

Penetration Testing LAB Setup Guide

(Internal Attacker - Beginner version)

By: magikh0e - magikh0e@ihtb.org

Last Edit: July 07 2012



This guide assumes a few things...

- 1. You have installed Backtrack before and you are familiar with using VirtualBox.**
- 2. You like breaking shit!**

Contents

Getting Started.....	3
Why setup a LAB?	3
LAB Setup	4
LAB Setup – Creating VirtualBox Instances.....	5
BackTrack	5
PfSense.....	7
LAB Setup - Vulnerable Machines.....	11
Metasploitable 2	12
Kioptrix – Level 1.....	12
PfSense Setup	14
Configuration	14
Extra Packages (optional).....	14
SNMP Setup (optional).....	14
PfSense - DHCP.....	15
Virtual Lab Layout & Diagrams.....	16
Virtual Box Layout	16
Virtual Network Diagram	17
Conclusion.....	18
Exploitation Guides	18

Getting Started

This penetration testing guide has been created with a few things in mind. One being the reader is a beginner in the field of penetration testing. Two being the attacks are designed from attacker with internal access into the network being penetrated. Future guides will extend upon this document bringing more advanced network setups and unique vulnerabilities.

After setting up this LAB environment, you will have the ability to exploit issues from the following categories:

1. Mis-configured Services and Applications
2. Backdoors planted into software
3. Un Intentional Backdoors
4. Weak Passwords
5. Web Applications
6. Plus lots more, how much can you find?

Why setup a LAB?

Penetration testing is a skill that takes practice to be perfect. In order to be good at it, you must have lots of practice and experience. Unfortunately hacking into computers or the networks that they live on in most cases is illegal. This is where a penetration testing lab comes into value. This LAB should never be used in any sort of publically accessible or production network, it has been made vulnerable intentionally ;)

LAB Setup

Prerequisites

Before getting started, you will need to have installed a working copy of VirtualBox.

VirtualBox: <https://www.virtualbox.org/wiki/Downloads>

Along with copies of the following files from the awesome projects below:

BackTrack R2: <http://www.backtrack-linux.org/downloads/>

PfSense 2.0.1: <http://www.pfsense.org/mirror.php?section=downloads>

I used: [pfsense-2.0.1-RELEASE-i386.iso.gz](#) - <http://files.chi.pfsense.org/mirror/downloads/pfSense-2.0.1-RELEASE-i386.iso.gz>

Metasploitable 2: <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Kioptrix - Level 1: <http://www.kioptrix.com/blog/>

To keep things neat and tidy, create a folder somewhere to place all the above files in. The inside of this folder create a *VirtualMachines* folder. Here you can store the extracted images, as well as virtual disk you will be creating for BackTrack and PfSense installs.

You will obviously need a pretty beefy machine in order to run all of the above machines virtually. At a bare minimal, only the following are required to be running. If you follow the exact guide, you will need at least 4GB ram minimum to allocate to all instances.

1. PfSense
2. BackTrack
3. Metasploitable 2 and/or Kioptrix – Level 1

LAB System Requirements

4GB of system ram for allocation to Virtual Instances.

You can potentially get away with using less, though 4 is recommended.

