**SeedUbuntu虚拟机使用手册**

**目录**

[1 Seed Ubuntu实验环境搭建 2](#_Toc68854847)

[1.1 实验环境 2](#_Toc68854848)

[1.2 虚拟机软件：vmware 2](#_Toc68854849)

[1.3 Ubuntu用户账号 2](#_Toc68854850)

[1.4 docker安装及镜像创建(可跳过) 2](#_Toc68854851)

[1.4.1 给SEEDUbuntu扩容 2](#_Toc68854852)

[1.4.2 安装docker 3](#_Toc68854853)

[1.4.3 安装docker-compose 5](#_Toc68854854)

[1.4.4 打包SEEDUbuntu镜像 5](#_Toc68854855)

[1.5 docker容器使用 6](#_Toc68854856)

[1.5.1 使用镜像创建容器 6](#_Toc68854857)

[1.5.2 容器操作 7](#_Toc68854858)

[1.5.3 telnet服务启动 7](#_Toc68854859)

[1.6 可能出现的问题 7](#_Toc68854860)

[2 应用软件 9](#_Toc68854861)

[3 服务器软件 11](#_Toc68854862)

[3.1 Apache HTTP Server 11](#_Toc68854863)

[3.2 MySQL Server 11](#_Toc68854864)

[3.3 Bind9 DNS Server 12](#_Toc68854865)

[3.4 Other Servers 12](#_Toc68854866)

[4 其他 13](#_Toc68854867)

[4.1 VM Customization Folder 13](#_Toc68854868)

[4.2 Package List 13](#_Toc68854869)

[4.3 Software Security Lab Tools 13](#_Toc68854870)

[参考 14](#_Toc68854871)

# Seed Ubuntu实验环境搭建

## 实验环境

提供的SEEDUbuntu16.04虚拟机(已安装docker)。

## 虚拟机软件：vmware

将虚拟机文件解压缩，用vmware打开虚拟机Ubuntu-seed目录下的Ubuntu-seed.vmx

(该虚拟机用vmware 15.5.0版本创建的，如果出现不兼容的情况，可以使用此版本)

## Ubuntu用户账号

虚拟机里**创建了**两个帐户。 用户名和密码如下：

1.用户名：root，密码：seedubuntu。 注意：Ubuntu不允许root从登录窗口直接登录。 您必须以普通用户身份登录，然后使用命令su登录root帐户。

2.用户ID：seed，密码：dees。 此帐户已获得root权限，但要使用root权限，需要用sudo命令。

## docker安装及镜像创建(可跳过)

此步骤针对原来就已经下载了seed虚拟机，但是虚拟机里面没有docker的同学。如果下载了本次实验提供的seed虚拟机，可以跳过此小节。

### 给SEEDUbuntu扩容

首先在虚拟机设置里面，选择硬盘，然后扩容。(使用vmware-diskmanager命令行工具也可)

打开虚拟机，apt-get install gparted

运行gparted，将除了/dev/sda1外的分区格式化，再进行扩展，建议80G（40G以上），这是因为打包生成的镜像导入创建的容器时，一个容器占用8G左右的空间。分好的分区如图1所示。

