Penetration Testing LAB Setup Guide

(External Attacker - Intermediate)

By: magikh0e - magikh0e@ihtb.org

Last Edit: *July 06 2012*

This guide assumes a few things...

1. **You have read the basic guide of this lab setup.**
2. **You like breaking more shit or need to test out some auditing tools.**

Contents

Getting Started..3

Why setup a LAB? 3

LAB Setup 4

LAB Setup – Creating Virtual Box Instances...5

Debian 6 5

LAB Setup – Network Setup & Reconfiguration..6

PfSense..6

Debian 6 14

Reconfiguring BackTrack...16

LAB Setup – Virtual and Vulnerable Machines 17

Metasploitable 2 – Attack of the clones 17

Virtual Lab Layout & Diagrams..18

Virtual Box Layout 18

Virtual Network Diagram 20

Conclusion..21

Getting Started

It’s simple. Go through the router, over the firewall. There is where you will find grandma’s house…

Good luck!

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

1. You will figure it out…

Why setup a LAB?

If you have made it this far, I am sure you now understand this. If not, go back to the Basic guide =)

LAB Setup

Prerequisites

Make sure you have read the basic version of this guide. A lot of the following setup will assume a basic lab has already been created.

For the intermediate penetration testing lab setup, you will be using the following.

-LAB Setup from the Basic Guide
Debian 6: http://www.debian.org/

IMPORTANT NOTE

In order to follow this guide, you must have already created the basic penetration testing LAB setup. If not, read the basic guide first before continuing:
http://magikh0e.ihtb.org/pubPapers/Penetration_Testing_LAB_Setup_Guide-iab.pdf

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 4.5GB ram minimum to allocate to all instances.

1. PfSense
2. BackTrack
3. Metasploitable 2-1
4. Metasploitable 2-2
5. Debian 6

LAB System Requirements

4.5GB of system ram for allocation to Virtual Instances.
23.0 GB hard drive space – ***17.4 GB*** without keeping archives and ISO files.

LAB Setup – Creating Virtual Box Instances

Debian 6

1. Create a new machine in Virtual Box for Debian 6.
   Operating System: Debian
   OS Type: Debian
   Memory: 512
   Startup Disk: 12.00 GB

   a. When creating the instance for Debian 6, you will need a minimal of 512mb of ram and a minimal of 12GB hard drive space for the instance.

   b. Edit the Network Interface of **Adapter 1** to match the following settings.
   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 **Debian 6** to the virtual disk that has just been created.

LAB Setup – Network Setup & Reconfiguration

PfSense

Resetting Back to Factory Defaults

1. At the PfSense console, Type **4** to proceed with a factory reset. Type **y** when asked if you wish to proceed with the reset.
    a. Once the reset is complete and a reboot has been performed, you will be asked to setup VLANs. Type **n**.
    b. Once at the '*Enter the WAN interface prompt type the WLAN1 interface'.*
       Type in ***le0***, and then press *Enter*
    c. You will now be prompted to specify the LAN interface. Type in ***le1***, and then press *Enter.*
    d. To continue press *Enter* again and then *y* when prompted to continue.
    e. PfSense should now be installed.

Initial Setup & Configuration

1. Once PfSense has been reset to defaults, 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 for the **LAN interface**: 192.168.13.1
    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**: 192.168.13.50.
    g. You will then be asked to specify the **ending IP Address** for the DHCP range. Use the following **IP Address**: 192.168.13.100.
    h. Type y if asked to enable web configuration.

At this point PfSense should be handing out addresses within: **192.168.13.50-192.168.13.100** range. To confirm, reboot the BackTrack instance and verify that it now has an address within the range specified above.

Accessing PfSense Interface

Now that PfSense has been restored to a default state, and confirmed to be handing out DHCP addresses properly. You can now begin reconfiguring PfSense for the intermediate labs 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://192.168.13.1

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, set a new password and click on the reload button.

NOTE: The Firefox that comes with BackTrack is bundled with *noscript*, so by default it will block some functionality from the PfSense website.

Once you see “Congratulations! PfSense is now configured.” The configuration has been completed. Click on “Click here to continue on to pfSense webConfigurator.” this will reload the web interface to get to the main configuration view.

Required Packages

A few packages are required to be installed for the intermediate LAB setup. If you have already done the optional parts from the beginner guide, you can skip this part.

Proxy Server with mod_security - ModSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pfSense using 1 IP address.

Snort - Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

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

Optional Packages

Depending on your purpose for building this LAB, you may also find the following packages useful.

Arpwatch - Arpwatch monitors Ethernet/ip address pairings. It also logs certain changes to syslog.
Dashboard Widget: Snort - Dashboard widget for Snort.
Nmap – d0h
ntop - ntop is a network probe that shows network usage in a way similar to what top does for processes.
System Patches - A package to apply and maintain custom system patches.

NOTE: If you are unable to get a list of Available Packages on the PfSense box, check and make sure that the WAN interface on your PfSense instance is receiving an IP address from your local DHCP server.

