User Manual of the Pre-built Ubuntu 16.04 Virtual Machine

1 Overview

Using `VirtualBox`, we have created a pre-built virtual machine (VM) image for `UbuntuLinux` (version 16.04). 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. The VM is available online from our SEED web page.

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.

2 VM Configurations

2.1 Configuration of the VM

The main configuration of this VM is summarized in the following. If you are using `VirtualBox`, 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` 16.04 with the `Linux` kernel v4.8.0-36-generic.
- Memory: 1024 MB RAM.
- Disk space: Maximum 20G disk space.

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

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., VirtualBox assigns 10.0.2.15 to each VM under NAT configuration). 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 can refer to the instruction "Network Configuration in VirtualBox for SEED Labs" under the following link: `http://www.cis.syr.edu/~wedu/seed/Documentation/Ubuntu11_04_VM/VirtualBox_MultipleVMs.pdf`. The instruction was written for Ubuntu 11.04, however, it also works for the updated Ubuntu 16.04 Virtual Machine as well.

3 Libraries and Software

3.1 Libraries and Applications Installed

Besides the packages coming with the `Ubuntu` 16.04 installation, the following libraries and applications are additionally installed using the `"apt-get install"` command.

```
terminator,curl,sublime-text,bless,ghex,libssl-dev,
openbsd-inetd,telnetd,openssh-server,vsftpd,bind9,
libnet1-dev,apache2,php,mysql-server,libapache2-mod-php,
php-mysqlnd,wireshark,netwox,libpcap-dev,zsh,git,python-pip,
capstone
```

3.2 Softwares configuration

Netlib/netwox/netwag. `Netwox` is a network toolbox; `netwag` is a GUI of `netwox`. They can be found in `/usr/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/`.

Firefox extensions. `Firefox` is installed by default in `Ubuntu` 16.04. We have installed the `LiveHTTPHeaders` extension. It can be launched in the "Tools" menu in `Firefox`.

Elgg web application. `Elgg` is a very popular open-source web application for social networking, and we use it as the basis for some of Web security labs. It should be noted that to access `Elgg`, the `apache2` http server and the MySQL database server must be running.

4 Tools

Shellnoob This tool (`https://github.com/reyammer/shellnoob`) assists in writing shellcode for labs like buffer overflow. For example, it can convert assembly instruction to shellcode for 32 bit and 64 bit architectures. It can be found in `/home/seed/source/shellnoob`.

RoPGadget This tool (`https://github.com/JonathanSalwan/ROPgadget`) relates to return oriented programming. It lets you search ROP gadgets in binaries to facilitate ROP exploitation. It can be found in `/home/seed/source/ropgadget`.

GDB-peda This tool (`https://github.com/longld/peda`) provides more information when debugging a program using gdb. It will run automatically when gdb is used. It is installed in the folder `/home/seed/source/gdbpeda`.

5 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.

5.1 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. elgg_admin : seedubuntu (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 db_name;

mysql> show tables;

mysql> select username,user_email from table_name;

mysql> quit
```

5.2 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 port 80. 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 `000-default.conf` 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:

`www.xsslabelgg.com`	`/var/www/XSS/Elgg`
`www.csrflabelgg.com`	`/var/www/CSRF/Elgg`
`www.csrflabattacker.com`	`/var/www/CSRF/Attacker`
`www.seedlabsqlinjection.com`	`/var/www/SQLInjection`

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.

5.3 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 openbsd-inetd start`".

SSH server. The `openssh` server is installed. It can be started by running "`service ssh start`".

6 Miscellanious Configuration

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

Display resolution In order to adjust the display resolution in VirtualBox, we have installed guest additions from the the menu in VirtualBox. This can be done by navigating to the `Devices` Virtualbox window option, and then selecting `Insert guest additions CD image`.

After installing the required additions, you can adjust the display resolution at "System Settings→ Displays → Monitor".

7 Configure Your VM securely

7.1 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;
```