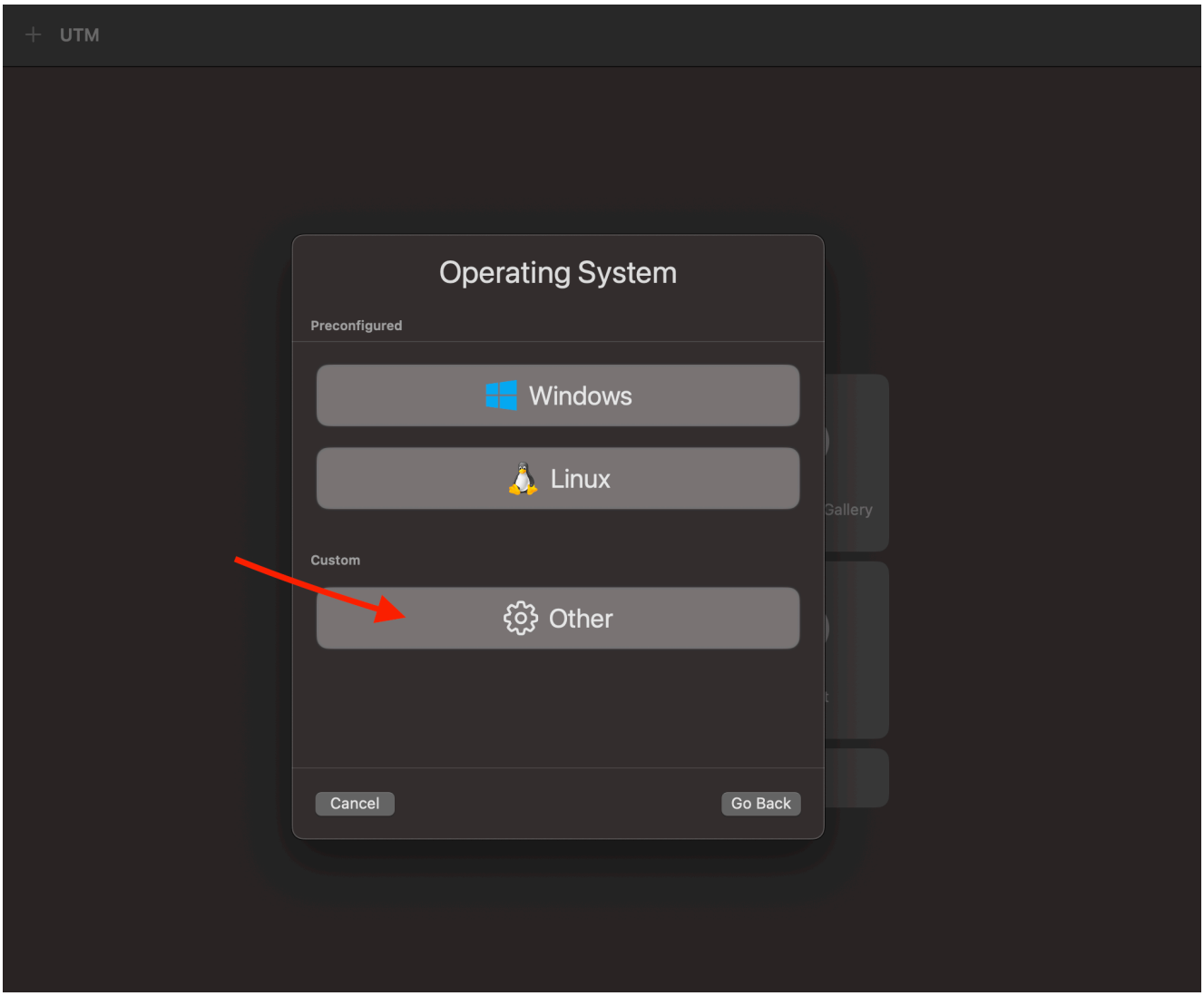


STEP 3 : Now click on ‘Emulate’ because Apple Silicon uses ARM architecture, while Metasploitable 2 is built for x86 (Intel/AMD).

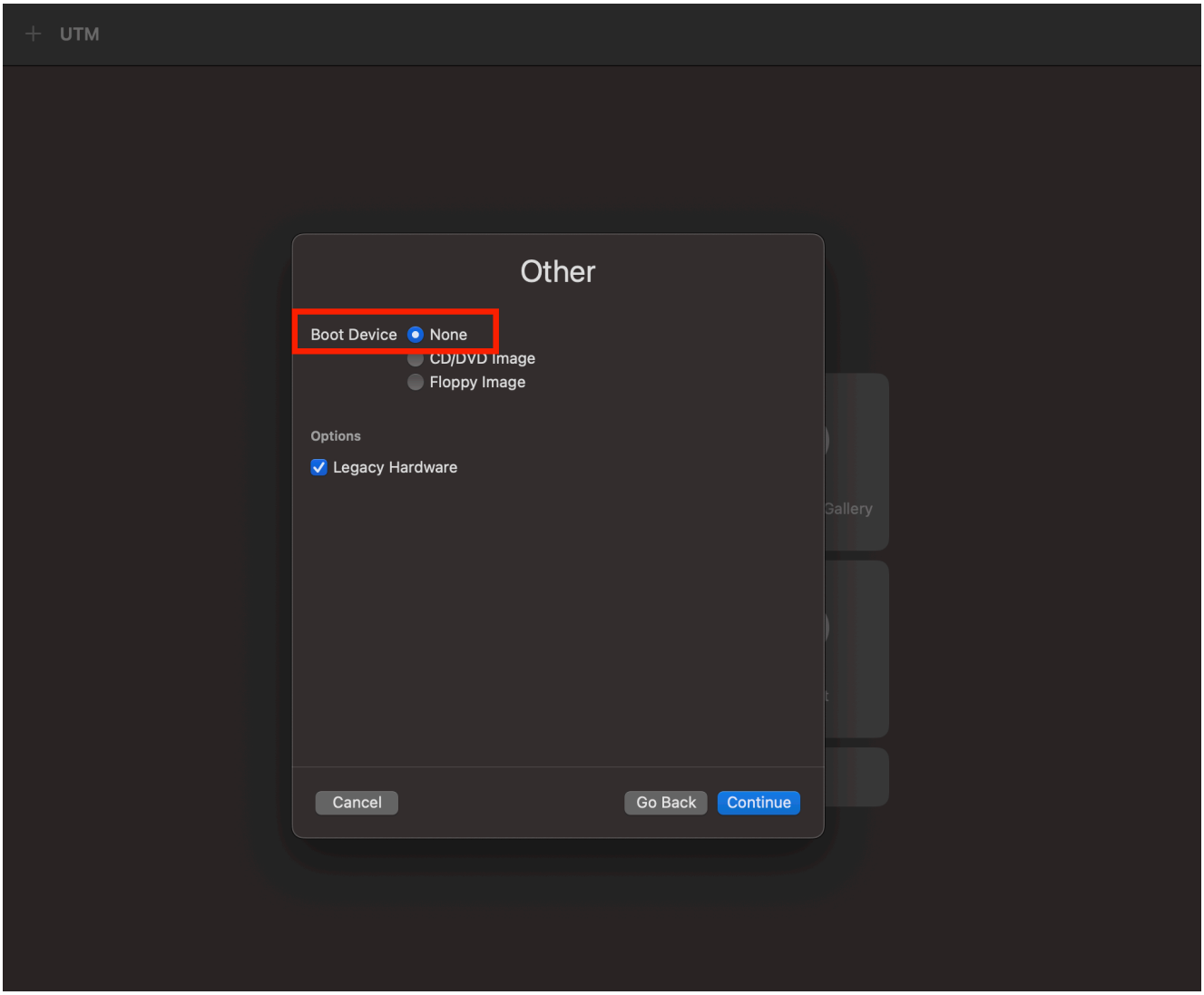
- UTM’s Virtualize mode can only run ARM-compatible operating systems natively.
- To run x86-based VMs like Metasploitable 2, UTM must emulate the x86 hardware using QEMU under the hood.



