LXCM Tutorial

Installing LXCM

To install LXCM, download it and run lxcm install.

```
wget https://iwalton.com/p/?lxcm -O lxcm
bash lxcm install
```

This will install all dependencies and configure the system to manage containers.

Getting Help

LXCM has a built-in help command feature listing command syntax. To access it, simply run the program without arguments:

```
lxcm
```

Creating a Template

To create a basic debian template for the exercises, run:

```
lxcm template debian debian
```

To get a listing of templates, run:

```
lxcm list-templates
```

Creating Containers

Create a new container, called mysql. Start the container and get a shell.

```
lxcm new debian mysql
lxcm start mysql
lxcm shell mysql
```

You are now in a shell within the container. Install mysql using the following command:

```
apt install mysql-server
service mysql start
mysql
CREATE USER 'test'@'%';
CREATE DATABASE testdb;
GRANT ALL PRIVILEGES ON testdb.* TO 'test'@'%' IDENTIFIED BY 'changeme';
[CTRL+D]
```

You are now running mysql in a container, but mysql needs to be reconfigured to listen to network connections. To do that, enter this command to install a text editor and edit the mysql configuration:

```
apt install vim
vim /etc/mysql/mariadb.conf.d/50-server.cnf
```

Find the bind-address directive (enter /bind) and change it to 0.0.0.0. Then restart mysql and exit:

```
service mysql restart
[CTRL+D]
```

To ensure mysql starts with the container, run:

```
lxcm edit-startup mysql
```

Then add this line to the startup configuration:

```
service mysql start
```

(The default editor for lxcm is vim. You need to press i to insert, then ESC :x ENTER to quit. You can also set the EDITOR environment variable to something else, if you prefer another editor.)

To forward traffic into the container, use a port forward:

```
lxcm forward add tcp 3306 3306 mysql all
```

We are using a port forward of type “all” in this example. You can use “private” to allow connections from other containers, or “public” to allow connections from other computers on the network.

To confirm the mysql server works, install a mysql client and connect to the database.

```
apt install mysql-client
ip a
mysql -h [your ip address] -u test -p
(Enter the password set earlier, which was changeme.)
```

Creating and Restoring Backups

To create a backup of the mysql container, enter this command:

```
lxcm backup mysql backup1
```

The backup, in this case is saved in “/var/lib/lxcm/containers/mysql/backups/backup1.sfs”. The backup only contains the changes from the template.

Let’s say the red team decides to make pain for you. In this case, they decided to delete everything:

```
lxcm execute mysql rm -rfv --no-preserve-root /
```

To recover from this, simply restore the backup:

```
lxcm restore backup1 mysql
lxcm start mysql
```

You will be asked if you want to create a backup of the damaged system first. This may be useful for analysis later.

Other Tips

Restarting Containers

To restart the mysql container, run:

```
lxcm restart mysql
```

Copying Files To and From Containers

There is a filesystem in /var/lib/lxcm/containers/mysql/mnt that corresponds to /mnt inside the container. You can copy files using this folder and the permissions will be adjusted appropriately.

Restoring Backups to Other Containers

If you want to investigate what happened to a system without having to keep it down, after restoring the system you can investigate it in another container. Follow these steps:

```
lxcm shell mysql
echo "echo YOU HAVE A VIRUS" >> ~/.bashrc
[CTRL+D]
lxcm restore backup1 mysql
lxcm start mysql
(Enter y for “create backup first”.)
lxcm new debian analysis
lxcm list-backups mysql
lxcm force-restore mysql "[backup name]” analysis
lxcm start analysis
lxcm shell analysis
```

Now you can examine the system without interrupting the original mysql container.

Migrating a System over SSH

If you have an existing system and you want to make it into a container, you can migrate it over SSH. Make sure the system has SSH as root enabled, then run the following:

```
lxcm migrate [system ip] [template name]
lxcm new [template name] [container name]
```

If you would like to save space, run this command before creating the container:

```
lxcm compress [template name]
```

You can also compress a template after creating a container, but you must restart the containers for the operation to take effect.

Create a Template from a Container

Suppose you want to create many more mysql servers. To make a template that includes the mysql configuration, enter this command:

```
lxcm compose mysql mysql-template
```

Firewall Policies

The container system can also manage firewall policies for the containers and the host, by generating iptables rules based on a custom syntax. See the lxcm help page and manual for details.