20.0 GB hard drive space – **15.4 GB** without keeping archives and ISO files.

LAB Setup – Creating VirtualBox Instances

BackTrack

1. Create a new machine in VirtualBox for BackTrack – R2.

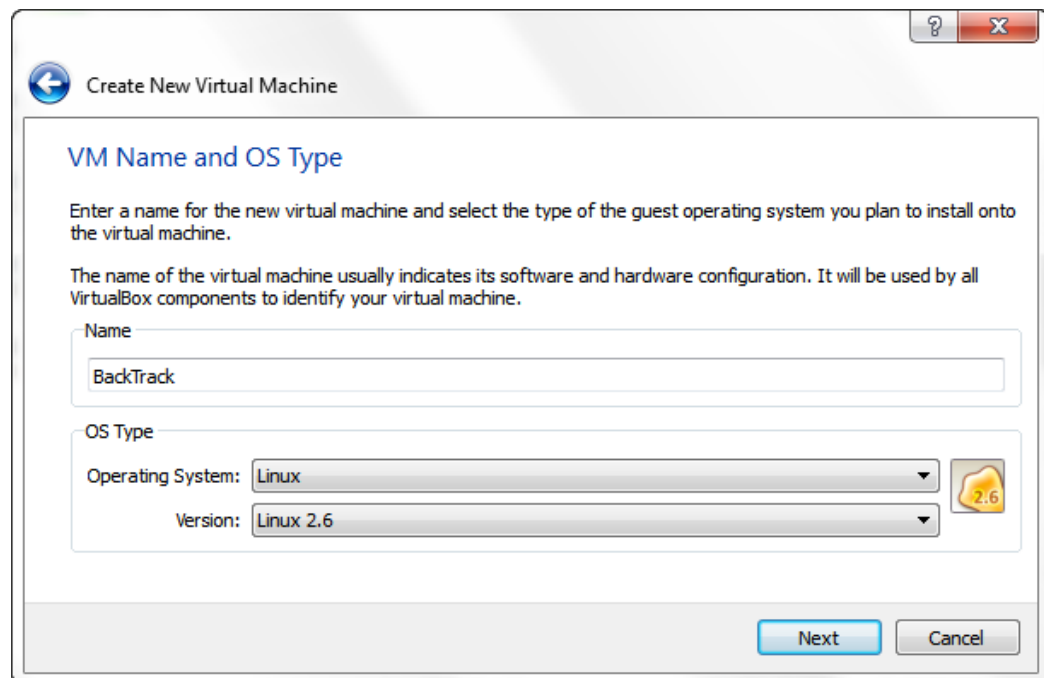
Name: BackTrack

Operating System: Linux

Memory: 512MB minimal – I used 1024MB.

Startup Disk: 12.00 GB minimal

- a. When creating the instance for BackTrack, you will need a minimal of 512mb of ram for this instance.



- b. Edit the Network settings of **Adapter 1** to match the following settings.

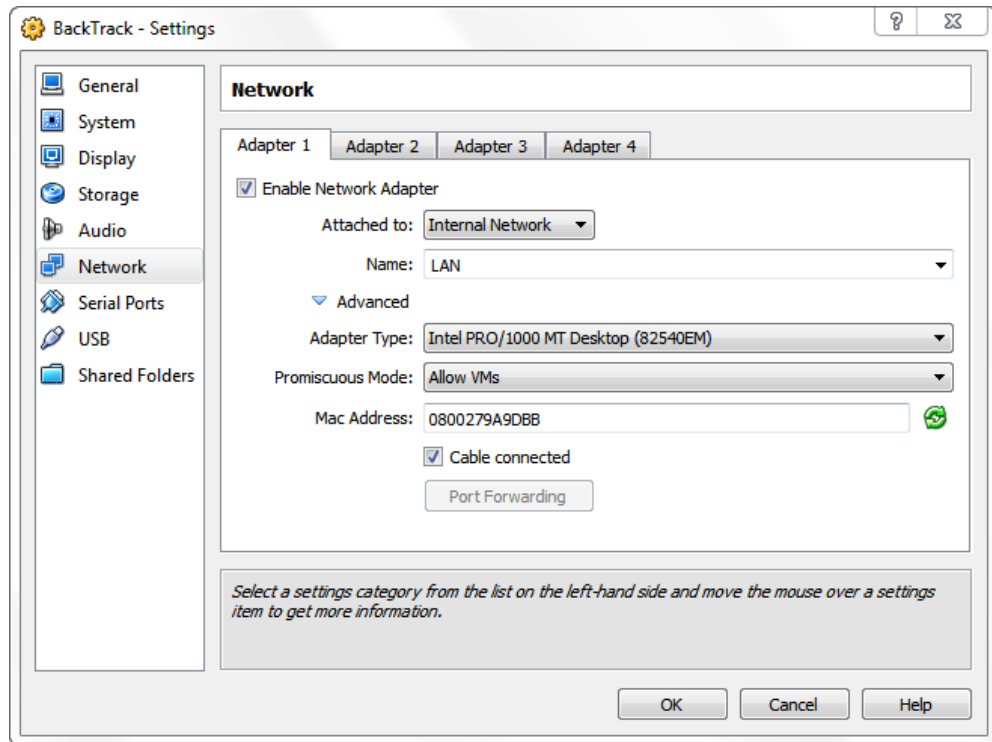
NOTE: While in the configuration, write down the instances MAC Address.

