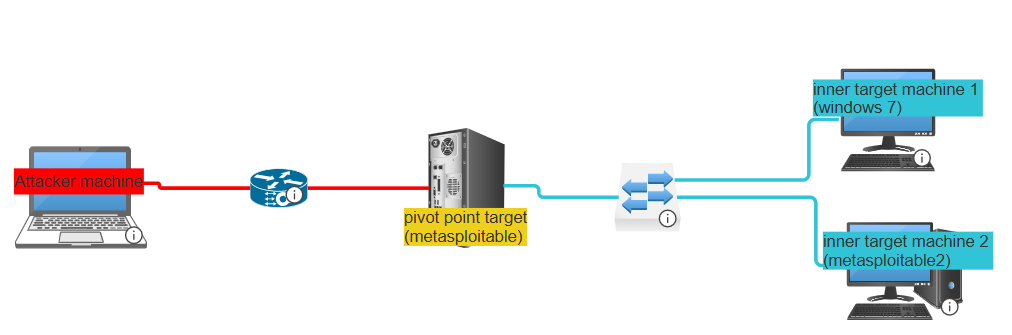
# Setting Up a Pivoting Home Lab

## Introduction

Pivoting is an essential skill in penetration testing, allowing attackers to move laterally within a compromised network to access systems that are not directly reachable. This guide walks through setting up a simple virtual lab to practice pivoting techniques using tools like Metasploit and basic networking configuration. The goal is to simulate a realistic internal network scenario where an attacker must rely on a pivot point to access deeper targets.

## Lab Topology Overview



We're going to build a lab that consists of:

* An **Attacker Machine** (e.g., Kali Linux)
* A **Pivot Machine** (e.g., Metasploitable)
* Two **Internal Target Machines** (e.g., Windows 7 and Metasploitable 2)

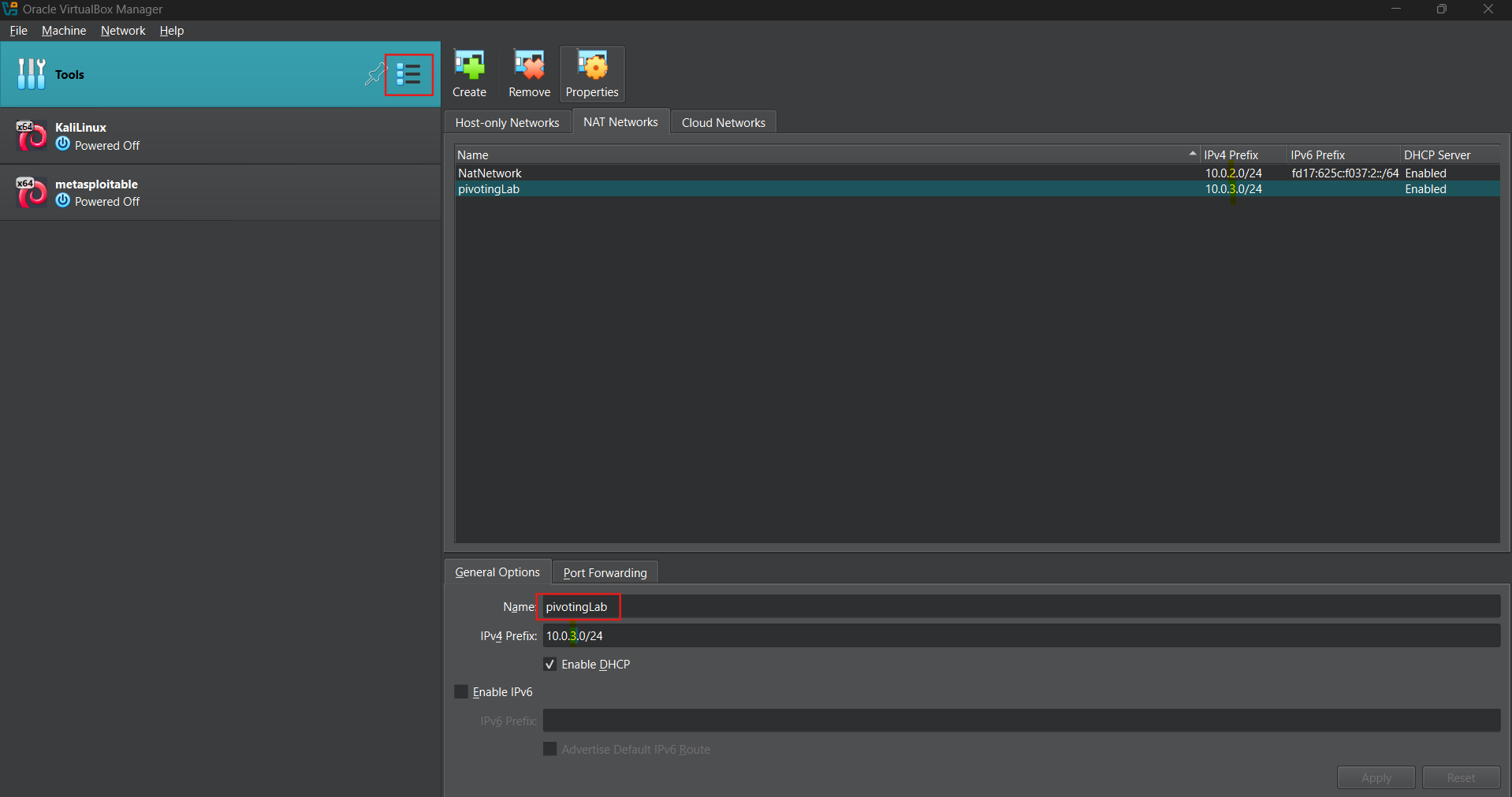
These machines are set up in two separate virtual networks:

