



# A PENTESTERS GUIDE

Setting up your local testbed

## Requirements:

- Install [Oracle Vbox](#)
- Install [Kali Linux](#)
- Install [Ubuntu](#)
- Download [Metasploitable 2](#)
- Download [Metasploitable 3](#)

## Setting Up Vbox Environment

- **Adding the Nat Network**
  - File → Preferences → Network → Green plus sign
  - Right click on the new Nat Network and rename it to Testbed (you can also change the subnet its under if you would like)
  - **IMPORTANT:** Make sure that the network is enabled and it is supporting DHCP
- **Mounting the iso**
  - Open Oracle Vbox and click the blue “New” button
  - Kali VM
    - Name it whatever you want (this will be your main pentesting box)
    - Type: Linux
    - Version: Debian 64-bit
    - Accept all default settings (if you would like to add more ram or storage feel free)
    - After you will see the VM on the left pane
    - Right click on VM and click Settings → Storage → Disk with green plus → Add → Navigate to the Kali iso
    - **While still in setting**
      - Network → Adapter 1 → Attach to: → Nat Network → Testbed
    - Start the machine
    - Default login
      - Username: kali
      - Password: kali
  - Ubuntu
    - Name it DVWA
    - Type: Linux
    - Version: Ubuntu 64-bit
    - Accept all default settings (if you would like to add more ram or storage feel free)
    - After you will see the VM on the left pane
    - Right click on VM and click Settings → Storage → Disk with green plus → Add → Navigate to the Ubuntu iso
    - **While still in setting**
      - Network → Adapter 1 → Attach to: → Nat Network → Testbed
    - Start the machine and run through the setup

- Metasploitable 2
  - After installing make sure to extract the file
  - Name it Metasploitable 2
  - Type: Linux
  - Version: Ubuntu 64-bit
  - When Hard Disk comes up choose “Use an existing virtual hard disk file”
    - Click the folder icon and navigate to the Metasploitable 2 file and open the VMDK
- Metasploitable 3
  - After installing from the link
  - In Vbox click Tools → Import
  - Browse to the OVA File and click import
  - Start the machine so it can load the Windows server

### **DVWA (Damn Vulnerable Web App):**

- Install Ubuntu 18.0 iso or newer to Oracle Vbox
- Run *apt update*
- Run *apt install net-tools*
  - This is just so you can use *ifconfig*
  - Only necessary for Ubuntu 18 or below
- Run *apt install docker.io*
  - This will allow you to pull docker files from the docker hub
- Run *docker pull vulnerables/web-dvwa*
- Run *nano* or *vim* to edit a new file called *start-dvwa*
  - Write this into text file → *docker run --rm -it -p 80:80 vulnerables/web-dvwa*
  - Make it executable *chmod +x start-dvwa*
  - Use *./start-dvwa* to start the server
- To access navigate to <http://127.0.0.1/login.php>
  - Default login
    - Username: admin
    - Password: password
- Click the button at the bottom of the page that says “Setup DVWA”