1. Linux Set Up
   1. Switch to Sudo
      1. Sudo -s
   2. Change all user passwords. Yes, especially the credentials given to you!
      1. passwd <username> <newpassword>
   3. Audit /etc/shadow for users with passwords set or no password at all.
      1. cat /etc/shadow
   4. Remove all SSH keys present on the box.
      1. find / -name authorized\_keys 2> /dev/null
      2. find / -name id\_rsa 2> /dev/null
   5. Audit sudo access given to users.
      1. cat /etc/sudoers
      2. cat /etc/sudoers.d/\*
      3. getent group sudo | cut -d: -f4 (The sudo group is Debian, wheel is for RHEL)
   6. Audit /etc/passwd to check for account shells and UIDs.
      1. cat /etc/passwd | grep :0:
      2. cat /etc/passwd | grep -v /bin/false | grep -v /sbin/nologin
   7. Verify that there are not any non-standard cron jobs on the system.
      1. cat /etc/cron.d/\*
      2. for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l; done
   8. Remove packages that could be used for malicious purposes if not needed.
      1. apt remove socat nc ncat nmap netcat (apt is for Debian, yum is for RHEL).
         1. Other packages must be manually inspected in order to prevent taking down critical services.
   9. Stop services that are not critical to the system or competition needs.
      1. systemctl --type=service --state=active
      2. systemctl stop servicename
   10. Identify SUID and SGID files. Cross-reference with <https://gtfobins.github.io/> to narrow down malicous instances of SUID and SGID files.
       1. find / -perm -4000 -print 2>/dev/null for SUID
       2. find / -perm -2000 -print 2>/dev/null for SGID
   11. Identify world-writable files and directories.
       1. find / -type d \( -perm -g+w -or -perm -o+w \) -exec ls -adl {} \; for directories
       2. find / ! -path "\*/proc/\*" -perm -2 -type f -print 2>/dev/null for files

Linux Monitoring

* 1. Audit listening to ports and established connections
     1. lsof -i -P -n
  2. Audit running processes.
     1. ps aux
  3. Monitor logs in /var/log/
  4. Monitor Users
     1. Who
  5. Kick User
     1. Killall -u <Username>
  6. LockUser
     1. Usermod -L <Username>
  7. Ban User
     1. usermod --lock --expiredate 1970-01-02 <username>