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 Ubuntu Linux (version 16.04). This VM can be used for all our Linux-based SEED labs. In this document, we describe the configuration of this VM, and give an overview of all the software tools installed. The VM is available online from our SEED web page.

Updating SEED VMs is quite time-consuming; building an VM is the easy part, the difficult part is to ensure that all the SEED labs are still working in the new VM. Many SEED labs do require changes: some are minor, but some are major. It took us over a year to prepare this Ubuntu 16.04 VM, revise all the SEED labs for this VM, and conduct a thorough testing in a real class. Due to such a high cost, we only plan to update our VM image once every four to six years.

2 VM VirtualBox Configuration

The VM is based on Ubuntu Linux OS 16.04 (32 bit). The Linux kernel version in the VM is v4.8.0-36-generic. The VM is built based the LTS (long term support) OS version released by Ubuntu. The 16.04 SEED VM can be found at the SEED website. The link is for a zip file that contains the disk (vmdk) for the VirtualBox VM. In order to setup the VM in VirtualBox, configure the networking for the VM, please follow the instructions listed in the same website.

Note: Please DO NOT update the Ubuntu OS in the VM. There is no guarantee that the labs will still work if such an update is performed.

3 Ubuntu User Accounts

We have created two accounts. 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. This account is already given the root privilege, but to use the privilege, you need to use the sudo command.

4 Application Software

The complete list of packages installed is provided in Section 6.2. Here we only highlight some of the most commonly used tool for SEED labs. They are already pinned to the launcher (see Figure 1) for easy access.

Figure 1: Application Shortcuts in the Launcher

Terminator. This is a terminal application that provides a convenient way to manage multiple terminal windows. There are two important features that should be kept in mind when using the VM: split screen and profiles. Terminator's screen can be split by right clicking in the window and selecting `split horizontally` or `split vertically`. In addition, we have set up three color/font profiles in terminator, which can be selected by right clicking in the window and selecting from the `profiles` menu. Figure 2 shows use of split screen and profiles.

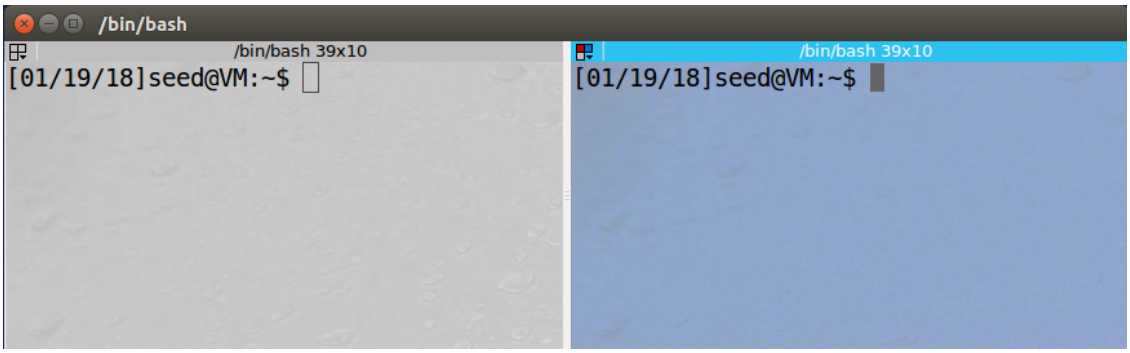

Figure 2: Terminator with split screen and different profiles

Text Editors. We provide two text editors in the VM, namely `gedit` and `sublime`. `gedit` is the default text editor that comes with the `Ubuntu` OS. Compared to `gedit`, `sublime` offers some additional features. A comparison of these tools can be found at [4].

Firefox Extensions. `Firefox` (version 60) is installed in the VM. We have installed the `HTTP Header Live` extension [5] to inspect HTTP packets in the web security labs. The extension can accessed via the sidebar icon in the top right corner of the browser. We have also installed a timestamp extension which can be accessed via the clock icon in the top right corner.

Networking. We have installed three tools to assist in the network security labs (all tools are installed in `/usr/bin/`):

1. `Netwox`: This is a network toolbox which is useful for generating different types of packets. It contains 222 network features. `netwag` is a graphical front-end of `netwox`. It should be noted that running `netwox/netwag` requires the root privilege.
2. `Wireshark`: This tool is a popular network protocol analyzer. It is useful in inspecting network packets.
3. `Scapy`: This tool is an interactive packet manipulation program.

GDB-peda. This tool [1] provides more information when debugging a program using `gdb`. It will run automatically when `gdb` is used.