1. **External Network (NAT)** — where the attacker and the pivot machine reside
2. **Internal Network (Host-only or NAT)** — only accessible by the pivot machine and internal targets

This setup simulates a scenario where an attacker must compromise the pivot machine first, then use it to reach internal systems.

## Lab setup

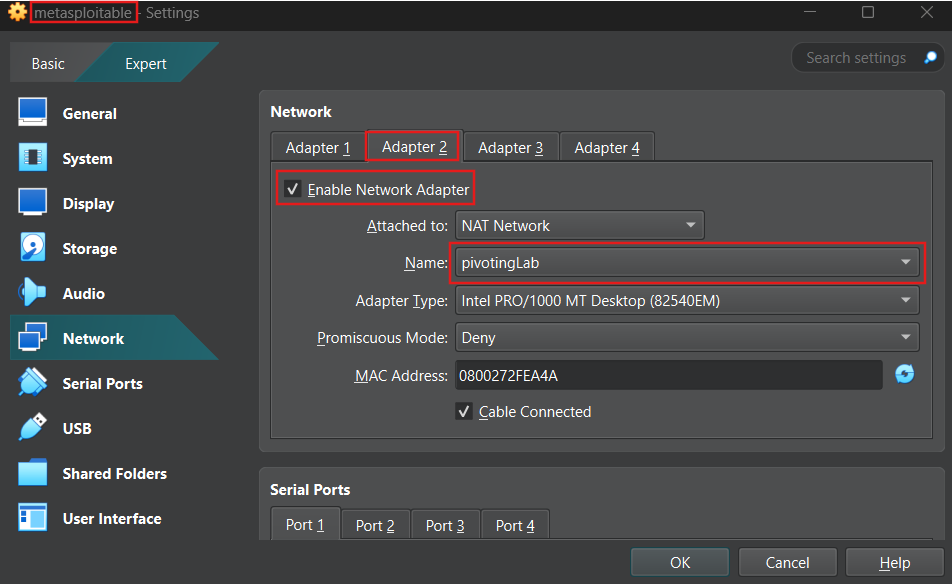
### a) Create an isolated network card (e.g. , Nat Network)



### b) Configure the Pivot Machine

On your virtualization platform (e.g., VirtualBox), go to the settings of the pivot machine (e.g., *Metasploitable*), and add a **second network adapter**:

