Account Policy
- Make script section that full scores account policies

Application Security
- Config files
- Dynamic script for app sec
- Know random files to remove
- Make effective system to deal with unknown app sec

Application Updates
- Use current software
    - Look for other options
    - Test out as much as possible

Defensive Countermeasures
- Harden kitty defender custom list ?
- I made a pretty decent defender script that covered most of it
- Look through past scoring

Forensics Questions

Local Policy
- Use hardening as the base but make a custom harding kitty list
    - For audit policies
        - Either add to harden kitty or just run the current version right after hardening kitty
- For server image
    - Make a custom GPMC import

Malware
- Current script
    - 5. Find "sus" services
        - Stanford service hunting system
            - Does not work very well imo
    - 27. Snipers go brr
        - Blue team sniper
    - 34. Detect Hidden Windows Tasks
    - 40. DLL Checks & Folder Checks
- Manual
    - Baseline services
        - Get list of all services on windows via registry
        - Compare to live image
    - Baseline system32 (maybe more folders (?))
        - System with hash comparison as well as name comparisons and rankings based on such
    - Blue team Sniper
        - Maybe fix / add code to the module that we want
    - Baseline windows tasks
        - Script should list out all windows tasks that are non standard

- Maybe check for hidden tasks as well
- Always go through registry for extra precaution
- DLL checks
- Maybe script of you want not sure honestly

Operating System Updates
- Updating actual image
- Look in to WSUS updates / offline updates
- Update based policies
- Create new part of script that does all of this

Prohibited Files
- Consider baseline the image / do manually with everything

Service Auditing
- Dynamic service auditing
- Have a list of windows crit services that user can enable which removes those from the turn off script
- SDDL service stuff
- Make sure crit services / maybe all services (?) restart on failure
- Advanced vulns like ppl mode

Uncategorized Operating System Settings
- Look through old vulns
- Script does a lot of this already
- We full scored semis for this cat
- Mostly just research / random commands / reg keys / system parts etc

Unwanted Software
- Appwiz.cpl / features
- Random folder/file on win10

User Auditing
- Current user auditing system only works for win 10
- Create server based user auditing that works like win 10
- Server script only does properties but not AD group stuff
- SAM
- RID hijacking
- Hidden SAM users
- Broken SAM Users
- Script everything but have final manual checks as well