STEP 4： Click on “Others”

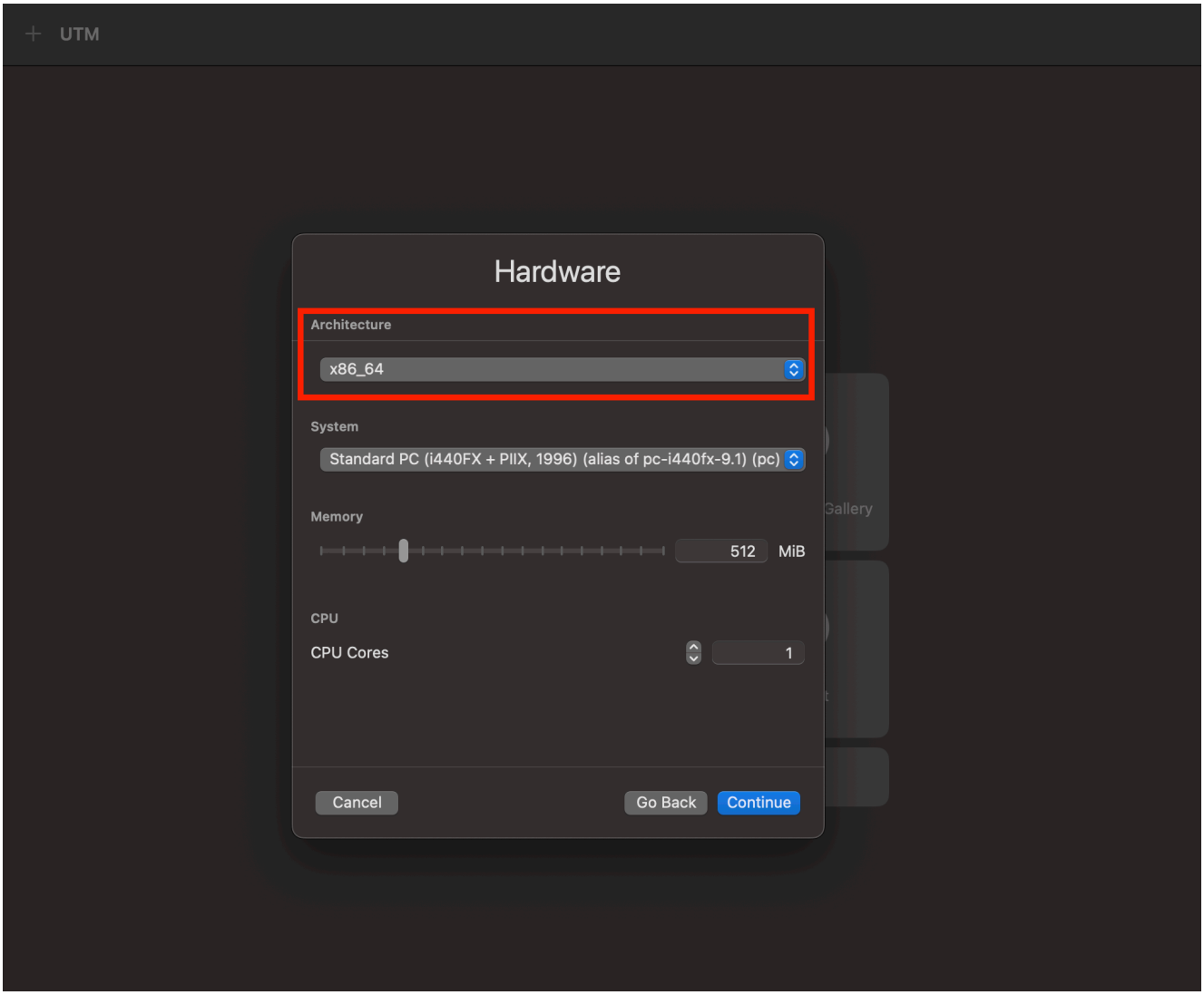


STEP 5 : Select ‘None’ and click on ‘Continue’

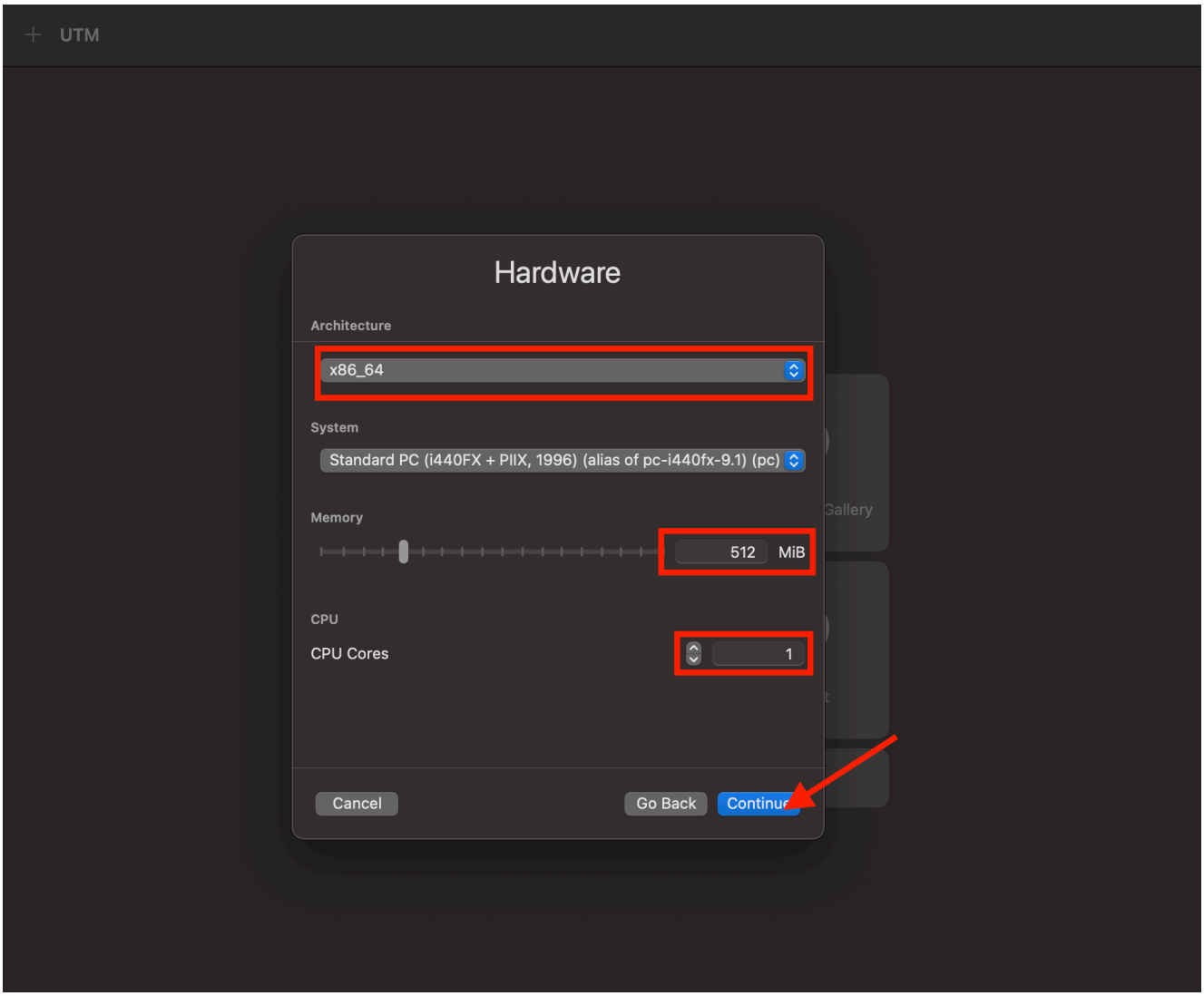


STEP 6 : Select ‘x86_64’ because Metasploitable 2 is based on Ubuntu Linux (32-bit or 64-bit) compiled for x86 architecture. Selecting x86_64 ensures compatibility with its kernel, binaries, and services.