DHCP Setup

You can now make use of the MAC Addresses you have taken note off earlier when creating the vulnerable lab machines in the basic guide and intermediate guide. You will need the MAC address from the following instances: **Metasploitable2-1, Metasploitable2-2,** and **Debian 6**

Static Reservations

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

    NOTE: This part seems to have a bug in that the range is usually not what was specified on the console. If you do not fix the range, you will get errors when attempting to create the reservations. If the ranges are not what were specified, correct them and apply the settings before proceeding with the next step.

2. Scroll to the bottom and add a new Static Reservation for the **Metasploitable 2-1**, **Metasploitable2-2** and **Debian 6** instances.

Metasploitable2-1:		**Metasploitable2-2**:		**Debian 6**:	
MAC Address:		**MAC Address**:		**MAC Address**:	
IP Address:	192.168.13.20	**IP Address**:	192.168.13.21	**IP Address**:	192.168.13.10
Hostname:	metasploitable2-1	**Hostname**:	Metasploitable2-2	**Hostname**:	Debian 6
Description:	metasploitable2-1	**Description**:	Metasploitable2-2	**Description**:	Debian 6

3. Once the above reservations have been created, you can now *save & apply* the settings to PfSense.

4. Verify the DHCP reservation by restarting each of the vulnerable instances.

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

```
192.168.13.20   box1
192.168.13.21   box2
192.168.13.10   debian
```

Firewall Configuration

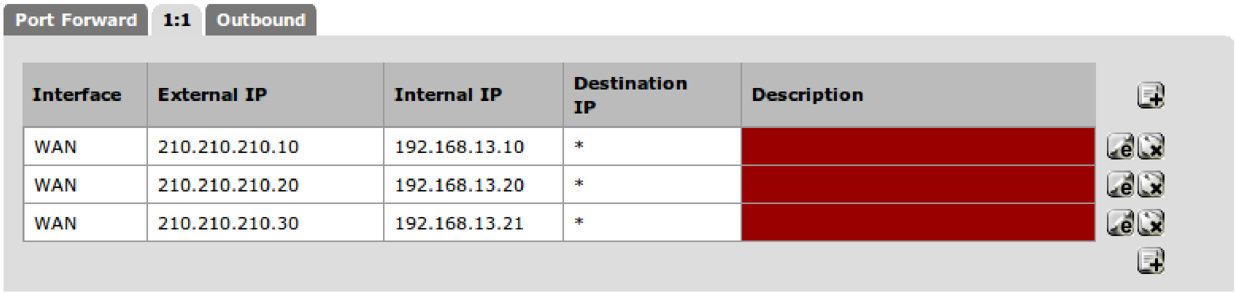
NAT and Virtual IPs

To mimic a real world environment, we will be using network address translation on the firewall into the LAB. The intermediate lab is designed to be from an external attacker's view, unlike the basic guide where the attacker had internal access into the network already. Here you will not find as many entry points changing the playing field and required skill levels.

Our simulated WAN network will live on the **210.210.210.0/24** subnet. You will need to create two 1:1 NATs as well as two Virtual IP Addresses.

1. Go to *Firewall->NAT* then select the *1:1* tab. Then click on the + icon to add a new NAT entry.
2. Add the following two entries then *save & apply* the changes.

    a. **External subnet IP**: 210.210.210.10
       Internal IP: 192.168.13.10
    b. **External subnet IP**: 210.210.210.20
       Internal IP: 192.168.13.20

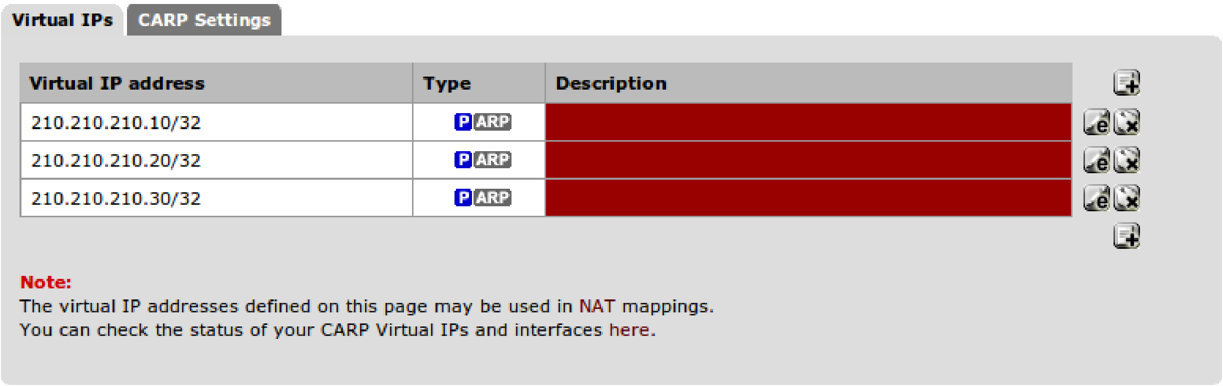


Interface	External IP	Internal IP	Destination IP	Description
WAN	210.210.210.10	192.168.13.10	*	[redacted]
WAN	210.210.210.20	192.168.13.20	*	[redacted]
WAN	210.210.210.30	192.168.13.21	*	[redacted]

PfSense will not automatically create proxy arps for **1:1** or ***static*** NATs. This is where the virtual IPs will come in handy.

