HOW TO SET UP A VIRTUAL LAB FOR CYBERSECURITY

A virtual lab is crucial in cybersecurity because it provides a safe, isolated environment to practice and experiment without risking real systems. It supports hands-on learning, allowing individuals to test tools, simulate attacks and defenses, and gain practical experience. Virtual labs are cost-effective, requiring only one machine to run multiple virtual systems. They also offer the flexibility to take snapshots and roll back changes, making experimentation easier. Also, having a lab is valuable for career development, as many certifications and employers expect real-world experience.

PURPOSE

This virtual lab is suitable for safely practicing ethical hacking, penetration testing, defensive security techniques, and learning cybersecurity tools like Wireshark, Metasploit, etc.

THE ENVIRONMENT

For this project, VirtualBox and Windows are the respective tool and operating system I have chosen to set up my local virtual lab environment with. VMware Workstation is an alternative to VirtualBox, and macOS, or Linux could be used instead of Windows as the host OS.

The host machine which in my case is my personal computer should have sufficient capacity because it will power all your virtual machines.

The following are specs that I would recommend to successfully set up a virtual lab that runs smoothly:

- **CPU**: Multi-core (Intel i5-i9 or its equivalent).
- **RAM**: *Minimum* 8 GB (16 GB and more, strongly recommended).
- **Storage**: 500 GB+ SSD.
- **OS**: Windows 10/11, macOS, or any Linux distro (Ubuntu etc.).

SET UP (Download and Install) VIRTUAL MACHINES

- **Kali Linux** (attacker machine)
- **Ubuntu server** (web server simulation)
- **Metasploitable 2** (vulnerable/target machine)
- **Parrot Security** (attacker machine)

- **VirtualBox** (the hypervisor)

VirtualBox

VirtualBox is a free virtualization tool by Oracle that lets you run multiple operating systems like Kali Linux, Ubuntu Server, or Windows on your main computer at the same time, without needing extra hardware. It is perfect for setting up ethical hacking labs, testing environments, or trying out new systems safely. You can create virtual machines (VMs), allocate RAM, mount ISO files, and configure networks like NAT or Host-Only. With features like snapshots, shared folders, and Guest Additions for better performance, VirtualBox is an essential tool for anyone working in cybersecurity.

Download

1. Go to the official website: https://www.virtualbox.org
2. Click **"Download VirtualBox"**.
3. Choose **"Windows host"** to download the .exe installer.

Install

1. Double-click the downloaded .exe file.
2. If prompted by Windows, click **"Yes"** to allow it to run.

Follow the Installation Wizard

1. Click **Next** to begin.
2. Choose installation options (default is fine for most users).
3. Click **Next** again, then **Yes** to allow network interfaces to reset.
4. Click **Install**.
5. Wait for it to install.
6. Check **"Start Oracle VM VirtualBox after installation"** and click **Finish**.

(Optional) Install Extension Pack

1. Back on the VirtualBox Downloads page, click on **VirtualBox Extension Pack**
2. Download and open it.
3. VirtualBox will prompt to install it — click **Install → Agree → Yes**.

Metasploitable 2

Metasploitable is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities.

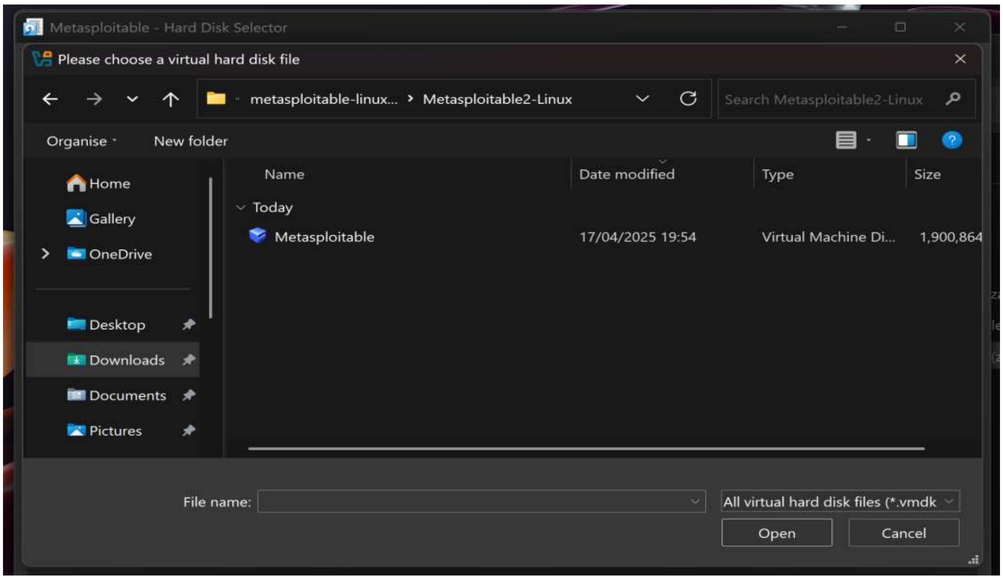
Download

1. Visit the official source (Rapid7 GitHub or InfoSec community mirrors):
   https://information.rapid7.com/metasploitable-download.html
   https://sourceforge.net/projects/metasploitable/

2. Download the **.zip file** (~800MB)

Extract the ZIP

1. Right-click the .zip file → "Extract All" or use 7-Zip/WinRAR.
2. It contains a **VMware VM** (.vmx and .vmdk files), but it also works in VirtualBox.



Metasploitable - Hard Disk Selector

Please choose a virtual hard disk file

metasploitable-linux... › Metasploitable2-Linux

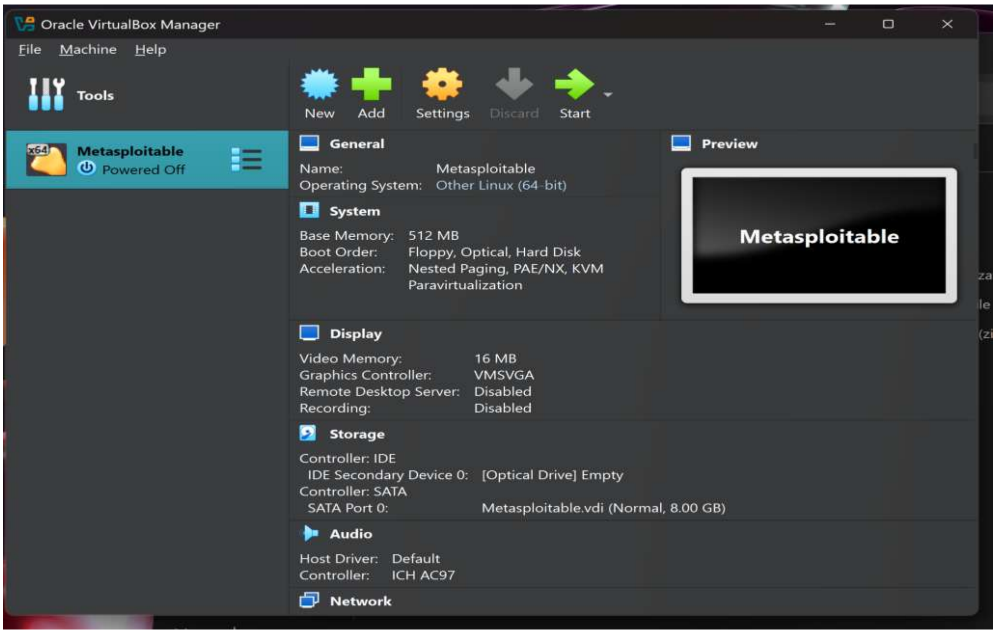
Name	Date modified	Type	Size
Today			
Metasploitable	17/04/2025 19:54	Virtual Machine Di...	1,900,864