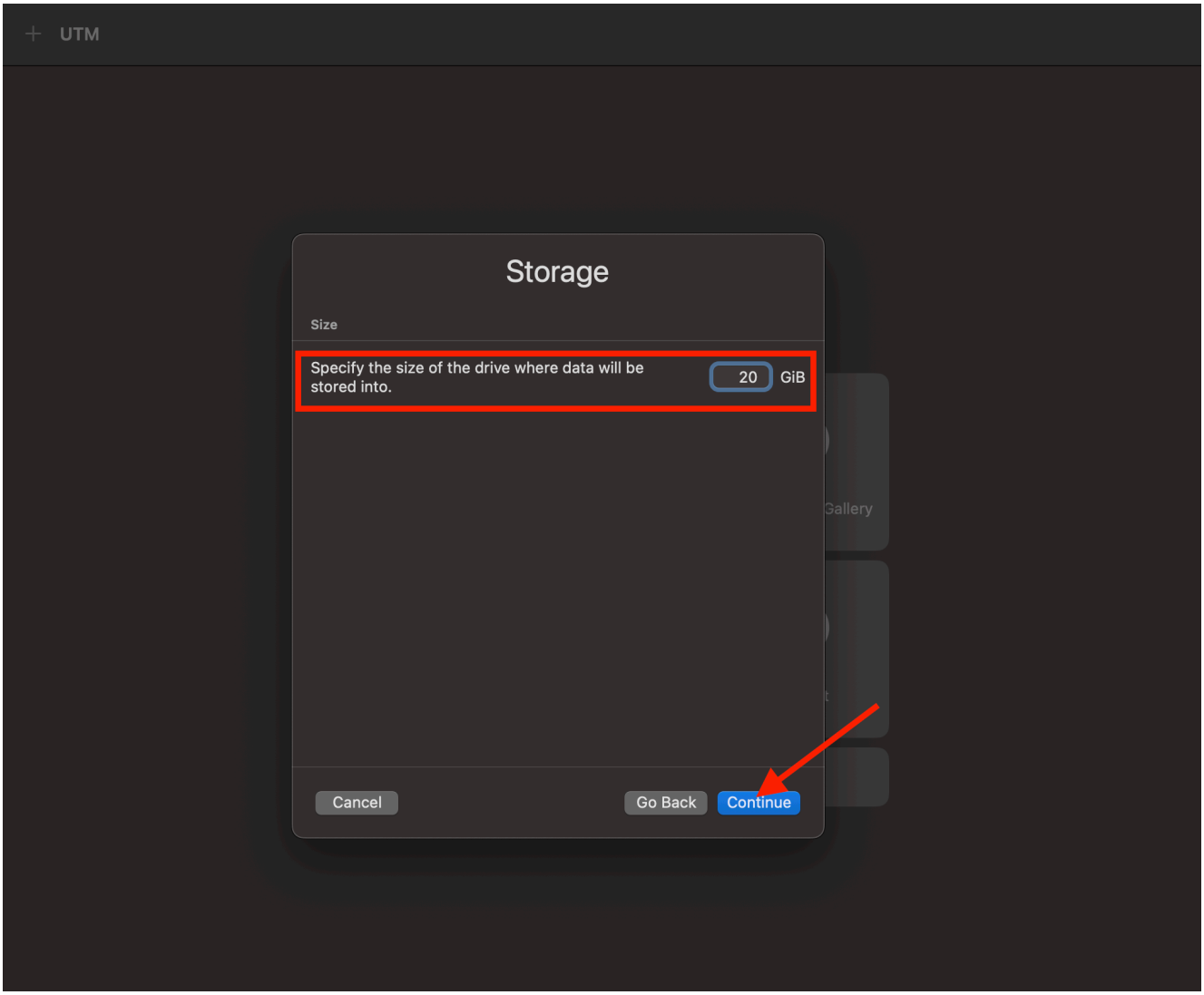
Choosing an incompatible architecture (like ARM or RISC-V) will cause the VM to fail during boot or crash during runtime, since the underlying binaries are not designed for those platforms.



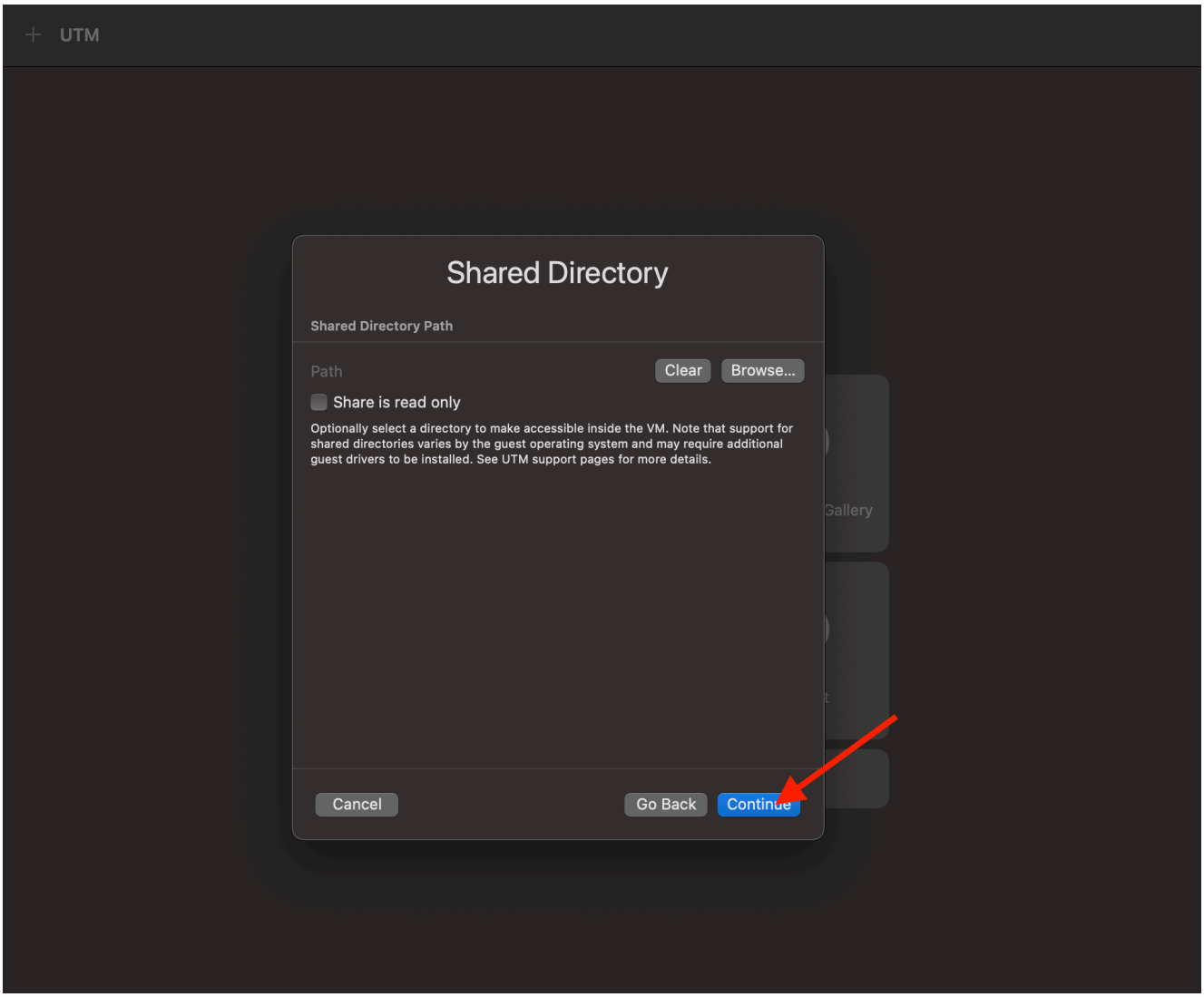
STEP 7 : Allocate more than the minimum 256 MB of memory.
For optimal performance, set the memory to 512 MiB and assign 1 CPU core.
Once configured, click ‘Continue’ to proceed with the virtual machine setup.



