* Physical Penetration Testing Kit
* Custom Hardware
  + Custom Pick set
    - “Bypass picks”
    - Specific picks to unlock Masterlocks #1-4 via a
    - Standard Lock picks
    - Discuss different handle types / making your own from windshield wipers
  + Bypass tools
    - Under door tool
    - See: <https://www.sparrowslockpicks.com/product_p/underdoor.htm>
    - Usage: <https://www.youtube.com/watch?v=_CcCOpNc_ZU>
    - Used to turn ADA compliant door levers. Research ADA requirements for doors to determine how big to make this tool
    - Shove knife
    - These all need to be cut out of some vaguely flexible steel material. Instructions will include stencils (vector images/jpeg) to be printed / cut out of the materials.
      * Covert variant
      * See: <https://www.sparrowslockpicks.com/product_p/hp.htm>
      * Used to open internal doors - often a bit smaller & harder to use - good for covert usage
      * Flexible variant
      * See: <https://www.sparrowslockpicks.com/product_p/hpflx.htm>
      * I need to find a thinner steel/plastic material
      * Bigger variant
      * See: <https://www.thefirestore.com/store/product.aspx/productId/1087/EMI-Quick-Pik-6-Shove-Knife/>
      * Kept in a bag or other larger carry case
    - Crash Bar Bypass
    - See: <https://www.reddit.com/r/physec/comments/9u48ws/made_a_collapsible_crashbar_bypass_tool_next_one/> Also See: <https://www.reddit.com/r/physec/comments/9t44px/is_there_something_like_an_under_door_tool_but/e8uv4mp?utm_source=share&utm_medium=web2x&context=3/>
    - Used to thread through the center of
    - Shims
    - Padlock shims or shims for other lock types
* Custom Hardware - Custom Software
  + PwnieExpress - DIY version
  + Raspi-based
  + VyOS to plug into the network and forward packets to a central control device AircrackNG: <https://www.aircrack-ng.org/doku.php>
  + Use AircrackNG to enter a wireless network MITM - See: <https://geekflare.com/mitm-attack-tools/>
    - Put it into another “smart device”
    - Dangerous smart lightbulb???
  + RFID cloner
  + In-depth on multiple RFID types: <https://www.blackhillsinfosec.com/rfid-proximity-cloning-attacks/> NFC easy project: getgenea.com/blog/how-to-clone-an-rfid-key-card-for-less-than-eleven-dollars/ See: [https://medium.com/@lp1/the-diy-portable-nfc-cloner-1ebdecfe5f66](https://medium.com/@lp1/the-diy-portable-nfc-cloner-1ebdecfe5f66) Needs a raspi
  + Interacting with NFC: <https://github.com/nfc-tools/libnfc> Also: <http://www.nfc-tools.org/>
  + Super-ultra-high-speed-sneaky idea: make it use haptic feedback (see: vibration) instead of a screen 1 buzz = RFID read 2 buzz = RFID written . . . ETC
* Stock Hardware - Custom Software
  + Rubber Ducky hardware
  + See: <https://medium.com/hackernoon/low-cost-usb-rubber-ducky-pen-test-tool-for-3-using-digispark-and-duck2spark-5d59afc1910>
  + ATTiny-85 Device: <https://www.gearbest.com/other-accessories/pp_227676.html?lkid=15666791>
  + Cheap hardware from Digispark (<$10) Given the difficulty of use, I could purchase 3-5 and have one for each script.
  + Also see: <https://gitlab.com/kerlkloss/Arduino_USB-Password-Typer> Uses a ATMega32U4 board as another option
    - Scripts to demonstrate compromise (yougotpwned.jpeg popup)
    - See: <https://blog.hartleybrody.com/rubber-ducky-guide/>
    - Good basic tutorial for Hak5 rubber ducky, but I can adapt it to my own custom hardware
    - Scripts to establish Command & Control (C2)
    - Lv. 0: Netcat/telnet shell
    - Lv. 1: Web Shell See: <https://hacksland.net/build-a-simple-web-shell/>
  + Raspi jump box
  + Set up a Raspi with Kali that “calls back” to a command & control server with SSH
* Target
* Create Documentation (DO AS YOU COMPLETE PROJECT)
  + Github Design Journal
  + <https://github.com/SirSertile/CNCS-Capstone/wiki>
  + This will hold notes / other capstone material
  + .stl files for any 3d printed tools
  + Some projects may use custom 3d printed boxes. Including .stl files either in my github or on thingiverse allows for full transparency and forking of 3d models for re-publishing and modification
  + Define usage of each tool
  + Short demo videos or diagrammed animations/illustrations
* Required
* Reach
* Research commonly used tools/tactics
* <https://warroom.rsmus.com/category/physical/>
  + Doors
  + Basic Tactics: <https://warroom.rsmus.com/physical-penetration-testing-basics-primer/>
    - Handles
      * Lock
      * Can be picked or bypassed. Certain locks (kaba simplex) can be disabled with a large magnet. Electronic locks are a bit more complicated. Might want to pick one up to play with.
      * Lever
      * Can be compromised with an under-the-door tool to actuate the latch from the other side
      * Latch
      * Can be disengaged with a shove knife and air wedge
    - Hinges
    - See: <https://www.reddit.com/r/specializedtools/comments/h9gf54/spring_hinge_pin_removal_tool/>
    - Removal of hinge pins allows removal of door, even if locked
    - Door sensor magnets
    - Plant strong magnets with tape/magnetizing to the door frame to prevent door sensors from triggering (actuated via magnets)
    - Automatic opening mechanisms
    - See: <https://null-byte.wonderhowto.com/how-to/oops-some-security-doors-can-be-picked-with-canned-air-0162979/>
    - Inverting a can and spraying it through the gap can open doors with automatic opening mechanisms
    - Potentially also actuating handicap buttons with other means
  + Various scopes / intensity of tests
  + See: <https://www.redteamsecure.com/penetration-testing/physical-penetration-testing> Also see: <https://www.triaxiomsecurity.com/our-physical-penetration-testing-methodology/>
  + Generally covers physical entry (bypassing barriers, physical access control)
  + Can cover social engineering/tailgating and rfid cloning
  + My guide will probably not cover as much social engineering.
  + Physical penetration tests often follow the same structure as cyber kill chain (recon, intrusion, exploit, priv esc, lateral movement, obfuscation, DoS, and exfiltration)
  + Physical pen tests often include: Recon of the area Intrusion into the target area (entering the area) Exploitation of vulnerabilities to enter the bldg Escalate your access into a privileged area ( kind of the same as exploitation of vulnerabilities to enter bldg ) Exfiltration of “flags” from the area
  + Rubber Ducky -> Compromise
  + See: <https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives>
  + Can be dropped en masse around the target area once entered ( bathroom, parking lot, front desk )
  + Like phishing, but physically!
* Legend
* Priority:
  + Required (Light Green): Must complete to finish capstone
  + Target (Yellow): Would like to complete
  + Reach (Red): Difficult to complete - REALLLYYY cool though Difficulty: I went with RPG item rarity colors because I’d already used green/yellow/red
  + Common / Easy (Dark Green)
  + Rare / Medium (Blue)
  + Epic / Hard (Purple)
  + Legendary / Legendary (Orange)
  + Unique / VERY HARD (Dark Red)