File name:

All virtual hard disk files (*.vmdk

Import into VirtualBox

1. Open **VirtualBox**.
2. Click **"New"**.
3. Set:
   a. **Name**: Metasploitable2
   b. **Type**: Linux
   c. **Version**: Other Linux (64-bit)



Metasploitable
Powered Off

General

Name: Metasploitable
Operating System: Other Linux (64-bit)

System

Base Memory: 512 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

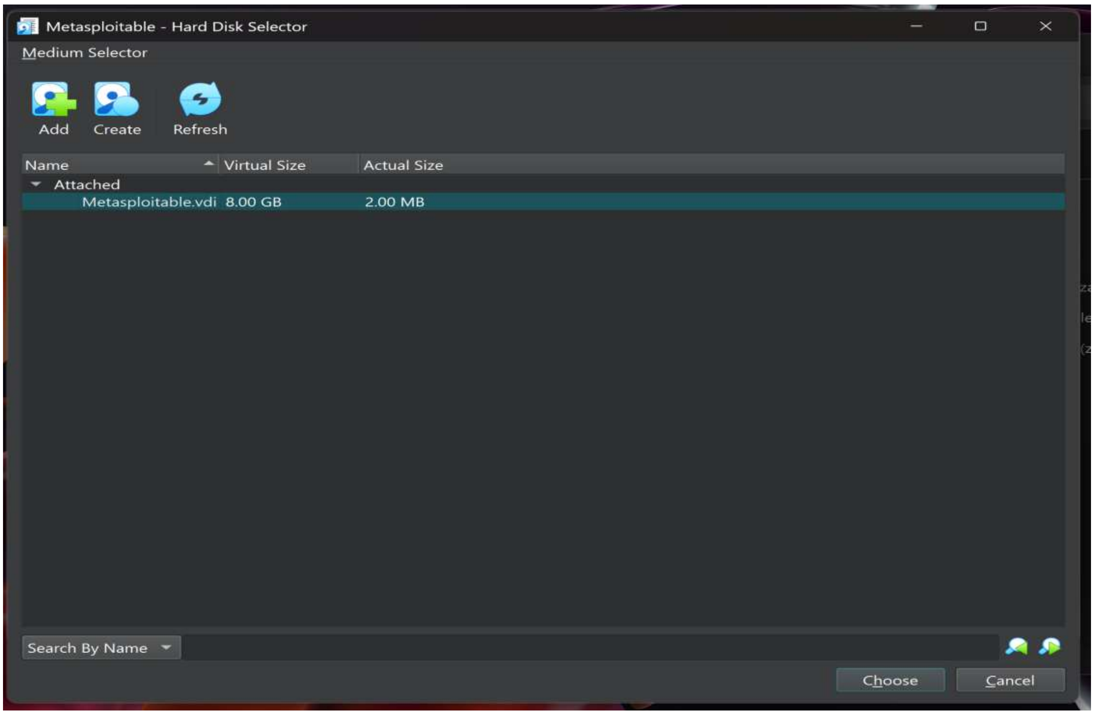
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vdi (Normal, 8.00 GB)

Audio

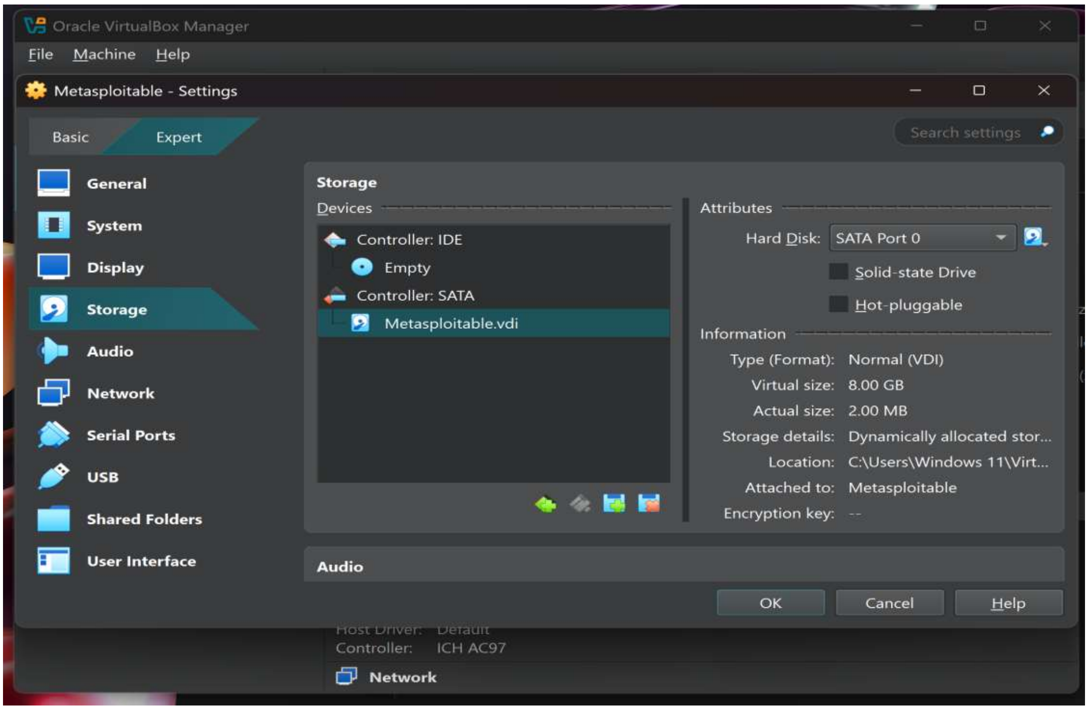
Host Driver: Default
Controller: ICH AC97

Network

4. Click **Next**, assign:
    a. **RAM**: at least **512MB–1GB**
5. Select **"Use an existing virtual hard disk file"**.
    a. Browse to the **.vmdk** file from the extracted folder.
6. Click **Create**.



Name	Virtual Size	Actual Size
Attached		
Metasploitable.vdi	8.00 GB	2.00 MB



Storage

Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - Metasploitable.vdi

Attributes

Hard Disk: SATA Port 0

□ Solid-state Drive

□ Hot-pluggable

Information

Type (Format):	Normal (VDI)
Virtual size:	8.00 GB
Actual size:	2.00 MB
Storage details:	Dynamically allocated stor...
Location:	C:\Users\Windows 11\Virt...
Attached to:	Metasploitable
Encryption key:	--