1. Go to *Firewall->Virtual IPs*, add a new virtual IP by clicking the + icon.
2. Add the following two entries then save & apply the changes.

    a. **Type**: Proxy ARP
       IP Address(es): 210.210.210.10
    b. **Type**: Proxy ARP
       IP Address(es): 210.210.210.20
    c. **Type**: Proxy ARP
       IP Address(es): 210.210.210.30



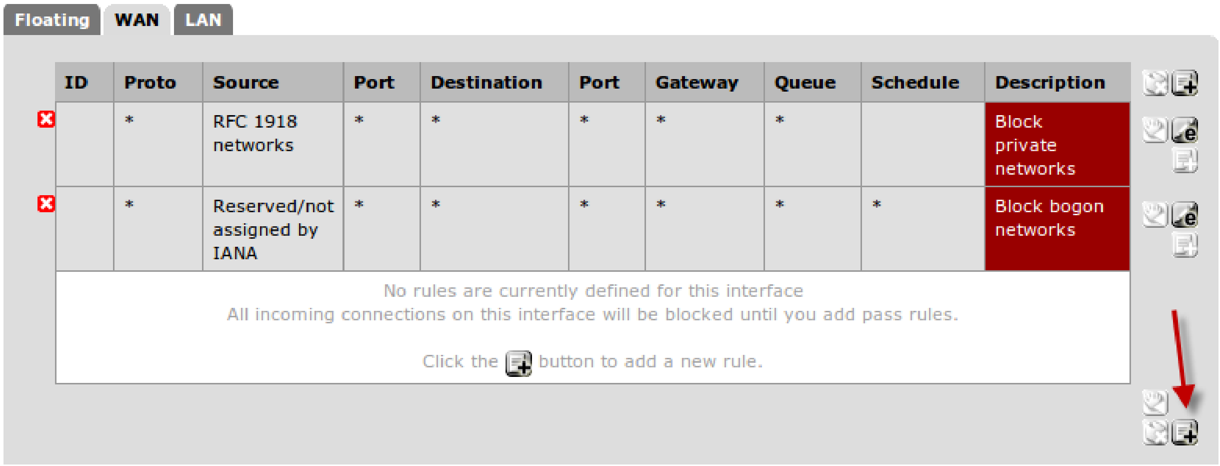
Virtual IPs | CARP Settings

Virtual IP address	Type	Description
210.210.210.10/32	P ARP	
210.210.210.20/32	P ARP	
210.210.210.30/32	P ARP	

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces here.

Once all the NATs and Virtual IPs have been created, you can now go on to create some firewall rules. To mimic real world examples as close as possible, only a bare minimal amounts of ports will be opened to the outside world. In this guide we will only be allowing: **DNS**, **FTP, HTTP, HTTPS, SSH** and **SMTP**. You can always adapt these rules to allow them to be more restrictive or loose.

By default only two rules should currently be define. We will now add some rules by doing the following.



Floating | WAN | LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☒		*	RFC 1918 networks	*	*	*	*	*		Block private networks
☒		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

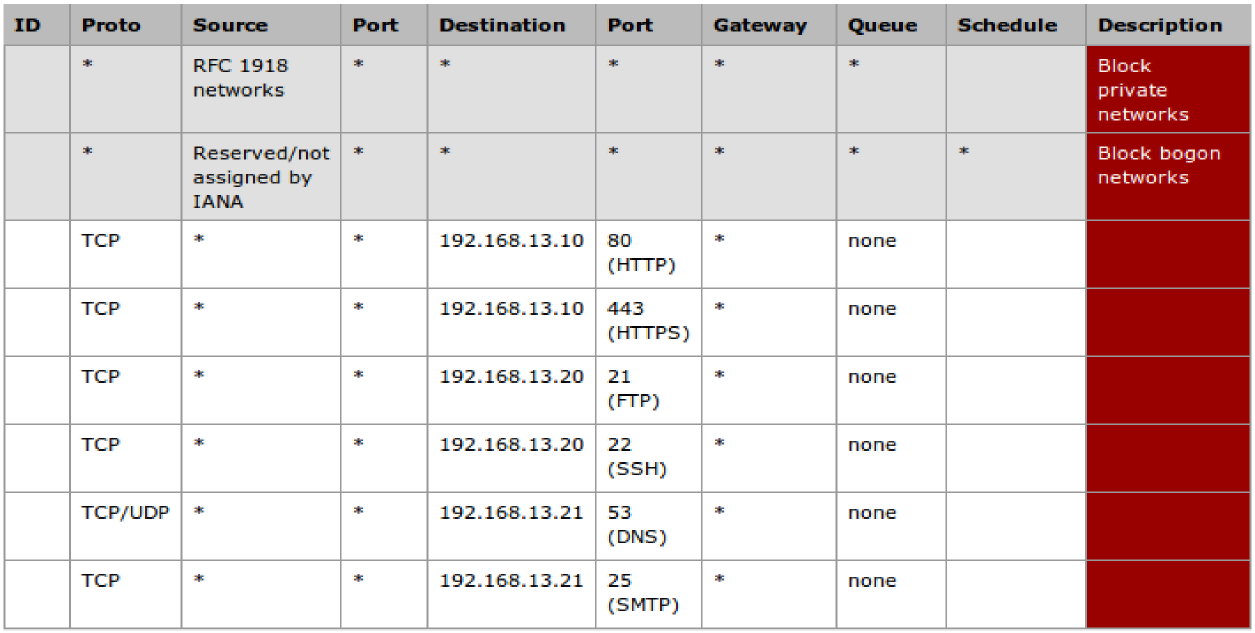
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the ⊞ button to add a new rule.

