#these are just some generally useful commands to use

#change permission of all files (and only files) in this directory and all sub
#directories to 644 (-rw-r--r--)
sudo find . -type f -exec chmod 644 {} +

#change permission of all directories (and only directories) in this
#directory and all subdirectories to 755 (-rwx-r-xr-x)
sudo find . -type d -exec chmod 755 {} +

#!/bin/bash

#Delete existing rules
iptables -F

#set default-deny on all
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

#allow icmp (so scoring can ping)
iptables -A INPUT -p icmp -j ACCEPT
iptables -A OUTPUT -p icmp -j ACCEPT

#allow already established connections
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#allow DNS and HTTP to get out (for browsing and updating with apt)
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

#allow new traffic to talk to web server
iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -p tcp --sport 3306 --dport 1024:65535 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp --sport 1024:65535 --dport 3306 -m state --state NEW -j ACCEPT