

Lab Setup

1) Set Up

The lab consists of a vulnerable web server that you are required to pentest.

You can use Sun VirtualBox or Vmware Player (both are free) to create a virtual machine and work in a virtual environment. Alternatively you can burn the iso to a bootable DVD and work from there.

You need to set up your hacking environment in the following way:



In this setup you will be using a VM (preferably Kali Linux) or your host OS with required pentest tools installed to attack the target assignment VM.

2) Installation

a) Download VMWare player and create a new Virtual Machine.



b) Select the filename of the target iso



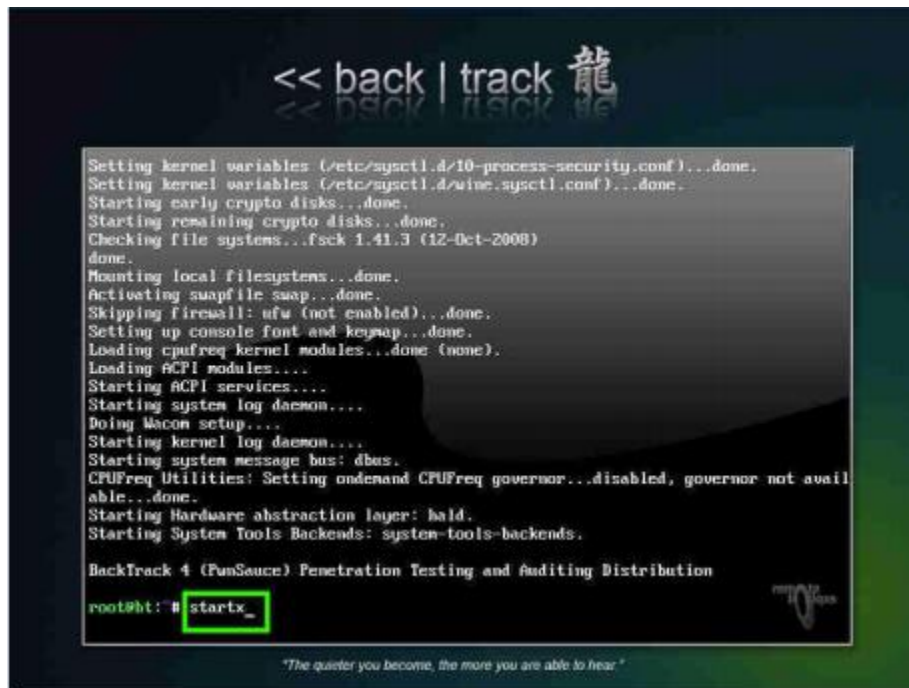
c) Pick Ubuntu as type of the virtual machine.



d) Select the size of the virtual hard drive. Anything greater than 4GB should work.

e) Select the RAM (suggested 1GB but you can start with 512mb and increase the RAM if the VM is slow).

f) Power on your VM.



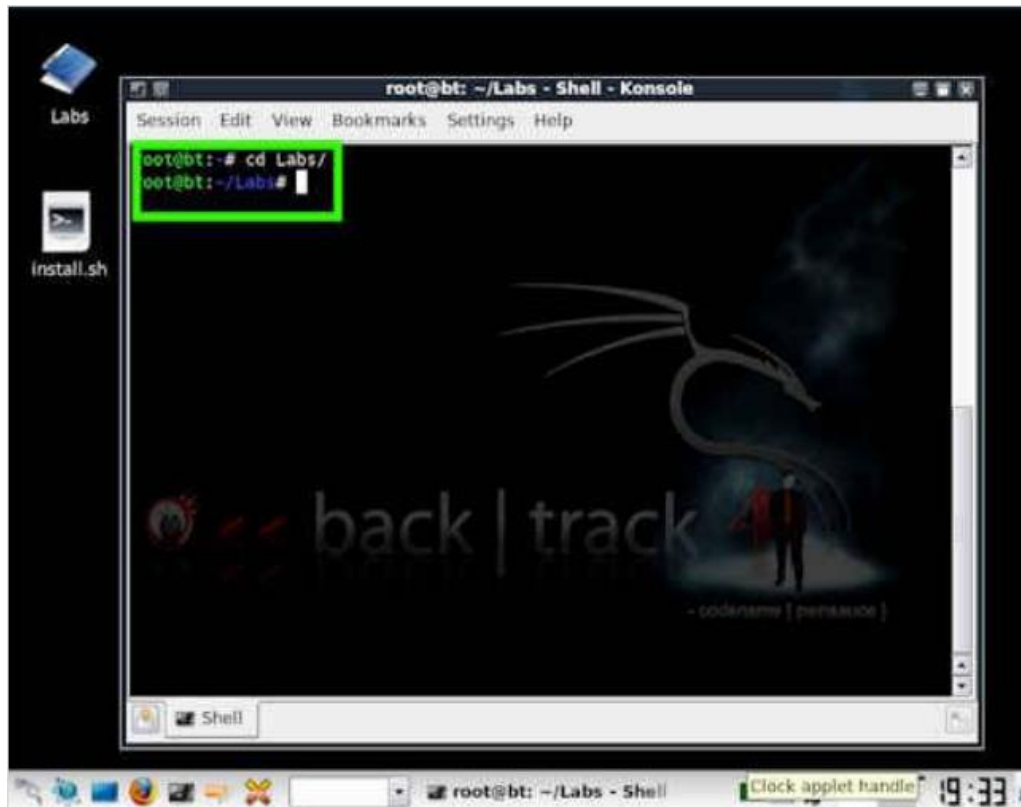
When the Backtrack 4 console appears, type **startx** and hit enter.