Adding new firewall rules to PfSense is simple.

1. Go to *Firewall->Virtual IPs*, add a new rule to the bottom by clicking the + icon.
2. Once in the **Firewall: Rules: Edit** menu.
   Create rules to match each of the following. Save and apply the rules once complete.

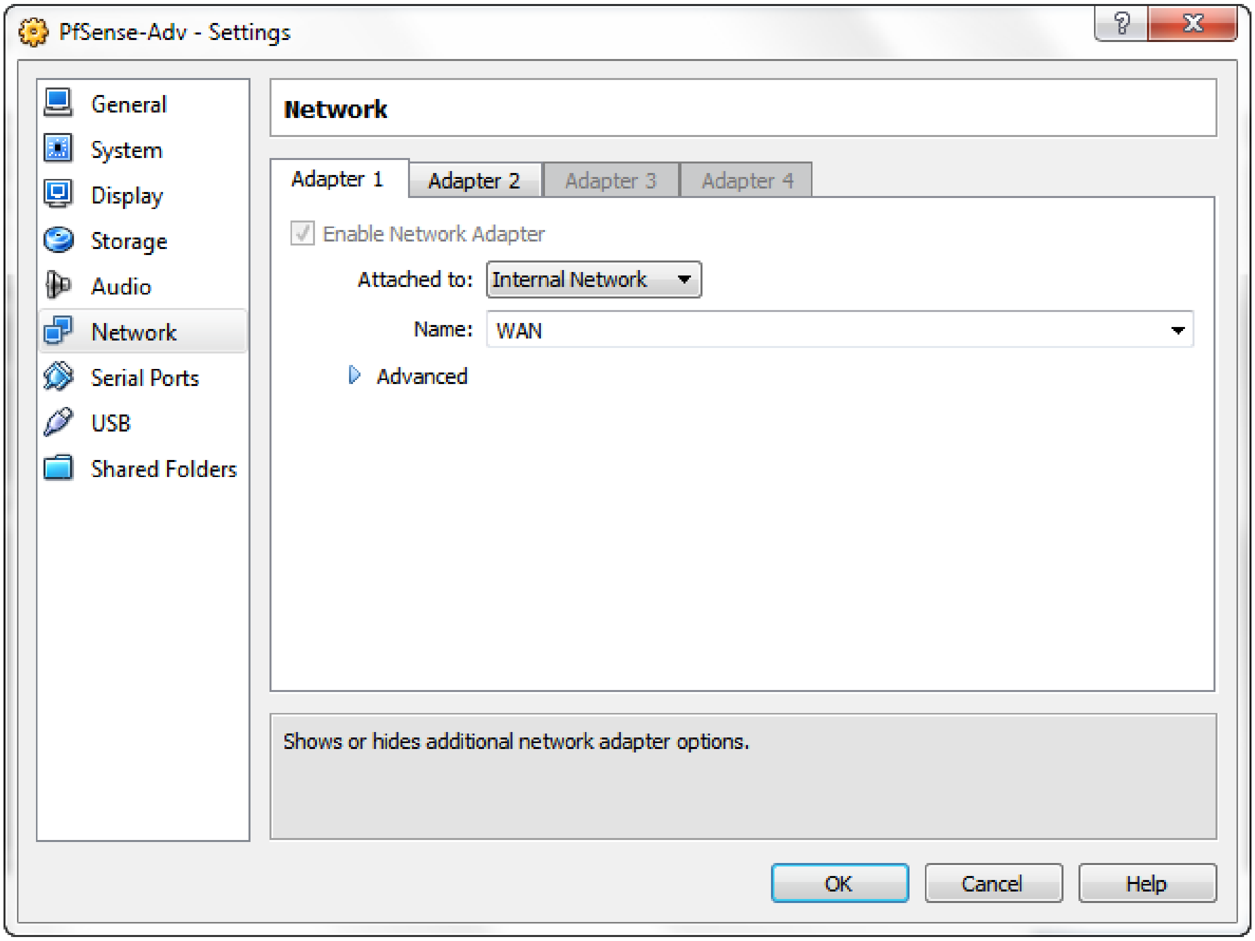
   a. **Action:** Pass
      Destination: Type: Single host or alias Destination: 192.168.13.10
      Destination port range: from: HTTP to: HTTP
   b. **Action:** Pass
      Destination: Type: Single host or alias Destination: 192.168.13.10
      Destination port range: from: HTTPS to: HTTPS
   c. **Action:** Pass
      Destination: Type: Single host or alias Destination: 192.168.13.20
      Destination port range: from: FTP to: FTP
   d. **Action:** Pass
      Destination: Type: Single host or alias Destination: 192.168.13.20
      Destination port range: from: SSH to: SSH
   e. **Action:** Pass
      Protocol: TCP/UDP
      Destination: Type: Single host or alias Destination: 192.168.13.21
      Destination port range: from: DNS to: DNS
   f. **Action:** Pass
      Destination: Type: Single host or alias Destination: 192.168.13.21
      Destination port range: from: SMTP to: SMTP