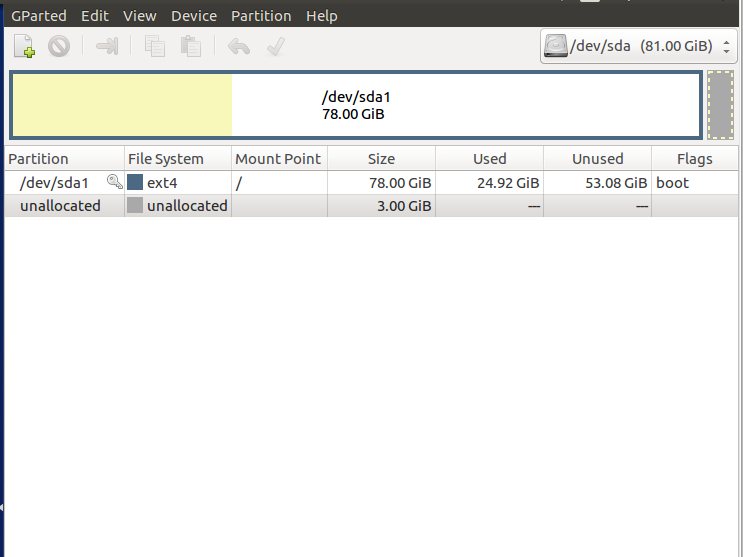


图 1 扩容后分区

### 安装docker

由于seedubuntu1604是i386架构的32位机器，不能安装docker-ce-cli、docker-ce，解决方法是安装docker.io，这区别在于docker.io是ubuntu团队进行维护的版本，版本较低，但不影响实验。

如果在之前有安装旧版本的docker 的话，需要卸载之后才能安装：

$ sudo apt-get remove docker docker-engine docker.io

更新

|  |
| --- |
| sudo apt-get update |

下载相关工具

|  |
| --- |
| sudo apt-get install \  apt-transport-https \  ca-certificates \  software-properties-common |

添加docker官方GPG密钥

|  |
| --- |
| curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add - |

设立仓库

|  |
| --- |
| $ sudo add-apt-repository \  "deb [arch=amd64] https://download.docker.com/linux/ubuntu \  $(lsb\_release -cs) \  stable" |

|  |
| --- |
| $ sudo apt-get update  $ sudo apt-get install docker.io |

安装docker

运行docker version可检验是否完成安装，如图2所示。

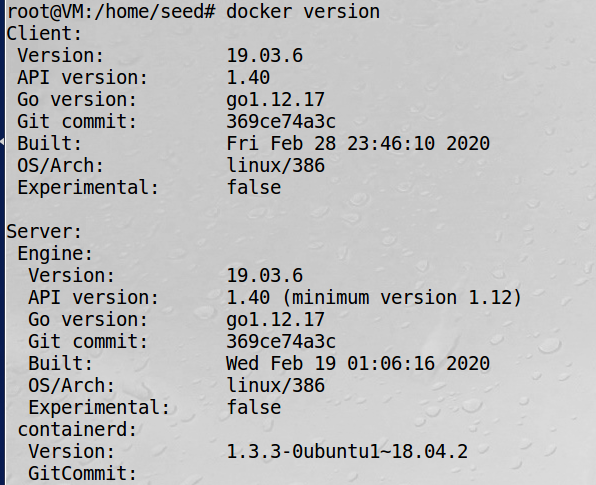


图 2 docker version

### 安装docker-compose

$sudo apt-get install docker-compose

安装成功后运行docker-compose version，如图3所示。

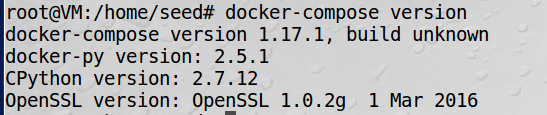


图 3 docker-compose version

### 打包SEEDUbuntu镜像

通过tar 备份目录

导入镜像

#tar -cvpf /home/buildrpm.tar --directory=/ --exclude=proc --exclude=sys --exclude=dev --exclude=run /

cat buildrpm.tar | docker import - seedubuntu。

导入镜像：

#cat buildrpm.tar | docker import - seedubuntu

## docker容器使用

虚拟机里面已经安装了docker，seed虚拟机压缩文件在/home/contain/buildrpm.tar

镜像也已经导入，镜像名字为seedubuntu

因为docker容器里面的系统没有图形界面，需要图形界面的主机可以直接用虚拟机，而不用容器。比如攻击机需要运行wireshark监听报文的话，攻击机可以直接用虚拟机，user和server机器可以用docker容器。