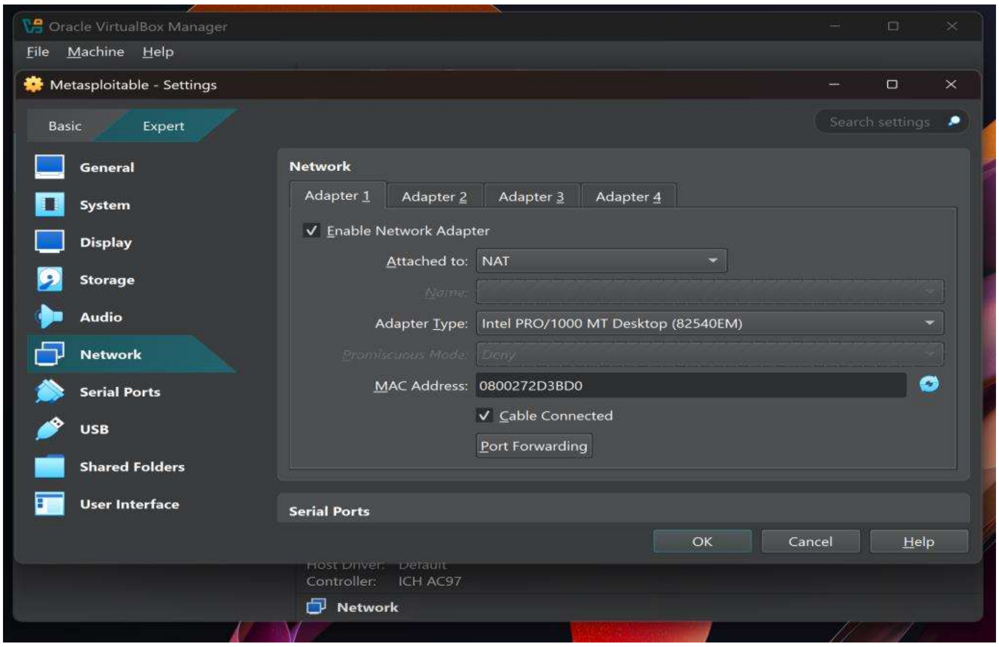
Audio

Host Driver: Default
Controller: ICH AC97

Network

Network Settings (Important!)

1. Go to **Settings → Network**.
2. Change **Adapter 1** to **Host-Only Adapter** *(so it's isolated but reachable from your host/Kali VM).*



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800272D3BD0

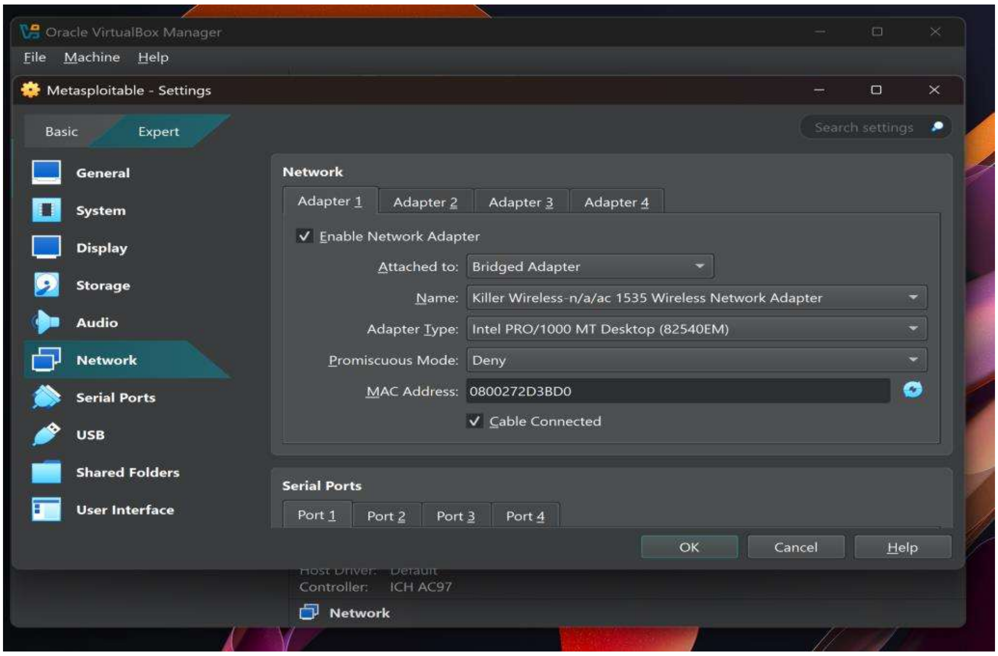
☑ Cable Connected

Port Forwarding

Serial Ports

Host Driver: Default
Controller: ICH AC97

Network



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Killer Wireless-n/a/ac 1535 Wireless Network Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800272D3BD0

☑ Cable Connected

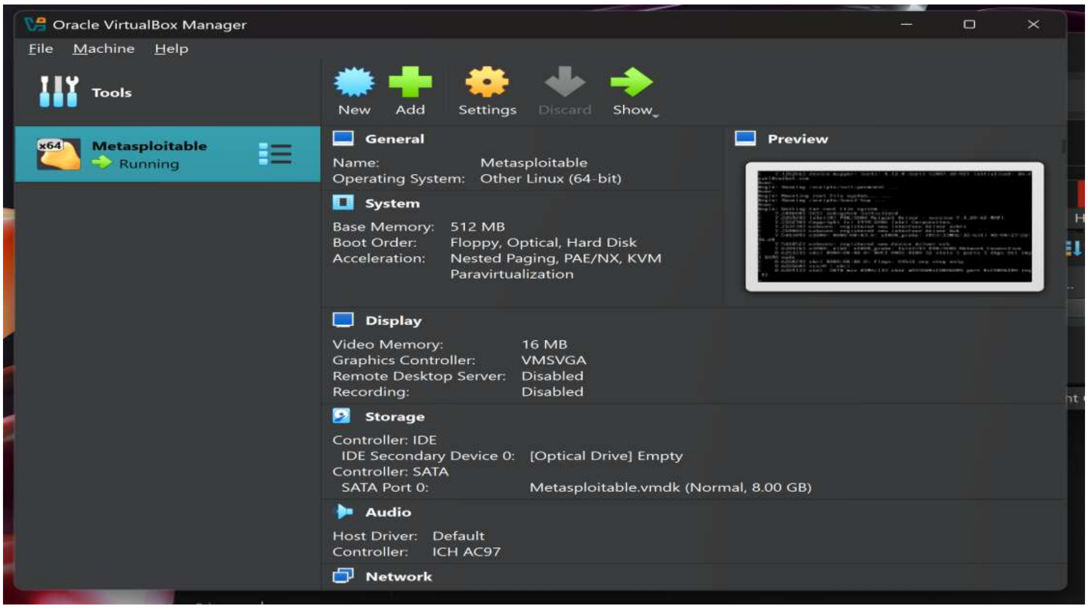
Serial Ports

Host Driver: Default
Controller: ICH AC97

Network

Start the VM

- Click **Start**.
- It'll boot into a login screen. The default login for username and password is: msfadmin



Metasploitable
Running

General

Name: Metasploitable
Operating System: Other Linux (64-bit)