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*		Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	TCP	*	*	192.168.13.10	80 (HTTP)	*	none		
	TCP	*	*	192.168.13.10	443 (HTTPS)	*	none		
	TCP	*	*	192.168.13.20	21 (FTP)	*	none		
	TCP	*	*	192.168.13.20	22 (SSH)	*	none		
	TCP/UDP	*	*	192.168.13.21	53 (DNS)	*	none		
	TCP	*	*	192.168.13.21	25 (SMTP)	*	none		

Once you have installed all the packages you wish to use and configured the appropriate firewall rules. It is off to grandma's house you go. But before you do that, now would be a good time to close down the LAB network from the outside world.

1. From the PfSense console select option **2** *'Set interface(s) IP address*'.
2. At the Enter the number of the interface you wish to configure prompt, type **1** to choose the **WAN** interface.
3. Type **n** when asked '*Configure WAN interface via DHCP*'.
4. When prompted, use the following IP Address for the **WAN interface**: 210.210.210.1
5. Use **24** at the *LAN IPv4 subnet bit count prompt*.
6. Type **y** if asked to enable web configuration.
7. From the **VBox Manager interface**, Edit the settings of the PfSense instance and change the Network Settings for **Adapter 1**.
    a. Change the existing settings to match the following then click OK.
    Attached to: Internal network
    Name: WAN



PfSense-Adv - Settings

Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: WAN

Shows or hides additional network adapter options.

8. From the PfSense console, Type **5** to reboot the instance.

Debian 6

The **Debian 6** instance will be serving as the HTTP load balancer serving request for **Metasploitable2-1** and **Metasploitable2-2**.

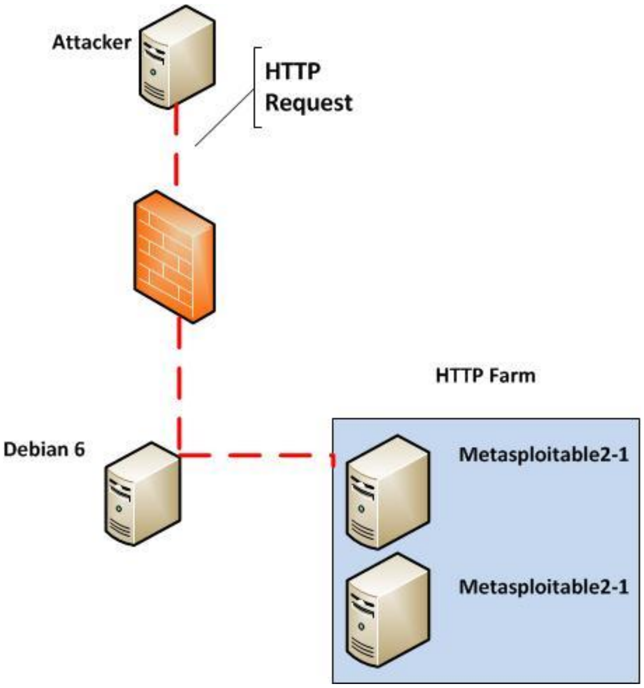
When installing Debian 6, I used the netinst ISO and performed a standard system install, excluding everything else. If you wish, you can install the graphical environment here. This will give the ability to manage the PfSense firewall from the Debian 6 instance. Once the LAB network has been locked down, only machines living on the **192.168.13.0/24** network will have access to PfSense configuration interface.

To get Debian 6 ready to rock, you will first need to install and configure some new packages.

1. Login to the Debian 6 instance and install ***haproxy*** by issuing the following command:
   apt-get install haproxy
2. Once *haproxy* has been installed, edit the file: /`etc/haproxy/haproxy.cfg`, configure this file to match the `haproxy.cfg` example on page 15. The save and close the file.
3. After editing the file, start up ***HA Proxy*** by issuing the following command on the Debian 6 instance.
   ***sudo haproxy -f* /etc/haproxy/haproxy.conf**

NOTE: See page 15 for configuration example.

HA Proxy should now up and running, though it will not work just yet. You will still need to bring up the two Metasploitable instances before testing this service.