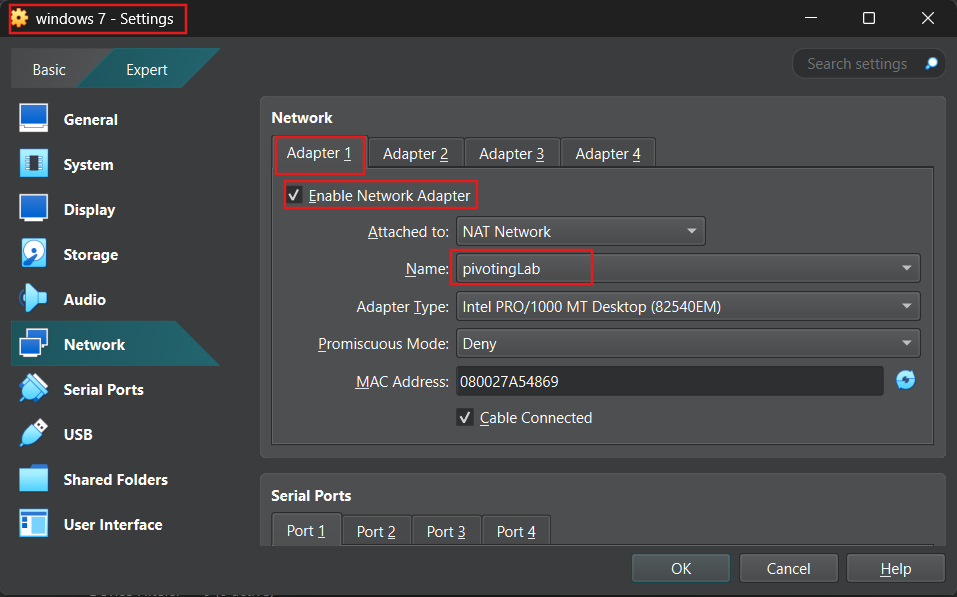
* Adapter 1: NAT or Bridged (connects to the attacker machine)
* Adapter 2: Nat network or Host-only or another isolated network (connects to the internal target machines)



### C) Configure the Internal Target Machines

Now set up the Windows 7 and Metasploitable 2 VMs:

* Each should have only **one network adapter**, connected to the same internal network as the pivot machine’s second adapter.
* These machines ***should not*** be reachable directly by the attacker



A computer screen shot of a computer

AI-generated content may be incorrect.

### d) Networking Configuration

Assuming the following IP assignments:

**Attacker Machine (Kali)**

* eth0: 10.0.2.9
* eth1: (none)

**Pivot Machine (Metasploitable)**

* eth0: 10.0.2.10
* eth1: 10.0.3.6

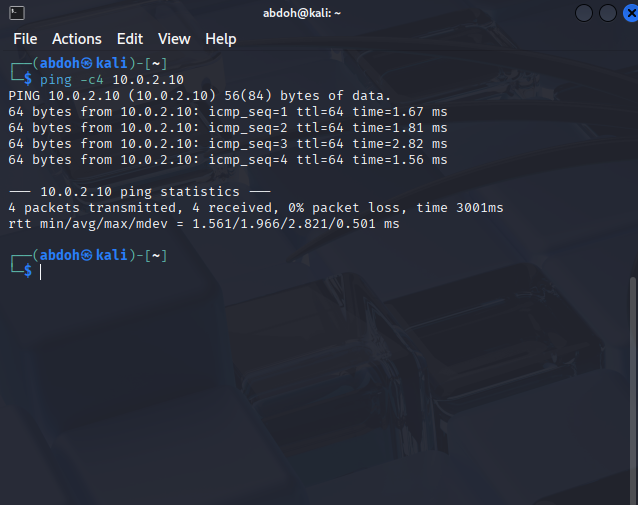
**Internal Target - Windows 7**

* eth0: 10.0.3.4
* eth1: (none)

## Test Connectivity

Make sure your machines can talk to each other where appropriate.

* From **attacker to pivot**: ping 10.0.2.10 — should succeed

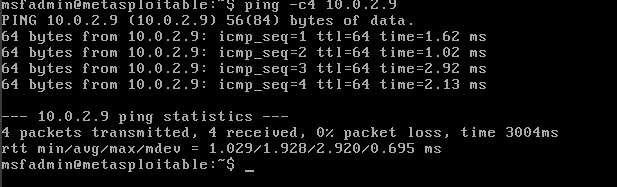


* From **attacker to internal target** (e.g., 10.0.3.4): ping should fail

A screenshot of a computer

AI-generated content may be incorrect.

* From **pivot to attacker**: ping 10.0.2.9 — should succeed



* From **pivot to internal target**: ping 10.0.3.4 — should succeed

A screenshot of a computer program

AI-generated content may be incorrect.

**Tip:** Disable the firewall on the Windows 7 machine to allow ICMP (ping) traffic.

A screenshot of a computer

AI-generated content may be incorrect.