🧪 Lab Guide 2 – Installing Virtual Machines

This lab sets up the three core virtual machines used throughout the course: **Windows 10/Windows Server** , **Metasploitable 2**, and **Kali Linux**. All VMs will use **NAT networking/Host-Only networking**.

Part 1 – Windows 10 Enterprise

Download ISO

- Windows 10 Enterprise ISO

Steps

1. In VirtualBox → **New** → Name: Win10-Ent, Type: *Microsoft Windows*, Version: *Windows 10 (64-bit)*.
2. Assign **4 GB RAM** (8 GB recommended).
3. Create a **60 GB VDI disk** (dynamically allocated).
4. Attach the ISO under **Settings** → **Storage**.
5. Set **Network Adapter 1** to **NAT**.
6. Start VM and install Windows with default options.

Part 2 – Metasploitable 2

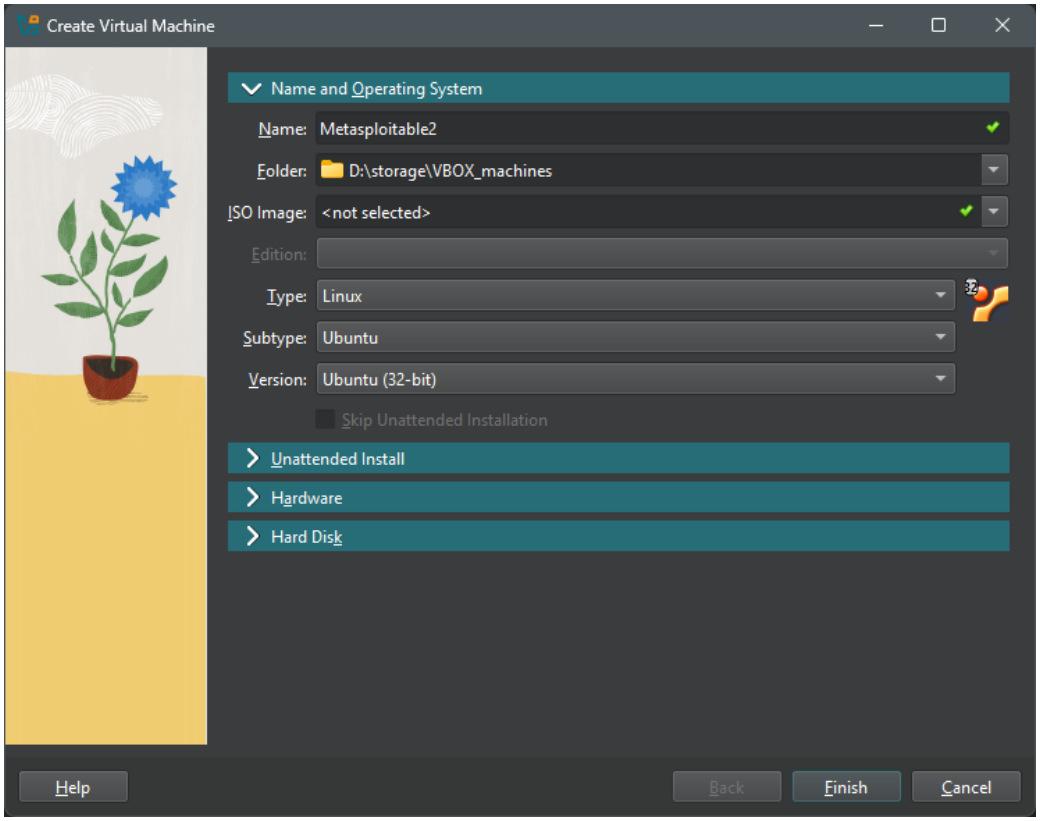
Download VM

- Metasploitable 2

  Extract the compressed file.

Steps

1. In VirtualBox → **New** → Name: Metasploitable2, Type: *Linux*, Version: *Ubuntu (32-bit)*.
2. Assign **1 GB RAM**.
3. Select **Use existing virtual disk file** → choose the Metasploitable VMDK.
4. Set **Network Adapter 1** to **NAT**.
5. Start VM. Login with msfadmin / msfadmin.



Part 3 – Kali Linux

Download ISO

- Kali Linux

Steps

1. In VirtualBox → **New** → Name: Kali, Type: *Linux*, Version: *Debian (64-bit)*.
2. Assign **4 GB RAM** (8 GB recommended).
3. Create a **40 GB VDI disk** (dynamically allocated).
4. Attach the ISO under **Settings** → **Storage**.
5. Set **Network Adapter 1** to **NAT**.
6. Start VM and run **Graphical Install** with defaults.

✅ After completing this lab, you will have three VMs ready to use for the upcoming modules:

- **Windows 10 Enterprise** – for Windows event logs
- **Metasploitable 2** – for vulnerable services and attack surface

- Kali Linux – for traffic generation and analysis tools