Attached to: Internal Network

Name: LAN

Promiscuous Mode: Allow VMs

MAC Address:



- c. Once the instance has been created, start the instance and then proceed to install BackTrack to the virtual disk that has just been created.



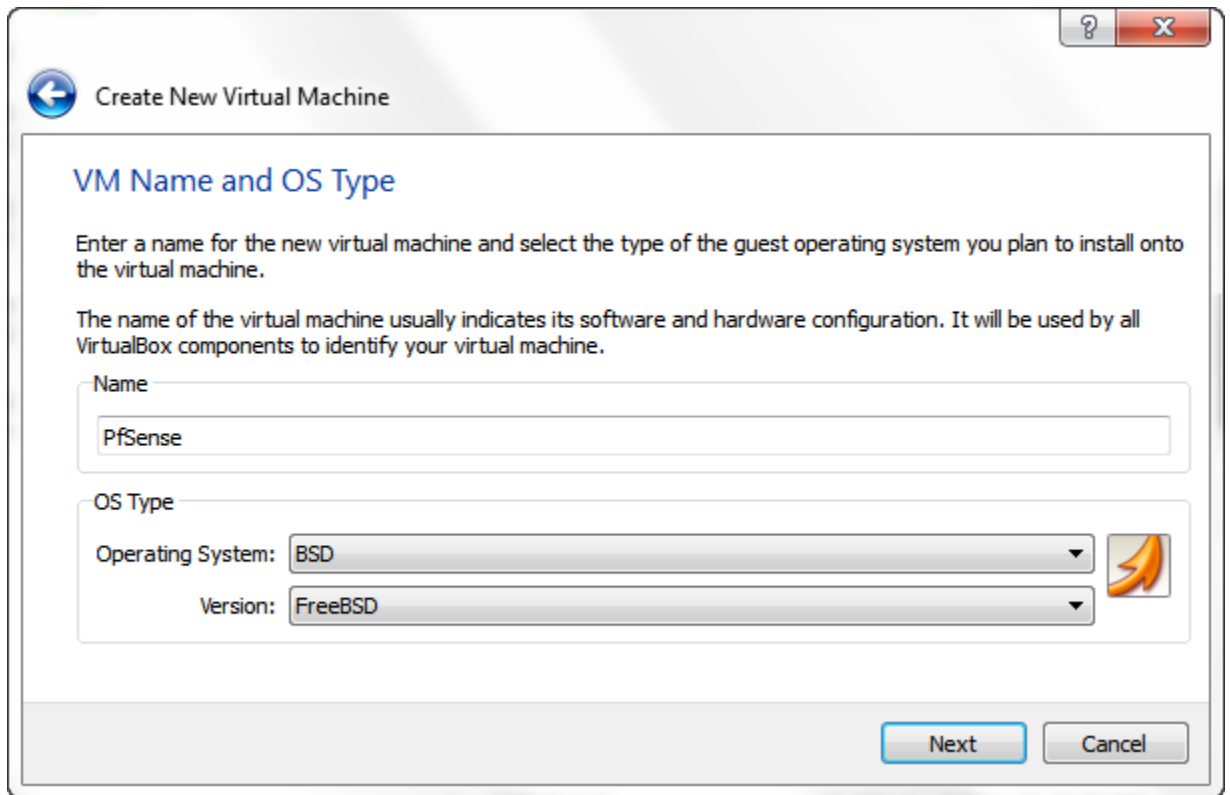
PfSense

1. Create another machine in VirtualBox for **PfSense 2.0.1**.

Operating System: FreeBSD

Memory: 512MB

Startup Disk: 5.00 GB minimal – you *should* not need over 10GB max.



VM Name and OS Type

Enter a name for the new virtual machine and select the type of the guest operating system you plan to install onto the virtual machine.

The name of the virtual machine usually indicates its software and hardware configuration. It will be used by all VirtualBox components to identify your virtual machine.

Name
PfSense

OS Type
Operating System: BSD
Version: FreeBSD

Next Cancel

NOTE: This instance will require a bit more configuration on the network adapter side of things.

