Demo outline

Offensive

CTF Scenario

- binja license (can use mine for demo) for re chall (Can also ask jordan if he has something fun)
- 010 license (can use mine for demo) for for chall
- Run an internal CTF challenge / CTFd which any members on our network have access to. Have an ubuntu / some sort of image ready that has the tools necessary for students to complete said challenge.
- Forensic pcap image -> login to shared box -> dl -> analyze (have multiple ppl do so = collaboration) (maybe a timesketch server or st)
- Malware Sandbox.
    - Show it running something and what students can learn from it.
    - Open to Student use for club “research”

Red Team Scenario

- Kali VM
- Attacking Metasploitable VM, DVWA
    - 24/7
- Attacking a “Client” which is just a staged Windows VM that looks like someone’s desktop.
    - What goes wrong? How do you attack an Average Joe VM?

Defensive

Threat Scenario

- Pull up SIEM (splunk or kibana or evebox or squil) and look through pre populated data

“Threat hunting exercise” on siem.

- We do have a splunk license we can use for now (peyton’s dev one)
- Root cause Analysis, What went wrong, What would someone at work be looking for?

Security Infrastructure Testing

- Show network map of a possible virtualized network that students could build

Other Cool Stuff

- Gitlab Instance for student projects w/ free CI/CD
- File share with sorted resources (PDFs of books)
    - Can be a managed solution or just an Nginx server pointed at a directory

Infra possibilities

- ESXi Host
- Ubiquiti EdgeRouter (Of some shape and size)
- Ubiquiti WAP