(Remember that Backtrack 4 root password is **toor**)

The desktop will look like the following screenshot. You can see the labs folder on the top left.



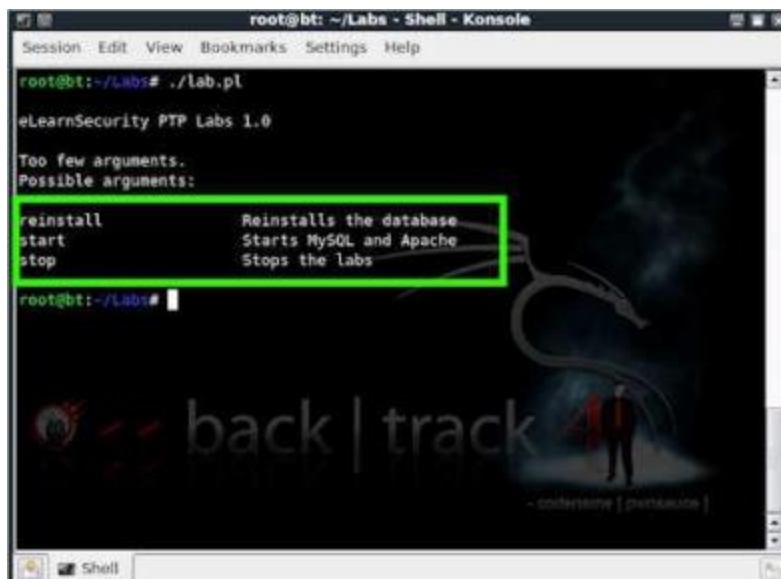
g) Start the labs.



Open a console and type **cd Labs** to enter the Labs folder.

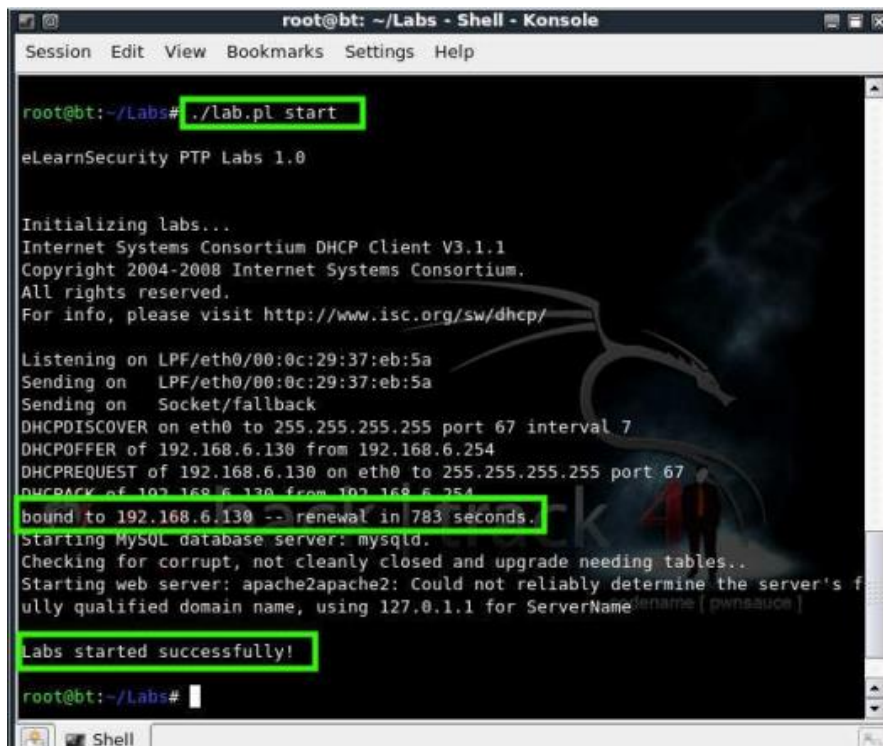
From here you can use the **lab.pl** script that will be used to start, stop and reinstall the labs.

Type **./lab.pl** for a list of accepted arguments.



Since we are configuring the Target machine, we need to start the labs environment, that is the web application that we want to test.

From the console type `./lab.pl` start to launch the labs:



```
root@bt: ~/Labs - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~/Labs# ./lab.pl start

eLearnSecurity PTP Labs 1.0

Initializing labs...
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:37:eb:5a
Sending on LPF/eth0/00:0c:29:37:eb:5a
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.6.130 from 192.168.6.254
DHCPREQUEST of 192.168.6.130 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.6.130 from 192.168.6.254
bound to 192.168.6.130 -- renewal in 783 seconds.
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
Labs started successfully!

root@bt:~/Labs#
```

The labs have now started. Please take note of the IP address given to this machine. In this case 192.168.6.130, but depending on your configuration you will be allocated a different address.

h) To access the web application you can now open up Firefox browser within the attacking VM/Host OS. and visit: <http://<IP address of your target VM>/foophones>



Note: Following the above configuration, you have a live environment. This means that the files and settings saved in the distro will not be persistent through sessions: you will lose any saved file after the reboot of the virtual machine. Do not store any file on the target VM.