System

Base Memory: 512 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

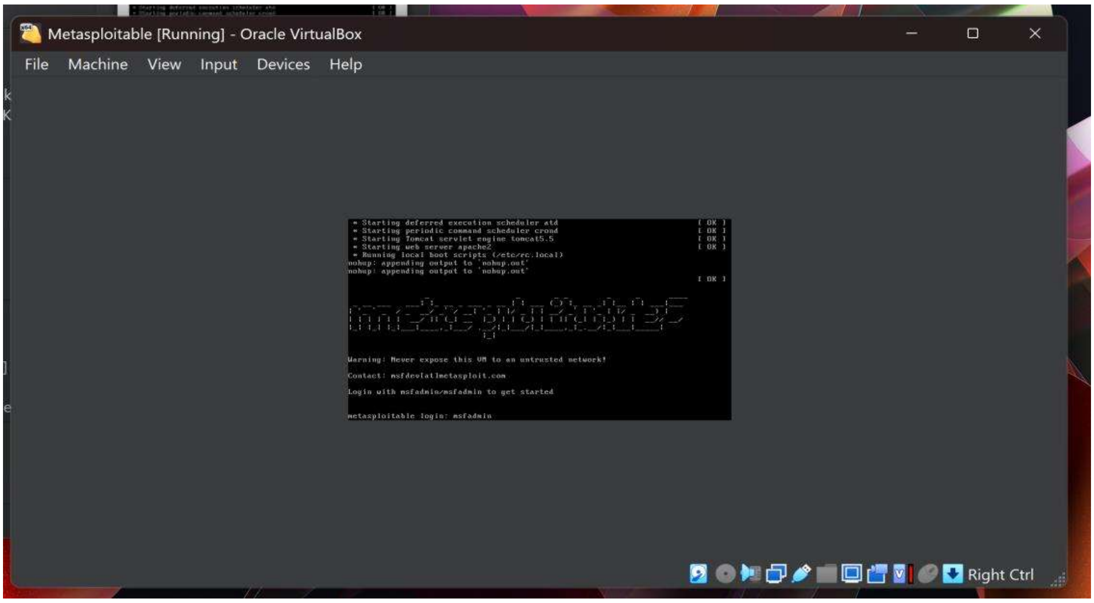
Storage

Controller: IDE
 IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
 SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network



```
 * Starting deferred execution scheduler atd                    [ OK ]
 * Starting periodic command scheduler crond                    [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                     [ OK ]
 * Starting web server apache2                                  [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'
                                                                [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
```

Kali Linux

VirtualBox must be installed before you attempt to install Kali Linux.

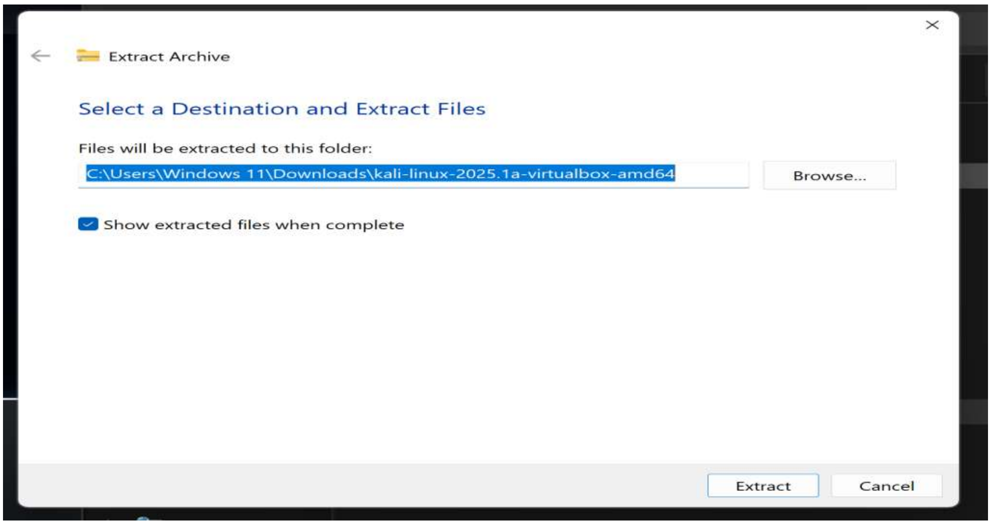
Download

Kali Linux ISO or prebuilt VM

VirtualBox image is recommended for beginners because it comes preinstalled and easy to use. The second option is the **Installer ISO** designed for custom installs.

Kali Linux can be download from the official site: https://www.kali.org/get-kali/

- Choose **Kali Linux VirtualBox Image**
- Download the .7z file (~4GB)



Extract Archive

Select a Destination and Extract Files

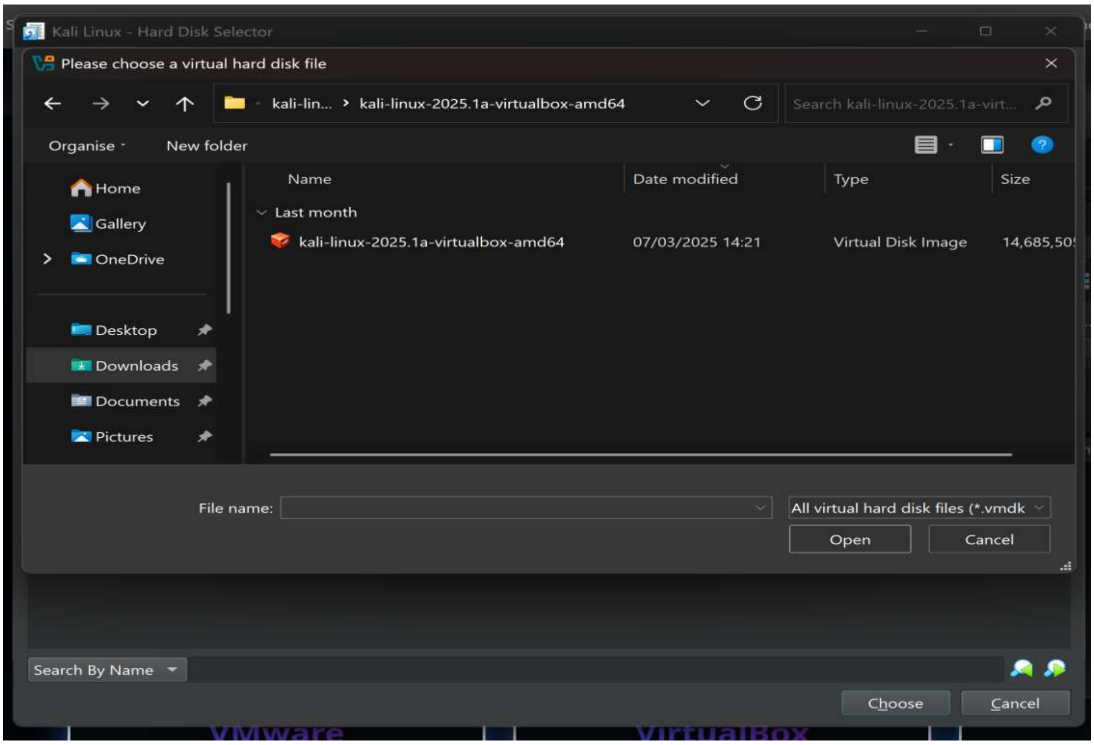
Files will be extracted to this folder:

C:\Users\Windows 11\Downloads\kali-linux-2025.1a-virtualbox-amd64

☑ Show extracted files when complete

Extract the File

- Use 7-Zip or WinRAR to extract the .7z archive.
- The folder contains a .vbox and .vdi file.