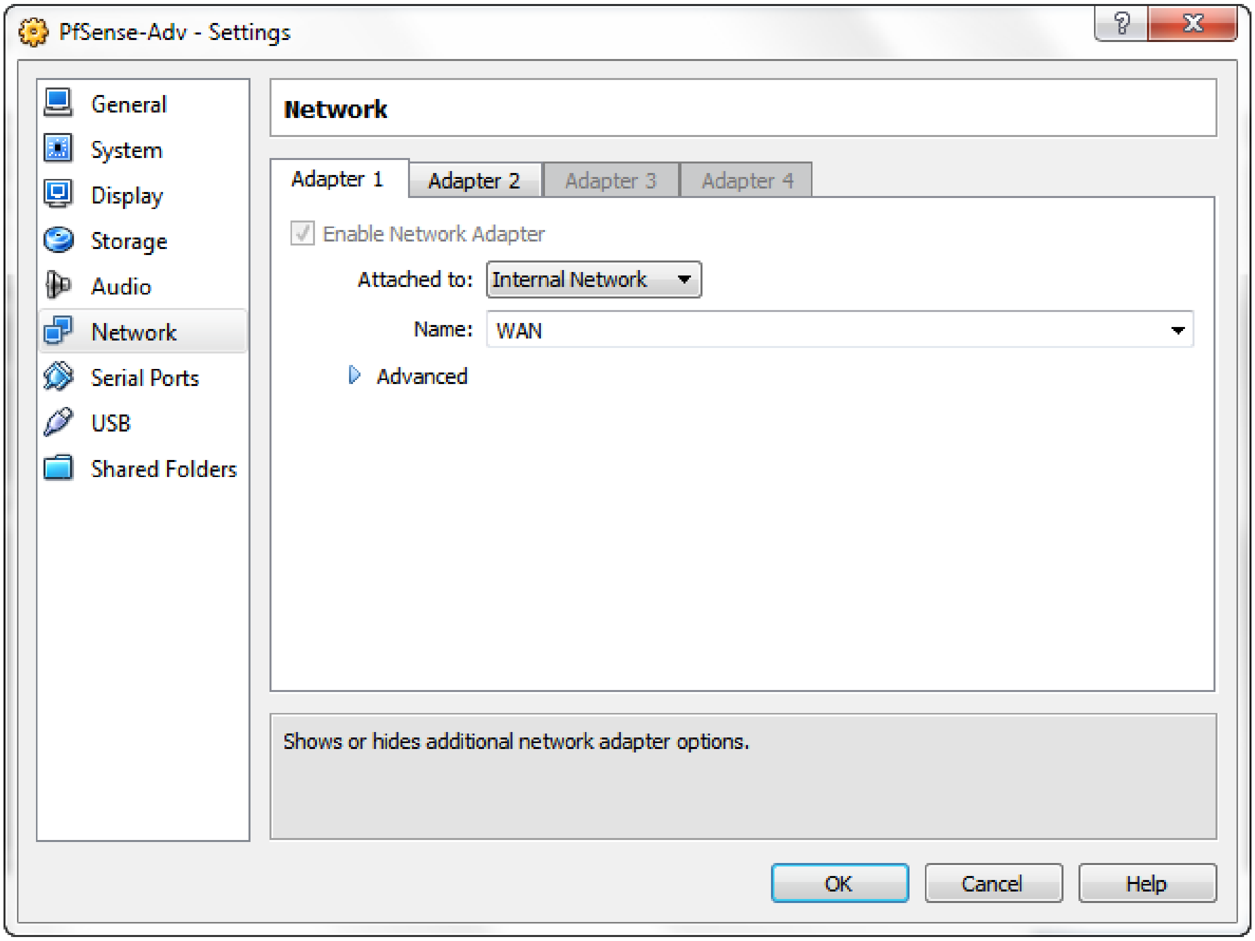
Penetration Testing LAB - HA Proxy Configuration Example

```
 global

                log 127.0.0.1           local0
                log 127.0.0.1           local1  notice
                maxconn 4096
                user    haproxy
                group   haproxy
                daemon

defaults

        log global
        mode http
        option  httplog
        option  dontlognull
        retries 3
        option  redispatch
        maxconn 2000
        contimeout      5000
        clitimeout      50000
        srvtimeout      50000

listen  PentestLABBalancer      192.168.13.10:80
        mode http
        cookie  PentestLABBalancer
        balance         source
        option  httpclose
        option  forwardfor
        stats   enable
        stats   auth    ihtb:ihtb
        server  web_1   192.168.13.20   cookie  PentestLABBalancerA     check
        server  web_1   192.168.13.21   cookie  PentestLABBalancerB     check
```

Reconfiguring BackTrack

The reconfiguration of BackTrack for the intermediate lab does not require many changes. The first being changing BackTracks network settings in VBox Manager.

1. From the VBox Manager interface, Edit the settings of the BackTrack instance and change the Network Settings for **Adapter 1**.
   a. Change the existing settings to match the following then click OK.
      Attached to: Internal network
      Name: WAN



☑ Enable Network Adapter

Attached to: Internal Network

Name: WAN

Shows or hides additional network adapter options.

2. Reboot BackTrack, then log back in. Before running ***startx*** issue the following commands in order to get BackTrack talking to the LAB WAN network on **210.210.210.0/24**

```
ifconfig eth0 210.210.210.2 promisc
route add default gw 210.210.210.1
```

NOTE: BackTrack will not keep these settings, so if you reboot they will need to be applied again.

LAB Setup – Virtual and Vulnerable Machines

What is a penetration testing LAB without things to exploit?