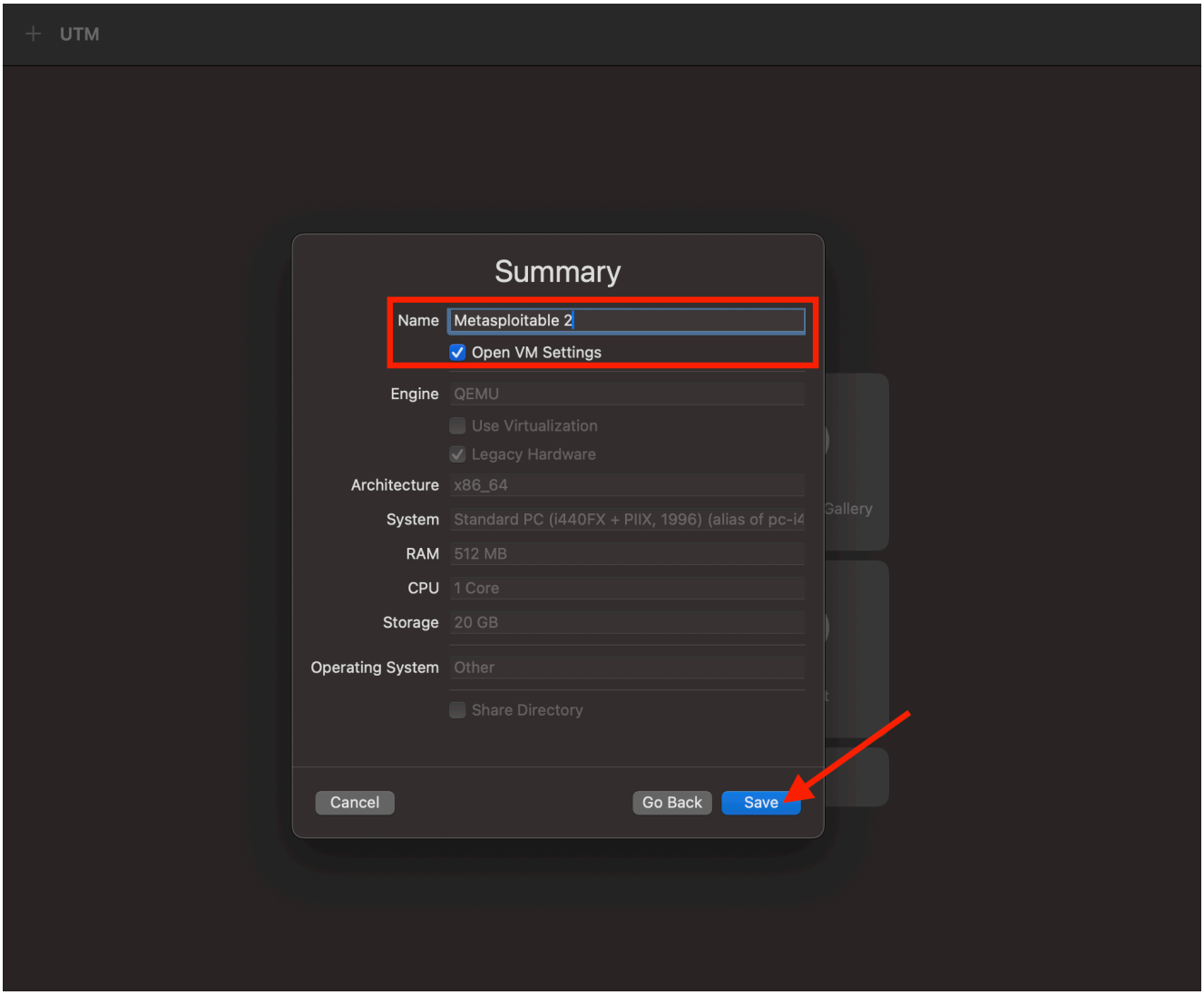
STEP 8 :Allocate at least 10 GiB of storage to meet the minimum requirement. For optimal performance , 20 GiB is recommended and click ‘Continue’.



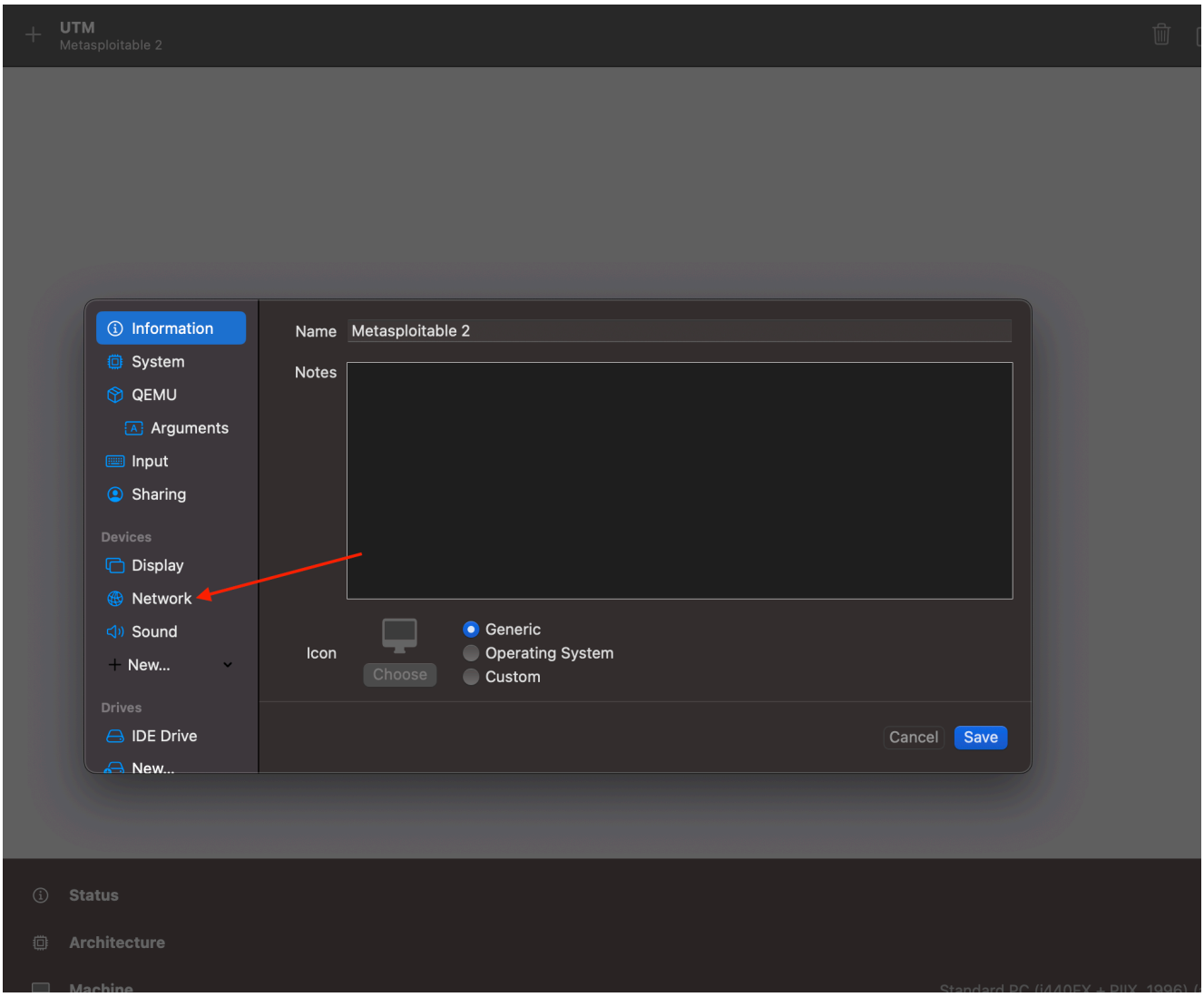
STEP 9 : Click on ‘Continue’