Kali Linux - Hard Disk Selector

Please choose a virtual hard disk file

kali-lin... > kali-linux-2025.1a-virtualbox-amd64

Name	Date modified	Type	Size
Last month			
kali-linux-2025.1a-virtualbox-amd64	07/03/2025 14:21	Virtual Disk Image	14,685,50

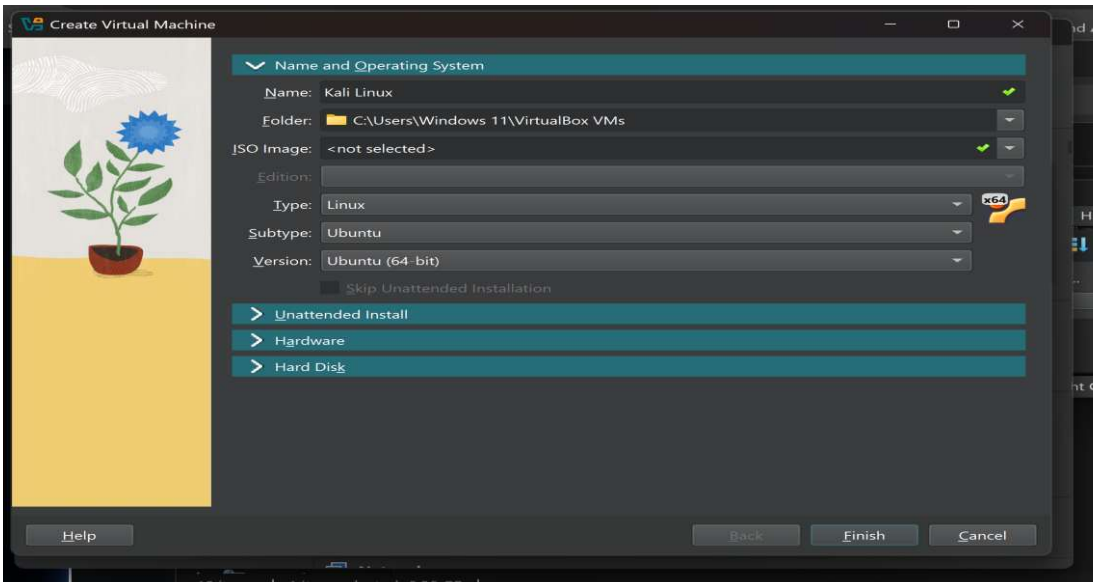
File name:

All virtual hard disk files (*.vmdk

Import into VirtualBox

1. Open **VirtualBox**
2. Click **NEW**

3. Click **File → Import Appliance**
4. Browse to the .ova file (or open .vbox file)
5. Click **Next → Import**
6. Set:
    a. **Name**: Kali Linux
    b. **Type**: Linux
    c. **Sub-type:** Ubuntu
    d. **Version**: Ubuntu (64-bit)



Name: Kali Linux

Folder: C:\Users\Windows 11\VirtualBox VMs

ISO Image: <not selected>

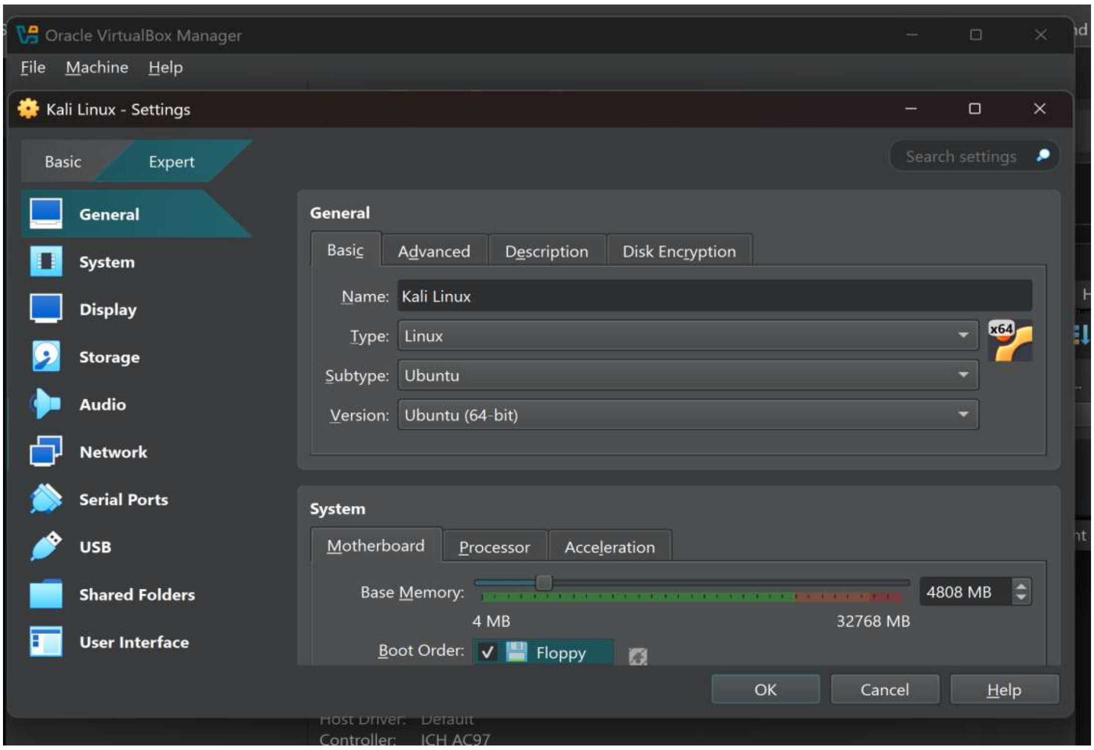
Edition:

Type: Linux

Subtype: Ubuntu

Version: Ubuntu (64-bit)

7. Click **Next**, then allocate RAM:
    a. **2 GB (2048 MB)** if you have 8GB+ on your host
    b. **1 GB (1024 MB)** minimum if on low-end hardware



General

Basic | Advanced | Description | Disk Encryption

Name: Kali Linux

Type: Linux

Subtype: Ubuntu

Version: Ubuntu (64-bit)

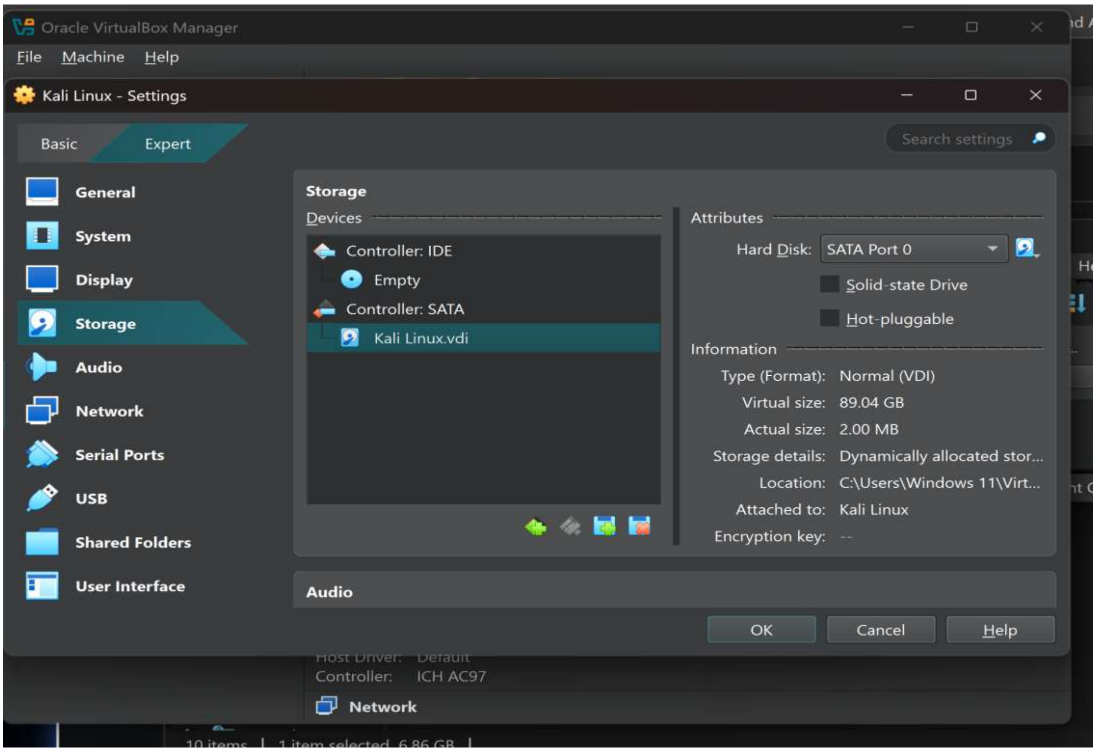
System

Motherboard | Processor | Acceleration

Base Memory: 4808 MB (4 MB – 32768 MB)