系统里面已经创建了一个名字为”server”的镜像，该镜像中已经安装了telnet服务。

### 使用镜像创建容器

如果需要创建一个新的名字为“user”的镜像，则可以使用以下命令：

# docker run -it --name=user --privileged “seedubuntu” /bin/bash

常用可选参数说明：

-i 表示以“交互模式”运行容器

-t 表示容器启动后会进入其命令行。加入这两个参数后，容器创建就能登录进去。即 分配一个伪终端。

–name 为创建的容器命名

-v 表示目录映射关系(前者是宿主机目录，后者是映射到宿主机上的目录，即 宿主机目录:容器中目录)，可以使 用多个-v 做多个目录或文件映射。注意:最好做目录映射，在宿主机上做修改，然后 共享到容器上。

-d 在run后面加上-d参数,则会创建一个守护式容器在后台运行(这样创建容器后不 会自动登录容器，如果只加-i -t 两个参数，创建后就会自动进去容器)。

-p 表示端口映射，前者是宿主机端口，后者是容器内的映射端口。可以使用多个-p 做多个端口映射

-e 为容器设置环境变量

–network=host 表示将主机的网络环境映射到容器中，容器的网络与主机相同

-it 创建一个伪终端交互界面，name指定容器名称，否则随机一个名字

--privileged 为了后续实验能够修改系统变量，需要添加上这个参数

docker [container] ps -a可以查看所有容器 (在新的docker版本中需要带container参数，因为此虚拟机的docker版本比较老，不需要此参数，其它命令类似)

### 容器操作

docker ps 可以查看正在运行的容器

docker exec -it <容器名/id> <运行后第一个命令>

#一般使用/bin/bash，否则无法进入交互界面

比如：进入容器user的命令行：

# docker exec -it user /bin/bash

# 停止一个已经在运行的容器

sudo docker stop 容器名或容器id

# 启动一个已经停止的容器

sudo docker start 容器名或容器id

#删除容器

sudo docker rm 容器名或容器id

### telnet服务启动

重启openbsd-inetd

$ sudo /etc/init.d/openbsd-inetd restart

查看telnet运行状态

$ sudo netstat -a | grep telnet

## 可能出现的问题

1. 新装的ubuntu虚拟机，执行sudo apt update,总会报(appstreamcli:21755): GLib-CRITICAL \*\*: g\_strchomp: assertion ‘string != NULL’ failed

解决：

$ sudo apt-get install libappstream4

1. find: ‘/run/user/1000/gvfs’: 权限不够 的解决办法

解决：其实这个目录是空的，查不查都没关系。所以，以下解决方式比较简粗暴：  
 umount /run/user/1000/gvfs // 卸载该文件  
 rm -rf /run/user/1000/gvfs // 删除该文件

1. 回显功能没启动

在telnet中使用回显功能，首先需要启动echo服务。默认情况下ubuntu 是不开启 telnet的回显功能的。

开启方法如下：

#apt-get install xinetd

之后，需要配置在xinetd中，启动echo服务，

$vi /etc/xinetd.d/echo

把disable字段的值从yes改成no

接着，启动xinetd服务

$sudo  service  xinetd start

# 应用软件

第4.2节提供了安装的完整软件包列表。 在这里，我们只强调一些最重要的，SEED实验常用的工具。 为了便于操作，已经将它们固定在启动器上（见图4）。



图4：启动器中的应用程序快捷方式

**Terminator**。这是一个终端应用程序，提供了一种管理多个终端窗口的便捷方式。 使用VM时，应记住两个重要功能：分屏和配置文件。通过右键单击窗口并选择水平分割或垂直分割，可以分割终端的屏幕。 此外，我们在Terminator中设置了三种颜色/字体配置文件，可以通过右键单击窗口并从配置文件菜单中选择。图5显示了分屏和配置文件的使用。

