Remember, Remember: **Google is your friend**, if you don’t know, look it up

* Load image
* Add team hash
* Look at image
* Read readme, then read again and record what to do
* Read forensics questions, and record what is needed to answer them
* Install and update Malwarebytes, but don’t run yet, proceed
* Open task manager
  + view running services
  + Go through them and document any unwanted or malicious services
* Look at user profiles, use command prompt too, will show hidden profiles
  + Remove any unauthorized users, their associated files too
  + Disable guest account unless
  + Make sure appropriate privileges are set
  + Make sure all have secure passwords, change them
    - Some numbers
    - Some symbols
    - Some capitols
    - At least 14 characters
* Check services again, then go to control panel and stop any malicious or unnecessary services (reference internet for default services, set everything to what it says, unless explicitly stated not to in the readme, if you’re not sure: disable it)
* Run Malwarebytes and (unless Linux, then install, update and run rkhunter and chkrootkit)
* Try to remove malware, especially if it’s a Trojan, document what is removed
* Manage software from control panel, if not absolutely necessary or explicitly required, delete
* Start installing service packs, keep running in background,
  + when done configure automatic updates
  + when done with that, check for updates and install
* Set secure password policies;
  + Minimum of 14 characters
  + 30 day max for admins
  + 90 day max for users
  + Minimum password age 10-30 days
  + Password history set to 5
  + Enable complexity requirements
  + Disable reversible encryption
  + Account lockout duration 30 minutes
  + Account lockout threshold = 3-10 invalid attempts
  + Reset account lockout counter to 30 minutes
* Set secure lockout duration
* Disable remote access, unless stated not to in the readme
* Disable file sharing, unless stated not to in the readme
* Check scheduled tasks (cron for Linux), for weird stuff, like reinstallation of malware
* Local Security policy and Group policy
  + Go to start and type in “mmc.exe”
  + Reference additional documentation
* Enable Firewall, if not already done
* Run port scan with zenmap (part of nmap)(if Linux, use network monitor), go through and document any suspicious ports
* Use ACLs and firewall to close ports
* Easter egg hunt (use “\*.jpeg” on whole file system at a time, for example)
  + Go through program files
  + Use backspace to go back up in file tree
* Audit Policy
* Browser security if you have time