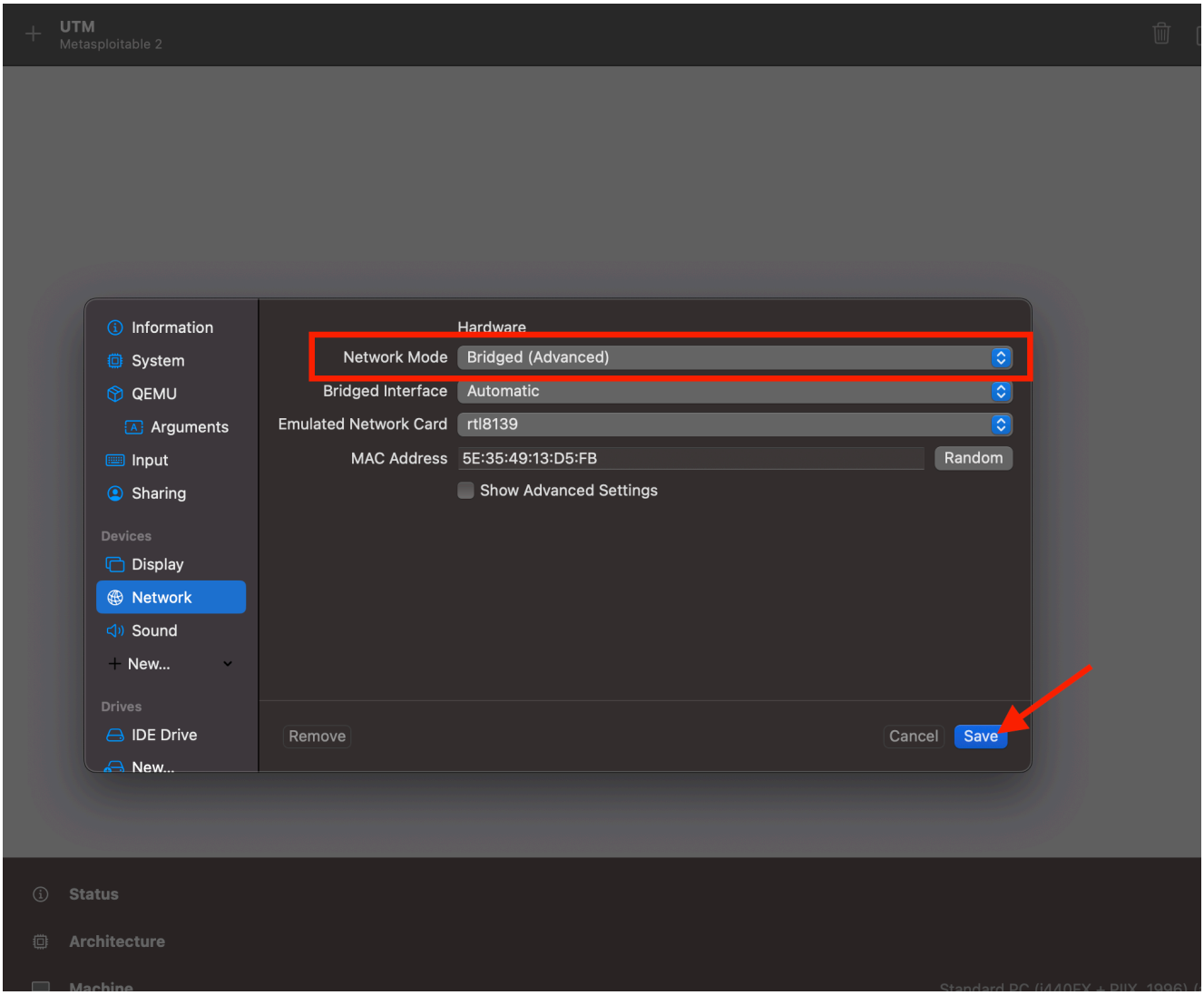
STEP 10 : Give your virtual machine a name, enable ‘Open VM Settings’ to customize configuration, then click ‘Save’ to finalize the setup.



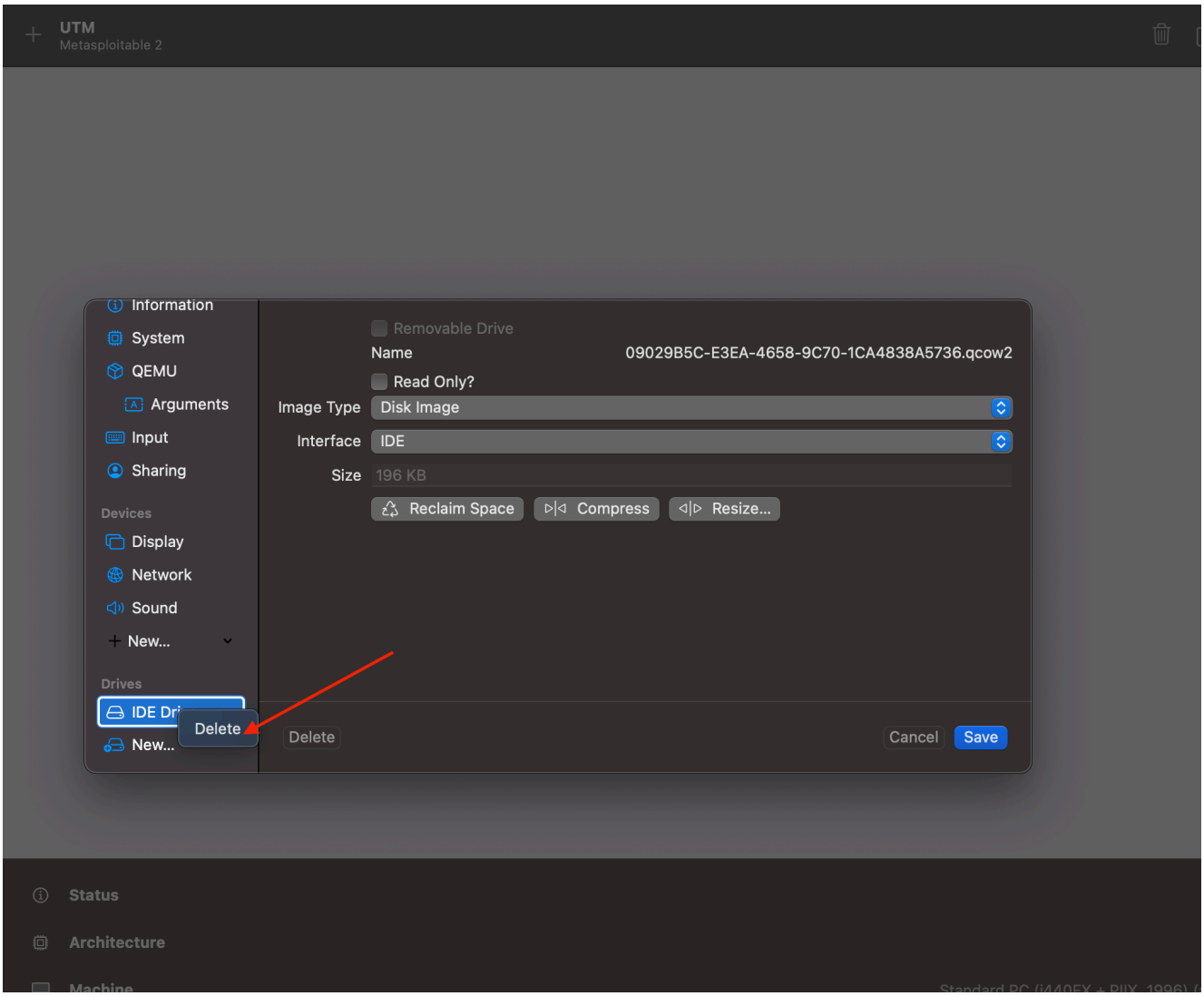
STEP 11 : Navigate to the ‘Network’ tab to set up connectivity options.



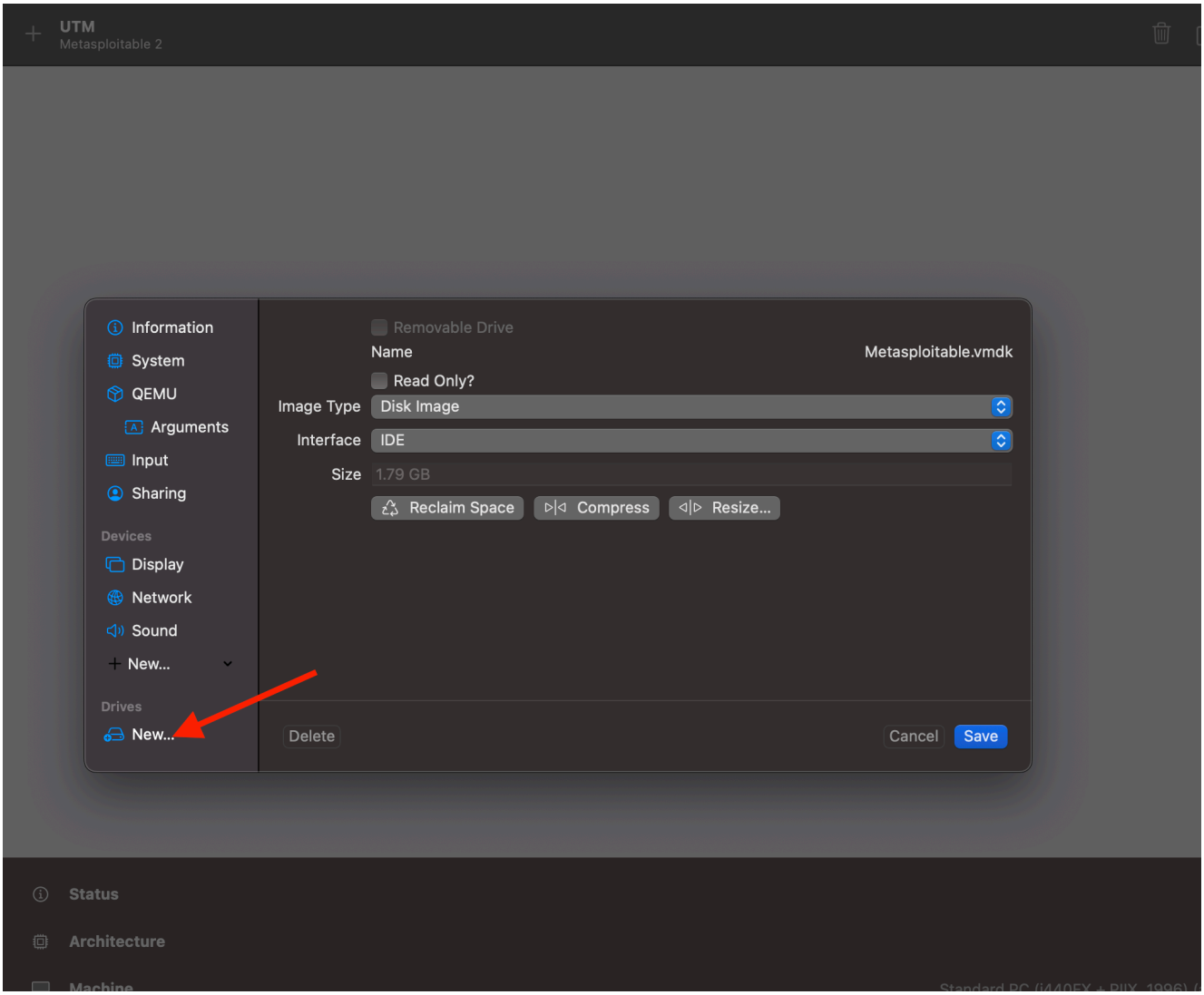
STEP 12 : In Network mode select ‘Bridged’ (important) and save . Using bridged mode allows Kali Linux and Metasploitable 2 to communicate directly over the network without needing port forwarding or NAT setup.