A boring networking lab ;)

Metasploitable 2 – Attack of the clones

In the intermediate lab, we will be using some load balanced web servers, so we will need to add another web server. Seeing the metasploitable 2 instance already has a web server and vulnerable applications installed. We will just clone another Metasploitable 2 instance using the existing one.

1. Using the Metasploitable 2 instance created in the basic version of this guide, you will need to create a clone of the instance in VBox.

   IMPORTANT NOTE:
   Be sure to select the *re-initialize MAC address* option when cloning the instance.

   a. From the VBox Manager window, Right click on Metasploitable 2 instance, then go to Clone. Take note of the newly created MAC address of the clone, it will be required later.

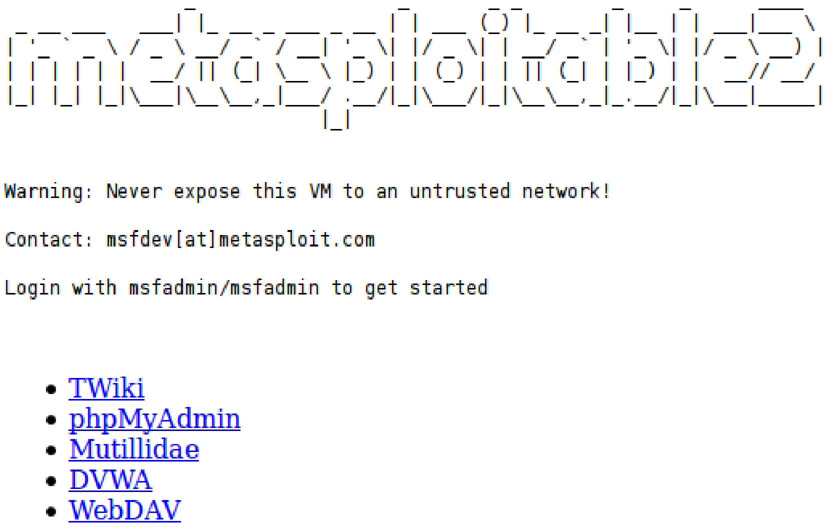
Under the Advanced menu, take note of the MAC address. You will need it later.

You should now have two (2) **Metasploitable 2** instances. Too simplify things, rename the original **Metasploitable 2** to **Metasploitable 2-1**.
Then rename the cloned copy of **Metasploitable2-1** to be **Metasploitable 2-2**.

Power on both instances, once they have both finished booting you can then test the HA Proxy setup from earlier. From the BackTrack instance, open the following URL using Firefox

