

User Manual of the Pre-built Ubuntu 9 Virtual Machine

Copyright © 2006 - 2009 Wenliang Du, Syracuse University.
The development of this document is funded by the National Science Foundation's Course, Curriculum, and Laboratory Improvement (CCLI) program under Award No. 0618680 and 0231122. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of the license can be found at <http://www.gnu.org/licenses/fdl.html>.

1 Overview

Using VMware, we have created a pre-built virtual machine (VM) image for UbuntuLinux (version 9). This VM can be used for all our SEED labs that are based on Linux. In this document, we describe the configuration of this VM, and give an overview of all the software tools that we have installed.

Updating the VM is quite time-consuming, because not only do we need to update the VM image, we have to make sure that all our labs are consistent with the newly built VM. Therefore, we only plan to update our VM image once every two years, and of course update all our labs once the VM is changed.

If you are using our SEED labs, and want to get a copy of our most recent VM image, please send us an email: wedu@syr.edu. We can either send you a DVD or let you download the image from us.

2 VM Configurations

2.1 Configuration of the VM

The main configuration of this VM is summarized in the following. If you are using VMware Workstation, you can adjust the configuration according to the resources of your host machine (e.g., you can assign more memory to this VM if your host machine has enough memory):

- Operating system: Ubuntu 9.04 with the Linux kernel v2.6.28.
- Memory: 256M RAM.
- Disk space: Maximum 8G disk space.

We have created two accounts in the VM. The usernames and passwords are listed in the following:

1. User ID: `root`, Password: `seedubuntu`.

Note: Ubuntu does not allow `root` to login directly from the login window. You have to login as a normal user, and then use the command `su` to login to the `root` account.

2. User ID: `seed`, Password: `dees`

2.2 Network setup

Currently the "Network connection" is set to "NAT", i.e., your VM is put in a private network, which uses your host machine as the router. The VMs in such a setting can connect to the Internet via the NAT mechanism, and they are not visible to the outside (their IP addresses are not routable from the outside, e.g., many use 192.168 prefix). This setting is sufficient for most of our SEED labs.

If you want your VMs to be visible to the outside (e.g., you want to host a HTTP server in a VM, and you want to access it through the Internet), then, you have to set the "Network connection" to "Bridged".

3 Libraries and Software

3.1 Libraries and Applications Installed

Besides the packages coming with the Ubuntu 9 installation, the following libraries and applications are additionally installed using the "apt-get install" command.

```
tcl, tk, libnet1, libnet1-dev, libpcap0.8-dev, libattr1-dev,  
vim, apache2, php5, libapache2-mod-php5, mysql-server,  
wireshark, bind9, nmap, sun-java6-jdk, xpdf, vsftpd, telnetd,  
zsh
```

The libcap 2.16 and netlib/netwox/netwag 5.35.0 have been compiled and installed from the source downloaded from the Internet.

3.2 Softwares configuration

Netlib/netwox/netwag 5.35.0. Netwox is a network toolbox; netwag is a GUI of netwox. They can be found in /usr/local/bin/. The ICMP spoofing bug of netwox has been fixed. It should be noted that running netwox/netwag requires the root privilege.

Wireshark. Wireshark is a network protocol analyzer for Unix and Windows. It is located in /usr/bin/. Wireshark requires the root privilege to run.

Nmap. Nmap is a free security scanner for network exploration and hacking. It is located in /usr/bin/. Some functions of nmap require root privilege.

Firefox extensions. Firefox is installed by default in Ubuntu 9. We have installed two useful extensions: LiveHTTPHeader and Firebug. They can be launched in the "Tools" menu in Firefox.

PhpBB2 Forum. For some labs, especially those related to web security, we need a non-trivial web application. For that purpose, we have installed the phpBB2 forum. Several versions of phpBB2 forum are installed; most of them were modified from the original phpBB2 to introduce different vulnerabilities.

It should be noted that to access the phpBB2 forum, the apache2 http server and the MySQL database server must be running.

Java. We have installed the Sun java JDK. The commands javac and java are available to compile and run java source code.

4 Pre-Installed Servers

Some of the SEED labs may need additional services that are not installed or enabled in the standard Ubuntu distribution. We have included them in our pre-built VM. Note: You need root privilege to start a server.

4.1 The MySQL Server

The database server MySQL is installed. It can be started by running `service mysql start`. Currently, there are two accounts in the MySQL server. The usernames and passwords are listed below.

1. root : seedubuntu
2. apache : apache (web applications use this account to connect to the mysql server)

You can access the MySQL database server by running the client-side application `/usr/bin/mysql`. The following is a simple demo on how to use `mysql`.

```
$ mysql -u root -pseedubuntu

mysql> show databases;

mysql> use origin_phpbb_db;

mysql> show tables;

mysql> select username,user_email from phpbb_users;

mysql> quit
```

4.2 The Apache2 Http Server

The `apache2` http server was installed using `apt-get install`. It can be started by issuing the `service apache2 start` command. The `apache2` server is configured to listen on both 80 and 8080 ports. All the web pages hosted by the server can be located under the `/var/www/` directory.