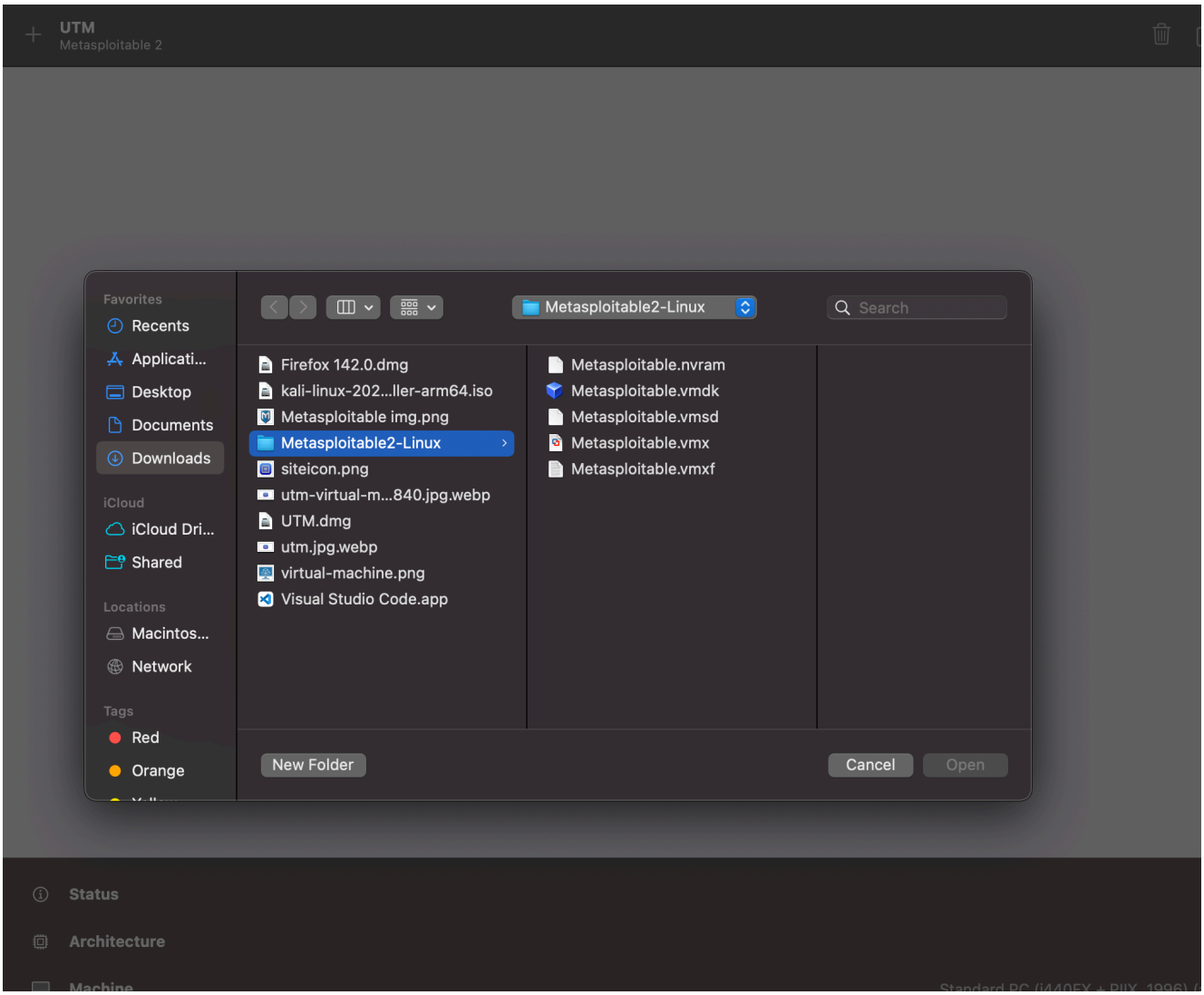
STEP 13 : In the Drives tab, right-click (or tap with two fingers) on the existing IDE Drive, then select ‘Delete’ to remove it from the configuration.



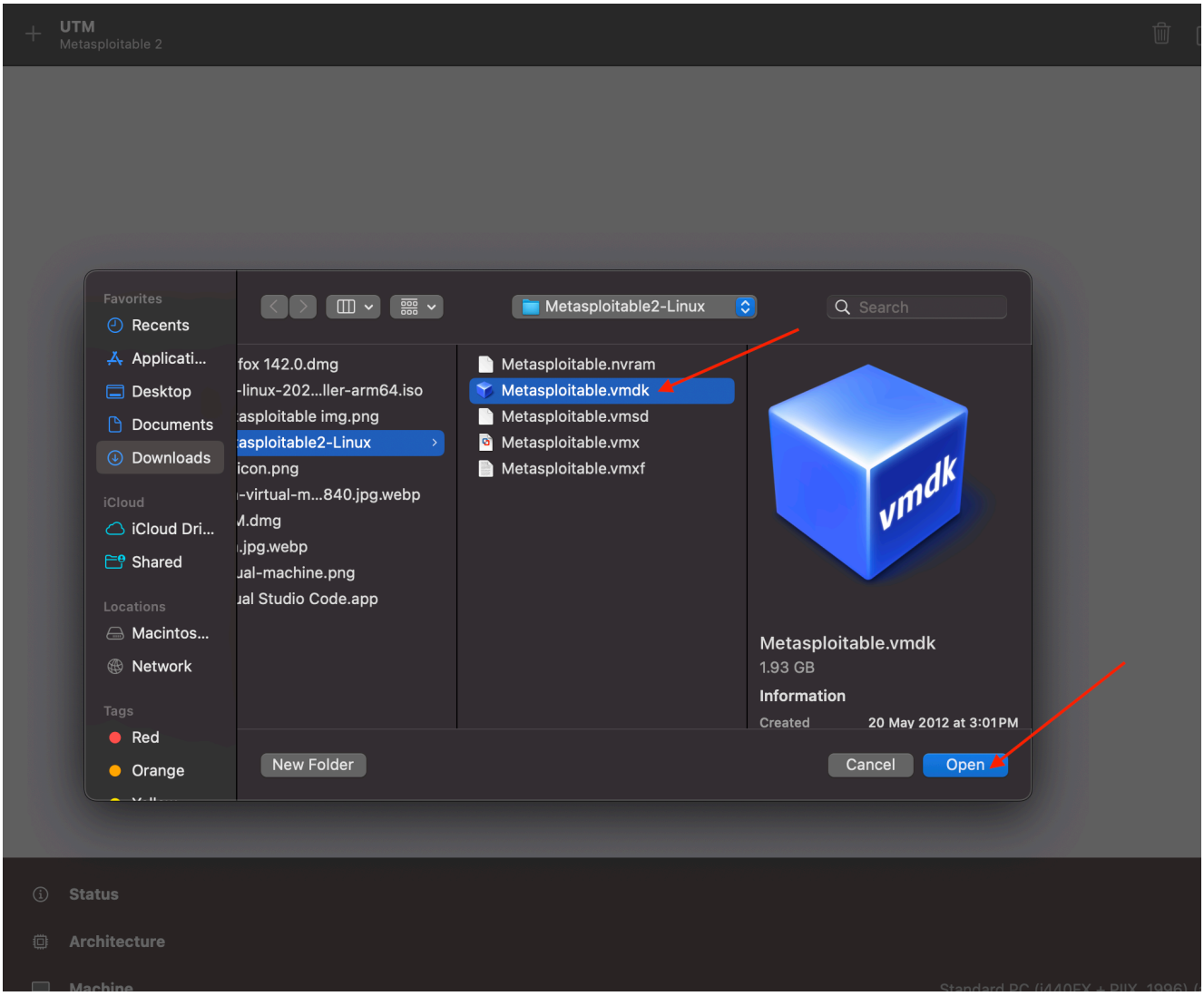
STEP 14 : After removing the previous drive, click ‘New’ to create a fresh virtual disk for your setup.