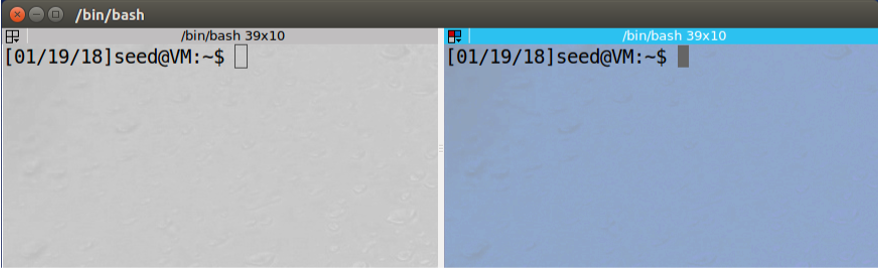


图5：具有分屏和不同配置文件的Terminator

**Text Editors**。 我们在VM中提供了两个文本编辑器，即gedit和sublime。 gedit是Ubuntu OS附带的默认文本编辑器。 与gedit相比，sublime提供了一些额外的功能。 这些工具的比较可以在[4]中找到。

**Firefox Extensions**。 Firefox（versio 60）已安装在VM中。 我们已经安装了HTTP Header Live extension [5]以检查Web安全实验中的HTTP数据包。 此扩展可以通过浏览器右上角的侧边栏图标访问。 我们还安装了一个时间戳扩展名，可以通过右上角的时钟图标访问。

**Networking**。我们已经安装了三个工具来协助网络安全实验（所有工具都安装在/usr/bin/中）：

1. Netwox：这是一个网络工具箱，可用于生成不同类型的数据包。 它包含222个网络功能。 netwag是netwox的图形前端。 运行netwox /netwag需要root权限。

2. Wireshark：这个工具是一种流行的网络协议分析器。 它在检查网络数据包时很有用。

3. Scapy：这个工具是一个交互式数据包操作程序。

**GDB-PEDA**。使用gdb调试程序时，此工具[1]提供了更多信息。它在使用gdb时自动运行。

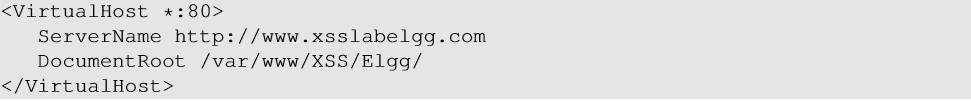
**Mobile Security Lab Software**。 为了支持移动安全实验，我们在文件夹/home/seed/android下设置了Android SDK 和NDK。 为了允许Android应用程序的逆向工程，我们安装了apktool。还安装了Oracle Java 8。

# 服务器软件

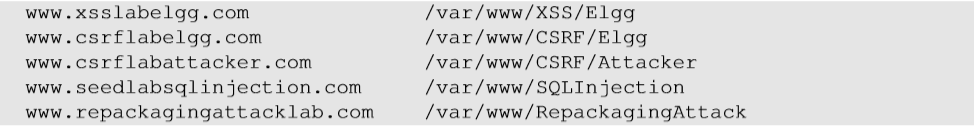
本节提到的所有服务都是由VM自动开启的。这可以通过在终端运行：service --status-all，进行验证。

## Apache HTTP Server

Apache2是一个开源HTTP服务器。 它用于托管Web安全SEED实验的所有网站。 我们使用virtual host功能，从而允许我们在同一台机器上运行多个网站。SEED VM中的所有网站都使用端口80。virtual host配置可以在以下文件中找到：/etc/apache2/sites-enabled/000-default.conf。以下代码段显示了VirtualHost的示例。



上面的代码段是用于XSS实验的Elgg网站的VirtualHost条目。 DocumentRoot指网站源代码所在的目录。与上述类似，我们在配置文件中有以下网站的条目：