Boot Order: ☑ Floppy

Host Driver: Default
Controller: ICH AC97



Storage

Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - Kali Linux.vdi

Attributes

Hard Disk: SATA Port 0

□ Solid-state Drive

□ Hot-pluggable

Information

Type (Format): Normal (VDI)
Virtual size: 89.04 GB
Actual size: 2.00 MB
Storage details: Dynamically allocated stor...
Location: C:\Users\Windows 11\Virt...
Attached to: Kali Linux
Encryption key: --

Host Driver: Default
Controller: ICH AC97
Network

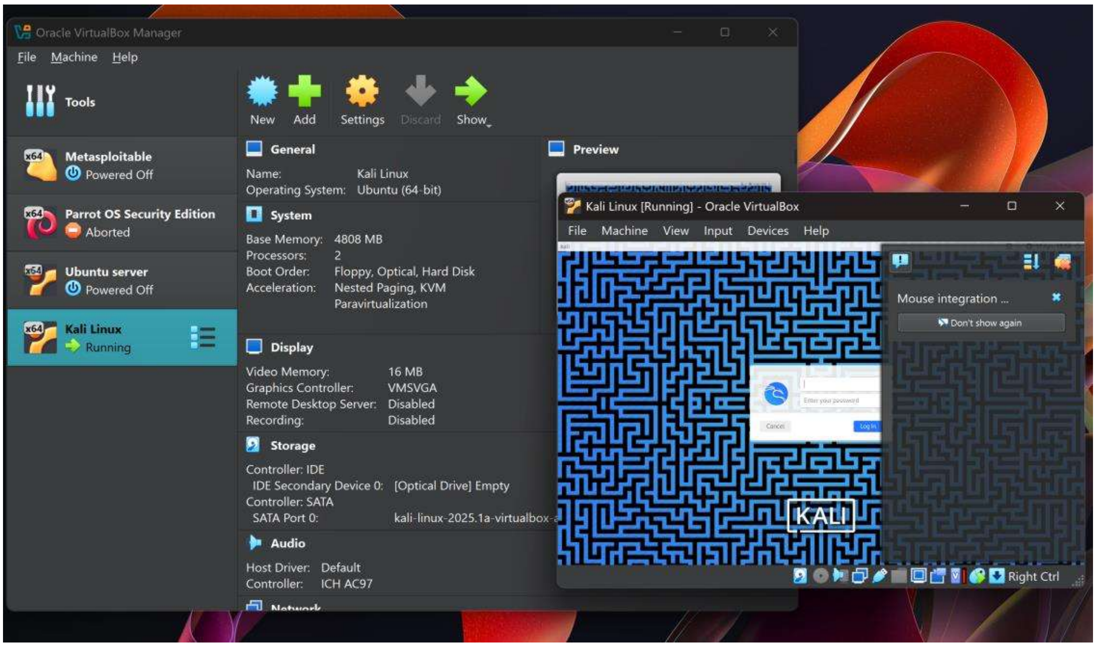
10 items | 1 item selected 6.86 GB |

Settings can be changed anytime by following the steps:

Settings → System → Motherboard → Base Memory

Start Machine

Reboot your computer after installing Kali Linux and login with the default username and password: kali


Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
Metasploitable Powered Off
Parrot OS Security Edition Aborted
Ubuntu server Powered Off
Kali Linux Running
Preview
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Don't show again
Cancel
Log In
KALI
Right Ctrl

General
Name: Kali Linux
Operating System: Ubuntu (64-bit)

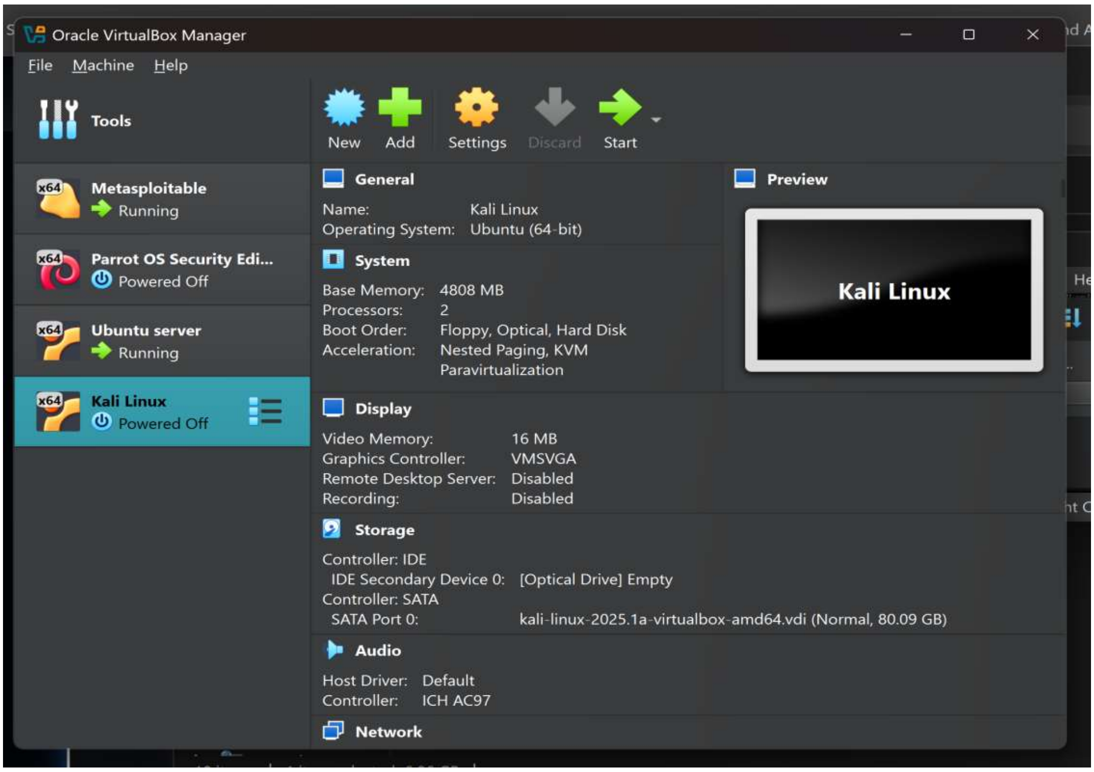
System
Base Memory: 4808 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.1a-virtualbox-

Audio
Host Driver: Default
Controller: ICH AC97

Network



General
Name: Kali Linux
Operating System: Ubuntu (64-bit)

System
Base Memory: 4808 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.1a-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network

Parrot Security

This is another great ethical hacking distro, like Kali Linux but it is more lightweight, and privacy focused.