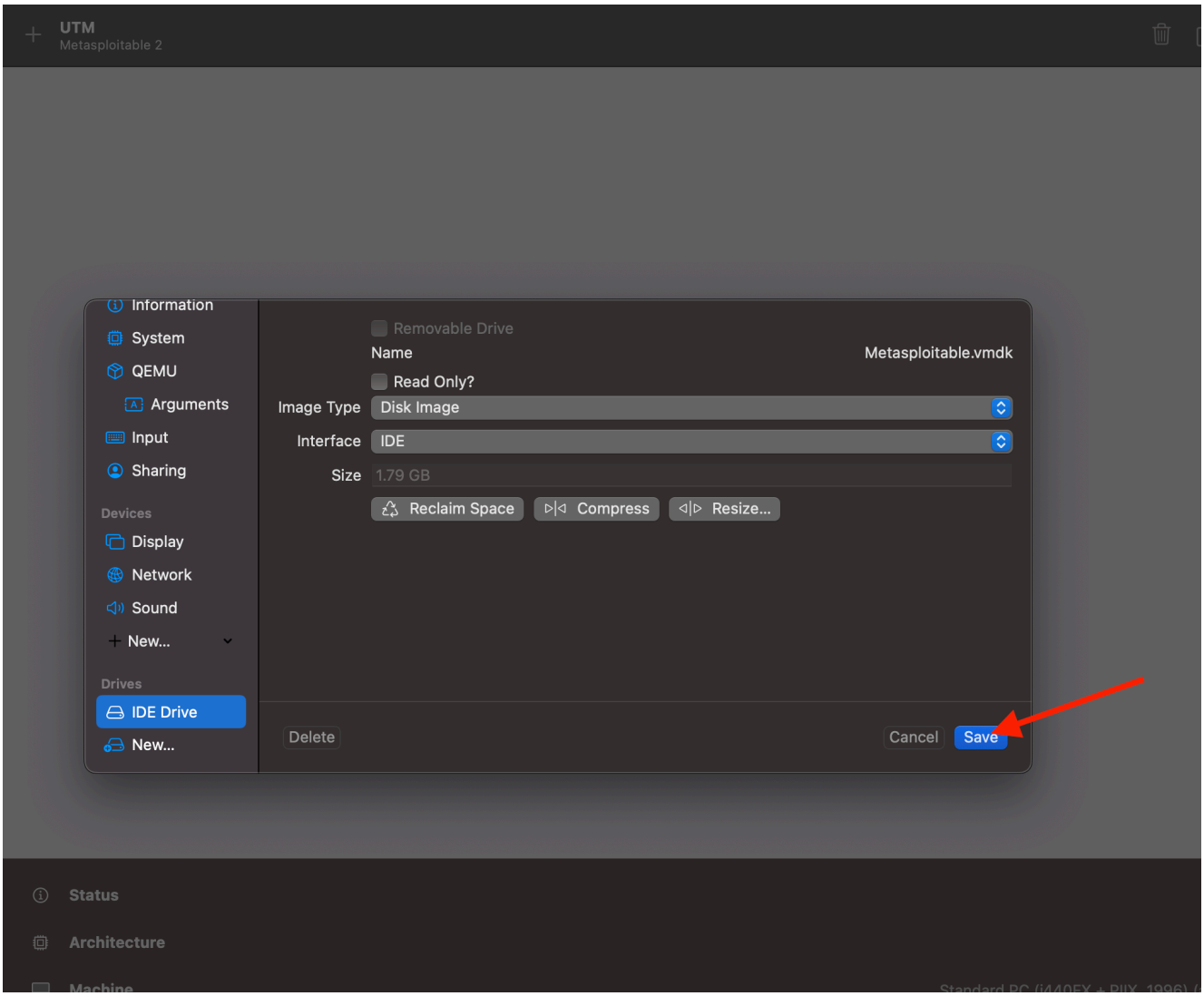
STEP 15 : Now, locate and select the Metasploitable2 folder you downloaded in Step 1 to attach the virtual disk to your VM.



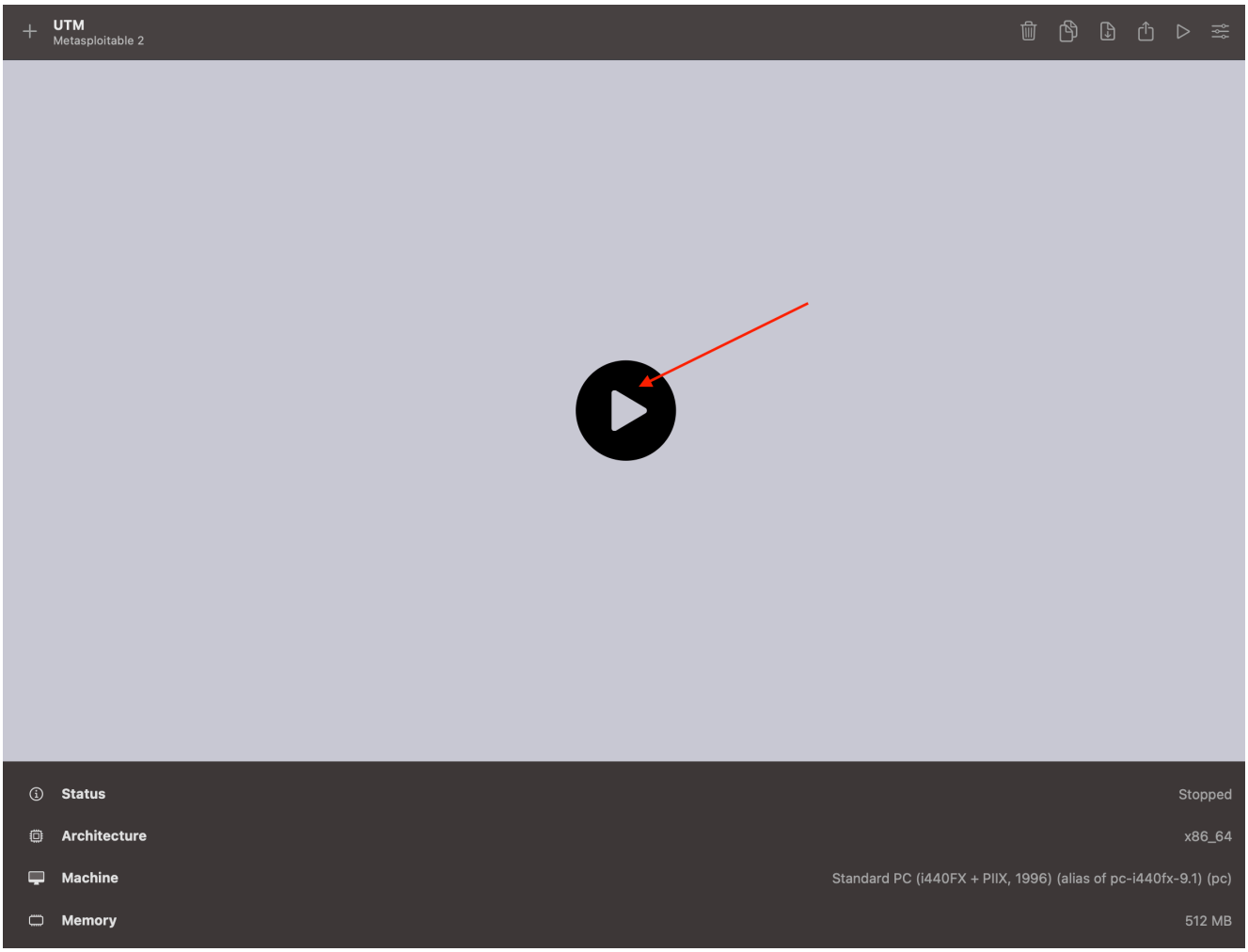
STEP 16 : In the folder select “**Metasploitable.vmdk**” file and click on ‘Open’