Installation & Network Configuration

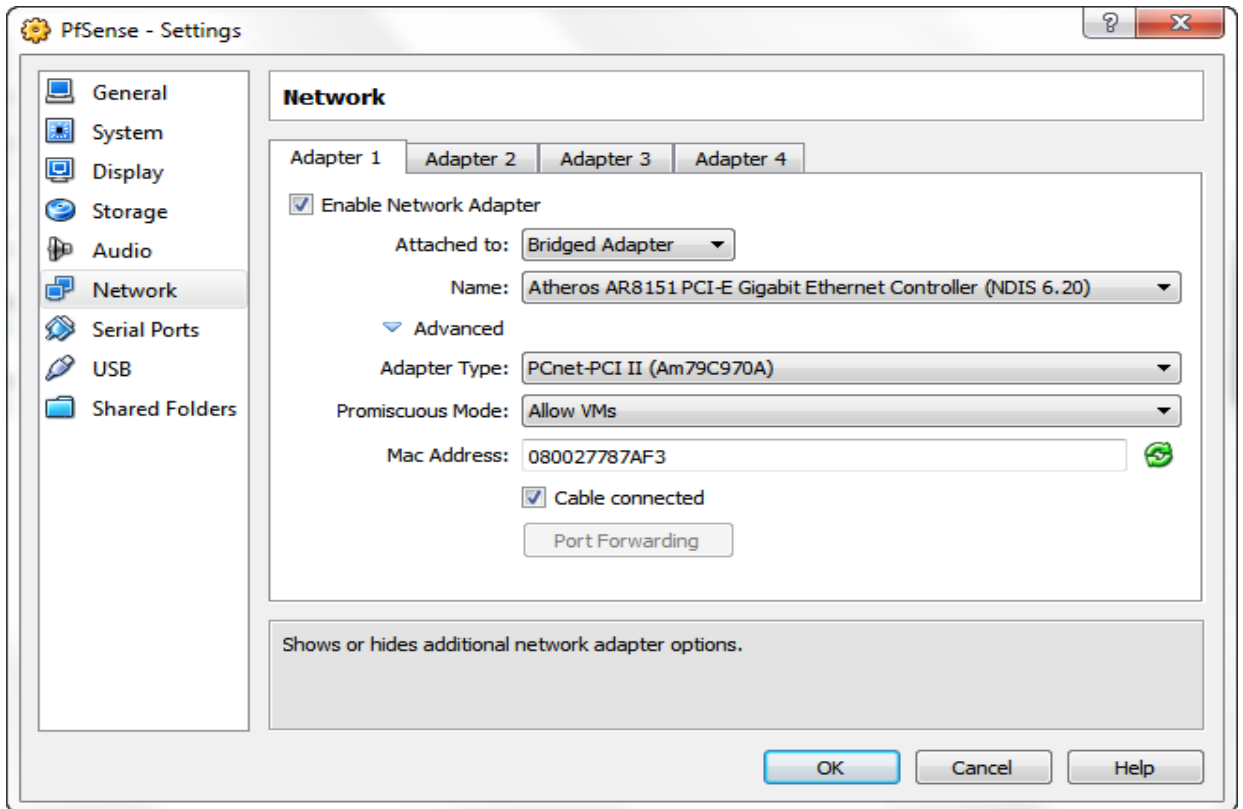
1. Edit the settings for this instance, and then add a new network card, then configure each interface to match the following settings.

