EE379K Enterprise Network Security Lab 2 Report

Student: Sean Wang, szw87
Professor: Mohit Tiwari, Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

September 20, 2019

Part 1 - Vulnerable Web-Apps

Setting up a web-service in a container

The Damn Vulnerable Web App in Docker was setup on low difficulty by following the guide [1]. Then, a PHP file (`part1/injection.php`) was uploaded to the web app, and could then be loaded and executed when navigated to. This PHP script prints the path to the current directory, the contents of the current directory, the contents fo the root, and the number of processes running in the system. The output of the script onto the webpage is shown below:

```
Path to current directory:
/var/www/html/hackable/uploads

Contents of current directory:
. .. dvwa_email.png injection.php

Contents of root:
. .. .dockerenv bin boot dev etc home lib lib64 main.sh
media mnt opt proc root run sbin srv sys tmp usr var

Number of processes running:
17
```

The server's view of the filesystem has a few differences from running `ls /` from the VM's terminal. For example, it shows files that are normally hidden, such as `.`, `..`, and `.dockerenv`. The things it doesn't show that `ls /` shows include `cdrom/`, `initrd.img`, `initrd.img.old`, `lib32/`, `libx32/`, `lost+found/`, `snap/`, `swapfile`, `vmlinuz`, `vmlinuz.old`. Additionally, running

```
ps aux --no-headers | wc -l
```

from the VM's terminal resulted in 223 instead of 17. This difference is due to how Docker creates and manages containers. Docker utilizes the Linux kernel's cgroups and namespaces in order to manage and monitor resource allocation, and utilizes the C library, `runC`, that gives each container its own root file system, similar to a `chroot jail` [2, 3]. As such, the root of the filesystem seen by the Docker container and the VM are not the same filesystem, explaining the difference in output of `ls /`. Additionally, through the use of namespaces, Docker has isolated the processes inside the container from the processes of the VM running Docker.

References

[1]

[2] J. Skilbeck, "Docker: What's Under the Hood?," January 2019.

[3] S. Grunert, "Demystifying Containers - Part I: Kernel Space," March 2019.