http://210.210.210.10/

If everything went well, you should get…

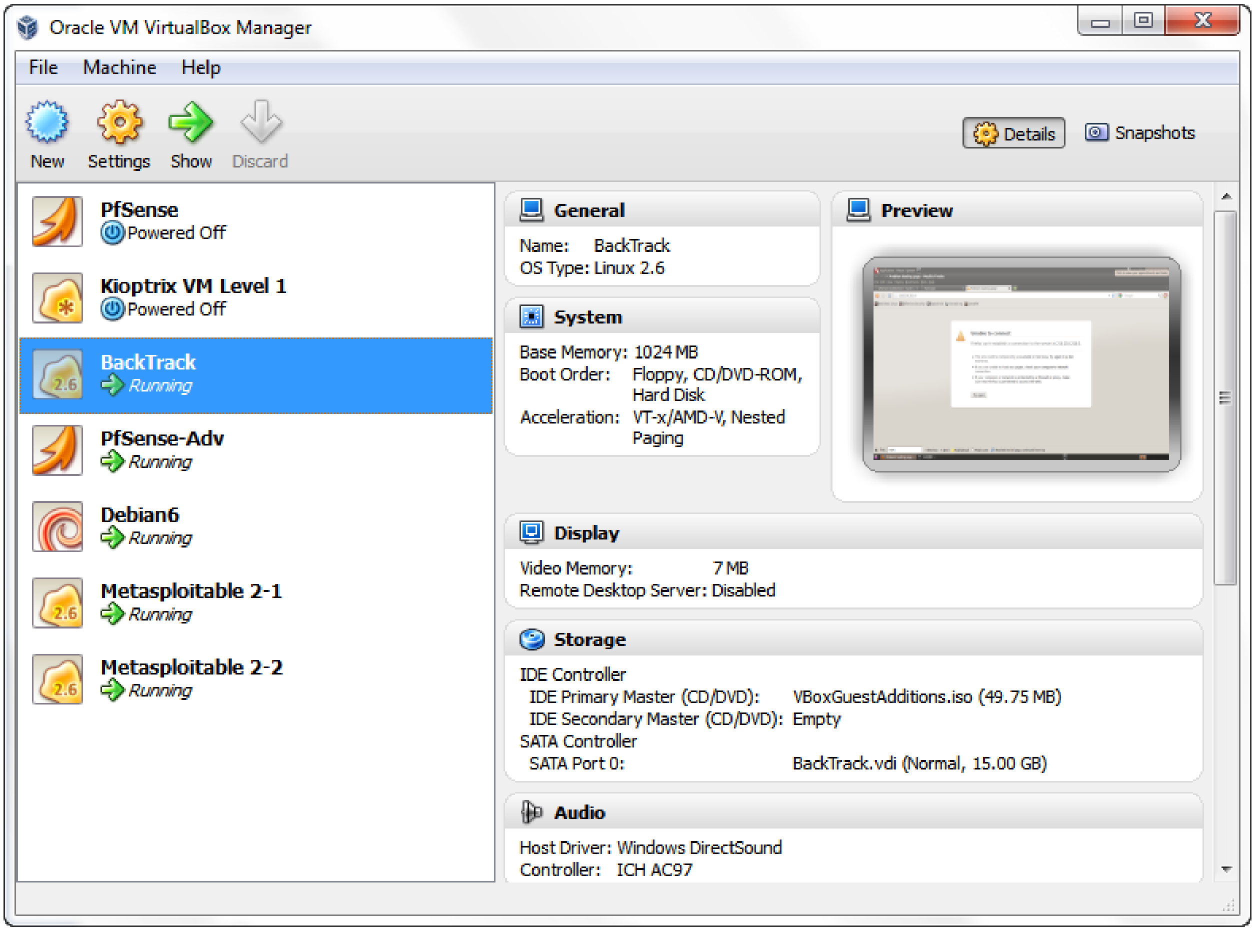


```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Virtual Lab Layout & Diagrams

Virtual Box Layout



PfSense
Powered Off

Kioptrix VM Level 1
Powered Off

BackTrack
Running

PfSense-Adv
Running

Debian6
Running

Metasploitable 2-1
Running

Metasploitable 2-2
Running

General

Name: BackTrack
OS Type: Linux 2.6

Preview

System

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 7 MB
Remote Desktop Server: Disabled

Storage

IDE Controller
IDE Primary Master (CD/DVD): VBoxGuestAdditions.iso (49.75 MB)
IDE Secondary Master (CD/DVD): Empty
SATA Controller
SATA Port 0: BackTrack.vdi (Normal, 15.00 GB)

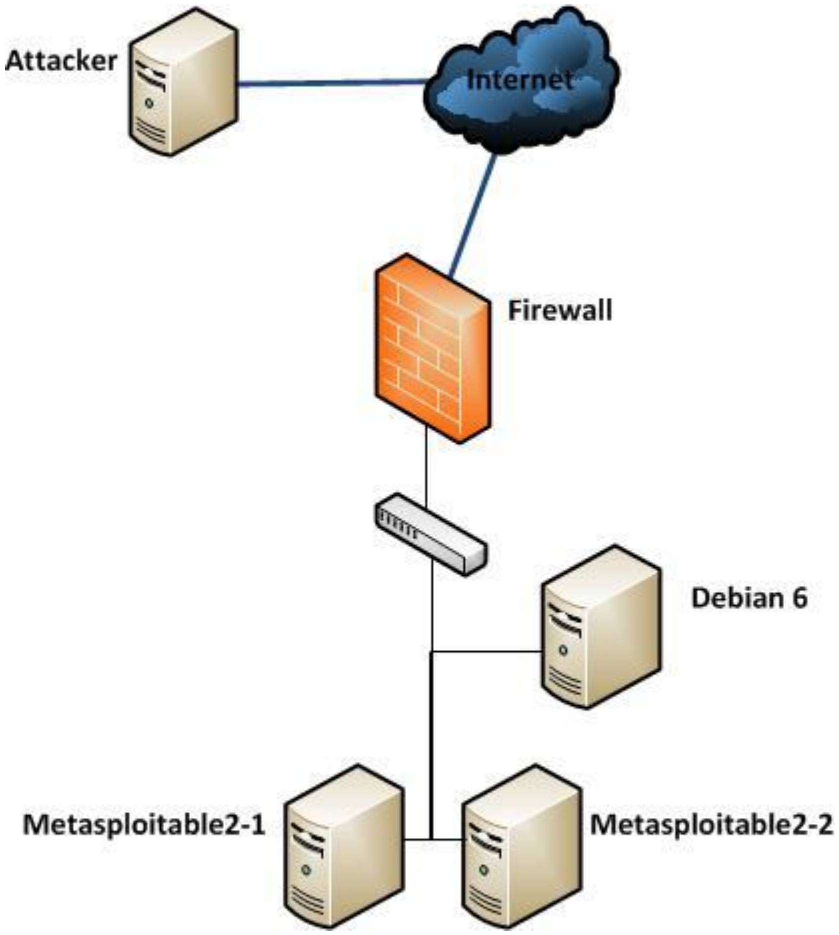
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Virtual Network Diagram

External Subnet:	210.210.210.0/24
Internal Subnet:	192.168.13.0/24

Firewall:	Internal: 192.168.13.1	External: 210.210.210.1
BackTrack / Attacker:	External: 210.210.210.2/32	
Debian 6:	Internal: 192.168.13.10	External: 210.210.210.10
Metasploitable2-1:	Internal: 192.168.13.20	External: 210.210.210.20
Metasploitable2-2:	Internal: 192.168.13.21	External: 210.210.210.30



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 external attacker's perspective. From the BackTrack machine you can now start exploring the **210.210.210.0/24** 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

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.