Mobile Security Lab Software. To support the mobile security labs, we have set up `Android` SDK and NDK in the `/home/seed/android` folder. To allow reverse engineering of Android apps, we have installed `apktool`. We have also installed Oracle Java 8.

5 Server Software

All services mentioned in this section are auto-started by the VM. This can be verified by running `service --status-all` in the terminal.

5.1 Apache HTTP Server

`Apache2` is an open source HTTP server. It is used to host all the websites for the web security SEED lab. We use the `virtual host` feature, which allows us to run multiple websites on the same machine. All the websites in the SEED VM use port 80. The `virtual host` configuration can be found in the file `/etc/apache2/sites-enabled/000-default.conf`. The following snippet shows an example of `VirtualHost`.

```
<VirtualHost *:80>
   ServerName http://www.xsslabelgg.com
   DocumentRoot /var/www/XSS/Elgg/
</VirtualHost>
```

The snippet above is the `VirtualHost` entry for the `Elgg` website used for the XSS lab. The `DocumentRoot` indicates the directory where the source code of the website is located. Similar to the above, we have entries for the following websites in the configuration file:

```
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
www.repackagingattacklab.com    /var/www/RepackagingAttack
```

We also configure the `/etc/hosts` file to associate the virtual machine's local IP address to the website hostnames. The snippet below shows the `/etc/hosts` entries:

```
127.0.0.1 www.xsslabelgg.com
127.0.0.1 www.csrflabelgg.com
127.0.0.1 www.csrflabattacker.com
127.0.0.1 www.seedlabsqlinjection.com
127.0.0.1 www.repackagingattacklab.com
```

5.2 MySQL Server

`MySQL` is an open source database management software. It is used in the VM to manage the databases corresponding for the installed websites. We have the following databases in the mysql server:

1. `Users` database for SQL injection site
2. `elgg_xss` database for the XSS site
3. `elgg_csrf` database for the CSRF site

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 Users;
mysql> show tables;
mysql> select * from credential;
mysql> quit
```

MySQL Accounts. Currently, there are two accounts in the MySQL server. The usernames and passwords are listed below.

1. User: `root`, Password: `seedubuntu`
2. User: `elgg_admin`, Password: `seedubuntu` (web applications use this account to connect to the `mysql` server)

phpMyAdmin. We have also installed `phpMyAdmin` which is a PHP tool that allows administration of `MySQL` through the browser. It can be accessed by navigating to `http://localhost/phpmyadmin`. The account for phpmyadmin has username `root` and password `seedubuntu`.

5.3 Bind9 DNS Server

`Bind9` is an open source implementation of components of the domain name system. It is primarily used in the SEED DNS network security lab. The main configuration file of `Bind9` is located in `/etc/bind/named.conf.options`. You also need to be aware of the file `/var/cache/bind/dump.db`, which is the currently configured dump file.

5.4 Other Servers

We have also installed an ftp server (`vsftpd`), a telnet server (`openbsd-inetd`) and a ssh server (`ssh`).

6 Miscellaneous

6.1 VM Customization Folder

In some of the labs, especially network security labs, we have to run several VMs, and switch back and forth among them. Since all these VMs look the same, it is difficult to know which VM we are in. We provide a customization folder to modify the look and feel of the VM that makes it easier to manage multiple VMs. This folder can be found in `/home/seed/Customization`. Since the networking labs involve up to three VMs, the customization folder provides icons and desktop backgrounds for three roles, namely user, proxy/server and attacker.

6.2 Package List

Besides the packages that come with the `Ubuntu` 16.04 installation, the following additional packages have been installed using the "`apt-get install`" command.

```
terminator, curl, sublime-text, bless, ghex, vim,
libssl-dev, openbsd-inetd, telnetd, openssh-server,
vsftpd, bind9, libnet1-dev, apache2, mysql-server,
php, libapache2-mod-php, php-mysqlnd, wireshark,
netwox, libpcap-dev, zsh, git, python-pip, capstone,
squid, scapy, oracle-java8-installer, adb
```

6.3 Software Security Lab Tools

We have installed two tools to assist us in exploring software security labs:

- **Shellnoob** This tool [3] 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 [2] 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`.

References

[1] Gdbpeda Github. `https://github.com/longld/peda`, 2017.

[2] RopGadget Github. https://github.com/JonathanSalwan/ROPgadget, 2017.

[3] Shellnoob Github. https://github.com/reyammer/shellnoob, 2017.

[4] Comparison of gedit and sublime. https://web.archive.org/save/https://www.slant.co/versus/40/58/~sublime-text_vs_gedit, 2018.

[5] Firefox HTTP Header Live Extension. https://addons.mozilla.org/en-US/firefox/addon/http-header-live/, 2018.