Exploits

- Three Ways to Attack - Social, Physical, Network
    - **Social**
        - Ask the person for access, phishing.
        - Cognitive biases - look at how these are exploited.
        - Spear phishing.
        - Water holing.
        - Baiting (dropping CDs or USB drivers and hoping people use them).
        - Tailgating.
    - **Physical**
        - Get hard drive access, will it be encrypted?
        - Boot from linux.
        - Brute force password.
        - Keyloggers.
        - Frequency jamming (bluetooth/wifi).
        - Covert listening devices.
        - Hidden cameras.
        - Disk encryption.
        - Trusted Platform Module.
        - Spying via unintentional radio or electrical signals, sounds, and vibrations (TEMPEST - NSA).
    - **Network**
        - Nmap.
        - Find CVEs for any services running.
        - Interception attacks.
        - Getting unsecured info over the network.
- Exploit Kits and Drive by Download Attack
- Remote Control
    - Remote code execution (RCE) and privilege.
    - Bind shell (opens port and waits for attacker).
    - Reverse shell (connects to port on attackers C2 server).
- Spoofing
    - Email spoofing.
    - IP address spoofing.
    - MAC spoofing.
    - Biometric spoofing.
    - ARP spoofing.
- Tools
    - Metasploit.
    - ExploitDB.

- Shodan - Google but for devices/servers connected to the internet.
- Google the version number of anything to look for exploits.
- Hak5 tools.