Download

1. Follow the official link below to download Parrot Security ISO https://www.parrotsec.org/download/
2. Choose **Parrot Security Edition** → ISO → **64-bit**

Import to VirtualBox

1. Open **VirtualBox** and Click **New**
2. Click **File** → **Import Appliance**
3. Browse to the downloaded Parrot Security file
4. Click **Next** and **Import**
5. Set:
   a. Name: Parrot OS
   b. Type: **Linux**
   c. Version: **Debian (64-bit)**
6. Click **Next**

Allocate RAM (Very Important)

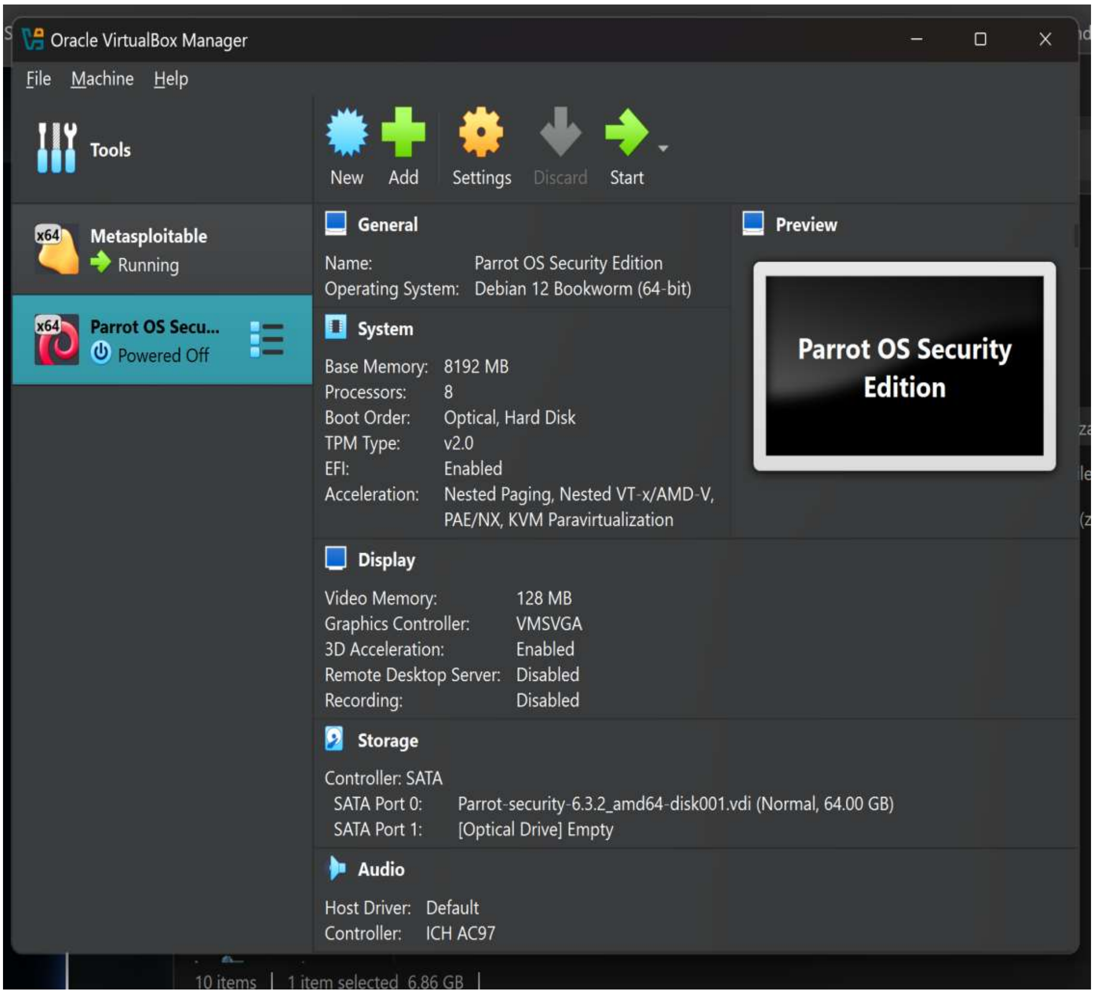
1. Allocate at least 2 GB (2048 MB) *(More if you have extra RAM — 4 GB is great)*

Create a Virtual Hard Disk

1. Choose **Create a virtual hard disk now**
2. Type: **VDI**
3. Storage: **Dynamically allocated**
4. Size: **20 GB or more**

Mount the Parrot ISO

1. Go to **Settings,** click on **Storage**
2. Under "Controller: IDE", click **Empty**
3. On the right side, click the **disc icon**
4. Choose your downloaded **Parrot ISO**



Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
Metasploitable
Running
Parrot OS Secu...
Powered Off
Preview
Parrot OS Security Edition
10 items | 1 item selected 6.86 GB |

General

Name: Parrot OS Security Edition
Operating System: Debian 12 Bookworm (64-bit)

System

Base Memory: 8192 MB
Processors: 8
Boot Order: Optical, Hard Disk
TPM Type: v2.0
EFI: Enabled
Acceleration: Nested Paging, Nested VT-x/AMD-V, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
3D Acceleration: Enabled
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Parrot-security-6.3.2_amd64-disk001.vdi (Normal, 64.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Default
Controller: ICH AC97

Start the VM & Install Parrot

1. Click **Start**
2. On boot screen, choose:
   a. **Install** (for full install)
   b. OR **Live Mode** (to try it without installing)

Complete Installation

1. Choose language, location, keyboard
2. Set your **user + password**
3. Select **Guided - Use entire disk** (safe choice)
4. Finish installation and reboot

Ubuntu server

Ubuntu Server is a lightweight, fast, and powerful version of Ubuntu designed specifically for running servers instead of desktop environments. It comes without a graphical user interface (GUI) by default, making it ideal for performance-critical tasks like hosting websites, setting up databases, creating cloud environments, or building cybersecurity labs. Ubuntu Server is highly stable, secure, and widely supported, with regular Long-Term Support (LTS) releases that offer updates and security patches for up to 5 years. It is a go-to choice for professionals who need a reliable server operating system that is free, open-source, and easy to customize.

Download

Use the official link below to download Ubuntu Server ISO https://ubuntu.com/download/server and select **Ubuntu Server 22.04 LTS.**

Create a New VM

1. Open **VirtualBox** and Click **New**
2. Name: Ubuntu Server
3. Type: **Linux**
4. Version: **Ubuntu (64-bit)**
5. Click **Next**

Allocate RAM

1. Recommended: **1024 MB (1 GB)** minimum
2. **2 GB** is better if your host PC can handle it.

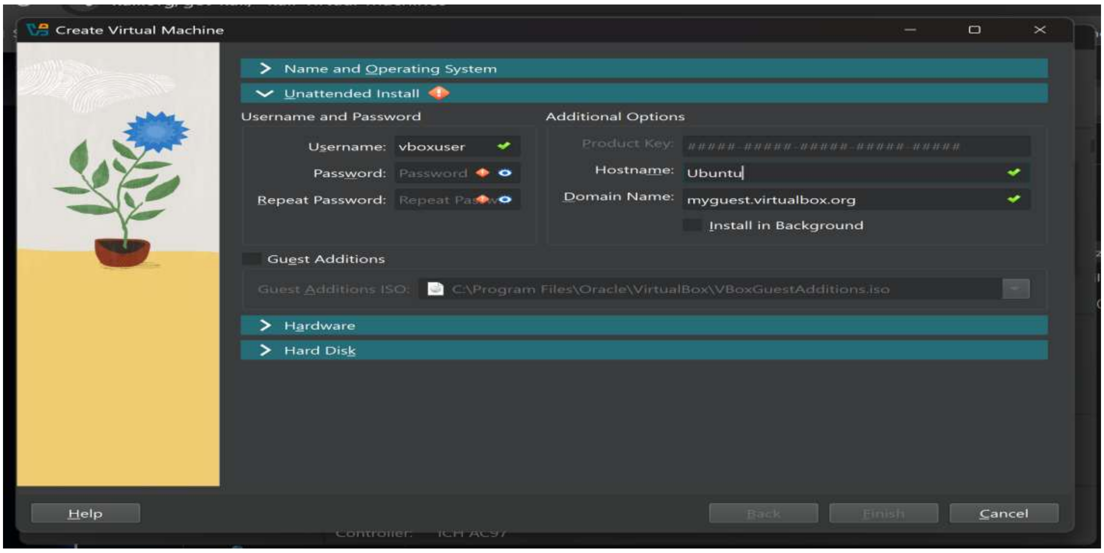
Create a Virtual Hard Disk

1. **Create a virtual hard disk now**
2. Disk type: **VDI**
3. Storage: **Dynamically allocated**

