```
#!/bin/bash
# Add missing users to the system
# Prerequisite: a file called readme exists with all the users listed in the README
for user in $(cat readme); do grep -q $user /etc/passwd || useradd -m -s /bin/bash $user; done
# Remove rogue users from the system
# Prerequisite: a file called readme exists with all the users listed in the README
# NOTE: this will have difficulty deleting toor; just remove that line from /etc/passwd yourself
for user in $(grep "bash" /etc/passwd | grep -v "^root" | cut -d':' -f1); do grep -q $user readme || deluser $user; done
#List out all cron jobs from each user
for user in $(cut -f1 -d: /etc/passwd); do echo $user; crontab -u $user -l; done
# Configure proper administrators
# Prerequisite: a file called admins exists with all the admins listed in the README
# NOTE: group modifications require a restart, so do it... also make sure the new group is ID 27, and the line is actually between 26 & 28
groupdel sudo; groupdel admin; groupadd sudo; while read user; do usermod -aG sudo $user; done < admins
# Change passwords for all users | UID >= 1000
awk -F':' '{ if($3 >= 1000) print $1 }' /etc/passwd | sed 's/$/:InSecT1234!@#$/' | chpasswd
# Change passwords for all non-daemon users
for user in $(grep "bash" /etc/passwd | cut -d':' -f1); do echo $user':InSecT1234!@#$' | chpasswd; done
# Monitor red team activity
apt install gnustep-gui-runtime entr
ls /etc/passwd | entr say Password file modified alert alert &
ls /etc/shadow | entr say Shadow file modified alert alert &
ls /etc/group | entr say Group file modified alert alert &
watch -d=1 w
watch -d=1 cat /etc/passwd
watch -d=1 cat /etc/shadow
watch -d=1 cat /etc/group
```