- Penetration Testing
    - Pentest
        - Simulate an attack
    - Similar to vulnerability scanning
    - Except we actually try to exploit the vulnerability
    - Often a compliance mandate
        - Regular penetration testing by a 3rd party
    - National Institute of Standards and Tech
- Rules of Engagement
    - An important document
        - Defines purpose and scope
        - Makes everyone aware of the test parameters
    - Types of testing and schedule
        - On site physical breach, internal test, external test
        - Normal working hours, after 6 pm only
    - The rules
        - IP address ranges
        - Emergency contacts
        - How to handle sensitive info
        - In scope and out of scope devices or application
- Working knowledge
    - How much do you know about the test?
        - Many different approaches
    - Unknown environment
        - The pentester knows nothing about the systems under attack
        - “Blind” attack
    - Known environment
        - Full disclosure
    - Partially known environment
        - A mix of known and unknown
        - Focus on certain systems or applications
- Exploiting vulnerabilities
    - Try to break into the system
        - Be careful. This can cause a denial of service or loss of data
        - Buffer overflows can cause instability
        - Gain privilege escalation
    - You may need to try many different vulnerabilities
        - Password brute force
        - Social engineering
        - Database injections
        - Buffer overflows
    - You’ll only be sure you’re vulnerable if you can bypass security
        - If you can get through, the attackers can get through
- The process

  - Initial exploitation
    - Get into the network
  - Lateral movement
    - Move from system to system
    - The inside of the network is relatively unprotected
  - Persistence
    - Once you’re there, you need to make sure there's a way back in
    - Set Up a backdoor, build user accounts, change or verify default passwords
  - The pivot
    - Gain access to systems that would normally not be accessible
    - Use a vulnerable system as a proxy or relay
- Pentest aftermath
  - Cleanup
    - Leave the network in its original state
    - Remove any binaries or temp files
    - Remove any backdoor
    - Delete user accounts created during the test
  - Bug Bounty
    - A reward for discovering vulnerabilities
    - Earn money for hacking a system
    - Document the vulnerabilities to earn cash

- Reconnaissance
  - Need information before the attack
    - Can't rush blindly into battle
  - Gathering a digital footprint
    - Learn everything you can
  - Understand the security posture
    - Firewalls, security configurations
  - Minimize the attack area
    - Focus on key systems
  - Create a network map
    - Identify routers, networks, remote sites
- Passive footprinting
  - Learn as much as you can from open sources
    - There's a lot of information out there
    - Remarkably difficult to protect or identify
  - Social Media
  - Corporate website
  - Online forums, Reddit
  - Social engineering attacks
  - Dumpster diving
  - Business organizations

- Open source Intelligence (OSINT)
    - Gathering info from many open sources
        - Find info on anyone or anything
        - The name is not related to OSS
    - Data is everywhere
    - Automated gathering
        - Many software tools available
- Wardriving or warflying
    - Combine WIFI monitoring and a GPS
        - Search from your car or plane
        - Search from a drone
- Huge amount of intel in a short period of time
    - And often some surprising results
- All of this is free
    - Kismet, inSSIDer
    - Wireless geographic logging engine wigle.net
- Active Footprinting
    - Trying the doors
        - Maybe one is unlocked
        - Don't open it yet
        - Relatively easy to be seen
    - Visible on network traffic and logs
    - Ping scans, port sans
    - DNS queries
    - OS scans, OS fingerprinting
    - Service scans, version scans

- Security teams
    - Cyber security involves many skills
        - Operational security, penetration testing, exploit research, web application hardening, etc.
    - Become an expert in your niche
        - Everyone has a role to play
    - The teams
        - Red team
        - Blue team
        - Purple team
        - White team
- Red Team
    - Offensive security team - hired attackers
    - Ethical hacking - find security holes
    - Exploit vulnerabilities
        - Gain access
    - Social engineering

        - Constant vigilance
    - Web application scanning
        - Test and test again
- Blue Team
    - Defensive security
        - Protecting the data
    - Operational security
        - Daily security tasks
    - Incident response
        - Damage control
    - Threat hunting
        - Find and fix the holes
    - Digital forensics
        - Find data everywhere
- Purple team
    - Red and blue teams working together
    - Competition isnt necessarily useful
        - Internal battles can stifle organizational security
        - Cooperate instead of compete
    - Deploy applications and data securely
    - Create a feedback loop
        - Red informs blue, blue informs red
- White Team
    - Not on a side
        - Manages the interactions between the red teams and blue teams
    - The referees in a security exercise
        - Enforce the rules
        - Resolves any issues
        - Determines the score
    - Manages the post event assessments
        - Lessons learned
        - results