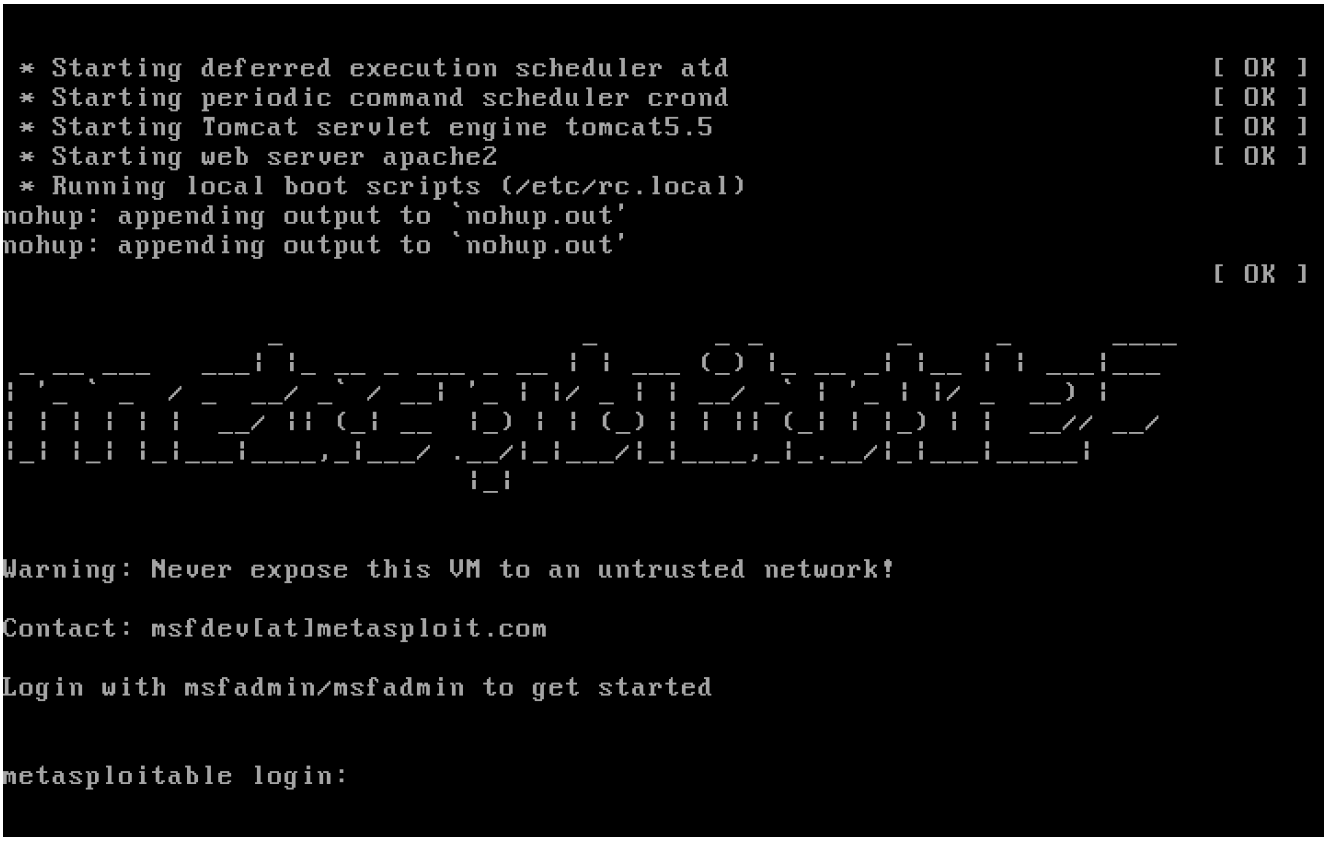
Step 17 : Click ‘Save’ to finalize and attach the virtual drive to your VM.



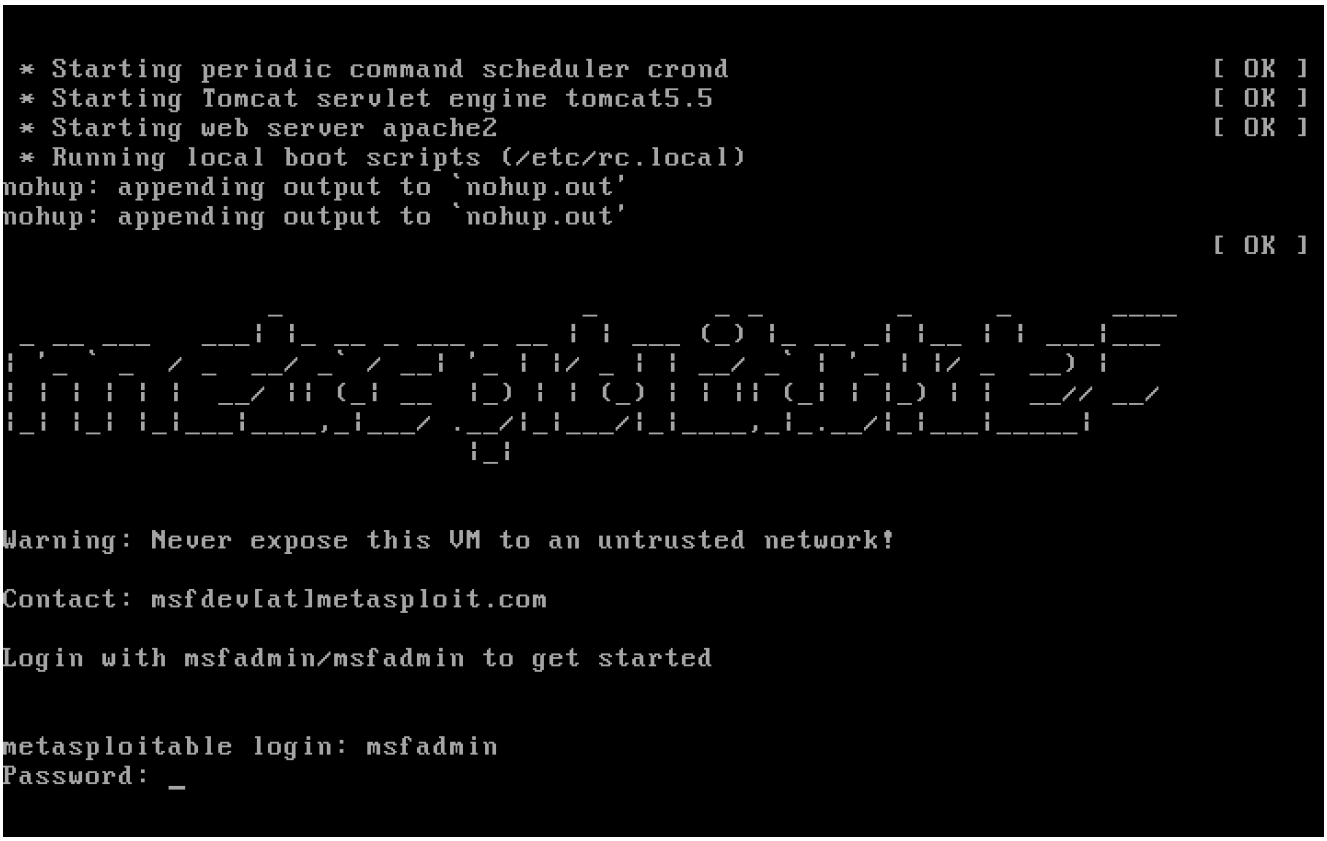
STEP 18 : Click the Play button to launch your virtual machine



STEP 19 :Your screen should now resemble this setup, confirming that Metasploitable 2 has launched successfully and is ready for use.



STEP 20 : Now, log in using the username: msfadmin and enter the password: msfadmin to access the Metasploitable 2 system.



Metasploitable 2 has been successfully installed and is now fully operational.