Breaking Boxes!

Don’t forget to sign in

Schedule for tonight 📅

- Quick .recaps from previous weeks
  - That was a joke about .pcaps, hahaha
- Break up into teams
- ~30-45 min of box breaking
- I'll go over the ways I messed up the boxes
  - How to fix? 😃
- Little bit of time to give me feedback

Quick disclaimer

- Some of the tasks tonight are intended to be a little bit tricky
  - **Don’t get discouraged!!**
    - It is OK if you don’t know how to do some of this stuff.
    - Be creative and try -- I’ll tell you at the end
    - Some things may be easier than others, **work together**
- **You can use the Windows hosts to try and recon these boxes / use tools**
  - Like Zenmap
    - (nmap is better)

NMAP/ Zenmap 👁️

- Your buddy tonight
- Things have been moved and scrambled to try and be tricky
- NMAP Cheat sheets exist

Website Enumeration Will Help You

...

This is all.

Scenario:

- **Some security professor made some VMs to run in their personal network.** He is using the following services to run his home network
  - FTP
  - Remote access
  - Web

Ye' Old'e Rules

- Note: **SSH attacks are off limits**
  - Do not attack SSH or attempt to brute force port 22.
  - I'm watching logs and you will be asked not to participate in future activities if you break this rule, as well as **Google Cloud access being revoked** 🙂
  - No messing with GSuite accounts, as they are linked with personal EMICH accounts
- Logging in with a **known password** for a user is not considered an attack.
- Ask if you have any questions

FTP File server 📁📂📁

- Generic file server
- Things to know / find out
  - Version
  - Which file server is it?
  - What directories can you write to?
  - Are there accounts on the box?
  - What port it runs on
  - Remember back to the configuration we made before.
    - What made that insecure?

Web 🌐

- James built a website for himself.
  - Rumor has it, Dr. Banfield can't remember passwords
- Stuff to find out
  - What version http is he using?
    - Which tool?
  - What port is his webserver on?
  - What pages exist
  - Is there an SSL cert?
  - Is there a login page?

Remote access

- James is lazy, and doesn't want to walk all the way to California to use his Google Cloud VMs.
- He has enabled remote access on one of his VMs, figure out which one it is and how to use it.
- Find his secrets

Good Luck!