4. Size: **20 GB** or more

Attach Ubuntu Server ISO

1. Go to **Settings → Storage**
2. Under “Controller: IDE”, click **Empty**
3. On the right, click the **disc icon**
4. Choose your **Ubuntu Server ISO** file



Create Virtual Machine

Unattended Install

Username and Password

Username: vboxuser

Password: Password

Repeat Password: Repeat Password

Additional Options

Product Key: #####-#####-#####-#####-#####

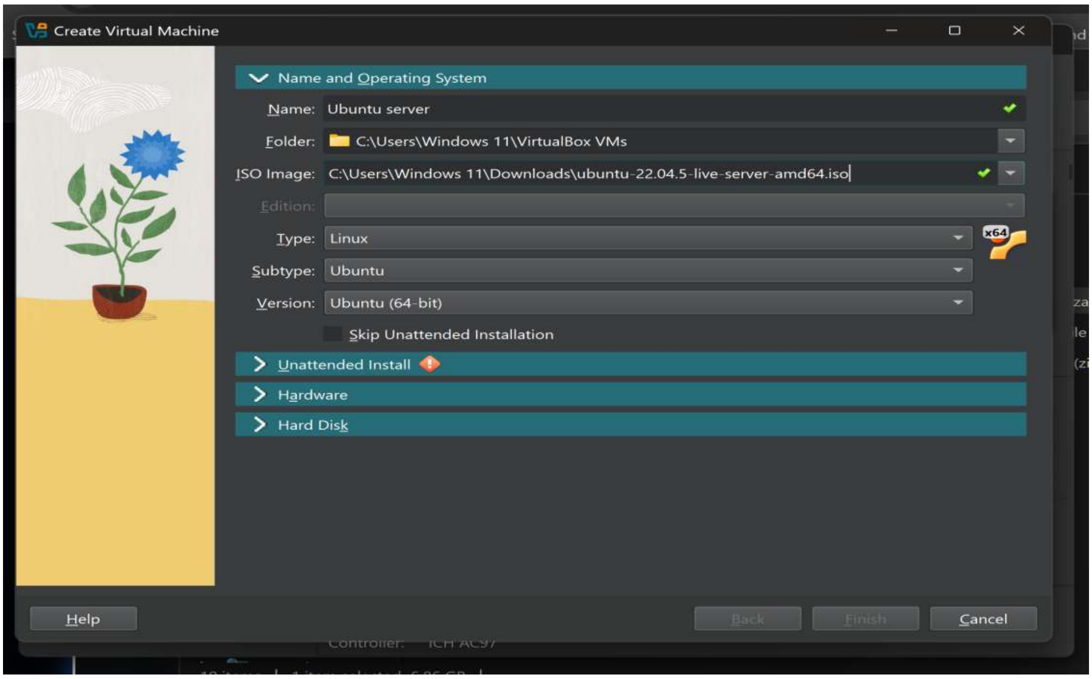
Hostname: Ubuntu

Domain Name: myguest.virtualbox.org

□ Install in Background

□ Guest Additions

Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso



Create Virtual Machine

Name and Operating System

Name: Ubuntu server

Folder: C:\Users\Windows 11\VirtualBox VMs

ISO Image: C:\Users\Windows 11\Downloads\ubuntu-22.04.5-live-server-amd64.iso

Edition:

Type: Linux

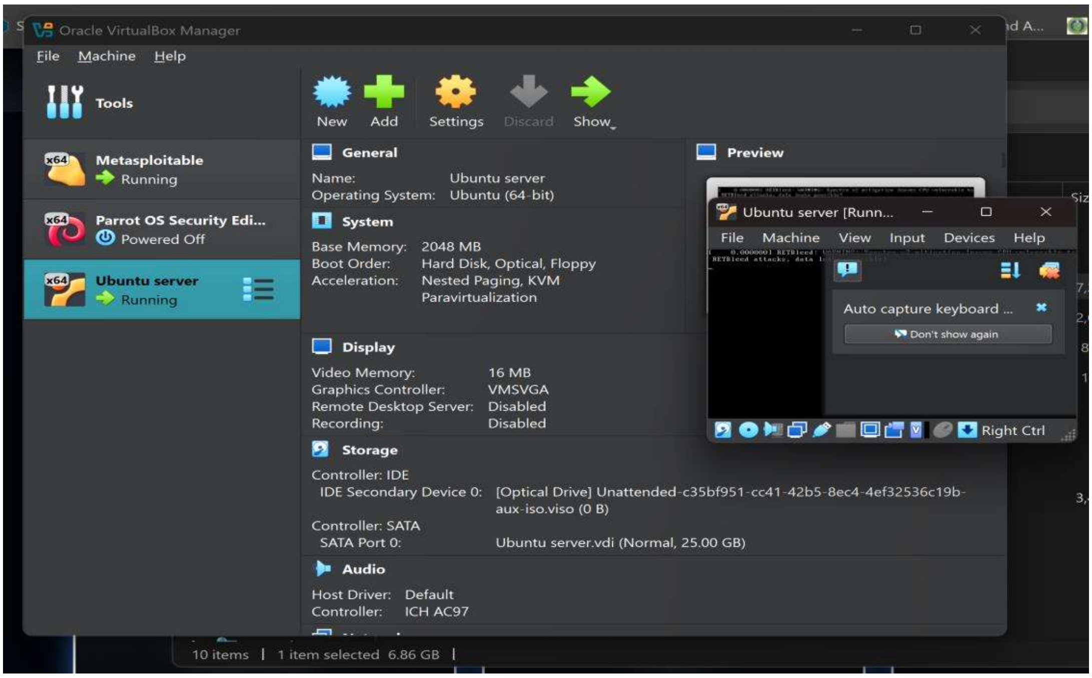
Subtype: Ubuntu

Version: Ubuntu (64-bit)

□ Skip Unattended Installation

Start the VM and Begin Installation

1. Click **Start**
2. It will boot from the ISO.
3. Choose: **Install Ubuntu Server**
4. Set up **Network Interface**:
    a. (Default automatic DHCP is fine unless you want static IP)
5. Configure **Proxy** if needed (skip if unsure)
6. Leave **Mirror Address** default (unless you know otherwise)
7. Disk Setup:
    a. Choose **Use an entire disk**
    b. Confirm changes
8. Set up **username**, **password**, and **hostname**



General
Name: Ubuntu server
Operating System: Ubuntu (64-bit)

System
Base Memory: 2048 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Unattended-c35bf951-cc41-42b5-8ec4-4ef32536c19b-aux-iso.viso (0 B)
Controller: SATA
SATA Port 0: Ubuntu server.vdi (Normal, 25.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97