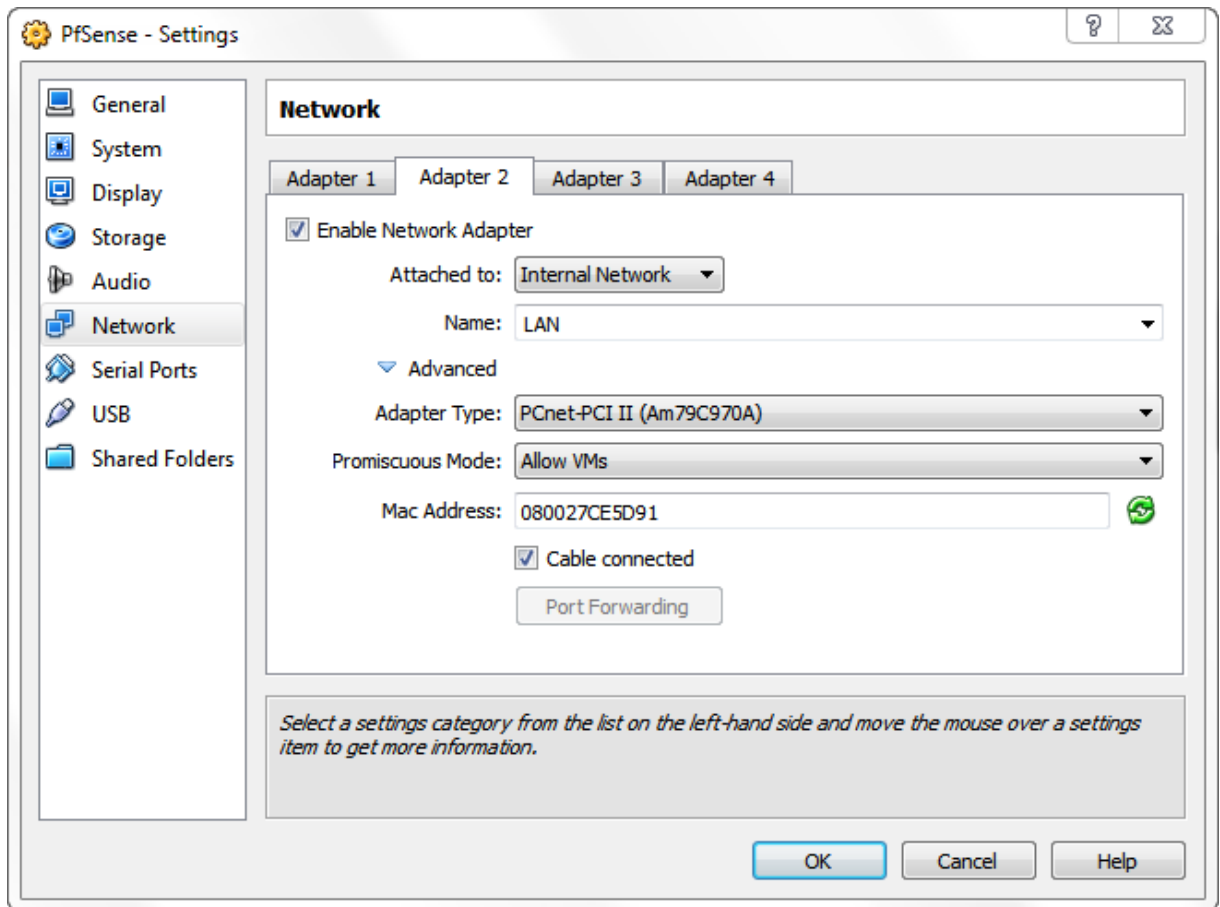
Adapter 1

Attached to: Bridged Adapter
Promiscuous Mode: Allow VMs
Advanced Menu:
Adapter Type: PCnet-PCI II

Adapter 2

Attached to: Internal Network
Name: LAN
Promiscuous Mode: Allow VMs
Advanced Menu:
Adapter Type: PCnet-PCI II





2. Make sure to set **Adapter Type** to **PCnet-PCI II**, or things will not work correctly.
3. Once the instance has been created, start it up and install **PfSense**.
 - a. Upon booting press **1** to continue with the start-up.
 - b. At the prompt, press **I** to proceed with the installation. Once prompted, use the following options in order.
 - i. Accept these settings.
 - ii. Quick/Easy Install
 - iii. OK
 - iv. Symmetric multiprocessing kernel
 - v. Reboot PfSense.

4. After PfSense reboots, you will be prompted with the option to create VLANs. Type *n* and then hit *Enter* to continue.
 - a. Once at the '*Enter the WAN interface prompt type the WLAN1 interface*'. Type in *le0*, and press *Enter*.
 - b. You will now be prompted to specify the **LAN** interface. Type in *le1*, and press *Enter*.
 - c. To continue press *Enter* again and then *y* when prompted to continue.
 - d. PfSense should now be installed.

5. Once PfSense has been installed, you will need to set the **IP Address** of the **LAN** interface.
 - a. From the PfSense console select **option 2** '*Set interface(s) IP address*'.
 - b. At the Enter the number of the interface you wish to configure: prompt, type **2** to choose the **LAN** interface.
 - c. When prompted, use the following **IP Address**: 192.168.12.1
 - d. Use **24** at the '*LAN IPv4 subnet bit count prompt*'.
 - e. Type **y** at the prompt when asked if you would like to enable the DHCP server on LAN.
 - f. When asked to provide the starting address range, use the following **starting IP Address**: 192.168.12.50
 - g. You will then be asked to specify the **ending IP Address** for the DHCP range. Use the following IP Address: 192.168.12.100.
 - h. Type **y** when asked to enable web configuration.

