Task 5 - Firewall Modifications

Now that our Nginx proxy is fully configured. The management group would like your group to block off direct access to the web server; that is all traffic should be routed through the proxy. The previous group was a fan of IPTables, however we would like you to implement it this system using just docker as that will likely be easier.

As with the previous task we found some old notes the former groups left.

Expected Outcome

1. This system is implemented using Docker
2. The website is only accessible through the proxy
    - Accessible through port 80
    - Accessible through port 443
3. The website is **not** accessible through port 8080 to non-local systems

Old Documentation

A neat alternative to a host-based system would be to use docker networks. We would at least need to do the following.

1. Implement Proxy Container
    - We have the config, we would just need to look into how we can add that to the container (Dockerfile, Volumes)
2. Create Network
    - Containers cannot communicate unless they are on the same network, unless specified they will be on the same default network
3. Restart ... <Fill in later>

Old Documentation (DO NOT IMPLEMENT)

The primary challenge with this task is blocking off a port only to non-local systems. Because the proxy is hosted locally, we cannot just block off the port to all communications as we would then be unable to access the website through the proxy.

With IPTables we can do this safely with two lines <UNTESTED>. However more are needed if our web-server is a container as traffic would be routed through the Forward chain (Which makes life painful) we would probably have to experiment with chains in the prerouting tables...

```
iptables -A INPUT --src 127.0.0.1 -J ACCEPT
iptables -A INPUT -p tcp --dport 8080 DROP
```