我们还配置了/etc/hosts文件，以将虚拟机的本地IP地址与网站主机名相关联。 下面的代码段显示了/etc/hosts条目：



## MySQL Server

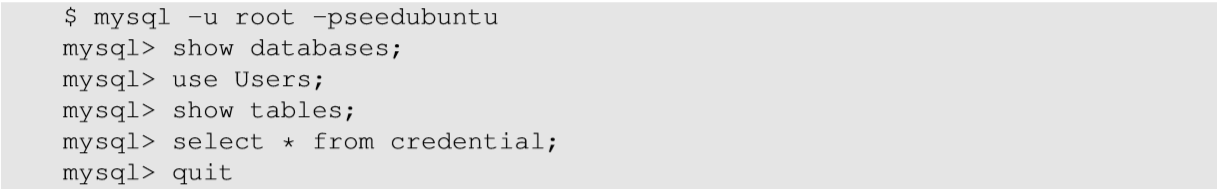
MySQL是一个开源数据库管理软件。它在VM中用于管理与已安装网站相对应的数据库。 我们在mysql服务器中有以下数据库：

1.用于SQL注入站点的用户数据库

2.用于XSS站点的elgg \_xss数据库

3. 用于CSRF站点的elgg\_csrf数据库

您可以通过客户端应用程序/usr/bin/mysql，访问MySQL数据库服务器。 以下是关于如何使用mysql的简单演示。



**MySQL Accounts**。目前，在 MySQL服务器中有两个账户。 用户名和密码如下所示。

1.用户：root，密码：seedubuntu

2.用户：elgg\_admin，密码：seedubuntu（Web应用程序使用此帐户连接到mysql服务器）

**phpMyAdmin**。 我们还安装了phpMyAdmin，这是一个允许通过浏览器管理MySQL的PHP工具。可以通过导航到http://localhost/phpmyadmin来访问它。phpmyadmin的帐户,用户名为root，密码为：seedubuntu。

## Bind9 DNS Server

Bind9是域名系统组件的开源实现。 它主要用于SEED DNS网络安全实验室。 Bind9的主要配置文件位于/etc/bind/named.conf.options中。您还需要了解文件/var/cache/bind/dump.db，它是当前配置的Dump文件。

## Other Servers

我们还安装了一个ftp服务器（vsftpd），一个telnet服务器（openbsd-inetd）和一个assh服务器（ssh）。

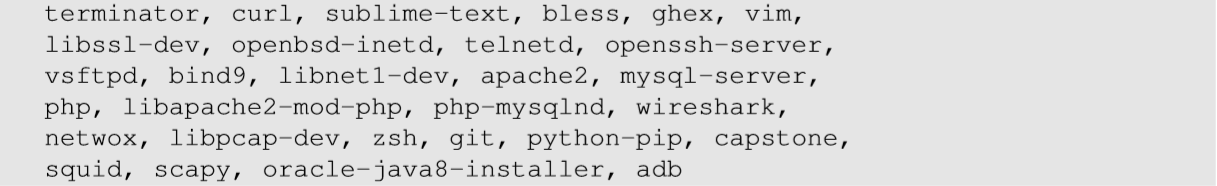
# 其他

## VM Customization Folder

在一些实验中，尤其是网络安全实验，我们必须运行多个VM，并在它们之间来回切换。 由于所有这些虚拟机看起来都一样，因此很难知道我们所在的虚拟机。我们提供了一个自定义文件夹来修改虚拟机的外观，使其更易于管理多个虚拟机。该文件夹可以在/home/seed/Customization中找到。 由于网络实验最多涉及三个VM，因此自定义文件夹为三个角色提供图标和桌面背景，即用户，代理/服务器和攻击者。

## Package List

除了Ubuntu16.04安装附带的软件包外，还使用“apt-get install”命令安装了以下附加软件包。



## Software Security Lab Tools

我们安装了两个工具来帮助我们探索软件安全实验：

•Shellnoob这个工具[3]帮助我们编写像缓冲区溢出实验的shellcode。例如，它可以将汇编指令转换为32位和64位架构的shellcode。 它可以在/home/seed/source/shellnoob中找到。

•RoPGadget这个工具[2]涉及面向回归的编程。它允许在二进制文件中搜索ROP小工具以促进ROP开发。 它可以在/home/seed/source/ropgadge中找到。

# 参考

[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.