At this point PfSense should be handing out addresses within: **192.168.12.50-192.168.12.100** range.

NOTE: *To confirm DHCP is working properly, reboot the BackTrack instance and verify that it now has an address within the range specified above.*

LAB Setup - Vulnerable Machines

What is a penetration testing LAB without things to exploit?

A boring networking lab ;)

For the beginner version of this guide, we will be using some freely available projects purposely built for penetrating. In this guide we will be using Metasploitable 2, provided by the metasploit project, and Kioptrix – Level 1 provided by kioptrix.com.

Metasploitable 2

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download from Sourceforge.net and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMware, VirtualBox, and other common virtualization platforms.

Kioptrix – Level 1

Kioptrix VM Image's are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games is to learn the basic tools and techniques in vulnerability assessment and exploitation. There is more ways than one to successfully complete the challenges.

Metasploitable 2

1. Create a new VBox Instance for **Metasploitable 2** using the following options.

Name: Metasploitable 2

OS Type: Linux 2.6

Memory: 512

Startup Disk: Metasploitable.vmdk (Normal, 8.00 GB)

NOTE: *Make sure you are selecting the **Use existing hard disk** option:
then browse to the Metasploitable.vmdk file that was downloaded earlier.*

2. Once the instance has been created, you will need to change some settings on **Adapter 1** in the Network settings. From the Network section.
Go to **Adapter 1** and change the following options.

Attached to: Internal Network

Name: LAN

NOTE: *Under the Advanced menu, take note of the MAC address. You will need it later.*

Kioptrix – Level 1

1. Create a new VBox Instance for **Kioptrix – Level 1** using the following options.

Name: Kioptrix VM Level 1

OS Type: Other Linux

Memory: 256

Startup Disk: Kioptrix Level 1.vmdk (Normal, 3.00 GB)

NOTE: *Make sure you are selecting the **Use existing hard disk** option:
The Kioptrix Level 1.vmdk file can be found within the download.*

3. Once the instance has been created, you will need to change some settings on **Adapter 1** in the Network settings. From the Network section.
Go to **Adapter 1** and change the following options.

Attached to: Internal Network

Name: LAN

NOTE: *Under the Advanced menu, take note of the MAC address. You will need it later.*

PfSense Setup

Configuration

Now that PfSense has been setup in a default state, and confirmed to be handing out DHCP addresses properly. We can now begin configuration of PfSense by accessing it via the web interface from the BackTrack machine using Firefox.

To access the PfSense web interface, open the following URL in Firefox: <http://192.168.12.1>

The default username is: **admin** and the default password is: **pfsense**.

Login to the web interface and follow the prompts through the guided wizard to complete installation. Nothing needs to be changed at this point, other than verifying the settings you have specified earlier.

Once the PfSense setup has finalized, reload the web interface to get to the main configuration view.

Extra Packages (optional)

A few **optional** packages can be installed.

These packages will not be used in this guide, though they will in the **External Attacker – Intermediate** version of this guide.

1. From the PfSense interface, go to System->Packages.
Then Install **Proxy Server with mod_security** by clicking the \pm icon next to the listing.
2. Once installed, go back to System->Packages.
Then install **snort**.

SNMP Setup (optional)

Since this is a penetration testing guide for beginners, let's start out by making the firewall it's self a little bit vulnerable. This will make something simple and easy to test out SNMP enumeration attacks or vulnerability scanners.

1. From the PfSense web interface, go to Services->SNMP.
2. Next to the **SNMP Daemon** section, check off **Enable**.
Then save the settings.

PfSense - DHCP

Now that PfSense has been setup and configured, you can now make use of the MAC Addresses you have taken note off earlier when creating the vulnerable lab machines.

Vulnerable machines - Static Reservations

1. Open up the PfSense web interface. Then go to Services->DHCP Server.
 - a. Verify that the range specified is the same range specified you have specified earlier in this guide during the PfSense setup.

NOTE: This never seems to be the same range as specified on the console initially.

