13 Limitations

The labtainers framework limits labs to the Linux execution environment. However, a lab designer could prescribe the inclusion of a separate VM, e.g., a Windows system, and that VM could be networked with the Linux VM that hosts the Docker containers as described in 8.3. Future work would be necessary to include artifacts from the Windows system within the framework's automated assessment and parameterization.

The user does not see the /etc/fstab file. Only virtual file systems can be mounted (or those mounted when the container is created.)

Kernel logs do not appear in `/var/log/kern.log`. For logging events such as iptables, consider using ulogd and a "NFLOG" directive in place of a "LOG" directive. See the dmz-lab as an example.

The available Docker network drivers do not permit IP address overlap between virtual networks. For example, you cannot define two 192.168.1.0/24 LANs.

Student use of the shell directive "source" will cause stdin/stdout to not be captured.

Inquisitive students will see evidence of artifact collection. Home directories on containers includes a `.local` directory that includes Labtainer scripts that manage capturing and collection of artifacts, and that directory contains the stdin and stdout files generated by student actions. Additionally, when the student starts a process that will have stdin and stdout captured, the student will see extra processes within that process tree, e.g., the `tee` function that generates copies of those data streams. All of the containers share the Linux kernel with the Linux host. Changes to kernel configuration settings, e.g., enabling ASLR, will be visible across all of the containers.

14 Notes

14.1 Firefox

14.1.1 Profile and configuration changes

The labtainer.firefox image includes a /var/tmp/home.tar which is expanded into the user home directory when parameterize.sh is run. This tar includes a profile in .mozilla that avoids firefox starting with its welcome pages and privacy statements. The labtainer.firefox image includes a customized /usr/bin/firefox that starts the browser in a new instance so it does not share existing browsers. The `about:config` was altered to disabled insecure field warnings for the labs that do not use SSL connections to web servers.

14.1.2 Browser history

If you wish to assess places a browser has visited, e.g., use a pregrade.sh to extract sites from the firefox places.sqlite file, put `places.sqlite` into the lab's /_bin/noskip file.

14.1.3 Slow browser startup

Some html, e.g., for the softplc, want to visit fonts.googleapis.com. If no gateway/dns is available, there is a long timeout. Try adding

```
ADD-HOST fonts.googleapis.com:127.0.0.1
```

to start.config to avoid the timeout.