For each SEED lab that uses the `apache2` http server, we have created one or several URLs. Basically, in the pre-built VM image, we use Apache server to host all the web sites used in the lab. The name-based virtual hosting feature in Apache could be used to host several web sites (or URLs) on the same machine. A configuration file named `default` in the directory `/etc/apache2/sites-available` contains the necessary directives for the configuration. The following is a list of URLs that we have pre-configured; their corresponding directories are also listed:

<code>www.csrfllabphpbb.com</code>	<code>/var/www/CSRF/CSRFLabPhpbb/</code>
<code>www.csrfllabattacker.com</code>	<code>/var/www/CSRF/Attacker/</code>
<code>www.sqlllabmysqlphpbb.com</code>	<code>/var/www/SQL/SQLLabMySQLPhpbb/</code>
<code>www.xsslabphpbb.com</code>	<code>/var/www/XSS/XSSLabPhpbb/</code>
<code>www.soplalab.com</code>	<code>/var/www/SOP/</code>
<code>www.soplalabattacker.com</code>	<code>/var/www/SOP/attacker/</code>
<code>www.originalphpbb.com</code>	<code>/var/www/OriginalPhpbb/</code>
<code>www.soplalab.com:8080</code>	<code>/var/www/SOP/</code>

Configuring DNS. The above URL is only accessible from inside of the virtual machine, because we have modified the `/etc/hosts` file to map each domain name to the virtual machine's local IP address (127.0.0.1). You may map any domain name to a particular IP address using the `/etc/hosts`. For

example you can map `http://www.example.com` to the local IP address by appending the following entry to `/etc/hosts` file:

```
127.0.0.1    www.example.com
```

Therefore, if your web server and browser are running on two different machines, you need to modify the `/etc/hosts` file on the browser's machine accordingly to map the target domain name to the web server's IP address.

4.3 Other Servers

DNS server The DNS server `bind9` is installed. It can be started by running `"service bind9 start"`. The configuration files are under `/etc/bind/`.

Ftp server. The `vsftpd` (very secure ftp daemon) server is installed. It can be started by running `"service vsftpd start"`.

Telnet server. The `telnetd` server is installed. It can be started by running `"service openssh-inetd start"`.

5 Miscellaneous Configuration

Time zone Currently the time zone is set to be New York, adjust that to the time zone of your location.

Display resolution The current Display resolution is 1024*768. You can change it at "System → Preferences → Display".

6 Configure Your VM securely

6.1 Change the password

For the sake of security and your own convenience, we suggest that you change the account password. To change the Ubuntu's account password. You need to login as root and issue the `"passwd username"` command. To change MySQL's root password. You can do it as following:

```
$ mysql -u root -pseedubuntu
```

Once in the prompt do this:

```
mysql> update user set User='NewRootName', Password='NewPassword'
      where user='root';
mysql> flush privileges;
```

6.2 Configure automatically start service

It's more convenient to start some commonly used service automatically during the system boot up, although most people do not want to start some server that they do not use.

Currently, most of the service we need for SEED labs are configured not to start automatically. You can use `chkconfig` to get the current configuration. You can also use `chkconfig` to modify the configuration. For example, to start the MySQL server automatically during the system bootup, run "`chkconfig mysqld on`".

7 Note

7.1 Don't install VMware Tool on the Ubuntu

Though it is highly recommended to install VMware Tool in a virtual machine, VMware Tool of VMware 6.5.0 can cause a mouse-focus problem. We suggest you not to install VMware Tool on the the pre-built Ubuntu VM. If you are using other versions of VMware, and do want to give it a try, please make a snapshot of your VM image, so that you can recover to the previous state in case it might go wrong.

7.2 Run the VM in proper version of VMWare

This VM is build on VMware Workstation v6.5.0. To use this VM, you should open SEEDUbuntu9.vmx in VMware Workstation v6.5.0(or newer version) or VMware Player. It's recommended that your host machine which VMware runs on should have at least 1G RAM, and 8G free disk space.

Note for Macintosh Users The pre-configured virtual machine is not compatible with VMware Fusion 1.x. If you are using VMware Fusion 1.x, then you may download a free upgrade to VMware fusion 2.5 from the following web site <http://www.vmware.com/download/fusion/>. Our pre-configured virtual machine has been tested on VMware Fusion 2.04 and 2.05.

7.3 X-Server Errors

Some of the labs need to change `/bin/sh`, making it pointing to `/bin/zsh` (originally, it points to `/bin/bash`). If you forget to change it back to `bash`, you may encounter an X server error during the system bootup. When this error happens, your X server cannot start, and you can only log into system in the text mode. To recover from this problem, follow these steps:

1. Login as root in the command prompt. When the X server error happens, the system will let you log into the root (you need to know the root password) in the text mode.
2. Execute the following commands ("`#`" is the prompt for root user, do not enter the "`#`").

```
# mount -o remount /
# cd /bin
# rm sh
# ln -s bash sh
```

Our goal is to change `/bin/sh` and let it point back to `/bin/bash`. However, if we login as a root at that time, we only have a read-only file system. We need to remount the whole file system to be able to write.

3. Reboot the system. The X Server error should go away.

8 Change Log

Version 1.1 on 25-Aug-2009

- Downloaded and installed libnet-1.0.2a.
- uninstalled libnet1-dev because it conflict with the new installation.
- Downloaded and installed pacgen-1.01. It's located on the Desktop of user 'seed'.

Version 1.0 on 23-Jun-2009

- Created as described above.