2. Scroll to the bottom and add a new Static Reservation for the Metasploitable 2 and Kioptrix instances. Using the MAC addresses you wrote down.

Metasploitable2:	Kioptrix - Level 1:
MAC Address: (the one you wrote down)	MAC Address: (the one you wrote down)
IP Address: 192.168.12.20	IP Address: 192.168.12.30
Hostname: metasploitable2	Hostname: kioptrix1
Description: metasploitable2	Description: kioptrix - level 1

3. Once the above reservations have been created, you can now save & apply the settings to PfSense.
4. Verify the configuration by restarting each vulnerable instance.

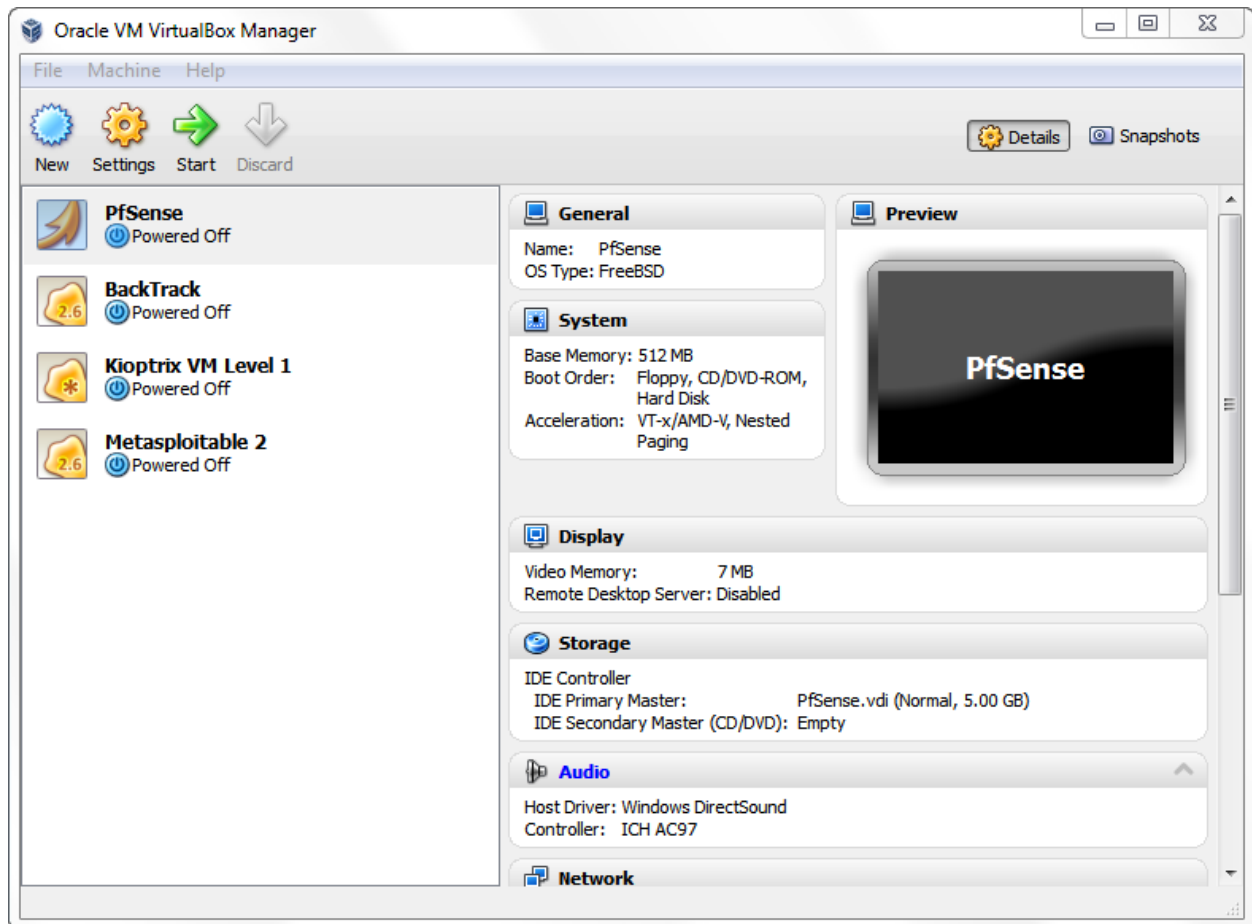
To simplify the setup, you can edit the `/etc/hosts` file on the BackTrack machine, adding the following entries:

