**Important Commands**

* See accounts that have empty passwords
  + awk -F: '($2 == "") {print}' /etc/shadow
* Display accounts with UID set to 0
  + awk -F: '($3 == "0") {print}' /etc/passwd
* List services that start at boot
  + chkconfig --list | grep '3:on'
* See logs of a service
  + journalctl -u network.service
* See listening network ports
  + Netstat -peanut
* **List all cron jobs (for every user)**
  + for user in $(cut -f1 -d: /etc/passwd); do echo $user; crontab -u $user -l; done
* **Kill all processes for a user**
  + pkill -9 -U username
* **Logs**
  + Tail -f /var/log/syslog

## **UFW**

* Deny an IP address
  + Sudo ufw deny from x.x.x.x/x
* Deny on specific interface
  + sudo ufw deny in on eth0 from 15.15.15.51
* Deny outgoing port
  + sudo ufw deny out 25
* Allow port 22
  + Sudo ufw allow 22
* Allow port 22 from specific IP address/range
  + Sudo ufw allow from x.x.x.x/x to any port 22
* Allow web traffic
  + sudo ufw allow proto tcp from any to any port 80,443

**First Checks**

* To check
  + /etc/sudoers
  + /etc/group
  + /etc/passwd
  + Delete user
    - Userdel test
  + Add group
    - Groupadd developers
  + Delete group
    - Groupdel testgroup
  + Add user
    - Useradd -m -g users -s /bin/bash test
  + Remove a user “test” from “testgroup”
    - Gpasswd -d test testgroup
  + Change password
    - Passwd *user*
* Change SSH configs
  + /etc/ssh/sshd\_config
  + Permitrootlogin no
  + AllowUsers josh calvin
  + AllowGroups ksucdc
  + MaxAuthTries 3
  + LoginGraceTime 30
  + ClientAliveInterval 600
  + DenyUsers eve mallory
  + DenyGroups developers
  + X11Forwarding no
  + listenAddress 192.168.1.0
  + Change port to non-standard port

**Web**

Inspect -> application -> cookies/local storage