192.168.12.20 metasploitable2

192.168.12.30 kioptrix1

Virtual Lab Layout & Diagrams

Virtual Box Layout



Virtual Network Diagram

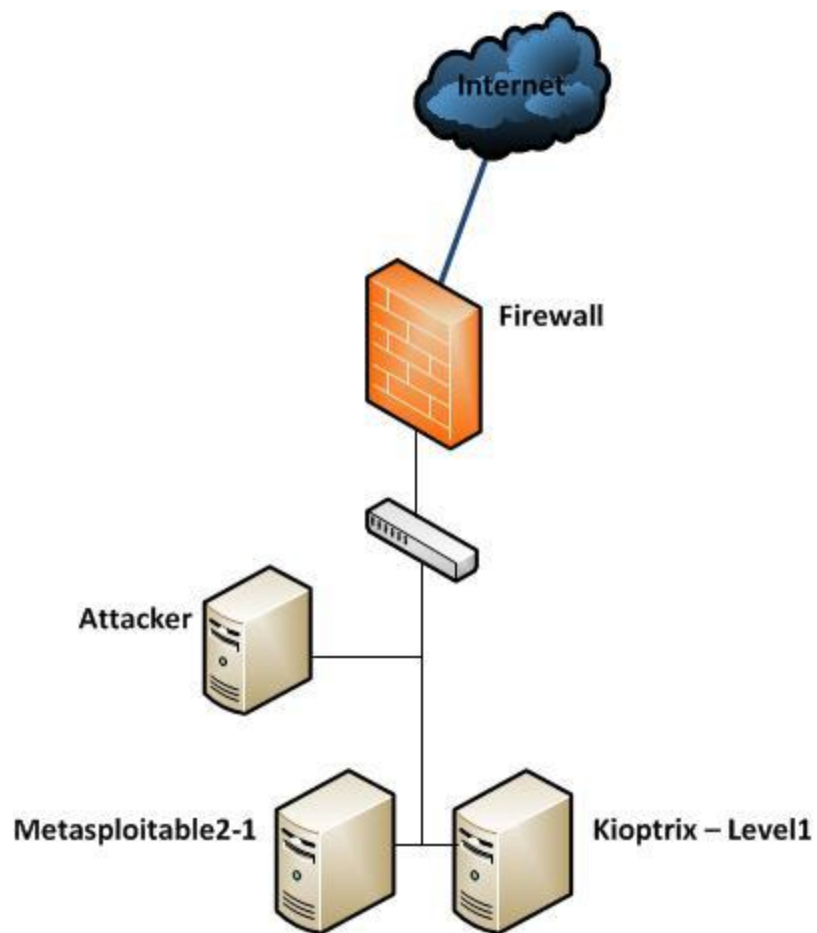
External Subnet: DHCP Assigned
Internal Subnet: 192.168.12.0/24

Firewall: Internal: 192.168.12.1 External: DHCP Assigned

BackTrack / Attacker: Internal: 192.168.12.x/24

Metasploitable2: Internal: 192.168.12.20

Kioptrix1: Internal: 192.168.12.30



Conclusion

Once everything has been started, you should now be ready to start testing out your skills in the newly created penetration testing LAB. Keep in mind this LAB has been designed with access from an internal attacker's perspective. From the BackTrack machine you can now start exploring the **192.168.12.0/24** network. Have fun!

If you have any questions or issues with the above instructions, please let me know. As this is an initial release, so expect some bugs or un-documented features to come up ;D

If you are completely clueless after following this guide, have a look at the following exploitation guides.

Exploitation Guides

If you are truly a beginner, this will help you out along the way. If not, carry on and start hacking...

Metasploitable 2 Exploitability Guide: <https://community.rapid7.com/docs/DOC-1875>

As always, Hackers do it with all sorts of characters...

Syntax Guide

Below is a reference point for syntax and highlighting used throughout this guide.

Information – Denotes required information.

command – Reference to a system command, normally not required to be run by the user for the instructions unless stated otherwise.

command – Reference to a system command to be ran by the user as part of the instructions.

Something: something – Reference to an option in the GUI application.

Action – Denotes some action to be performed with the current GUI application.

File name – Specifies a file name.